Dell Security Management Server

Guida all'installazione e alla migrazione v10.2.1

Messaggi di N.B., Attenzione e Avvertenza

N.B.: un messaggio N.B. (Nota Bene) indica informazioni importanti che contribuiscono a migliorare l'utilizzo del prodotto.

ATTENZIONE: Un messaggio di ATTENZIONE indica un danno potenziale all'hardware o la perdita di dati, e spiega come evitare il problema.

AVVERTENZA: Un messaggio di AVVERTENZA indica un rischio di danni materiali, lesioni personali o morte.

2019-01

Rev. A01

Sommario

1

Introduzione

Informazioni su Security Management Server

Security Management Server ha le seguenti funzioni:

- Gestione centralizzata di dispositivi, utenti e criteri di protezione
- Controlli e rapporti di conformità centralizzati
- Separazione dei compiti dell'amministratore
- Creazione e gestione dei criteri di protezione basati sui ruoli
- Distribuzione dei criteri di protezione quando i client si connettono
- Ripristino dei dispositivi assistito dall'amministratore
- Percorsi attendibili per la comunicazione tra componenti
- Generazione di chiavi di crittografia univoche e deposito automatico e sicuro delle chiavi

Contattare Dell ProSupport

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell è disponibile all'indirizzo dell.com/support. L'assistenza online comprende driver, manuali, consulenze tecniche, FAQ e problemi emergenti.

Assicurarsi di avere a portata di mano il codice di matricola o il codice di servizio rapido per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono al di fuori degli Stati Uniti, vedere Numeri di telefono internazionali di Dell ProSupport.

2

Requisiti e architettura

Questa sezione descrive in dettaglio i requisiti hardware e software e i suggerimenti sulla progettazione dell'architettura per l'implementazione di Dell Security Management Server.

Progettazione dell'architettura di Security Management Server

Le soluzioni Endpoint Security Suite Enterprise e Data Guardian Dell Encryption sono prodotti altamente scalabili, in base al numero di endpoint individuati per la crittografia all'interno dell'organizzazione.

Componenti dell'architettura

Di seguito, si riportano le configurazioni hardware consigliate adattabili alla maggior parte degli ambienti.

Security Management Server

- Sistema operativo: MS Windows 2008 R2 Standard (x64) o versioni più recenti
- Macchina fisica/virtuale
- CPU: 4 core
- RAM: 16 GB
- Unità C: 30 GB di spazio disponibile su disco per i registri e i database delle applicazioni

> **N.B.: È probabile che vengano consumati fino a 10 GB per un database di eventi locale archiviato su PostgreSQL.**

front-end esterno

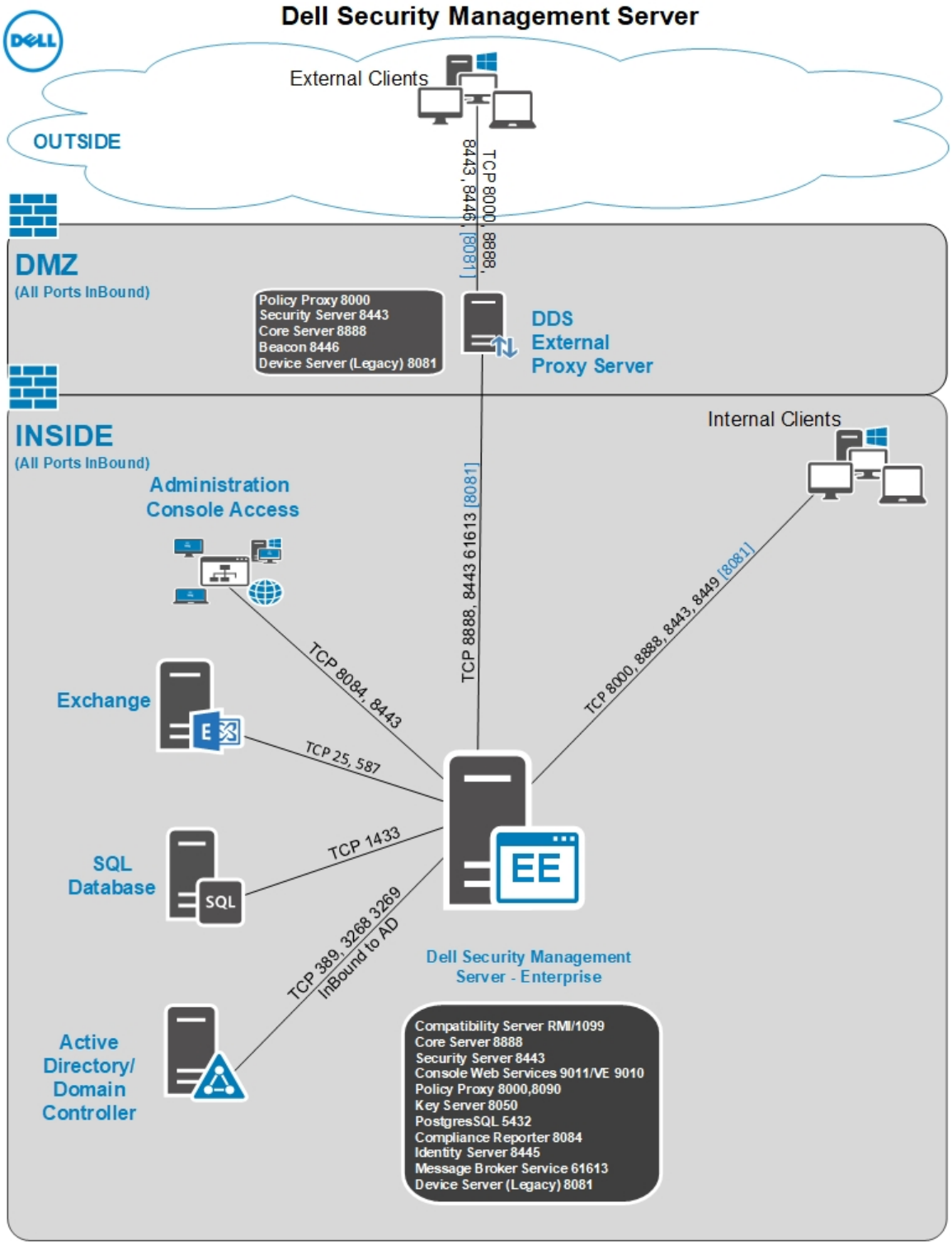
- Sistema operativo: MS Windows 2008 R2 Standard (x64) o versioni superiori
- Macchina fisica/virtuale
- CPU: 2 core
- RAM: 8 GB
- Unità C: 20 GB di spazio disponibile su disco per i registri

Specifiche hardware di SQL Server

- CPU: 4 core
- RAM: 24 GB
- Unità dati: 100 - 150 GB di spazio disponibile su disco (variabile a seconda dell'ambiente)
- Unità registro: 50 GB di spazio disponibile su disco (variabile a seconda dell'ambiente)

> **N.B.: Dell consiglia di seguire le procedure consigliate per SQL Server, anche se le informazioni di cui sopra dovrebbero coprire la maggior parte degli ambienti.**

Di seguito, si riporta un deployment di base per Dell Security Management Server.



N.B.: Se l'organizzazione dispone di oltre 20.000 endpoint, contattare Dell ProSupport per ricevere assistenza.

Requisiti

I prerequisiti hardware e software per l'installazione del software Security Management Server sono riportati di seguito.

Prima di avviare l'installazione, accertarsi che tutte le patch e gli aggiornamenti siano applicati ai server usati per l'installazione.

Hardware

La tabella seguente illustra in dettaglio i requisiti hardware *minimi* per Security Management Server Consultare Progettazione dell'architettura Security Management Server per ulteriori informazioni sulla scalabilità in base alla dimensione dell'implementazione.

Requisiti hardware
Processore
CPU Quad-Core moderna (1,5 GHz+)
RAM
16 GB
Spazio libero su disco
20 GB di spazio libero su disco
N.B.: È probabile che vengano consumati fino a 10 GB per un database di eventi locale archiviato su PostgreSQL
Scheda di rete
10/100/1000 o superiore
Varie
È richiesto un ambiente IPv4 o IPv6 o ibrido IPv4/IPv6

La tabella seguente descrive in dettaglio i requisiti hardware *minimi* per un server front-end/proxy Security Management Server.

Requisiti hardware
Processore
CPU Dual-Core moderna
RAM
8 GB
Spazio libero su disco
20 GB di spazio libero su disco per i file di registro
Scheda di rete
10/100/1000 o superiore
Varie
È richiesto un ambiente IPv4 o IPv6 o ibrido IPv4/IPv6

Virtualizzazione

Security Management Server può essere installato in un ambiente virtuale. Si consigliano solo i seguenti ambienti.

Security Management Server v10.2.1 è stato convalidato sulle seguenti piattaforme.

Hyper-V Server installato con installazione completa o base o come ruolo in Windows Server 2012 e Windows Server 2016.

- Hyper-V Server
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - L'hardware deve essere conforme ai requisiti minimi Hyper-V
  - Almeno 4 GB di RAM per la risorsa immagine dedicata
  - Deve essere eseguito come macchina virtuale di Generazione 1
  - Vedere https://technet.microsoft.com/en-us/library/hh923062.aspx per maggiori informazioni

Security Management Server v10.2.1 è stato convalidato con VMware ESXi 5.5, VMware ESXi 6.0 e VMware ESXi 6.5.

N.B.: Quando sono in esecuzione VMware ESXi e Windows Server 2012 R2 o Windows Server 2016, si consiglia l'uso degli adattatori Ethernet VMXNET3.

- VMware ESXi 5.5
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Visitare http://www.vmware.com/resources/compatibility/search.php per un elenco completo di sistemi operativi host supportati
  - L'hardware deve essere conforme ai requisiti minimi VMware
  - Almeno 4 GB di RAM per la risorsa immagine dedicata
  - Per maggiori informazioni, visitare il sito http://pubs.vmware.com/vsphere-55/index.jsp
- VMware ESXi 6.0
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Visitare http://www.vmware.com/resources/compatibility/search.php per un elenco completo di sistemi operativi host supportati
  - L'hardware deve essere conforme ai requisiti minimi VMware
  - Almeno 4 GB di RAM per la risorsa immagine dedicata
  - Per maggiori informazioni, visitare il sito http://pubs.vmware.com/vsphere-60/index.jsp
- VMware ESXi 6.5
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Visitare http://www.vmware.com/resources/compatibility/search.php per un elenco completo di sistemi operativi host supportati
  - L'hardware deve essere conforme ai requisiti minimi VMware
  - Almeno 4 GB di RAM per la risorsa immagine dedicata
  - Per maggiori informazioni, visitare il sito http://pubs.vmware.com/vsphere-65/index.jsp

N.B.: Il database di SQL Server che ospita Security Management Server deve essere eseguito in un computer separato per motivi di prestazioni.

SQL Server

Negli ambienti più grandi, si consiglia vivamente di eseguire il server del database SQL in un sistema ridondante, come un cluster SQL, al fine di garantire disponibilità e continuità dei dati. Si consiglia inoltre di eseguire giornalmente backup completi con la registrazione transazionale attiva, al fine di garantire che le nuove chiavi generate dall'attivazione di un utente/dispositivo siano recuperabili.

Le attività di manutenzione del database devono comprendere la ricostruzione degli indici dei database e la raccolta dei dati statistici.

Software

La tabella seguente descrive in dettaglio i requisiti software per Security Management Server e il server proxy.

N.B.: Per via della natura sensibile dei dati conservati da Security Management Server e per rispettare la regola di privilegio minimo, Dell consiglia l'installazione di Security Management Server sul sistema operativo dedicato o in modo che faccia parte di un application server con ruoli e diritti limitati, attivati per assicurare un ambiente sicuro. Ciò implica la mancata installazione di Security Management Server su server di infrastrutture privilegiati. Consultare https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models per ulteriori informazioni sull'implementazione della regola di privilegio minimo.

N.B.: Universal Account Control (Controllo account universale UAC) deve essere disattivato quando si installa in una directory protetta. Dopo aver disabilitato il controllo UAC, è necessario riavviare il server per rendere effettiva tale modifica.

N.B.: Percorsi dei registri di sistema di Policy Proxy (se installato): HKLM\SOFTWARE\Wow6432Node\Dell

N.B.: Percorso del registro di sistema per i Windows Server: HKLM\SOFTWARE\Dell

Prerequisiti

- **Visual C++ 2010 Redistributable Package**

  Se non è installato, verrà installato dal programma di installazione.
- **Visual C++ 2013 Redistributable Package**

  Se non è installato, verrà installato dal programma di installazione.
- **Visual C++ 2015 Redistributable Package**

  Se non è installato, verrà installato dal programma di installazione.
- **.NET Framework versione 3.5 SP1**
- **.NET Framework versione 4.5**

  Microsoft ha pubblicato gli aggiornamenti della sicurezza di .NET Framework versione 4.5.
- **SQL Native Client 2012**

  Se si utilizza SQL Server 2012 o SQL Server 2016.

  Se non è installato, verrà installato dal programma di installazione.

Security Management Server - Server back-end e Dell Front End Server

- **Windows Server 2008 R2 SP0-SP1 a 64 bit**

  - Standard Edition

  - Enterprise Edition
- **Windows Server 2012 R2**

- Standard Edition

- Datacenter Edition

- **Windows Server 2016**

  - Standard Edition

  - Datacenter Edition

Archivio LDAP

- Active Directory 2008 R2
- Active Directory 2012 R2
- Active Directory 2016

Console di gestione e Compliance Reporter

- Internet Explorer 11.x o versione successiva
- Mozilla Firefox 41.x o versione successiva
- Google Chrome 46.x o versione successiva

N.B.: È necessario che il browser accetti i cookie.

Ambienti virtuali consigliati per i componenti di Security Management Server

Security Management Server può essere installato in un ambiente virtuale.

Attualmente Dell supporta l'hosting di Dell Security Management Server o di Dell Security Management Server Virtual in un ambiente di Infrastructure as a Service (IaaS) ospitato su cloud, come Amazon Web Services, Azure e molti altri vendor. Il supporto per questi ambienti è limitato alla funzionalità di Security Management Server. L'amministrazione e la sicurezza di queste macchine virtuali saranno responsabilità dell'amministratore della soluzione IaaS.

Ulteriori requisiti dell'infrastruttura. Ulteriori requisiti dell'infrastruttura, come Active Directory e SQL Server, sono ancora necessari per garantire un corretto funzionamento.

N.B.: Il database di SQL Server che ospita Security Management Server deve essere eseguito in un computer separato.

Database

- **SQL Server 2008 R2 -** Standard Edition/Enterprise Edition
- **SQL Server 2012** - Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2014** - Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2016 -** Standard Edition/Enterprise Edition
- **SQL Server 2017 -** Standard Edition/Enterprise Edition

N.B.: Le Express Edition non sono supportate per ambienti di produzione. Le Express Edition possono essere usate esclusivamente per PoC e valutazioni.

N.B.: Di seguito, si riportano i requisiti delle autorizzazioni SQL. L'utente che esegue l'installazione e i servizi deve disporre di diritti come amministratore locale. Inoltre, sono necessari diritti di amministratore locale per l'account di servizio che gestisce i servizi Dell Security Management Server.

Tipo	Azione	Scenario	Privilegio SQL richiesto
Back-end	Aggiornamento	Per definizione, gli aggiornamenti dispongono già di database e accesso/utente stabiliti	db_owner
Back-end	Ripristina l'installazione	Il ripristino implica un database esistente e un accesso.	db_owner
Back-end	Nuova installazione	Usa un database esistente	db_owner
Back-end	Nuova installazione	Crea nuovo database	dbcreator, db_owner
Back-end	Nuova installazione	Usa un accesso esistente	db_owner
Back-end	Nuova installazione	Crea nuovo accesso	securityadmin
Back-end	Disinstallare	NA	NA
Proxy front end	Qualsiasi	NA	NA

N.B.: Se il Controllo account utente (UAC) è attivato, è necessario disattivarlo prima dell'installazione su Windows Server 2008 R2, quando l'installazione viene eseguita in C:\Program Files. ed è necessario riavviare il server per rendere effettiva tale modifica.

Durante l'installazione, per impostare il database sono richieste le credenziali di Autenticazione di Windows o SQL. Indipendentemente dal tipo di credenziali utilizzate, l'account deve disporre dei privilegi appropriati per poter effettuare l'azione. La tabella precedente mostra in dettaglio i privilegi necessari per ogni tipo di installazione. Inoltre, l'account utilizzato per creare e configurare il database deve avere il proprio schema predefinito impostato su dbo.

Questi privilegi sono necessari solo durante l'installazione per configurare il database. Una volta installato Security Management Server, l'account utilizzato per gestire l'accesso SQL può essere ristretto ai ruoli pubblici e db_owner.

In caso di dubbi sui privilegi di accesso o sulla connettività al database, chiedere conferma all'amministratore del database prima di iniziare l'installazione.

Supporto lingue per la console di gestione

La console di gestione remota dispone dell'interfaccia utente multilingue (MUI, Multilingual User Interface) e supporta le seguenti lingue:

Supporto lingue	
EN - Inglese	JA - Giapponese
ES - Spagnolo	KO - Coreano
FR - Francese	PT-BR - Portoghese (Brasile)
IT - Italiano	PT-PT - Portoghese (Portogallo)
DE - Tedesco	

3

Configurazione di preinstallazione

Prima di iniziare, consultare le *Avvertenze tecniche Security Management Server* per eventuali soluzioni alternative o problemi noti riguardanti Security Management Server.

La configurazione di preinstallazione dei server in cui si intende installare Security Management Server è molto importante. Prestare particolare attenzione a questa sezione per garantire un'installazione corretta di Security Management Server.

Configurazione

1 Se abilitata, disattivare Protezione avanzata (ESC, Enhanced Security Configuration) di Internet Explorer. Aggiungere l'URL di Dell Server ai siti attendibili nelle opzioni di sicurezza del browser. Riavviare il server.

2 Aprire le seguenti porte per ciascun componente:

Interna:

Comunicazione Active Directory: TCP/389

Comunicazione tramite posta elettronica (opzionale): 25

Su front-end (se necessario):

Comunicazione da Policy Proxy a Message Broker: STOMP/61613

Comunicazione a Security Server back-end: HTTPS/8443

Comunicazione a Core Server back-end: HTTPS/8888

Comunicazione alle porte RMI - 1099

Comunicazione a Device Server back-end: HTTP(S)/8443 - Se la versione di Security Management Server è v7.7 o successiva. Se la versione di Dell Server è precedente alla v7.7, HTTP(S)/8081.

Server beacon: HTTP/8446 (se si utilizza Data Guardian)

Esterna (se necessario):

Database SQL: TCP/1433

Management Console: HTTPS/8443

LDAP: TCP/389/636 (controller di dominio locale), TCP/3268/3269 (catalogo globale), TCP/135/49125+ (RPC)

Compatibility Server: TCP/1099

Compliance Reporter: HTTP(S)/8084 (configurata automaticamente all'installazione)

Identity Server: HTTPS/8445

Core Server: HTTPS/8888 (8888 è configurata automaticamente all'installazione)

Device Server: HTTP(S)/8443 (Security Management Server v7.7 o versione successiva) o HTTP(S)/8081 (versione di Dell Server precedente alla v7.7)

Key Server: TCP/8050

Policy Proxy: TCP/8000

Security Server: HTTPS/8443

Client Authentication: HTTPS/8449 (se si usa Server Encryption)

Client communication, se si utilizza Advanced Threat Prevention: HTTPS/TCP/443

Creazione di un database di Dell Server

3 Queste istruzioni sono opzionali. Il programma di installazione crea un database per l'utente se non ne esiste già uno. Se si preferisce impostare un database prima di installare Security Management Server, seguire le istruzioni seguenti per creare sia il database che l'utente SQL in SQL Management Studio.

Quando si installa Security Management Server, seguire le istruzioni in Installare un server back-end con un database esistente.

Security Management Server è preparato per l'Autenticazione SQL e Windows. Il metodo di autenticazione predefinito è l'Autenticazione SQL.

Dopo aver creato il database, creare un utente del database Dell con diritti db_owner. Il db_owner può assegnare autorizzazioni, eseguire backup e ripristino del database, creare ed eliminare oggetti, e gestire account e ruoli utente senza limitazioni. Inoltre, accertarsi che tale utente abbia autorizzazioni/privilegi per eseguire le procedure archiviate.

Quando si utilizza un'istanza SQL Server non predefinita, dopo l'installazione di Security Management Server occorre specificare la porta dinamica di tale istanza nella scheda Database del Server Configuration Tool. Per ulteriori informazioni, consultare Server Configuration Tool. In alternativa, abilitare il servizio SQL Server Browser e accertarsi che la porta UDP 1434 sia aperta. Per ulteriori informazioni, vedere https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

Le regole di confronto non predefinite supportate per il database SQL o l'istanza SQL sono "SQL_Latin1_General_CP1_CI_AS".

Per creare il database e l'utente SQL in SQL Management Studio, scegliere tra:

Installare Visual C++ 2010/2013/2015 Redistributable Package

4 *Se non è già installato*, installare Microsoft Visual C++ 2010, 2013 e 2015 Redistributable Package. Se lo si desidera, è possibile consentire al programma di installazione di Security Management Server di installare questi componenti.

Windows Server 2008 R2 - http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5555

Installare .NET Framework 4.5

5 *Se non è già installato*, installare .NET Framework 4.5.

Windows Server 2008 R2 - https://www.microsoft.com/en-us/download/details.aspx?id=42643

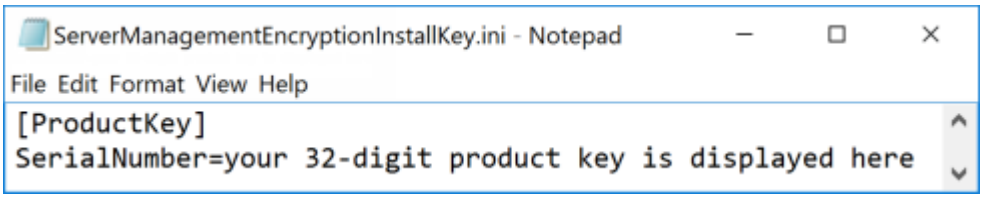
Installare SQL Native Client 2012

6 *Se si utilizza SQL Server 2012 o SQL Server 2016*, installare SQL Native Client 2012. Se lo si desidera, è possibile consentire al programma di installazione di Security Management Server di installare questo componente.

http://www.microsoft.com/en-us/download/details.aspx?id=35580

Facoltativo

7 **Per una nuova installazione**: copiare il codice Product Key (il nome del file è *EnterpriseServerInstallKey.ini*) in **C:\Windows** per popolare automaticamente il codice Product Key di 32 caratteri nel programma di installazione di Security Management Server.



La configurazione di preinstallazione del server è completa. Continuare con Installare o aggiornare/migrare.

4

Installazione o aggiornamento/migrazione

Questo capitolo fornisce le istruzioni per quanto segue:

- Nuova installazione - Per installare un nuovo Security Management Server.
- Aggiornamento/migrazione - Per eseguire l'aggiornamento da un Enterprise Server v9.2 o versione successiva, esistente e funzionale.
- Disinstallare Security Management Server - Per rimuovere l'installazione in uso, se necessario.

Se l'installazione deve includere più di un server principale (back-end), contattare il proprio rappresentante di Dell ProSupport.

Prima di iniziare l'installazione o l'aggiornamento/migrazione

Prima di iniziare, accertarsi di aver completato la procedura appropriata di Configurazione di preinstallazione.

Leggere le *Consulenze tecniche di* Security Management Server per eventuali soluzioni alternative correnti o problemi noti che riguardano l'installazione di Security Management Server.

Per ridurre i tempi di installazione su istanze di Server 2016, aggiungere le esclusioni riportate di seguito per Windows Defender:

- C:\Program Files\Dell\Enterprise Edition
- C:\Windows\Installer
- Il percorso del file da cui è stato eseguito il programma di installazione

Dell consiglia di usare le procedure consigliate per il database di Dell Server e di includere il software Dell nel piano di ripristino di emergenza della propria organizzazione.

Se si intende distribuire i componenti Dell nella DMZ, verificare che dispongano di una protezione adeguata contro gli attacchi.

Per la produzione, Dell consiglia vivamente di installare SQL Server in un server dedicato.

La procedura consigliata prevede di installare il server back-end prima di installare e configurare un server front-end.

I file di registro dell'installazione si trovano in questa directory: **C:\Users\<UtenteConnesso>\AppData\Local\Temp**

Nuova installazione

Scegliere una delle due opzioni per l'installazione del server back-end:

- Installare un server back-end e un nuovo database - Per installare un nuovo Security Management Server e un nuovo database.
- Installare un server back-end con un database esistente - Per installare un nuovo Security Management Server e connetterlo a un database SQL creato durante la Configurazione di preinstallazione o ad un database SQL esistente di versione v9.x o successiva, quando la versione di schema corrisponde alla versione di Security Management Server da installare. È necessario migrare un database v9.2 o versione successiva allo schema più recente con la versione più recente del Server Configuration Tool. Per istruzioni sulla migrazione dei database con il Server Configuration Tool, consultare Migrare il database. Per ottenere il Server Configuration Tool più recente o migrare a una versione di database precedente alla v9.2, contattare Dell ProSupport per assistenza.

N.B.:
Se si dispone di un Enterprise Server v9.2, o versione successiva, funzionale, fare riferimento alle istruzioni contenute in **Aggiornare/migrare server back-end**.

Se si installa un server front-end, eseguire questa installazione in seguito a quella del server back-end:

- Installare un server front-end - Per installare un server front-end in modo che comunichi con un server back-end.

Installare un server back-end e un nuovo database

1 Nel supporto di installazione di Dell, passare alla directory di Security Management Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Security Management Server-x64 nella directory principale del server in cui si sta installando Security Management Server. ***Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.***

2 Fare doppio clic su **setup.exe**.

3 Selezionare la lingua di installazione, quindi fare clic su **OK**.

4 Se i prerequisiti non sono già installati, viene visualizzato il messaggio che informa l'utente quali prerequisiti verranno installati. Fare clic su **Installa**.

5 Nella schermata iniziale, fare clic su **Avanti**.

6 Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.

7 Se è stato copiato il file EnterpriseServerInstallKey.ini in C:\Windows come descritto nella Configurazione di preinstallazione, fare clic su **Avanti**. Altrimenti, immettere il Product Key da 32 caratteri e fare clic su **Avanti**. Il codice Product Key si trova nel file EnterpriseServerInstallKey.ini.

8 Selezionare **Installazione back-end** e fare clic su **Avanti**.

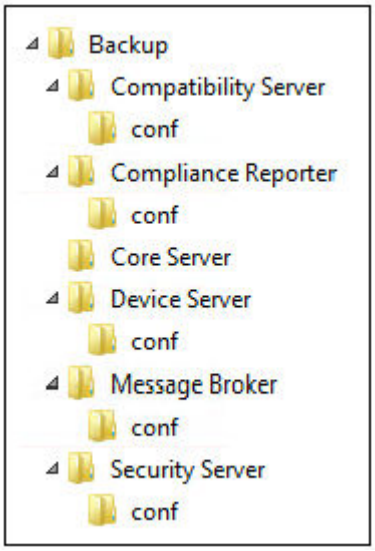
9 Per installare Security Management Server nel percorso predefinito C:\Program Files\Dell, fare clic su **Avanti**. Altrimenti, fare clic su **Modifica** per selezionare un altro diverso, quindi fare clic su **Avanti**.

10 Per selezionare un percorso in cui archiviare i file di configurazione del backup, fare clic su **Modifica**, passare alla cartella desiderata, quindi fare clic su **Avanti**.

Dell consiglia di selezionare, per il backup, un percorso di rete remoto o un'unità esterna.

Dopo l'installazione, deve essere eseguito il backup manuale di eventuali modifiche ai file di configurazione, incluse le modifiche apportate con Server Configuration Tool, in tali cartelle. I file di configurazione rappresentano una parte importante delle informazioni totali usate per ripristinare manualmente Dell Server, se necessario.

N.B.: La struttura di cartelle creata dal programma di installazione durante la fase di installazione (esempio mostrato qui di seguito) deve rimanere invariata.



11 È possibile scegliere i tipi di certificati digitali da usare. **È consigliabile utilizzare un certificato digitale proveniente da un'autorità di certificazione attendibile.**

Selezionare l'opzione "a" o "b" qui di seguito:

a Per usare un certificato esistente acquistato da un'autorità CA, selezionare **Importa un certificato esistente** e fare clic su **Avanti**.

Fare clic su **Sfoglia** per immettere il percorso del certificato.

Immettere la password associata al certificato. Il file dell'archivio chiavi deve essere .p12 o pfx. Per istruzioni, consultare Esportazione di un certificato in .PFX usando la console di gestione dei certificati.

Fare clic su **Avanti**.

> **N.B.:**
> Per usare questa impostazione, il certificato CA da importare deve avere la catena di attendibilità completa. In caso di dubbi, riesportare il certificato CA e accertarsi che le opzioni seguenti siano selezionate nell'"Esportazione guidata certificati":
>
> - Scambio informazioni personali - PKCS #12 (.PFX)
> - Includi tutti i certificati nel percorso di certificazione se possibile
> - Esporta tutte le proprietà estese

OPPURE

b Per creare un certificato autofirmato, selezionare **Crea un certificato autofirmato e importalo nell'archivio chiavi** e fare clic su **Avanti**.

Nella finestra di dialogo *Crea certificato autofirmato* immettere le seguenti informazioni:

Nome del computer completo (esempio: nomecomputer.dominio.com)

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.

N.B.: Per impostazione predefinita, il certificato scade dopo 10 anni.

12 Per Server Encryption, è possibile scegliere i tipi di certificati digitali da usare. È consigliabile utilizzare un certificato digitale proveniente da un'autorità di certificazione attendibile.

Selezionare l'opzione "a" o "b" qui di seguito:

a Per usare un certificato esistente acquistato da un'autorità CA, selezionare **Importa un certificato esistente** e fare clic su **Avanti**.

Fare clic su **Sfoglia** per immettere il percorso del certificato.

Immettere la password associata al certificato. Il file dell'archivio chiavi deve essere .p12 o pfx. Per istruzioni, consultare Esportazione di un certificato in .PFX usando la console di gestione dei certificati.

Fare clic su **Avanti**.

N.B.:

Per usare questa impostazione, il certificato CA da importare deve avere la catena di attendibilità completa. In caso di dubbi, riesportare il certificato CA e accertarsi che le opzioni seguenti siano selezionate nell'"Esportazione guidata certificati":

- Scambio informazioni personali - PKCS #12 (.PFX)
- Includi tutti i certificati nel percorso di certificazione se possibile
- Esporta tutte le proprietà estese

OPPURE

b Per creare un certificato autofirmato, selezionare **Crea un certificato autofirmato e importalo nell'archivio chiavi e fare clic su Avanti.**

Nella finestra di dialogo *Crea certificato autofirmato* immettere le seguenti informazioni:

Nome del computer completo (esempio: nomecomputer.dominio.com)

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.

N.B.: Per impostazione predefinita, il certificato scade dopo 10 anni.

13 Dalla finestra di dialogo *Configurazione dell'installazione del server back-end*, è possibile visualizzare o modificare nomi host e porte.

- Per accettare i nomi host e le porte predefiniti, nella finestra di dialogo *Configurazione dell'installazione del server back-end* fare clic su **Avanti**.
- Se si sta usando un server front-end, selezionare **Compatibile con Front End per comunicare con i client internamente in rete o esternamente in DMZ** e immettere il nome host del Security Server front-end (ad esempio server.dominio.com).
- Per visualizzare o modificare i nomi host, fare clic su **Modifica nomi host**. Modificare i nomi host solo se necessario. Dell consiglia di usare le impostazioni predefinite.

N.B.: Un nome host non può contenere il carattere "_" (sottolineato).

Al termine, fare clic su **OK**.

- Per visualizzare o modificare le porte, fare clic su **Modifica porte**. Modificare le porte solo se necessario. Dell consiglia di usare le impostazioni predefinite. Al termine, fare clic su **OK**.

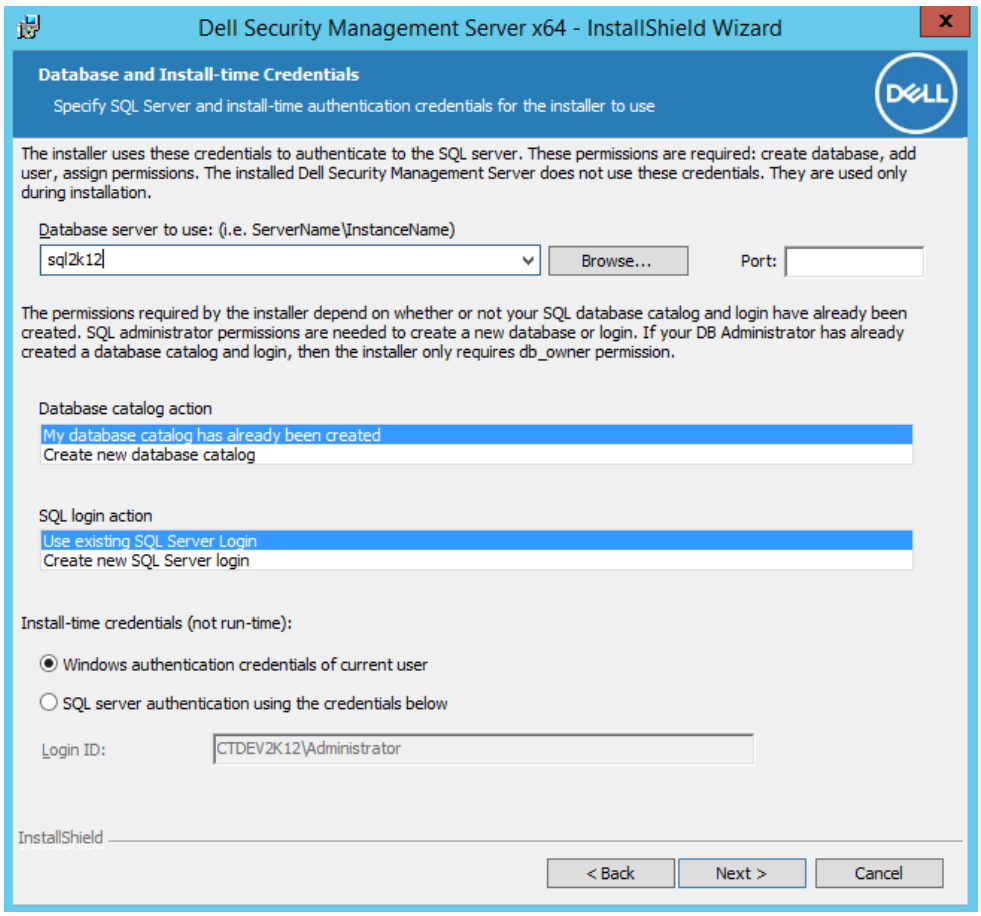
14 Per creare un nuovo database, seguire la seguente procedura:

a Fare clic su **Sfoglia** per selezionare il server in cui installare il database.

b Selezionare il metodo di autenticazione che deve usare il programma di installazione per configurare il database di Dell Server. Dopo l'installazione, il prodotto installato non utilizza le credenziali specificate qui.

- **Credenziali di autenticazione di Windows dell'utente corrente**

  Se si sceglie l'Autenticazione di Windows, per l'autenticazione vengono utilizzate le stesse credenziali utilizzate per accedere a Windows (i campi *Nome utente* e *Password* non sono modificabili). Accertarsi che l'account disponga dei diritti di amministratore del sistema e della possibilità di gestire SQL Server.



OPPURE

- **Autenticazione di SQL Server usando le credenziali seguenti**

  Se si usa l'autenticazione SQL, l'account SQL usato deve avere diritti di amministratore di sistema nell'SQL Server.

  Il programma di installazione deve eseguire l'autenticazione all'SQL Server con le seguenti autorizzazioni: creare database, aggiungere utenti, assegnare autorizzazioni.

c Identificare il catalogo del database:

Immettere il nome del catalogo di un nuovo database. Nella schermata successiva verrà richiesto di creare il nuovo catalogo.

d Fare clic su **Avanti**.

e Per confermare che si desidera far creare un database al programma di installazione, fare clic su **Sì**. Per tornare alla schermata precedente per apportare modifiche, fare clic su **No**.

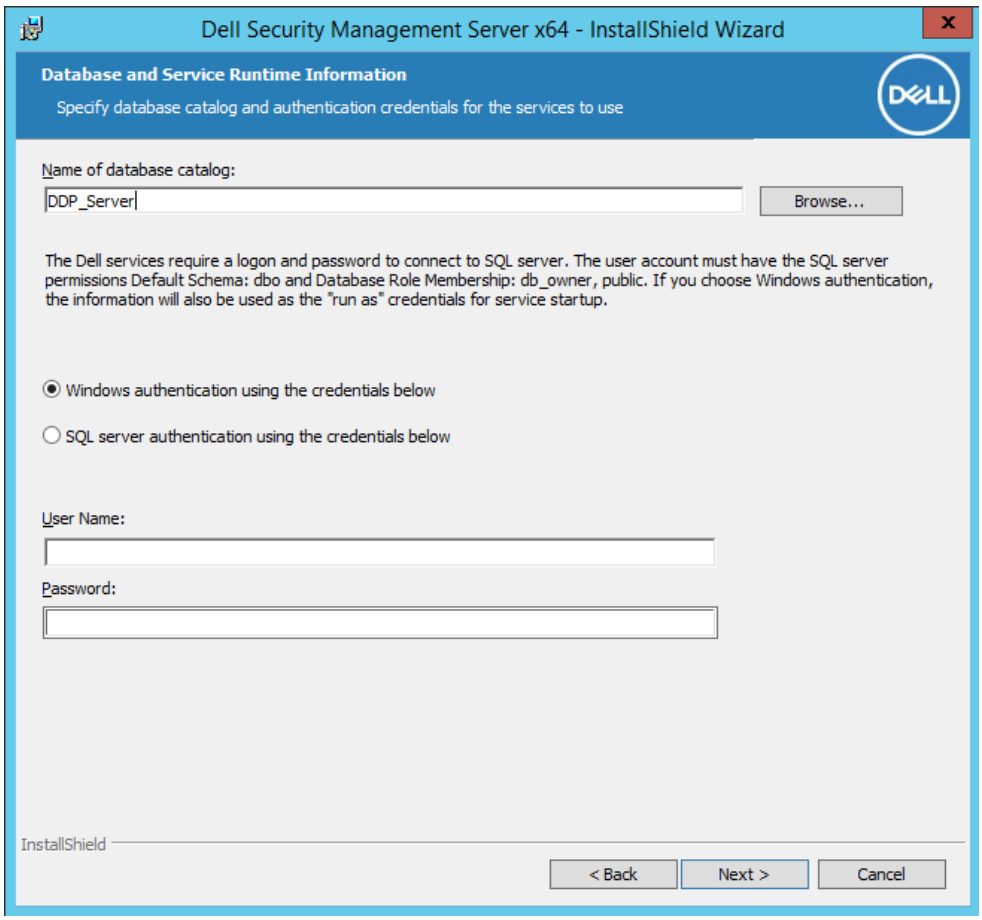
15 Selezionare il metodo di autenticazione per il prodotto da usare. Questa fase connette un account al prodotto.

- **Autenticazione di Windows**

Selezionare **Autenticazione di Windows usando le credenziali seguenti,** immettere le credenziali per il prodotto da usare e fare clic su **Avanti**.

Accertarsi che l'account disponga dei diritti di amministratore del sistema e della possibilità di gestire SQL Server. L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

Tali credenziali vengono utilizzate dai servizi Dell anche quando utilizzano Security Management Server.



OPPURE

- **Autenticazione di SQL Server**

  Selezionare **Autenticazione di SQL Server usando le credenziali seguenti**, immettere le credenziali di SQL Server che i servizi Dell devono usare per gestire Security Management Server, quindi fare clic su **Avanti**.

  L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

16 Nella finestra di dialogo *Installazione del programma*, fare clic su **Installa**.
Una finestra di dialogo di stato visualizza lo stato del processo di installazione.

17 Al completamento dell'installazione, fare clic su **Fine**.
Le attività di installazione del server back-end sono state completate.

Al termine dell'installazione i servizi Dell verranno riavviati. Non sarà necessario riavviare Dell Server.

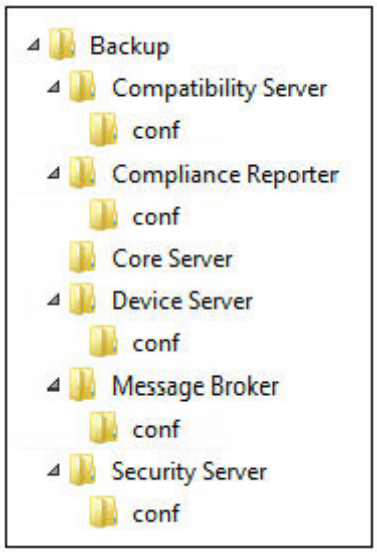
Installare un server back-end con un database esistente

N.B.:
Se si dispone di un Dell Server v9.2, o versione successiva, funzionale, fare riferimento alle istruzioni contenute in Aggiornare/migrare server back-end.

È possibile installare un nuovo Security Management Server e connetterlo a un database SQL creato durante la Configurazione di preinstallazione o a un database SQL esistente di versione v9.x o successiva, quando la versione di schema corrisponde alla versione di Security Management Server da installare.

L'account utente dal quale si esegue l'installazione deve avere privilegi di proprietario del database per il database SQL. In caso di dubbi sui privilegi di accesso o sulla connettività al database, chiedere conferma all'amministratore del database prima di iniziare l'installazione.

Se il database esistente è stato installato in precedenza con Security Management Server, prima di iniziare l'installazione accertarsi che sia stato eseguito il backup del database, dei file di configurazione e del secretKeyStore in un percorso a cui si possa accedere dal server in cui si sta installando Security Management Server. Sarà necessario accedere a tali file per configurare Security Management Server e il database esistente. La struttura di cartelle creata dal programma di installazione durante l'installazione (esempio mostrato qui di seguito) deve rimanere invariata.



1. Nel supporto di installazione di Dell, passare alla directory di Security Management Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Security Management Server-x64 nella directory principale del server in cui si sta installando Security Management Server. ***Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.***
2. Fare doppio clic su **setup.exe**.
3. Selezionare la lingua di installazione, quindi fare clic su **OK**.
4. Se i prerequisiti non sono già installati, viene visualizzato il messaggio che informa l'utente quali prerequisiti verranno installati. Fare clic su **Installa**.
5. Nella schermata iniziale, fare clic su **Avanti**.
6. Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.
7. Se è stato copiato il file **EnterpriseServerInstallKey.ini** in **C:\Windows** come descritto nella Configurazione di preinstallazione, fare clic su **Avanti**. Altrimenti, immettere il Product Key da 32 caratteri e fare clic su **Avanti**. Il codice Product Key si trova nel file **EnterpriseServerInstallKey.ini**.
8. Selezionare **Installazione back-end** e **Installazione di ripristino**, quindi fare clic su **Avanti**.

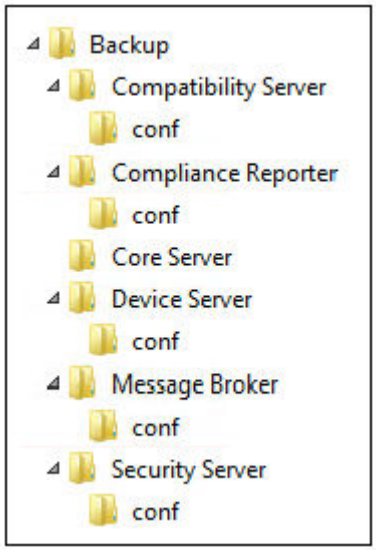
9 Per installare Security Management Server nel percorso predefinito **C:\Program Files\Dell**, fare clic su **Avanti**. Altrimenti, fare clic su **Modifica** per selezionare un percorso diverso, quindi fare clic su **Avanti**.

10 Per selezionare un percorso in cui archiviare i file di ripristino della configurazione di backup, fare clic su **Modifica**, passare alla cartella desiderata, quindi fare clic su **Avanti**.

Dell consiglia di selezionare, per il backup, un percorso di rete remoto o un'unità esterna.

Dopo l'installazione, deve essere eseguito il backup manuale di eventuali modifiche ai file di configurazione, incluse le modifiche apportate con Server Configuration Tool, in tali cartelle. I file di configurazione rappresentano una parte importante delle informazioni totali usate per ripristinare manualmente il Dell server.

N.B.: La struttura di cartelle creata dal programma di installazione durante l'installazione (esempio mostrato qui di seguito) deve rimanere invariata.



11 È possibile scegliere i tipi di certificati digitali da usare. **È consigliabile utilizzare un certificato digitale proveniente da un'autorità di certificazione attendibile.**

Selezionare l'opzione "a" o "b" qui di seguito:

a Per usare un certificato esistente acquistato da un'autorità CA, selezionare **Importa un certificato esistente** e fare clic su **Avanti**.

Fare clic su **Sfoglia** per immettere il percorso del certificato.

Immettere la password associata al certificato. Il file dell'archivio chiavi deve essere .p12 o pfx. Per istruzioni, consultare Esportazione di un certificato in .PFX usando la console di gestione dei certificati.

Fare clic su **Avanti**.

N.B.:

Per usare questa impostazione, il certificato CA da importare deve avere la catena di attendibilità completa. In caso di dubbi, riesportare il certificato CA e accertarsi che le opzioni seguenti siano selezionate nell'"Esportazione guidata certificati":

- Scambio informazioni personali - PKCS #12 (.PFX)
- Includi tutti i certificati nel percorso di certificazione se possibile
- Esporta tutte le proprietà estese

OPPURE

b Per creare un certificato autofirmato, selezionare **Crea un certificato autofirmato e importalo nell'archivio chiavi e fare clic su Avanti.**

Nella finestra di dialogo *Crea certificato autofirmato* immettere le seguenti informazioni:

Nome del computer completo (esempio: nomecomputer.dominio.com)

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.

N.B.: Per impostazione predefinita, il certificato scade dopo 10 anni.

12 Dalla finestra di dialogo *Configurazione dell'installazione del server back-end*, è possibile visualizzare o modificare nomi host e porte.

- Per accettare i nomi host e le porte predefiniti, nella finestra di dialogo *Configurazione dell'installazione del server back-end* fare clic su **Avanti**.
- Se si sta usando un server front-end, selezionare **Compatibile con Front End per comunicare con i client internamente in rete o esternamente in DMZ** e immettere il nome host del Security Server front-end (ad esempio server.dominio.com).
- Per visualizzare o modificare i nomi host, fare clic su **Modifica nomi host**. Modificare i nomi host solo se necessario. Dell consiglia di usare le impostazioni predefinite.

  N.B.: Un nome host non può contenere il carattere "_" (sottolineato).

  Al termine, fare clic su **OK**.
- Per visualizzare o modificare le porte, fare clic su **Modifica porte**. Modificare le porte solo se necessario. Dell consiglia di usare le impostazioni predefinite. Al termine, fare clic su **OK**.

13 Specificare il metodo di autenticazione per il programma di installazione da usare.

a Fare clic su **Sfoglia** per selezionare il server in cui si trova il database.

b Selezionare il tipo di autenticazione.

- **Credenziali di autenticazione di Windows dell'utente corrente**

  Se si sceglie l'Autenticazione di Windows, per l'autenticazione vengono utilizzate le stesse credenziali utilizzate per accedere a Windows (i campi *Nome utente* e *Password*non sono modificabili). Accertarsi che l'account disponga dei diritti di amministratore del sistema e della possibilità di gestire SQL Server.

  OPPURE

- **Autenticazione di SQL Server usando le credenziali seguenti**

  Se si usa l'autenticazione SQL, l'account SQL usato deve avere diritti di amministratore di sistema nell'SQL Server.

  Il programma di installazione deve eseguire l'autenticazione all'SQL Server con le seguenti autorizzazioni: creare database, aggiungere utenti, assegnare autorizzazioni.

c Fare clic su **Sfoglia** per selezionare il nome di catalogo del database esistente.

d Fare clic su **Avanti**.

14 Se viene visualizzata la finestra di dialogo Errore database esistente, selezionare l'opzione appropriata.

Se il programma di installazione rileva un problema relativo al database, viene visualizzata la finestra di dialogo *Errore del database esistente*. Le opzioni nella finestra di dialogo dipendono dalle circostanze:

- Lo schema del database è di una versione precedente (fare riferimento al punto a).
- Il database ha già uno schema di database che corrisponde alla versione attualmente in fase di installazione. (fare riferimento al punto b).

a Quando lo schema del database è di una versione precedente, selezionare **Esci dal programma di installazione per terminare l'installazione**. Successivamente, eseguire il backup del database.

Le opzioni seguenti DEVONO essere usate solo avvalendosi dell'assistenza di Dell ProSupport:

- L'opzione **Migra questo database allo schema corrente** viene usata per ripristinare un buon database da un'implementazione del server non riuscita. Questa opzione usa i file di ripristino nella cartella \Backup per riconnetterli al database, quindi migra il database allo schema corrente. Questa opzione deve essere usata *solo* dopo aver prima provato a reinstallare la versione corretta di Security Management Server, eseguendo poi il programma di installazione più recente per l'aggiornamento.
- L'opzione **Procedi senza migrare il database** installa i file di Security Management Serversenza configurare completamente il database. La configurazione del database deve essere completata manualmente in un secondo momento usando il Server Configuration Tool e sarà necessario apportare altre modifiche manualmente.

b Quando lo schema del database dispone già dello schema della versione in uso ma non è connesso al back-end di Security Management Server è considerato un *Ripristino*. Se non è stata selezionata l'opzione **Installazione di ripristino** in questa fase, viene visualizzata questa finestra di dialogo:

- Selezionare **Modalità di installazione di ripristino** per proseguire l'installazione con il database selezionato.
- Selezionare **Seleziona un nuovo database** per sceglierne uno diverso.
- Selezionare **Esci dal programma di installazione per terminare l'installazione**.

c Fare clic su **Avanti**.

15 Selezionare il metodo di autenticazione per il prodotto da usare. Questo è l'account che il prodotto usa per gestire il database e i servizi Dell.

- **Per usare l'autenticazione di Windows**

  Selezionare <3>Autenticazione di Windows usando le credenziali seguenti</3>**,** immettere le credenziali per l'account che il prodotto può usare e fare clic su **Avanti**.

  Accertarsi che l'account disponga dei diritti di amministratore del sistema e della possibilità di gestire SQL Server. L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

  OPPURE

- **Per usare l'autenticazione di SQL Server**

  Selezionare **Autenticazione di SQL Server usando le credenziali seguenti**, immettere le credenziali di SQL Server e fare clic su **Avanti.**

  L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

16 Nella finestra di dialogo *Installazione del programma*, fare clic su **Installa**.

Una finestra di dialogo di stato visualizza lo stato del processo di installazione.

Al completamento dell'installazione, fare clic su **Fine**.

Le attività di installazione del server back-end sono state completate.

Al termine dell'installazione i servizi Dell verranno riavviati. Non è necessario riavviare il server.

Installare server front-end

Installazione del server front-end fornisce un'opzione front-end (modalità DMZ) per l'uso con Security Management Server. Se si intende distribuire i componenti Dell nella DMZ, verificare che dispongano di una protezione adeguata contro gli attacchi.

N.B.: Il servizio beacon è installato come parte di questa installazione per supportare il beacon di richiamata di Data Guardian, che inserisce un beacon di richiamata in ciascun file protetto da Data Guardian quando si consentono o si applicano documenti Office protetti nell'ambiente. Ciò consente la comunicazione tra tutti i dispositivi in qualsiasi posizione e il server front-end. Accertarsi che la sicurezza di rete necessaria sia configurata prima di utilizzare il beacon richiamata.

Per eseguire questa installazione, è necessario il nome host completo del server DMZ.

1 Nel supporto di installazione di Dell, passare alla directory di Security Management Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Security Management Server-x64 nella directory principale del server in cui si sta installando Security Management Server. ***Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.***

2 Fare doppio clic su **setup.exe**.

3 Selezionare la lingua di installazione, quindi fare clic su **OK**.

4 Se i prerequisiti non sono già installati, viene visualizzato il messaggio che informa l'utente quali prerequisiti verranno installati. Fare clic su **Installa**.

5 Fare clic su **Avanti** nella finestra di dialogo Introduzione.

6 Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.

7 Se è stato copiato il file EnterpriseServerInstallKey.ini in C:\Windows come descritto nella Configurazione di pre-installazione, fare clic su **Avanti**. Altrimenti, immettere il Product Key da 32 caratteri e fare clic su **Avanti**. Il codice Product Key si trova nel file EnterpriseServerInstallKey.ini.

8 Selezionare **Installazione front-end** e fare clic su **Avanti**.

9 Per installare il server front-end nel percorso predefinito C:\Program Files\Dell, fare clic su **Avanti**. Altrimenti, fare clic su **Modifica** per selezionare un altro diverso, quindi fare clic su **Avanti**.

10 È possibile scegliere i tipi di certificati digitali da usare.

N.B.: È consigliabile utilizzare un certificato digitale proveniente da un'autorità di certificazione attendibile.

Selezionare l'opzione "a" o "b" qui di seguito:

a Per usare un certificato esistente acquistato da un'autorità CA, selezionare **Importa un certificato esistente** e fare clic su **Avanti**. Fare clic su **Sfoglia** per immettere il percorso del certificato.

Immettere la password associata al certificato. Il file dell'archivio chiavi deve essere .p12 o pfx. Per istruzioni, consultare Esportazione di un certificato in .PFX usando la console di gestione dei certificati.

Fare clic su **Avanti**.

N.B.:

Per usare questa impostazione, il certificato CA da importare deve avere la catena di attendibilità completa. In caso di dubbi, riesportare il certificato CA e accertarsi che le opzioni seguenti siano selezionate nell'"Esportazione guidata certificati":

- Scambio informazioni personali - PKCS #12 (.PFX)
- Includi tutti i certificati nel percorso di certificazione se possibile
- Esporta tutte le proprietà estese

b Per creare un certificato autofirmato, selezionare **Crea un certificato autofirmato e importalo nell'archivio chiavi e fare clic su Avanti.**

Nella finestra di dialogo *Crea certificato autofirmato* immettere le seguenti informazioni:

Nome del computer completo (esempio: nomecomputer.dominio.com)

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.

> **N.B.: Per impostazione predefinita, il certificato scade dopo 10 anni.**

11 Nella finestra di dialogo *Configurazione del server front-end*, immettere il nome host completo o l'alias DNS del server back-end, selezionare **Dell Security Management Server**, quindi fare clic su **Avanti**.

12 Dalla finestra di dialogo *Configurazione dell'installazione del server front-end*, è possibile visualizzare o modificare nomi host e porte.

- Per accettare i nomi host e le porte predefiniti, nella finestra di dialogo *Configurazione dell'installazione del server front-end* fare clic su **Avanti**.
- Per visualizzare o modificare i nomi host, nella finestra di dialogo *Configurazione del server front-end* fare clic su **Modifica nomi host**. Modificare i nomi host solo se necessario. Dell consiglia di usare le impostazioni predefinite.

  > **N.B.:**
  > Un nome host non può contenere il carattere "_" (sottolineato).

  Deselezionare un proxy solo se si è certi di non volerlo configurare per l'installazione. Se si deseleziona un proxy in questa finestra di dialogo, non viene installato.

  Al termine, fare clic su **OK**.
- Per visualizzare o modificare le porte, nella finestra di dialogo *Configurazione del server front-end* cliccare su **Modifica porte rivolte verso l'esterno** o **Modifica porte di connessione interne**. Modificare le porte solo se necessario. Dell consiglia di usare le impostazioni predefinite.

  Se si deseleziona un proxy nella finestra di dialogo *Modifica nomi host front-end*, la relativa porta non verrà visualizzata nelle finestre di dialogo Porte esterne o Porte interne.

  Al termine, fare clic su **OK**.

13 Nella finestra di dialogo *Installazione del programma*, fare clic su **Installa**.
Una finestra di dialogo di stato visualizza lo stato del processo di installazione.

14 Al completamento dell'installazione, fare clic su **Fine**.
Le attività di installazione del server front-end sono state completate.

Aggiornamento/migrazione

È possibile aggiornare Enterprise Server v9.2 e versioni successive a Security Management Server v9.x. Se la versione di Dell Server è precedente alla v9.2, è necessario prima eseguire l'aggiornamento alla v9.2 e quindi alla v9.x.

Prima di iniziare l'aggiornamento/migrazione

Prima di iniziare, accertarsi di aver completato tutta la procedura di Configurazione di preinstallazione.

Leggere le Security Management Server *Technical Advisories* (Consulenze tecniche di Security Management Server) per eventuali soluzioni alternative correnti o problemi noti che riguardano l'installazione di Security Management Server.

L'account utente dal quale si esegue l'installazione deve avere privilegi di proprietario del database per il database SQL. In caso di dubbi sui privilegi di accesso o sulla connettività al database, chiedere conferma all'amministratore del database prima di iniziare l'installazione.

Dell consiglia di usare le procedure consigliate per il database di Dell Server e di includere il software Dell nel piano di ripristino di emergenza della propria organizzazione.

Se si intende distribuire i componenti Dell nella DMZ, verificare che dispongano di una protezione adeguata contro gli attacchi.

Per la produzione, Dell consiglia di installare SQL Server in un server dedicato.

Per sfruttare le funzionalità complete dei criteri, Dell consiglia di eseguire l'aggiornamento alle versioni più recenti di Security Management Server e dei client.

Security Management Server v9.x supporta:

- Encryption Enterprise:
  - Client Windows v7.x/8.x
  - Client Mac v7.x/8.x
  - Client SED v8.x
  - Authentication v8.x
  - BitLocker Manager v7.2x+ e v8.x
  - Data Guardian v1.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprisev1.x
- Aggiornamento/migrazione da Security Management Serverv9.2 o versione successiva (quando si esegue la migrazione di Security Management Server da una versione precedente alla v9.2, contattare Dell ProSupport per assistenza).

Quando si effettua l'aggiornamento/la migrazione di Security Management Server ad una versione che include i nuovi criteri introdotti in tale versione, eseguire il commit del criterio aggiornato dopo l'aggiornamento/la migrazione, per garantire che le impostazioni preferite dei criteri siano implementate per i nuovi criteri, piuttosto che i valori predefiniti.

In generale, il nostro percorso di aggiornamento consigliato è quello di aggiornare/migrare Security Management Server e i relativi componenti, per poi proseguire con l'installazione/aggiornamento del client.

Applicare le modifiche ai criteri

1 Eseguire l'accesso alla Management Console come amministratore Dell.

2 Nel menu a sinistra, fare clic su **Gestione** > **Esegui commit**.

3 In *Commento*, immettere una descrizione della modifica.

4 Fare clic su **Commit criteri**.

5 Al completamento del commit, disconnettersi dalla Management Console.

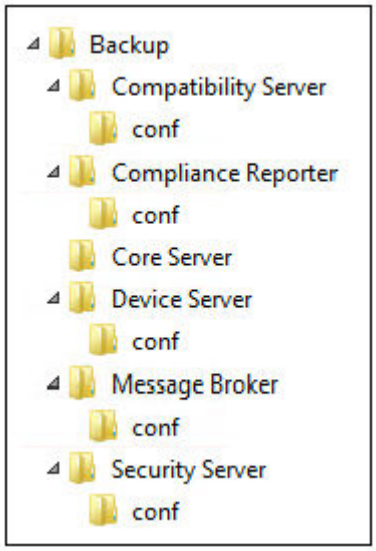
Accertarsi che i servizi Dell siano in esecuzione

6 Dal menu *Start* di Windows, fare clic su **Start** > **Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e, se necessario, fare clic su **Avvia il servizio**.

Eseguire il backup dell'installazione esistente

7 Eseguire il backup dell'intera installazione esistente in un percorso alternativo. Il backup deve includere database SQL, secretKeyStore e file di configurazione. Molti file dell'installazione esistente sono necessari al completamento del processo di aggiornamento/migrazione.

> **N.B.:**
> La struttura di cartelle creata dal programma di installazione durante l'installazione (esempio mostrato qui di seguito) deve rimanere invariata



Eseguire l'aggiornamento/la migrazione dei server back-end

1 Nel supporto di installazione di Dell, passare alla directory di Security Management Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Security Management Server-x64 nella directory principale del server in cui si sta installando Security Management Server. ***Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.***

2 Fare doppio clic su **setup.exe**.

3 Selezionare la lingua di installazione, quindi fare clic su **OK**.

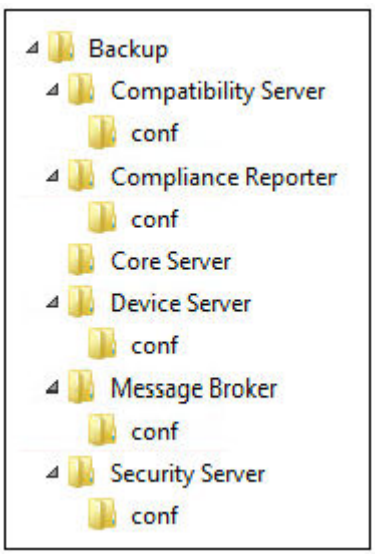
4 Nella schermata iniziale, fare clic su **Avanti**.

5 Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.

6 Per selezionare un percorso in cui archiviare i file di configurazione del backup, fare clic su **Modifica**, passare alla cartella desiderata e fare clic su **Avanti**.

Dell consiglia di selezionare, per il backup, un percorso di rete remoto o un'unità esterna.

La struttura di cartelle creata dal programma di installazione durante l'installazione (esempio mostrato qui di seguito) deve rimanere invariata.



7 Quando il programma di installazione salva correttamente il database esistente, la finestra di dialogo viene precompilata.

Per connettere il database esistente, specificare il metodo di autenticazione da usare. Dopo l'installazione, il prodotto installato non utilizza le credenziali specificate qui.

a Selezionare il tipo di autenticazione del database:

- **Credenziali di autenticazione di Windows dell'utente corrente**

  Se si sceglie l'Autenticazione di Windows, per l'autenticazione vengono utilizzate le stesse credenziali utilizzate per accedere a Windows (i campi *Nome utente* e *Password* non sono modificabili).

  Accertarsi che l'account disponga dei diritti di amministratore del sistema e della possibilità di gestire SQL Server. L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

  OPPURE

- **Autenticazione di SQL Server usando le credenziali seguenti**

  Se si usa l'autenticazione SQL, l'account SQL usato deve avere diritti di amministratore di sistema nell'SQL Server.

  Il programma di installazione deve eseguire l'autenticazione all'SQL Server con le seguenti autorizzazioni: creare database, aggiungere utenti, assegnare autorizzazioni.

b Fare clic su **Avanti**.

8 Se la finestra di dialogo Informazioni sull'account del runtime del servizio non viene pre-popolata, specificare il metodo di autenticazione che il prodotto può usare dopo l'installazione.

a Selezionare il tipo di autenticazione.

b Immettere nome utente e password dell'account di servizio del dominio che i servizi Dell useranno per accedere all'SQL Server e fare clic su **Avanti**.

L'account utente deve essere nel formato DOMINIO\Nomeutente ed essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza a ruoli del database per: dbo_owner, public.

9 Se non è stato eseguito il backup del database, è ***necessario*** eseguirlo prima di continuare l'installazione. ***Non sarà possibile ripristinare l'aggiornamento del database.*** Solo dopo aver eseguito il backup del database, selezionare **Sì, il backup del database è stato eseguito**, quindi fare clic su **Avanti**.

10 Fare clic su **Installa** per avviare l'installazione.

Una finestra di dialogo di stato visualizza lo stato del processo di aggiornamento.

11 Al completamento dell'installazione, fare clic su **Fine**.

Al termine della migrazione i servizi Dell verranno riavviati. Non sarà necessario riavviare Dell Server.

Il programma di installazione esegue automaticamente le procedure ai punti 12-13. La procedura consigliata è quella di controllare tali valori per accertarsi che le modifiche siano state apportate correttamente.

12 Nel backup dell'installazione, copiare/incollare: <directory installazione Compatibility Server>\conf\secretKeyStore nella nuova installazione:

<directory installazione Compatibility Server>\conf\secretKeyStore

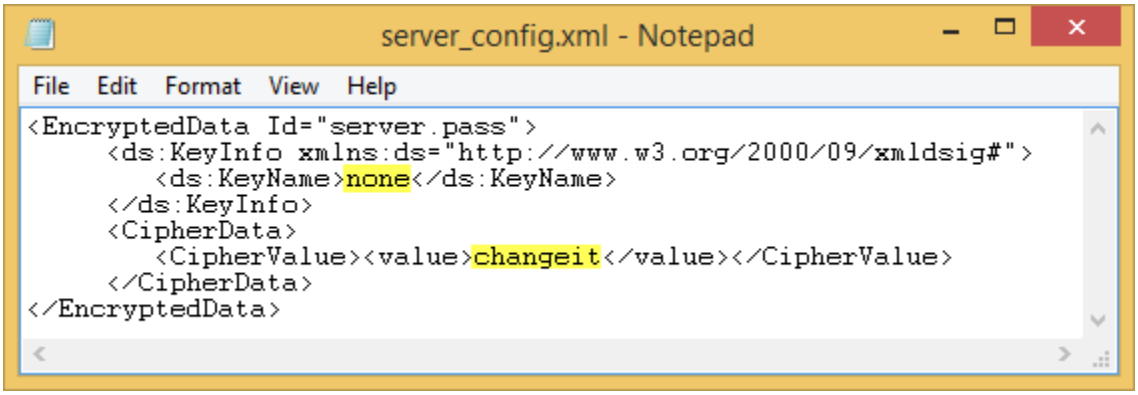
13 Nella nuova installazione, aprire <directory installazione Compatibility Server>\conf\server_config.xml e sostituire il valore **server.pass** con il valore del backup di <directory installazione Compatibility Server>\conf\server_config.xml, come segue:

Istruzioni per server.pass:

Se si conosce la password, fare riferimento al file server_config.xml di esempio e apportare le seguenti modifiche:

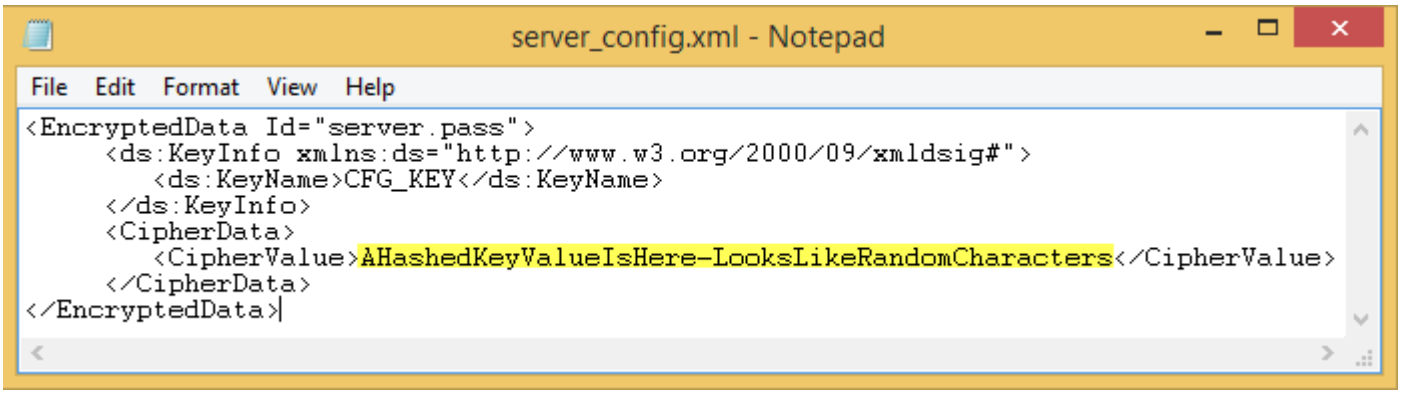
- Modificare il *KeyName* dal valore **CFG_KEY** a **none.**
- Immettere la password come testo non crittografato e racchiuderla tra *<value> </value>*, che in questo esempio è **<value>changeit</value>**
- All'avvio di Security Management Server, la password come testo non crittografato ha un hash e il valore con hash sostituisce il testo non crittografato.

Password nota



Se non si conosce la password, tagliare e incollare la sezione simile alla sezione mostrata nella Figura 4-2 dal backup del file <directory installazione Compatibility Server>\conf\server_config.xml nella sezione corrispondente nel nuovo file *server_config.xml*.

Password sconosciuta



Salvare e chiudere i file.

N.B.:
Mai provare a modificare la password di Security Management Server modificando il valore server.pass in server_config.xml. Se si modifica questo valore, si perde l'accesso al database.

Le attività di migrazione del server back-end sono state completate.

Eseguire l'aggiornamento/la migrazione dei server front-end

N.B.: A partire dalla versione 9.5, il servizio beacon viene installato come parte di questo aggiornamento utilizzando il nome host predefinito e la porta 8446. Il servizio beacon supporta il beacon di richiamata di Data Guardian, che inserisce un beacon di richiamata in ciascun file protetto da Data Guardian quando si consentono o si applicano documenti Office protetti nell'ambiente. Ciò consente la comunicazione tra tutti i dispositivi in qualsiasi posizione e il server front-end. Accertarsi che la sicurezza di rete necessaria sia configurata prima di utilizzare il beacon richiamata.

1. Nel supporto di installazione di Dell, passare alla directory di Security Management Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Security Management Server-x64 nella directory principale del server in cui si sta installando Security Management Server. ***Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.***
2. Fare doppio clic su **setup.exe**.
3. Selezionare la lingua di installazione, quindi fare clic su **OK**.
4. Se i prerequisiti non sono già installati, viene visualizzato il messaggio che informa l'utente quali prerequisiti verranno installati. Fare clic su **Installa**.

5 Nella schermata iniziale, fare clic su **Avanti**.

6 Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.

7 Nella finestra di dialogo *Installazione del programma*, fare clic su **Installa**.

Una finestra di dialogo di stato visualizza lo stato del processo di installazione.

8 Al completamento dell'installazione, fare clic su **Fine**.

9 Impostare il server back-end in modo che comunichi con il server front-end.

a Nel server back-end, andare a <directory installazione Security Server>\conf\ e aprire il file application.properties.

b Individuare publicdns.server.host e impostare il nome su un nome host risolvibile dall'esterno.

c Individuare publicdns.server.port e impostare la porta (quella predefinita è 8443).

Al termine dell'installazione i servizi Dell verranno riavviati. Non sarà necessario riavviare Dell Server finché le attività di Configurazione di postinstallazione non saranno state completate.

Installazione in modalità disconnessa

La modalità disconnessa isola Security Management Server da Internet e da una LAN o un'altra rete non protetta. Dopo averlo installato in modalità disconnessa, Security Management Server resta in modalità disconnessa e non può essere riportato in modalità connessa.

Security Management Server è installato in modalità disconnessa tramite riga di comando.

La seguente tabella elenca gli switch disponibili.

Opzione	Significato
/v	Consente di passare variabili al file .msi all'interno di *.exe
/s	Modalità non interattiva

La tabella seguente elenca le opzioni disponibili per la visualizzazione.

Opzione	Significato
/q	La finestra di dialogo non viene visualizzata e il sistema si riavvia automaticamente al termine del processo
/qb	Finestra di dialogo con pulsante **Annulla**
/qn	L'interfaccia utente non viene visualizzata

La tabella seguente descrive in dettaglio i parametri disponibili per l'installazione. Questi parametri possono essere specificati nella riga di comando o richiamati da un file utilizzando la proprietà:

```
INSTALL_VALUES_FILE=\"<file_path>\" "
```

Parametri
AGREE_TO_LICENSE=Sì - Questo valore deve essere "Sì."
PRODUCT_SN=xxxxx - Opzionale se si è in possesso delle informazioni di licenza nella posizione standard; in caso contrario, immetterlo qui.
INSTALLDIR=<path> - Opzionale.
BACKUPDIR=<path> - Questa è la posizione in cui vengono archiviati i file di ripristino.

N.B.: La struttura di cartelle creata dal programma di installazione durante la fase di installazione (esempio mostrato qui di seguito) deve rimanere invariata.

Parametri

AIRGAP=1 - Questo valore deve essere "1" per installare Security Management Server in modalità disconnessa.

SSL_TYPE=n - Dove n è 1 per importare un certificato esistente che è stato acquistato da un'autorità CA e 2 per creare un certificato autofirmato. Il valore SSL_TYPE determina quali proprietà SSL sono richieste.

Sono necessari i seguenti requisiti con SSL_TYPE=1:

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

Sono necessari i seguenti requisiti con SSL_TYPE=2:

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY - Facoltativo, impostazione predefinita = "USA"

SSL_STATENAME

SSOS_TYPE=n - Dove n è 1 per importare un certificato esistente che è stato acquistato da un'autorità CA e 2 per creare un certificato autofirmato. Il valore SSOS_TYPE determina quali proprietà SSOS sono richieste.

Sono necessari i seguenti requisiti con SSOS_TYPE=1:

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

Sono necessari i seguenti requisiti con SSOS_TYPE=2:

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY - Facoltativo, impostazione predefinita = "USA"

SSOS_STATENAME

DISPLAY_SQLSERVER - Questo valore viene analizzato per ottenere un'istanza SQL Server e le informazioni sulla porta.

Esempio:

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE - Opzionale. Il valore predefinito è FALSE, ciò significa che il database non viene creato. Il database deve essere già presente sul server.

Per creare un nuovo database, impostare questo valore su TRUE.

IS_SQLSERVER_AUTHENTICATION=0 - Opzionale. Il valore predefinito è 0, che indica che le credenziali di autenticazione Windows dell'utente connesso vengono utilizzate per l'autenticazione sul server SQL. Per utilizzare l'autenticazione SQL, impostare questo valore su 1.

Parametri

N.B.: Il programma di installazione deve eseguire l'autenticazione all'SQL Server con le seguenti autorizzazioni: creare database, aggiungere utenti, assegnare autorizzazioni. Le credenziali sono valide per l'installazione non per l'esecuzione.

Se viene utilizzata l'autenticazione SQL, sono necessari i seguenti requisiti:

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION - Richiesto. Specificare il metodo di autenticazione per il prodotto da usare. Questa fase connette un account al prodotto. Tali credenziali vengono utilizzate dai servizi Dell anche quando gestiscono Security Management Server. Per utilizzare l'autenticazione Windows, impostare questo valore su 0. Per utilizzare l'autenticazione SQL, impostare il valore su 1.

N.B.: Accertarsi che l'account disponga dei diritti di amministratore del sistema e della possibilità di gestire SQL Server. L'account utente deve essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

SQL_EE_USERNAME - Richiesto. Con l'autenticazione Windows, utilizzare questo formato: DOMINIO\Nome utente. Con l'autenticazione SQL, specificare il nome utente.

SQL_EE_PASSWORD - Richiesto. Specificare la password associata a questo nome utente Windows o SQL.

Se viene utilizzata l'autenticazione SQL, (EE_SQLSERVER_AUTHENTICATION= 1) sono validi i seguenti requisiti:

RUNAS_KEYSERVER_USER - Impostare la chiave server "esegui come" su nome utente Windows in questo formato: Dominio\Utente. Deve trattarsi di un account utente Windows.

RUNAS_KEYSERVER_PSWD - Impostare la chiave server "esegui come" password Windows associata all'account utente di Windows.

SQL_ADD_LOGIN=T - Opzionale. L'impostazione predefinita è null (questo accesso non viene aggiunto). Quando il valore è impostato su T, se SQL_EE_USERNAME non è un accesso o un utente per il database, il programma di installazione tenta di aggiungere le credenziali di autenticazione SQL dell'utente e di impostare i privilegi per consentire l'uso delle credenziali dal prodotto.

I seguenti sono i parametri del nome host. Modificare i nomi host solo se necessario. Dell consiglia di usare le impostazioni predefinite. Il formato deve essere `server.domain.com`.

N.B.: Un nome host non può contenere il carattere "_" (sottolineato).

CORESERVERHOST - Opzionale. Nome host Core Server.

RMIHOST - Opzionale. Nome host server compatibilità.

REPORTERHOST - Opzionale. Nome host Compliance Reporter.

DEVICEHOST - Opzionale. Nome host Device Server.

KEYSERVERHOST - Opzionale. Nome host chiave server.

TIGAHOST - Opzionale. Nome host Security Server.

SMTP_HOST - Opzionale. Nome host SMTP.

ACTIVEMQHOST - Opzionale. Nome host Message Broker.

I seguenti sono i parametri della porta. Modificare le porte solo se necessario. Dell consiglia di usare le impostazioni predefinite

SERVERPORT_CLIENTAUTH - Opzionale.

REPORTERPORT - Opzionale.

Parametri
DEVICEPORT - Opzionale.
KEYSERVERPORT - Opzionale.
GKPORT - Opzionale.
TIGAPORT - Opzionale.
SMTP_PORT - Opzionale.
ACTIVEMQ_TCP - Opzionale.
ACTIVEMQ_STOMP - Opzionale.

Installare Security Management Server in modalità disconnessa

Nel seguente esempio Security Management Server viene installato in modalità invisibile all'utente con una finestra di dialogo di avanzamento, utilizzando i parametri di installazione elencati nel file, `C:\mysetups\eeoptions.txt\" "`

```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE=\"C:\mysetups\eeoptions.txt\" "
```

Disinstallare Security Management Server

1. Nel supporto di installazione di Dell, passare alla directory di Security Management Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Security Management Server-x64 nella directory principale del server in cui si sta disinstallando Security Management Server. ***Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.***
2. Fare doppio clic su **setup.exe**.
3. Nella schermata iniziale, fare clic su **Avanti**.
4. Nella finestra di dialogo *Rimuovere il programma*, fare clic su **Rimuovi**.

   Una finestra di dialogo di stato visualizza lo stato del processo di disinstallazione.
5. Al completamento della disinstallazione, fare clic su **Fine**.

5

Configurazione di postinstallazione

Leggere le *Consulenze tecniche di Security Management Server* per soluzioni alternative correnti o problemi noti che riguardano la configurazione di Security Management Server.

Sia che si stia effettuando la prima installazione di Security Management Server sia che si stia aggiornando un'installazione esistente, sarà necessario configurare alcuni componenti dell'ambiente.

Configurazione della modalità DMZ

Se Security Server è distribuito in una DMZ e una rete privata, e solo il server DMZ ha un certificato di dominio da un'Autorità di certificazione (CA) attendibile, è necessario eseguire alcune fasi manualmente per aggiungere il certificato attendibile nell'archivio chiavi Java della rete privata di Security Server.

Se si usa un certificato attendibile, ignorare questa sezione.

N.B.: Dell consiglia vivamente di usare i certificati di dominio di un'Autorità di certificazione attendibile per i server DMZ e della rete privata.

Per informazioni sull'aggiornamento del certificato per Dell Encryption con un certificato esistente nell'archivio chiavi Microsoft, vedere http://www.dell.com/support/article/us/en/19/sln297240/.

Server Configuration Tool

Quando diventano necessarie configurazioni dell'ambiente in seguito al completamento dell'installazione, usare il Server Configuration Tool per apportare le modifiche.

Il Server Configuration Tool consente di:

- Aggiungere certificati nuovi o aggiornati
- Importare un certificato di Dell Manager
- Importare un certificato di identità
- Configurare le impostazioni per il Certificato SSL server
- Configurare le impostazioni SMTP per Data Guardian o servizi e-mail
- Modificare nome del database, percorso o credenziali
- Migrare il database

Non è possibile eseguire Dell Core Server e Compatibility Server contemporaneamente al Server Configuration Tool. Interrompere il servizio Core Server e il servizio Compatibility Server in *Servizi* (**Start > Esegui**. Digitare ***services.msc***) prima di avviare Server Configuration Tool.

Per avviare il Server Configuration Tool, passare a **Start** > **Dell** > **Esegui Server Configuration Tool** .

I registri di Server Configuration Tool si trovano in **C:\Program Files\Dell\Enterprise Edition\Configuration Tool\Logs.**

Aggiungere certificati nuovi o aggiornati

È possibile scegliere quale tipo di certificati usare: autofirmati o firmati:

- I certificati **autofirmati** sono firmati dal proprio creatore. I certificati autofirmati sono appropriati per progetti pilota, Proof of Concept, ecc. Per un ambiente di produzione, Dell consiglia l'utilizzo di certificati firmati dall'autorità di certificazione pubblica o dal dominio.
- I certificati **firmati** (dall'autorità di certificazione pubblica o dal dominio) sono firmati da un'autorità di certificazione pubblica o da un dominio. Nel caso dei certificati firmati da un'autorità di certificazione (CA) pubblica, di solito il certificato della CA di firma esiste già nell'archivio certificati Microsoft e, pertanto, la catena di attendibilità viene stabilita automaticamente. Per i certificati firmati dalla CA di dominio, se la workstation è stata aggiunta al dominio, il certificato della CA di firma dal dominio sarà stato aggiunto all'archivio certificati Microsoft della workstation, creando così anche la catena di attendibilità.

I componenti interessati dalla configurazione del certificato sono:

- Servizi Java (per esempio Device Server e così via)
- Applicazioni .NET (Core Server)
- Convalida di smart card usate per l'autenticazione di preavvio (Security Server)
- Importazione di chiavi di crittografia private da usare per firmare i bundle dei criteri inviati a Dell Manager. Dell Manager esegue la convalida SSL per i client di crittografia gestiti con unità autocrittografanti o BitLocker Manager.
- Workstation client:
  - Workstation su cui è in esecuzione BitLocker Manager
  - Workstation su cui è in esecuzione Encryption Enterprise (Windows)
  - Workstation su cui è in esecuzione Endpoint Security Suite Enterprise

Informazioni sul tipo di certificati da usare:

L'autenticazione di preavvio tramite le smart card richiede la convalida SSL con Security Server. Dell Manager esegue la convalida SSL quando viene effettuata la connessione a Dell Core Server. Per questi tipi di connessioni, la CA di firma dovrà essere nell'archivio chiavi (l'archivio chiavi Java o l'archivio chiavi Microsoft a seconda del componente Dell Server in questione). Se vengono scelti i certificati autofirmati, sono disponibili le seguenti opzioni:

- Convalida di smart card usate per l'autenticazione di preavvio:
  - Importazione del certificato di firma dell'"Agenzia principale" e della catena di attendibilità completa nell'archivio chiavi Java di Security Server. È necessario importare la catena di attendibilità completa.

Dell Manager:

- Inserire il certificato di firma "Agenzia principale" (dal certificato autofirmato generato) in "Autorità di certificazione radice attendibile" della workstation (per il "computer locale") nell'archivio chiavi Microsoft.
- Modificare il comportamento della convalida SSL lato server. Per disattivare la convalida dell'attendibilità SSL lato server, selezionare **Disattiva controllo catena di attendibilità** nella scheda Impostazioni.

Vi sono due metodi per creare un certificato - *Rapido* e *Avanzato*.

Scegliere **un** metodo:

- Rapido - Scegliere questo metodo per generare un certificato autofirmato per tutti i componenti. Questo è il metodo più semplice, ma i certificati autofirmati sono appropriati solo per progetti pilota, Proof of Concept, ecc. Per un ambiente di produzione, Dell consiglia l'utilizzo di certificati firmati dall'autorità di certificazione pubblica o dal dominio.
- Avanzato - Scegliere questo metodo per configurare ciascun componente separatamente.

Rapido

1 Dal menu principale, selezionare **Azioni** > **Configura i certificati**.

2 All'avvio della configurazione guidata, selezionare **Rapido** e fare clic su **Avanti**. Se disponibili, vengono usate le informazioni del certificato autofirmato creato durante l'installazione di Security Management Server.

3 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

La configurazione del certificato è completa. La parte restante di questa sezione descrive in dettaglio il metodo Avanzato per creare un certificato.

Avanzato

Vi sono due percorsi per creare un certificato - *Genera certificato autofirmato* e *Utilizza impostazioni correnti*. Scegliere **un** percorso:

- Percorso 1 - Genera certificato autofirmato
- Percorso 2 - Utilizza impostazioni correnti

Percorso 1 - Genera certificato autofirmato

1 Dal menu principale, selezionare **Azioni** > **Configura i certificati**.

2 All'avvio della configurazione guidata, selezionare **Avanzato** e fare clic su **Avanti**.

3 Selezionare **Genera certificato autofirmato** e fare clic su **Avanti**. Se disponibili, vengono usate le informazioni del certificato autofirmato creato durante l'installazione di Security Management Server.

4 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

La configurazione del certificato è completa. La parte restante di questa sezione descrive in dettaglio l'altro metodo per creare un certificato.

Percorso 2 - Utilizza impostazioni correnti

1 Dal menu principale, selezionare **Azioni** > **Configura i certificati**.

2 All'avvio della configurazione guidata, selezionare **Avanzato** e fare clic su **Avanti**.

3 Selezionare **Utilizza impostazioni correnti** e fare clic su **Avanti**.

4 Nella finestra *Certificato SSL per Compatibility Server* , selezionare **Genera certificato autofirmato** e fare clic su **Avanti**. Se disponibili, vengono usate le informazioni del certificato autofirmato creato durante l'installazione di Security Management Server.

   Fare clic su **Avanti**.

5 Nella finestra *Certificato SSL per Core Server*, selezionare uno dei seguenti:

   - *Seleziona certificato* - Selezionare questa opzione per usare un certificato esistente. Fare clic su **Avanti**.

     Individuare il percorso del certificato esistente, immettere la password associata al certificato esistente, quindi fare clic su **Avanti**.

     Al termine fare clic su **Fine**.
   - *Genera certificato autofirmato* - Se disponibili, vengono usate le informazioni del certificato autofirmato creato durante l'installazione di Security Management Server. Selezionando questa opzione non verrà visualizzata la finestra Certificato di sicurezza messaggi (la finestra verrà visualizzata se si seleziona l'opzione *Utilizza impostazioni correnti*) e verrà utilizzato il certificato creato per Dell Compatibility Server.

     Verificare che il nome computer completo sia corretto. Fare clic su **Avanti**.

     Viene visualizzato un messaggio di avviso per informare l'utente che esiste già un certificato con lo stesso nome. Quando viene richiesto se si desidera utilizzarlo, fare clic su **Sì**.

     Al termine fare clic su **Fine**.
   - *Utilizza impostazioni correnti* - Selezionare questa opzione per cambiare l'impostazione di un certificato in qualsiasi momento dopo la configurazione iniziale di Security Management Server. Selezionare questa opzione per mantenere il certificato già configurato. Dopo aver selezionato questa opzione verrà visualizzata la finestra Certificato di sicurezza messaggi.

Nella finestra Certificato di sicurezza messaggi, selezionare **uno** dei seguenti:

- *Seleziona certificato* - Selezionare questa opzione per usare un certificato esistente. Fare clic su **Avanti**.

  Individuare il percorso del certificato esistente, immettere la password associata al certificato esistente, quindi fare clic su **Avanti**.

  Al termine fare clic su **Fine**.
- *Genera certificato autofirmato* - Se disponibili, vengono usate le informazioni del certificato autofirmato creato durante l'installazione di Security Management Server.

  Fare clic su **Avanti**.

  Al termine fare clic su **Fine**.

La configurazione del certificato è completa.

Al completamento delle modifiche:

1. Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.
2. Chiudere Dell Server Configuration Tool.
3. Fare clic su **Start** > **Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e fare clic su **Avvia il servizio**.

Importare un certificato di Dell Manager

Se il deployment include client Security Management Server gestiti in remoto con Encryption Management Agent, è necessario importare il certificato appena creato o quello esistente. Il certificato Dell Manager serve da veicolo per proteggere la chiave privata utilizzata per firmare i bundle di policy inviati a client Security Management Server gestiti in remoto ed Encryption Management Agent. Questo certificato può essere indipendente da tutti gli altri certificati. Inoltre, se questa chiave è compromessa può essere sostituita con una nuova e Dell Manager richiederà una nuova chiave pubblica se non è in grado di decrittografare i bundle dei criteri.

1. Aprire Microsoft Management Console.
2. Fare clic su **File > Aggiungi/Rimuovi snap-in**.
3. Fare clic su **Aggiungi**.
4. Nella finestra *Aggiungi snap-in indipendente*, selezionare **Certificati** e fare clic su **Aggiungi**.
5. Selezionare **Account del computer** e fare clic su **Avanti**.
6. Nella finestra *Seleziona computer*, selezionare **Computer locale (il computer su cui è in esecuzione questa console)** e fare clic su **Fine**.
7. Fare clic su **Chiudi**.
8. Fare clic su **OK**.
9. Nella cartella *principale della console*, espandere *Certificati (computer locale)*.
10. Andare alla cartella *Personale* e individuare il certificato desiderato.
11. Evidenziare il certificato desiderato, fare clic con il pulsante destro del mouse su **Tutte le attività** > **Esporta**.
12. Quando si apre l'Esportazione guidata certificati, fare clic su **Avanti**.
13. Selezionare **Esporta la chiave privata** e fare clic su **Avanti**.
14. Selezionare **Scambio informazioni personali - PKCS #12 (.PFX)**, quindi selezionare le sotto-opzioni **Includi tutti i certificati nel percorso di certificazione se possibile** ed **Esporta tutte le proprietà estese**. Fare clic su **Avanti**.
15. Immettere e confermare la password. È possibile usare una password a scelta. Scegliere una password che risulti facile da ricordare, ma difficile da individuare per chiunque altro. Fare clic su **Avanti**.
16. Fare clic su **Sfoglia** per passare al percorso in cui si desidera salvare il file.

17 Nel campo *Nome file*, immettere il nome con cui salvare il file. Fare clic su **Salva**.

18 Fare clic su **Avanti**.

19 Fare clic su **Fine**.

20 Viene visualizzato un messaggio che conferma il completamento dell'esportazione. Chiudere la MMC.

21 Tornare al Dell Server Configuration Tool.

22 Dal menu principale selezionare **Azioni** > **Importa certificato DM**.

23 Passare al percorso in cui è stato salvato il file esportato. Selezionare il file e fare clic su **Apri**.

24 Immettere la password associata al file e fare clic su **OK**.

L'importazione del certificato di Dell Manager è ora completa.

Al completamento delle modifiche:

1 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

2 Chiudere Dell Server Configuration Tool.

3 Fare clic su **Start** > **Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e fare clic su **Avvia il servizio**.

Importare un certificato BETA SSL/TLS

Se la distribuzione include Server Encryption, è necessario importare il certificato appena creato (o esistente). Il certificato BETA SSL/TLS protegge la chiave privata utilizzata per firmare i bundle di policy inviati a server client.

1 Dal menu principale, selezionare **Azioni** > **Importa certificato BETA SSL/TLS**.

2 Sfogliare per selezionare un certificato e fare clic su **Avanti**.

3 Quando viene richiesta la *password del certificato*, immettere la password associata al certificato esistente.

4 Nella finestra di dialogo Account di Windows, selezionare un'opzione:

   a Per modificare le credenziali associate al certificato di identità, selezionare **Utilizza credenziali diverse per l'account di Windows con il certificato di identità**.

   b Per continuare ad usare le credenziali dell'account che ha effettuato l'accesso, fare clic su **Avanti**.

5 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

Configurare le impostazioni per il Certificato SSL server

In Server Configuration Tool, fare clic sulla scheda **Impostazioni**.

Dell Manager:

Per disattivare la convalida dell'attendibilità SSL di Dell Manager lato server, selezionare **Disattiva controllo catena di attendibilità**.

SCEP:

Se si utilizza Mobile Edition, immettere l'URL del server che ospita SCEP.

N.B.: A partire dalla v9.8, Mobile Edition non è più supportato.

Al completamento delle modifiche:

1 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

2 Chiudere Dell Server Configuration Tool.

3 Fare clic su **Start** > **Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e fare clic su **Avvia il servizio**.

Configurare le impostazioni SMTP

In Server Configuration Tool, fare clic sulla scheda **SMTP**.

Questa scheda configura le impostazioni SMTP per Data Guardian, comunicati sui prodotti, notifiche e messaggi di inoltro delle minacce di Advanced Threat Prevention.

Al termine delle modifiche di configurazione, riavviare il servizio del Security Server. Il servizio del Security Server deve essere riavviato per l'aggiornamento delle impostazioni.

Immettere le informazioni seguenti:

1 In *Nome host*, immettere l'FQDN del server SMTP, come smtpservername.domain.com.

2 In *Nome utente*, immettere il nome utente che accederà al server di posta. Il formato può essere DOMINIO\mrossi, mrossi o qualsiasi forma richiesta dalla propria organizzazione.

3 Nel campo *Password*, immettere la password associata al nome utente.

4 In *Indirizzo origine*, immettere l'indirizzo e-mail che originerà l'e-mail. È possibile utilizzare l'account del nome utente (mrossi@dominio.com), ma anche un altro account a cui il nome utente specificato è in grado di accedere per inviare le e-mail (RegistrazioneCloud@dominio.com).

5 Nel campo *Porta*, immettere il numero di porta (in genere 25).

6 Nel menu*Autenticazione*, selezionare *Vero* o *Falso*.

N.B.: I campi di nome utente e password devono essere lasciati vuoti se l'autenticazione è impostata su Falso.

Al completamento delle modifiche:

1 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

2 Chiudere Dell Server Configuration Tool.

3 Fare clic su **Start** > **Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e fare clic su **Avvia il servizio**.

Modificare nome del database, percorso o credenziali

Nel Server Configuration Tool, fare clic sulla scheda **Database**.

1 Nel campo *Nome server*, immettere il nome di dominio completo (incluso, se presente, il nome dell'istanza) del server che ospita il database. Per esempio, SQLTest.domain.com\DellDB.

Dell consiglia di usare un nome di dominio completo, benché sia possibile utilizzare un indirizzo IP.

2 Nel campo *Porta server*, immettere il numero di porta.

Quando si utilizza un'istanza SQL Server non predefinita, occorre specificare la porta dinamica di tale istanza nel campo *Porta:*. In alternativa, abilitare il servizio SQL Server Browser e accertarsi che la porta UDP 1434 sia aperta. Per maggiori informazioni, consultare https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

3 In *Database*, immettere il nome del database.

4 In *Autenticazione:* selezionare **Autenticazione Windows** o **Autenticazione di SQL Server**. Se si sceglie l'Autenticazione di Windows, per l'autenticazione vengono utilizzate le stesse credenziali utilizzate per accedere a Windows (i campi *Nome utente* e *Password* non sono modificabili).

5 In *Nome utente:*, immettere il nome utente appropriato associato al database.

6 In *Password:*, immettere la password del nome utente elencato nel campo *Nome utente*.

7 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

8 Per testare la configurazione del database, dal menu principale selezionare **Azioni** > **Testa la configurazione del database**. Viene avviata la configurazione guidata.

9 Nella finestra *Test della configurazione* leggere le informazioni sul test e fare clic su **Avanti**.

10 Se nella scheda *Database* è stata selezionata la voce Autenticazione di Windows, è possibile immettere facoltativamente delle credenziali alternative per consentire l'uso delle stesse credenziali utilizzate per eseguire Security Management Server. Fare clic su **Avanti**.

11 Nella finestra *Testa la configurazione*, vengono visualizzati i risultati di Testa le impostazioni di connessione, Test di compatibilità e Test database migrato.

12 Fare clic su **Fine**.

N.B.:
Se il database o l'istanza SQL sono configurati con regole di confronto non predefinite, queste devono fare distinzione tra maiuscole e minuscole. Per un elenco di regole di confronto e distinzione tra maiuscole e minuscole, consultare https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Al completamento delle modifiche:

1 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

2 Chiudere Dell Server Configuration Tool.

3 Fare clic su **Start** > **Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e fare clic su **Avvia il servizio**.

Migrare il database

È possibile eseguire la migrazione di un database v9.2 o versione successiva allo schema più recente con l'ultimo aggiornamento del server.

Nel Server Configuration Tool, fare clic sulla scheda **Database**.

1 Se non si è ancora effettuato il backup del database del Dell Server esistente, **farlo adesso**.

2 Dal menu principale, selezionare **Azioni > Migra il database**. Viene avviata la configurazione guidata.

3 Nella finestra *Migra il database Enterprise*, viene visualizzato un avviso. Confermare che è stato eseguito il backup dell'intero database o che non è necessario eseguire il backup del database esistente. Fare clic su **Avanti**.

I messaggi informativi nella finestra *Migrazione database* visualizzano lo stato della migrazione.

Al termine, verificare l'eventuale presenza di errori.

N.B.: Un messaggio di errore identificato da  **indica che un'attività del database non è riuscita ed è necessario intraprendere un'azione correttiva prima che il database possa essere migrato correttamente. Fare clic su Fine, correggere gli errori del database e ripetere la procedura descritta in questa sezione.**

4 Fare clic su **Fine**.

Al completamento della migrazione:

1 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

2 Chiudere Dell Server Configuration Tool.

3 Fare clic su **Start** > **Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e fare clic su **Avvia il servizio**.

6

Attività di amministrazione

Assegnare un ruolo amministratore Dell

1 In qualità di amministratore di Security Management Server Virtual, accedere alla console di gestione all'indirizzo https://server.domain.com:8443/webui/. Le credenziali predefinite sono **superadmin/changeit.**

2 Nel riquadro sinistro fare clic su **Popolamenti** > **Domini**.

3 Fare clic su un dominio al quale aggiungere un utente.

4 Nella pagina Dettagli dominio, fare clic sulla scheda **Membri**.

5 Fare clic su **Aggiungi utente**.

6 Immettere un filtro per cercare il nome utente per Nome comune, Nome principale utente (UPN, Universal Principal Name) o SamAccountName. Il carattere jolly è *.

È necessario definire Nome comune, Nome principale utente e SamAccountName per ogni utente nel server di directory aziendale. Se un utente è membro di un gruppo o di un dominio, ma non viene visualizzato nell'elenco dei membri del gruppo o del dominio nella gestione, assicurarsi che nel server di directory aziendale per l'utente siano stati definiti correttamente tutti e tre i nomi.

La query eseguirà automaticamente la ricerca per Nome comune, UPN e infine SamAccountName, finché non viene trovata una corrispondenza.

7 Selezionare gli utenti da aggiungere al dominio dall'*Elenco utenti directory*. Utilizzare <MAIUSC><clic> o <Ctrl><clic> per selezionare più utenti.

8 Fare clic su **Aggiungi**.

9 Dalla barra del menu, fare clic sulla scheda **Dettagli e azioni** dell'utente specificato.

10 Scorrere la barra del menu e selezionare la scheda **Amministratore**.

11 Selezionare i ruoli dell'amministratore da aggiungere a questo utente.

12 Fare clic su **Salva**.

Accedere con ruolo amministratore Dell

1 Disconnettersi dalla Management Console.

2 Accedere alla Management Console con le credenziali dell'utente del dominio.

Caricare la licenza di accesso client

Le licenze di accesso client vengono inviate separatamente dai file di installazione, al momento dell'acquisto iniziale o successivamente se ne sono state aggiunte altre.

1 Nel riquadro sinistro fare clic su **Gestione**.

2 Fare clic su **Gestione licenza**.

3 Fare clic su **Scegli file** per individuare e selezionare il file Licenza client.

Eseguire il commit dei criteri

Al termine dell'installazione, eseguire il commit dei criteri.

Per eseguire il commit dei criteri al termine dell'installazione o, in seguito, dopo aver salvato le modifiche ai criteri, seguire la seguente procedura:

1 Nel riquadro sinistro fare clic su **Gestione** > **Esegui commit**.
2 In *Commento*, immettere una descrizione della modifica.
3 Fare clic su **Commit criteri**.

Configurare Dell Compliance Reporter

1 Nel riquadro sinistro fare clic su **Compliance Reporter**.
2 Quando si avvia Dell Compliance Reporter, accedere usando le credenziali predefinite *superadmin/changeit*.

Eseguire i backup

Ai fini del ripristino d'emergenza, assicurarsi che venga eseguito il backup dei seguenti percorsi ogni settimana, con differenziali notturni. Per ulteriori informazioni sulla pianificazione del ripristino di emergenza, fare riferimento a http://www.dell.com/support/article/us/en/04/sln292355/plan-for-disaster-recovery-and-high-availability-with-dell-security-management-server-dell-data-protection-server?lang=en. Per ulteriori informazioni sul backup dei dati di Compliance Reporter, fare riferimento a http://www.dell.com/support/article/de/en/debsdt1/sln289096/how-to-backup-and-import-custom-compliance-reports-in-dell-security-management-server-dell-data-protection-enterprise-edition-server?lang=en.

Backup di Security Management Server

Eseguire regolarmente il backup dei file archiviati nel percorso selezionato per il backup dei file di configurazione durante l'installazione (punto 10 a pagina 27) oppure l'aggiornamento/migrazione (punto 6 a pagina 68). I backup settimanali di questi dati sono accettabili in quanto dovrebbero essere modificati raramente ed è possibile riconfigurarli manualmente, se necessario. Le informazioni di archiviazione dei file più importanti, necessarie per connettersi al database:

<cartella di installazione>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<cartella di installazione>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<cartella di installazione>\Enterprise Edition\Compatibility Server\conf\gkconfig.xml

Backup di SQL Server

Eseguire backup notturni completi con la registrazione transazionale attiva ed eseguire backup differenziali del database ogni 3-4 ore. Se è disponibile un database di backup, si consiglia di eseguire i registri e/o le attività di log shipping delle transazioni ad intervalli di 15 minuti (o se possibile ad intervalli più brevi). Come sempre, Dell consiglia di usare le procedure consigliate per il database del Dell Server e di includere il software Dell nel piano di ripristino di emergenza della propria organizzazione.

Per ulteriori informazioni sulle procedure consigliate di SQL Server, consultare il seguente elenco da implementare durante l'installazione di Dell Security, se non ancora implementato.

Backup di PostgreSQL Server

Gli eventi di controllo sono memorizzati nel Server PostgreSQL, di cui dovrebbe essere normalmente eseguito il backup. Per istruzioni, fare riferimento a https://www.postgresql.org/docs/9.5/static/backup.html.

Dell consiglia di usare le procedure consigliate per il database PostgreSQ e di includere il software Dell nel piano di ripristino di emergenza della propria organizzazione.

7

Porte

La tabella seguente descrive ciascun componente e la relativa funzione.

Nome	Porta predefinita	Descrizione
Compliance Reporter	HTTP(S)/ 8084	Fornisce una visualizzazione completa dell'ambiente per la creazione di rapporti di controllo e conformità.
Management Console	HTTP(S)/ 8443	Console di amministrazione e centro di controllo per la distribuzione a livello aziendale.
Core Server	HTTPS/ 8888	Gestisce il flusso dei criteri, le licenze e la registrazione per l'autenticazione di preavvio, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Elabora i dati di inventario utilizzati da Compliance Reporter e dalla Management Console. Raccoglie e archivia i dati di autenticazione. Controlla l'accesso basato sui ruoli.
Device Server	HTTPS/ 8081	Supporta le attivazioni e il recupero delle password. Un componente di Security Management Server. Richiesto per Encryption Enterprise (Windows e Mac)
Security Server	HTTPS/ 8443	Comunica con Policy Proxy e gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, Data Guardian, la comunicazione SED-PBA e Active Directory per l'autenticazione o la riconciliazione, inclusa la convalida dell'identità per l'autenticazione nella Management Console. Richiede l'accesso al database SQL.
Compatibility Server	TCP/ 1099	Servizio per la gestione dell'architettura aziendale. Raccoglie e archivia i dati di inventario iniziali durante l'attivazione e i dati dei criteri durante le migrazioni. Elabora i dati basati sui gruppi di utenti.
Message Broker Service	TCP/ 61616 e STOMP/ 61613	Gestisce la comunicazione tra i servizi di Dell Server. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy. Richiede l'accesso al database SQL.
Key Server	TCP/ 8050	Negozia, autentica e crittografa una connessione client tramite le API Kerberos. Richiede l'accesso al database SQL per estrarre i dati della chiave.
Policy Proxy	TCP/ 8000	Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario.

Nome	Porta predefinita	Descrizione
LDAP	TCP/ 389/636 (controller di dominio locale), 3268/3269 (catalogo globale) TCP/ 135/ 49125+ (RPC)	Porta 389 - Questa porta è usata per richiedere informazioni dal controller di dominio locale. Le richieste LDAP inviate alla porta 389 possono essere usate per cercare gli oggetti solo nel dominio principale del catalogo globale. Tuttavia, l'applicazione richiedente può ottenere tutti gli attributi per tali oggetti. Per esempio, una richiesta alla porta 389 potrebbe essere usata per ottenere il reparto di un utente. Porta 3268 - Questa porta è usata per le query destinate specificamente al catalogo globale. Le richieste LDAP inviate alla porta 3268 possono essere usate per cercare gli oggetti nell'intero insieme di strutture. Tuttavia, è possibile restituire solo gli attributi contrassegnati per la replica al catalogo globale. Per esempio, non è possibile restituire il reparto di un utente usando la porta 3268 poiché questo attributo non è replicato al catalogo globale.
Database di Microsoft SQL Server	TCP/ 1433	La porta SQL Server predefinita è la 1433 e alle porte dei client viene assegnato un valore casuale tra 1024 e 5000.
Autenticazione client	HTTPS/ 8449	Consente ai server client di eseguire l'autenticazione a Dell Server. Richiesto per Server Encryption.
Beacon richiamata	HTTP/TCP 8446	Consente di inserire un beacon richiamata in ciascun file Office protetto, quando si esegue la modalità Office protetto di Data Guardian.

8

Procedure consigliate per SQL Server

L'elenco seguente illustra le procedure consigliate per SQL Server da implementare durante l'installazione di Dell Security, se non ancora implementate.

1 Accertarsi che la dimensione del blocco NTFS in cui si trovano il file di dati e il file di registro sia 64 kB. Gli extent di SQL Server (unità base di SQL Storage) sono di 64 KB.

   Per maggiori informazioni, cercare gli articoli TechNet di Microsoft "Understanding Pages and Extents" (Informazioni su pagine ed extent).

   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx

2 Come linea guida generale, impostare la quantità massima di memoria di SQL Server all'80% della memoria installata.

   Per maggiori informazioni, cercare gli articoli TechNet di Microsoft *Server Memory Server Configuration Options* (Opzioni di configurazione del server Server Memory).

   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29
   - Microsoft SQL Server 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3 Impostare -t1222 sulle proprietà di avvio dell'istanza per accertarsi che le informazioni di blocco vengano acquisite nel caso in cui dovesse verificarsi un blocco.

   Per maggiori informazioni, cercare gli articoli TechNet di Microsoft sui "Flag di traccia (Transact-SQL)".

   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29
   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

4 Accertarsi che tutti gli indici siano coperti da un processo di manutenzione settimanale per la ricostruzione degli stessi.

9

Certificati

In questo capitolo viene descritto come ottenere i certificati da utilizzare con Security Management Server.

Per informazioni su come configurare l'autenticazione SmartCard, consultare http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en.

Per informazioni sui requisiti minimi per richiedere i certificati SSL/TLS per l'utilizzo da parte del server Dell Data Security, consultare http://www.dell.com/support/article/us/en/19/sln307037/dell-data-protection-enterprise-edition-and-virtual-edition-dell-security-management-sever-and-virtual-server-ssl-tls-certificate-minimum-requirements?lang=en.

Per informazioni sull'aggiornamento del certificato per Dell Encryption con un certificato esistente nell'archivio chiavi Microsoft, vedere http://www.dell.com/support/article/us/en/19/sln297240/.

Creare un certificato autofirmato e generare una richiesta di firma del certificato

Questa sezione descrive in dettaglio la procedura per creare un certificato autofirmato per i componenti basati su Java. Questo processo **non può** essere usato per creare un certificato autofirmato per componenti basati su .NET.

Dell consiglia un certificato autofirmato *solo* in un ambiente non di produzione.

Se l'organizzazione richiede un certificato server SSL oppure è necessario creare un certificato per altri motivi, questa sezione descrive il processo per creare un archivio chiavi Java usando Keytool.

Se l'organizzazione intende usare le smart card per l'autenticazione, è necessario usare Keytool per importare la catena di attendibilità completa dei certificati usati nel certificato dell'utente della smart card.

Keytool crea chiavi private passate dal formato della richiesta di firma del certificato (CSR, Certificate Signing Request) ad un'Autorità di certificazione (CA, Certificate Authority), come VeriSign® o Entrust®. La CA quindi, in base a questa richiesta, creerà un certificato server che essa stessa firma. Il certificato server verrà quindi scaricato in un file insieme a quello dell'autorità di firma. Entrambi verranno infine importati nel file dell'Autorità di certificazione.

Generare una nuova coppia di chiavi e un certificato autofirmato

1 Passare alla directory **conf** di Compliance Reporter, Security Server o Device Server.

2 Eseguire il backup del database di certificati predefinito:

Fare clic su **Start** > **Esegui** e digitare `move cacerts cacerts.old`.

3 Aggiungere Keytool al percorso di sistema. Nel prompt dei comandi digitare il seguente comando:

```
set path=%path%;<Dell Java Install Dir>\bin
```

4 Per generare un certificato, eseguire Keytool come mostrato:

```
keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell -keystore .\cacerts
```

5 Immettere le seguenti informazioni quando richiesto da Keytool.

> **N.B.:**
> Prima di modificare i file di configurazione, eseguirne il backup. Modificare esclusivamente i parametri specificati. La modifica di altri dati in questi file, inclusi i tag, può provocare la corruzione ed errori del sistema. Dell non può garantire la risoluzione dei problemi derivanti da modifiche non autorizzate a questi file senza dover reinstallare Security Management Server.

- *Password Keystore*: immettere una password (i caratteri non supportati sono <>;&" ') e impostare la variabile nel file **conf** del componente sullo stesso valore, come segue:

  <directory installazione Compliance Reporter>\conf\eserver.properties. Set the value eserver.keystore.password =

  <directory di installazione di Device Server>\conf\application.properties. Impostare il valore keystore.password =

  <directory di installazione di Security Server>\conf\application.properties. Impostare il valore keystore.password =
- *Nome di server completo*: immettere il nome completo del server in cui è installato il componente in uso. Questo nome completo include il nome host e il nome di dominio (ad esempio, server.dominio.com).
- *Unità organizzativa*: immettere il valore appropriato (ad esempio Sicurezza).
- *Organizzazione*: immettere il valore appropriato (ad esempio Dell).
- *Città o località*: immettere il valore appropriato (ad esempio Roma).
- *Stato o provincia*: immettere il nome esteso dello stato o della provincia (ad esempio Italia).
- codice Paese di due lettere.
- L'utilità richiede di verificare la correttezza delle informazioni. Se sì, digitare `yes`.

  Se no, digitare `no`. Keytool visualizza ciascun valore immesso in precedenza. Fare clic su **Invio** per accettare o modificare il valore, e fare clic su **Invio**.
- *Password della chiave per l'alias*: se non si immette un'altra password qui, verrà utilizzata la password Keystore.

Richiedere un certificato firmato da un'Autorità di certificazione

Usare questa procedura per generare una richiesta di firma del certificato (CSR) per il certificato autofirmato creato in Generare una nuova coppia di chiavi e un certificato autofirmato.

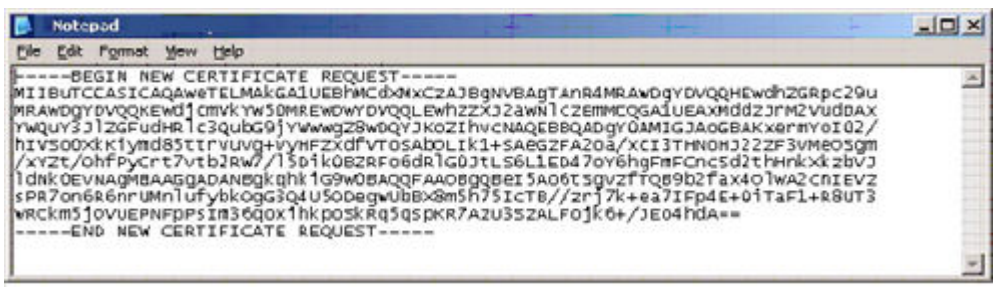
1 Sostituire lo stesso valore usato in precedenza per <**certificatealias**>:

```
keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
<csr-filename>
```

Per esempio, `keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file Dell.csr`

Il file .csr contiene una coppia BEGIN/END da utilizzare durante la creazione del certificato nella CA.

File .CSR di esempio



2 Seguire la procedura organizzativa per acquisire un certificato server SSL da un'autorità di certificazione. Inviare il contenuto del <nome file csr> per la firma.

> **N.B.:**
> È possibile richiedere un certificato valido in diversi modi. Un metodo di esempio è illustrato in **Metodo di esempio per richiedere un certificato**.

3 Alla ricezione del certificato firmato, archiviarlo in un file.

4 La procedura consigliata è quella di eseguire il backup del certificato in caso di errore durante il processo di importazione, onde evitare di dover ripetere per intero la procedura.

Importare un certificato radice

Se l'Autorità di certificazione del certificato radice è Verisign (ma non Verisign Test), passare alla procedura successiva e importare il certificato firmato.

Il certificato radice dell'Autorità di certificazione convalida i certificati firmati.

1 Effettuare **una** delle seguenti operazioni:

- Scaricare il certificato radice dell'Autorità di certificazione e archiviarlo in un file.
- Ottenere il certificato radice del server di directory aziendale.

2 Effettuare **una** delle seguenti operazioni:

- Se si abilita SSL per Compliance Reporter, Security Server o Device Server, passare alla directory **conf** del componente.
- Se si abilita SSL tra Security Management Server e il server di directory aziendale, passare a <**directory di installazione Dell> \Java Runtimes\jre1.x.x_xx\lib\security** (la password predefinita per il file cacerts JRE è **changeit**).

3 Per installare il certificato radice, eseguire Keytool nel modo seguente:

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file <ca-cert-filename>
```

Per esempio `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

Metodo di esempio per richiedere un certificato

Un metodo di esempio per richiedere un certificato consiste nell'usare un browser Web per accedere al server Microsoft CA, installato internamente dall'organizzazione.

1 Passare al server Microsoft CA. L'indirizzo IP è fornito dall'organizzazione.

2 Selezionare **Richiedi certificato** e fare clic su **Avanti**.

Servizi certificati Microsoft

3 Selezionare **Richiesta avanzata** e fare clic su **Avanti**.

Scegli tipo di richiesta

4 Selezionare l'opzione per **inviare una richiesta di certificato mediante un file PKCS #10 con codifica Base64** e fare clic su **Avanti**.

Richiesta certificato avanzata

5 Incollare il contenuto della richiesta CSR nella casella di testo. Selezionare un modello di certificato del **Server Web** e fare clic su **Invia**.

Invia una richiesta salvata

6 Salvare il certificato. Selezionare **Codifica DER** e fare clic su **Scarica certificato CA**.

Scarica certificato CA

7 Salvare il certificato. Selezionare **Codifica DER** e fare clic su **Scarica percorso certificato CA**.

Scarica percorso certificato CA

8 Importare il certificato dell'autorità di firma convertito. Tornare al prompt dei comandi. Tipo:

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 Una volta importato il certificato dell'autorità di firma, sarà possibile importare il certificato server (è possibile creare la catena di attendibilità). Tipo:

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

Usare l'alias del certificato autofirmato per associare la richiesta CSR al certificato server.

10 Un elenco dei file dell'Autorità di certificazione indica che il certificato server presenta una **lunghezza per la catena di certificati** pari a **2**, che indica che il certificato non è autofirmato. Tipo:

```
keytool -list -v -keystore cacerts
```

L'impronta del secondo certificato nella catena è il certificato dell'autorità di firma importato (elencato anche al di sotto del certificato server nell'elenco).

Esportare un certificato in .PFX usando la console di gestione dei certificati

Quando si dispone di un certificato sotto forma di file .crt nella MMC, deve essere convertito in un file .pfx per l'uso con Keytool quando Security Server è usato in modalità DMZ *e* quando si importa un certificato Dell Manager nel Server Configuration Tool.

1 Aprire Microsoft Management Console.
2 Fare clic su **File > Aggiungi/Rimuovi snap-in**.
3 Fare clic su **Aggiungi**.
4 Nella finestra *Aggiungi snap-in indipendente*, selezionare **Certificati** e fare clic su **Aggiungi**.
5 Selezionare **Account del computer** e fare clic su **Avanti**.
6 Nella finestra *Seleziona computer*, selezionare **Computer locale (il computer su cui è in esecuzione questa console)** e fare clic su **Fine**.
7 Fare clic su **Chiudi**.
8 Fare clic su **OK**.
9 Nella cartella *principale della console*, espandere *Certificati (computer locale)*.
10 Andare alla cartella *Personale* e individuare il certificato desiderato.
11 Evidenziare il certificato desiderato, fare clic con il pulsante destro del mouse su **Tutte le attività** > **Esporta**.
12 Quando si apre l'Esportazione guidata certificati, fare clic su **Avanti**.
13 Selezionare **Esporta la chiave privata** e fare clic su **Avanti**.
14 Selezionare **Scambio informazioni personali - PKCS #12 (.PFX)**, quindi selezionare le sotto-opzioni **Includi tutti i certificati nel percorso di certificazione se possibile** ed **Esporta tutte le proprietà estese**. Fare clic su **Avanti**.
15 Immettere e confermare la password. È possibile usare una password a scelta. Scegliere una password che risulti facile da ricordare, ma difficile da individuare per chiunque altro. Fare clic su **Avanti**.
16 Fare clic su **Sfoglia** per passare al percorso in cui si desidera salvare il file.
17 Nel campo *Nome file*, immettere il nome con cui salvare il file. Fare clic su **Salva**.
18 Fare clic su **Avanti**.

19 Fare clic su **Fine**.

Viene visualizzato un messaggio che conferma il completamento dell'esportazione. Chiudere la MMC.

Aggiungere un certificato attendibile per la firma al Security Server quando è stato usato un certificato non attendibile per SSL

1 Interrompere il servizio Security Server, se in esecuzione.

2 Eseguire il backup del file dell'Autorità di certificazione in <directory installazione Security Server>\conf\.

Usare Keytool per completare le operazioni seguenti:

3 Esportare il PFX attendibile in un file di testo e documentare l'Alias:

```
keytool -list -v -keystore "
```

4 Importare il PFX nel file dell'Autorità di certificazione in <directory installazione Security Server>\conf\.

```
keytool -importkeystore -v -srckeystore "
```

5 Modificare il valore keystore.alias.signing in <directory installazione Security Server>\conf\application.properties.

```
keystore.alias.signing=AliasNamePreviouslyDocumented
```

Avviare il servizio Security Server.