Dell Security Management Server Virtual

Quick Start and Installation Guide v11.9

December 2023
Rev. A01

DELL Technologies

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 evidenzia la possibilità che si verifichi un danno all'hardware o una perdita di dati ed indica come evitare il problema.

AVVERTENZA: un messaggio di AVVERTENZA evidenzia un potenziale rischio di danni alla proprietà, lesioni personali o morte.

Contents

1

Guida introduttiva

Questa Guida introduttiva è concepita per gli utenti più esperti, per consentire una configurazione e un avvio rapido del Dell Server. Come regola generale, Dell consiglia di installare prima il Dell Server, quindi i client.

Per istruzioni più dettagliate, consultare la Guida all'installazione di Security Management Server Virtual.

Per informazioni sui prerequisiti del Dell Server, consultare le sezioni Prerequisiti di Security Management Server Virtual, Prerequisiti della Management Console e Prerequisiti della modalità proxy.

Per informazioni su come aggiornare un Dell Server, consultare Aggiornare Security Management Server Virtual.

Installazione

1. Individuare la directory in cui sono archiviati i file di Dell Data Security e cliccare due volte per importarli in VMware Security Management Server Virtual **v11.x.x Build x.ova**.

   N.B.: OVA è ora firmato da SHA256 e non può essere importato all'interno del thick client VMware. Per informazioni, consultare https://kb.vmware.com/s/article/2151537.

2. Accendere Security Management Server Virtual.
3. Seguire le istruzioni visualizzate.

Configurazione

Prima di attivare gli utenti, è necessario completare le seguenti attività di configurazione del terminale di Security Management Server Virtual:

- Configurare le impostazioni SMTP
- Importare un certificato esistente o registrare un nuovo certificato server
- Aggiornare Security Management Server Virtual
- Installare un client FTP che supporta SFTP sulla porta 22 e impostare gli utenti File Transfer Protocol (FTP).

  Se sono presenti dispositivi esterni alla rete aziendale, consultare Installare e configurare la modalità proxy.

Apertura della Management Console

Aprire la Management Console a questo indirizzo: https://server.domain.com:8443/webui/

Le credenziali predefinite sono **superadmin/changeit.**

Per un elenco dei browser Web supportati, consultare la sezione Prerequisiti della Management Console.

Attività di amministrazione

Avviare la Management Console, se questa operazione non è stata già eseguita. Le credenziali predefinite sono **superadmin/changeit.**

Dell Technologies consiglia di assegnare i ruoli di amministratore appena possibile. Per completare questa operazione, consultare Assegnare un ruolo amministratore Dell.

Cliccare su "?" nell'angolo in alto a destra della Management Console per avviare la *guida dell'amministratore.* Viene visualizzata la pagina iniziale. Fare clic su **Aggiungi domini**.

Per ogni organizzazione vengono impostati dei criteri di base; tuttavia, è necessario modificare tali criteri in base alle specifiche esigenze, come illustrato di seguito (tutte le attivazioni prevedono licenze e diritti):

- La crittografia basata su criteri viene attivata con la crittografia Common-Key.
- I computer con self-encrypting drive sono crittografati.
- La gestione BitLocker è disabilitata.
- La prevenzione avanzata delle minacce è disabilitata.
- La protezione dalle minacce è disabilitata.
- I supporti esterni non verranno crittografati.
- Le porte non saranno gestite dal controllo porte.
- I dispositivi con Full Disk Encryption installato non verranno crittografati.

Consultare l'argomento della guida dell'amministratore *Gestire i criteri* per passare ai gruppi di tecnologie e alle descrizioni dei criteri.

Le attività della Guida introduttiva sono state completate.

2

Guida dettagliata all'installazione

La presente Guida all'installazione consente ad utenti meno esperti di installare e configurare Security Management Server Virtual. Come regola generale, Dell consiglia di installare prima Security Management Server Virtual, quindi i client.

Per informazioni su come aggiornare un Security Management Server Virtual esistente, consultare Aggiornare Security Management Server Virtual.

Informazioni su Security Management Server Virtual

La console di gestione consente agli amministratori di monitorare lo stato degli endpoint, l'applicazione dei criteri e la protezione in tutta l'azienda. La modalità proxy fornisce un'opzione front-end per la modalità DMZ per l'uso con Security Management Server Virtual.

Security Management Server Virtual ha le seguenti funzioni:

- Gestione centralizzata di un massimo di 3500 dispositivi
- Creazione e gestione dei criteri di protezione basati sui ruoli
- Ripristino dei dispositivi assistito dall'amministratore
- Separazione dei compiti dell'amministratore
- Distribuzione automatica dei criteri di protezione
- Percorsi attendibili per la comunicazione tra componenti
- Generazione di chiavi di crittografia univoche e deposito automatico e sicuro delle chiavi
- Controlli e rapporti di conformità centralizzati
- Generazione automatica di certificati autofirmati

Contattare Dell ProSupport for Software

Per assistenza telefonica sui prodotti Dell, chiamare il numero 877-459-7304, interno 4310039, 24x7.

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 for Software.

Requisiti

Security Management Server Virtual

Hardware

The recommended disk space for Security Management Server Virtual is 80 GB.

Virtualized Environment

Security Management Server Virtual v11.7 has been validated with the following virtualized environments.

Dell currently supports hosting the Dell Security Management Server or Dell Security Management Server Virtual within a Cloud-hosted Infrastructure as a Service (IaaS) environment, such as Amazon Web Services, Azure, and several other vendors. Support for these environments is only limited to the functionality of the application server hosted within these Virtual Machines, the administration and security of these Virtual Machines is up to the administrator of the IaaS solution.

Additional infrastructure requirements (Active Directory, as well as SQL Server for the Dell Security Management Server) are still required for proper functionality.

Virtualized Environments
• VMware Workstation 14.0 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware Workstation 14.1 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware Workstation 15.0 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware Workstation 15.1 ○ 64-bit CPU required ○ 8 GB RAM required ○ 80 GB Hard Drive Space ○ Host computer with at least two cores ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware ESXi 6.0 ○ 64-bit x86 CPU required ○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An Operating System is not required. ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
• VMware ESXi 6.5 ○ 64-bit x86 CPU required

Virtualized Environments
○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An Operating System is not required. ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
● VMware ESXi 6.7 ○ 64-bit x86 CPU required ○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An Operating System is not required. ○ See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 for a complete list of supported Host Operating Systems. ○ Hardware must conform to minimum VMware requirements. ○ See https://kb.vmware.com/s/article/1003746 for more information.
● Hyper-V Server (Full or Core installation) ○ 64-bit x86 CPU required ○ Host computer with at least two cores ○ 8 GB RAM minimum required ○ 80 GB Hard Drive Space ○ An operating system is not required. ○ Hardware must conform to minimum Hyper-V requirements. ○ Must be run as a Generation 1 Virtual Machine. **NOTE:** For information about setting up Hyper-V, follow instructions for Endpoint Operating Systems: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v or for Server Operating Systems: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

Management Console

Browser Internet

N.B.:

Il browser deve accettare i cookie.

La tabella seguente descrive in dettaglio i browser Internet supportati.

Browser Internet
● Mozilla Firefox 41.x o versione successiva ● Google Chrome 46.x o versione successiva ● Microsoft Edge (Chromium) ● Microsoft Edge

Accedere alla Management Console

Poiché Internet Explorer non è più supportato, è necessario installare un browser di terze parti per accedere correttamente alla Management Console.

Se Internet Explorer è richiesto per convalidare la Management Console, è necessario disabilitare la configurazione di sicurezza avanzata di Internet Explorer per il tipo di account che corrisponde all'amministratore che ha eseguito l'accesso.

Modalità proxy

Hardware

La tabella seguente descrive in dettaglio i requisiti hardware *minimi*.

Processore Moderna dual-core CPU (1,5 GHz +)
RAM 2 GB minimo di RAM dedicata/4 GB di RAM dedicata consigliati
Spazio libero su disco 1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale)
Scheda di rete Scheda di interfaccia di rete 10/100/1000
Varie IPv4, IPv6 o una combinazione di IPv4 e IPv6 sono supportati.

Software

La tabella seguente descrive in dettaglio il software che deve essere presente prima dell'installazione del server in modalità proxy.

Prerequisiti
• **Windows Installer 4.0 o versione successiva** È necessario installare Windows Installer 4.0 o versione successiva nel server in cui è in corso l'installazione.
• **Microsoft Visual C++ 2010 Redistributable Package** Se non è installato, verrà installato dal programma di installazione.
• **Microsoft .NET Framework versione 4.6.1** Microsoft ha pubblicato gli aggiornamenti della sicurezza di .NET Framework versione 4.6.1.

N.B.:

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

Posizione del registro di sistema per i Windows Server: HKLM\SOFTWARE\Dell.

Nella tabella riportata di seguito, sono indicati in dettaglio i requisiti software per il server in modalità proxy.

Sistema operativo
• **Windows Server 2022** - Standard Edition - Datacenter Edition
• **Windows Server 2019** - Standard Edition - Datacenter Edition

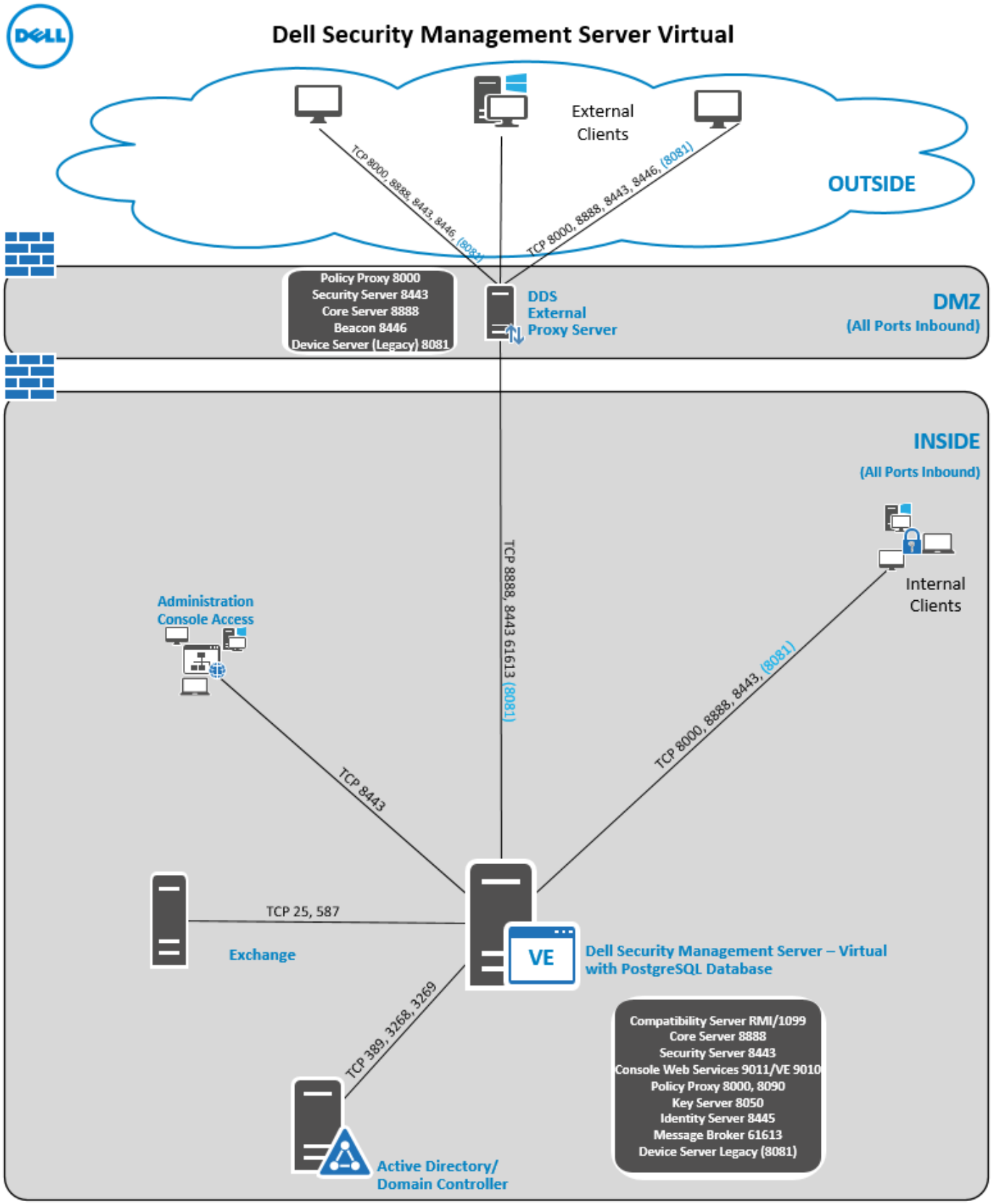
Sistema operativo
• **Windows Server 2016** - Standard Edition - Datacenter Edition
• **Windows Server 2012 R2** - Standard Edition - Datacenter Edition
• **Archivio LDAP** - Active Directory 2008 R2 - Active Directory 2012 R2 - Active Directory 2016 - Hybrid Azure Active Directory

Progettazione dell'architettura di Security Management Server Virtual

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

Componenti dell'architettura

Di seguito viene fornito un basic deployment per Dell Security Management Server Virtual.


Dell Security Management Server Virtual
External Clients
OUTSIDE
TCP 8000, 8888, 8443, 8446, (8081)
TCP 8000, 8888, 8443, 8446, (8081)
Policy Proxy 8000
Security Server 8443
Core Server 8888
Beacon 8446
Device Server (Legacy) 8081
DDS External Proxy Server
DMZ
(All Ports Inbound)
INSIDE
(All Ports Inbound)
Internal Clients
Administration Console Access
TCP 8888, 8443 61613 (8081)
TCP 8443
TCP 8000, 8888, 8443, (8081)
TCP 25, 587
Exchange
VE
Dell Security Management Server – Virtual with PostgreSQL Database
TCP 389, 3268, 3269
Compatibility Server RMI/1099
Core Server 8888
Security Server 8443
Console Web Services 9011/VE 9010
Policy Proxy 8000, 8090
Key Server 8050
Identity Server 8445
Message Broker 61613
Device Server Legacy (8081)
Active Directory/ Domain Controller

Scaricare e installare il file OVA

In occasione dell'installazione iniziale, Security Management Server Virtual viene fornito come file OVA, una Open Virtual Application (Applicazione virtuale aperta) usata per fornire un software in esecuzione in una macchina virtuale. Il file OVA è disponibile all'indirizzo www.dell.com/support, nelle pagine del supporto dei prodotti Dell Data Security elencati di seguito:

- Crittografia
- Dettagli su Endpoint Security Suite Enterprise

Per scaricare il file OVA:

1. Accedere alla pagina *Driver e download* per i prodotti appropriati riportati sopra.
2. Cliccare su **Driver e download**.
3. Selezionare la versione VMware ESXi appropriata.
4. Scaricare il pacchetto appropriato.

Per installare il file OVA:

Prima di iniziare, verificare che siano soddisfatti tutti i Requisiti del sistema e dell'ambiente virtuale.

1. Effettuare una delle seguenti operazioni:

VMware	Nei supporti di installazione di Dell, individuare *Security Management Server Virtual v11.x.x Build x.ova* e cliccare due volte per l'importazione in VMware. Seguire le istruzioni visualizzate. **N.B.:** Se l'importazione fallisce quando si utilizza VMware, il web client è il percorso suggerito per l'importazione del file OVA. Per ulteriori informazioni, vedere https://kb.vmware.com/s/article/2151537.
Hyper-V Seguire le istruzioni per Windows 10 https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/.	Requisiti: • Macchina virtuale di prima generazione • Security Management Server Virtual è disponibile in formato VHDX. Un disco non deve essere definito e il disco deve essere aggiunto alla macchina virtuale dopo essere stato creato all'interno di Hyper-V. Vedere https://docs.microsoft.com/it-it/windows-server/virtualization/hyper-v/get-started/create-a-virtual-machine-in-hyper-v.
Sistemi operativi basati su server	Seguire le istruzioni: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.
ESXi Seguire le istruzioni:https://kb.vmware.com/s/article/2109708	Processo di importazione OAV: Vedere https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.html.hostclient.doc/GUID-FBEED81C-F9D9-4193-BDCC-CC4A60C20A4E_copy.html.

2. Accendere Security Management Server Virtual.
3. Selezionare la lingua per il contratto di licenza, quindi selezionare **Visualizza EULA**.
4. Leggere il contratto, quindi selezionare **Accetta EULA**.
5. Se è disponibile un aggiornamento, selezionare **Accetta**.
6. Selezionare **Modalità connessa** o **Modalità disconnessa**.

N.B.:

Se si seleziona **Modalità disconnessa**, non è possibile attivare la modalità connessa.

La modalità disconnessa isola il Dell Server da Internet e da una LAN non protetta o da un'altra rete. Tutti gli aggiornamenti devono essere eseguiti manualmente. Per ulteriori informazioni sulla modalità disconnessa e sui criteri, fare riferimento alla *guida dell'amministratore*.

7. Nella schermata *Imposta password delluser*, immettere la password corrente (predefinita), ossia **delluser**, quindi immettere una password univoca, reinserire la password univoca e selezionare **Applica**.

   Le password devono includere i seguenti elementi:

   - Almeno 8 caratteri
   - Almeno 1 lettera maiuscola
   - Almeno 1 cifra
   - Almeno 1 carattere speciale

   N.B.: È possibile mantenere la password predefinita selezionando **Annulla**, oppure premendo **Esc** sulla tastiera.
8. Selezionare **Chiudi** per accedere alla finestra Configura nome host.
9. Nella finestra di dialogo *Configura nome host*, utilizzare il tasto BACKSPACE per rimuovere il nome host predefinito. Inserire un nome host univoco e selezionare **OK**.
10. Nella finestra di dialogo *Configura impostazioni di rete*, scegliere una delle opzioni seguenti, quindi selezionare **OK**.

    - (Impostazione predefinita) Usa DHCP (IPv4)
    - (Impostazione consigliata) Nel campo *Usa DHCP*, premere la barra spaziatrice per rimuovere la X e inserire manualmente questi indirizzi, se applicabili:

      IP statico

      Network mask

      Gateway predefinito

      Server DNS 1

      Server DNS 2

      Server DNS 3

      È possibile selezionare IPv6 o IPv4 per una configurazione statica.

    - **N.B.:** Quando si usa un IP statico, è necessario creare anche una voce host nel server DNS.
11. Alla richiesta di conferma del fuso orario, selezionare **OK**.
12. Quando viene visualizzato il messaggio che indica il completamento della configurazione al primo avvio, selezionare **OK**.
13. Configurare le impostazioni SMTP.
14. Importare un certificato esistente o registrare un nuovo certificato server.
15. Aggiornare Security Management Server Virtual.
16. Installare un client FTP che supporta SFTP sulla porta 22 e impostare gli utenti File Transfer Protocol (FTP).

    Le attività di installazione di Security Management Server Virtual sono completate.

Apertura della Management Console

Aprire la Management Console a questo indirizzo: https://server.domain.com:8443/webui/

Le credenziali predefinite sono **superadmin/changeit.**

Per un elenco dei browser Web supportati, consultare la sezione Prerequisiti della Management Console.

Installare e configurare la modalità proxy

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

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

1. Nel supporto di installazione di Dell, accedere 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 Virtual. ***Le operazioni di copia e incolla o di trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.***

2. Cliccare due volte su **setup.exe**.
3. Selezionare la lingua di installazione, quindi cliccare su **OK**.
4. Se i prerequisiti non sono già installati, viene visualizzato il messaggio che informa l'utente quali prerequisiti verranno installati. Cliccare su **Installa**.
5. Cliccare su **Avanti** nella finestra di dialogo Introduzione.
6. Leggere il contratto di licenza, accettare i termini, quindi cliccare su **Avanti**.
7. Inserire il codice Product Key di 32 caratteri e cliccare su **Avanti**. Il codice Product Key si trova nel file `EnterpriseServerInstallKey.ini`.
8. Selezionare **Installazione front-end** e cliccare su **Avanti**.
9. Per installare il server front-end nel percorso predefinito `C:\Program Files\Dell`, cliccare su **Avanti**. Altrimenti, cliccare su **Modifica** per selezionare un altro diverso, quindi cliccare 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 cliccare su **Avanti**.
    b. Per creare un certificato autofirmato, selezionare **Crea un certificato autofirmato e importalo nell'archivio chiavi e cliccare 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 o dell'area geografica

       Cliccare 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 cliccare 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* cliccare su **Avanti**.
    - Per visualizzare o modificare i nomi host, nella finestra di dialogo *Configurazione del server front-end* cliccare su **Modifica nomi host**. Modificare i nomi host solo se necessario. Dell Technologies 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, cliccare 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 Technologies 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, cliccare su **OK**.

13. Nella finestra di dialogo *Installazione del programma*, cliccare su **Installa**.
14. Al completamento dell'installazione, cliccare su **Fine**.

Attività di configurazione del terminale di base di

Le operazioni di configurazione di base sono accessibili dal menu principale.

Controllare la dashboard di sistema

Per verificare lo stato dei servizi del Dell Server, nel menu principale selezionare **Dashboard sistema**.

Il widget *Informazioni sistema* mostra la versione attuale, il nome host, l'indirizzo IP e l'utilizzo di CPU, memoria e disco.

Il widget *Cronologia versioni* mostra le modifiche delle versioni dello schema del database. I dati provengono dalla tabella "Informazioni" e sono ordinati per ora, con la versione più recente nella parte superiore.

La seguente tabella descrive ciascun servizio e la relativa funzione nel widget *Integrità servizio.*

Nome	Descrizione
Message Broker	Bus di Enterprise Server
Identity Server	Gestisce le richieste di autenticazione del dominio.
Compatibility Server	Servizio per la gestione dell'architettura aziendale.
Security Server	Fornisce il meccanismo di controllo dei comandi e della comunicazione con Active Directory.
Core Server	Servizio per la gestione dell'architettura aziendale. Questo servizio gestisce inoltre tutti i dispositivi di attivazione, policy e raccolta dell'inventario basati su agente.
Core Server HA (elevata disponibilità)	Un servizio ad elevata disponibilità che consente una maggiore sicurezza e migliori prestazioni delle connessioni HTTPS nella gestione dell'architettura aziendale.
Inventory Server	Elabora la coda di inventario.
Forensic Server	Fornisce servizi Web per l'API Forensic.
Policy Proxy	Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario.

I servizi vengono monitorati e riavviati automaticamente, se necessario.

N.B.: Se il processo databasecustomizer non riesce, i server passano allo stato Esecuzione non riuscita. Per controllare il registro databasecustomizer, nel menu principale selezionare Visualizza registri.

Modificare il nome host

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare Security Management Server Virtual.

1. Dal menu *Configurazione di base*, selezionare **Nome host**.

2. Utilizzare il tasto BACKSPACE per rimuovere il nome host esistente, quindi sostituirlo con un nuovo nome host e selezionare **OK**.

Modificare le impostazioni di rete

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare Security Management Server Virtual.

1. Dal menu *Configurazione di base*, selezionare **Rete**.
2. Nella schermata *Configura impostazioni di rete*, scegliere una delle opzioni seguenti, quindi selezionare **OK**.
   - (Impostazione predefinita) Usa DHCP (IPv4).
   - (Impostazione consigliata) Nel campo *Usa DHCP*, premere la barra spaziatrice per rimuovere la X e inserire manualmente questi indirizzi, se applicabili:

     IP statico

     Network mask

     Gateway predefinito

     Server DNS 1

     Server DNS 2

     Server DNS 3

     È possibile selezionare IPv6 o IPv4 per una configurazione statica.

     N.B.:

     Quando si utilizza un IP statico, è necessario creare una voce host nel server DNS.

Abilitare il supporto del server DMZ

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare Security Management Server Virtual.

1. Dal menu *Configurazione avanzata*, selezionare **Supporto server DMZ.**
2. Usare la barra spaziatrice per inserire una **X** nel campo Abilita supporto server DMZ
3. Immettere il nome di dominio completo del server DMZ e selezionare **OK**.

N.B.: Per sfruttare al meglio un server DMZ, fare riferimento alle istruzioni per l'installazione di un server proxy sopra, Installare e configurare la modalità proxy.

Modificare il fuso orario

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare Security Management Server Virtual.

1. Dal menu *Configurazione di base*, selezionare **Fuso orario**.
2. Nella schermata *Fuso orario*, usare i tasti freccia per evidenziare il fuso orario, quindi selezionare **Invio**.

Aggiornare Security Management Server Virtual

Per informazioni su un aggiornamento specifico, vedere gli avvisi tecnici di Security Management Server Virtual, disponibili all'indirizzodell.com/support. Per visualizzare la versione e la data di installazione di un aggiornamento già applicato, controllare la *Dashboard di sistema*.

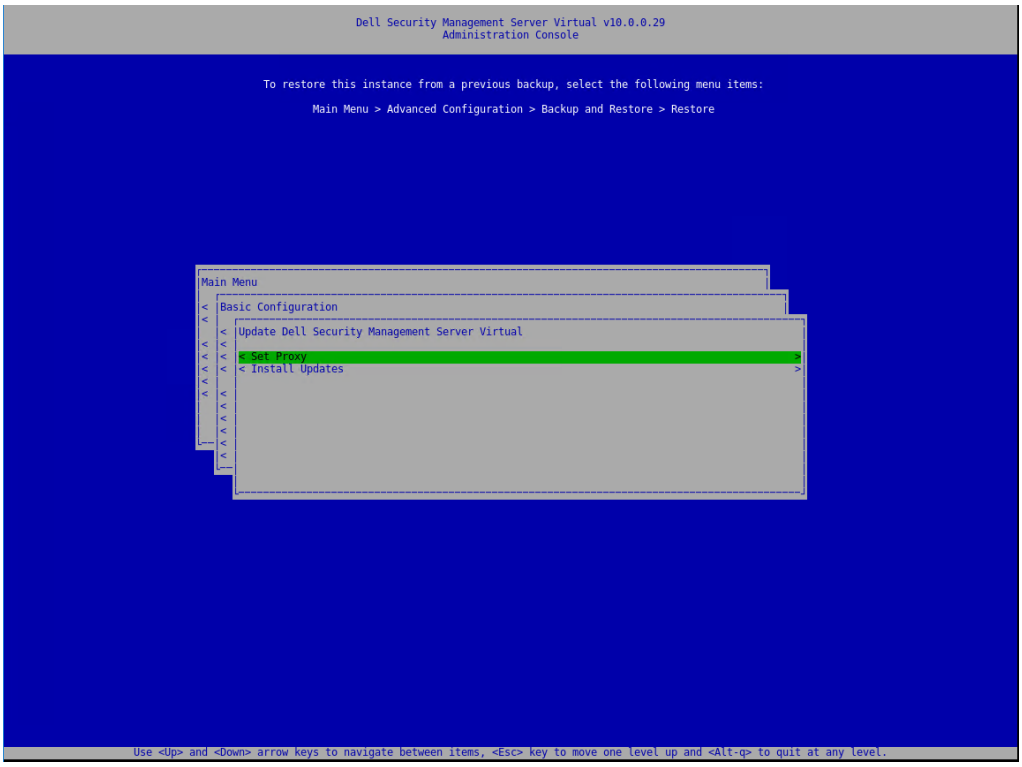
Per ricevere notifiche tramite posta elettronica quando sono disponibili aggiornamenti del Dell Server, consultare Configurare le impostazioni SMTP.

Se sono state effettuate delle modifiche ai criteri ma non ne è stato ancora eseguito il commit nella Management Console, applicare le modifiche dei criteri prima di aggiornare il Dell Server:

1. Eseguire l'accesso alla Management Console come amministratore Dell.
2. Nel menu a sinistra, fare clic su **Gestione** > **Esegui commit**.
3. Immettere una descrizione della modifica nel campo Commento.
4. Fare clic su **Commit criteri**.
5. Al completamento del commit, disconnettersi dalla Management Console.

Aggiornare Security Management Server Virtual (modalità connessa)

1. Dell consiglia di eseguire un backup periodico. Prima dell'aggiornamento, verificare che il processo di backup abbia funzionato correttamente. Consultare Eseguire backup e ripristino.
2. Dal menu **Configurazione di base**, selezionare **Aggiornare Dell Security Management Server Virtual**.



N.B.: Il numero di versione potrebbe essere diverso da quello dell'acquisizione della schermata allegata.

3. Selezionare l'azione desiderata:
   - Configura impostazioni proxy - Selezionare questa opzione per configurare le impostazioni proxy per scaricare gli aggiornamenti.

     Nella schermata *Configura impostazioni proxy*, premere la barra spaziatrice per inserire una **X** nel campo *Usa proxy*. Immettere HTTPS e HTTP. Se è richiesta l'autenticazione firewall, premere la barra spaziatrice per inserire una **X** nel campo Autenticazione richiesta. Immettere nome utente e password, quindi selezionare **OK**.

     N.B.: Questa opzione Set proxy ora anche gli aggiornamenti le impostazioni proxy per le varie applicazioni basate su Java per tirare con forza On-The -casella le licenze, nonché le comunicazioni per gli endpoint Security Suite Enterprise SaaS e Dell/Credant all'infrastruttura di back-end.

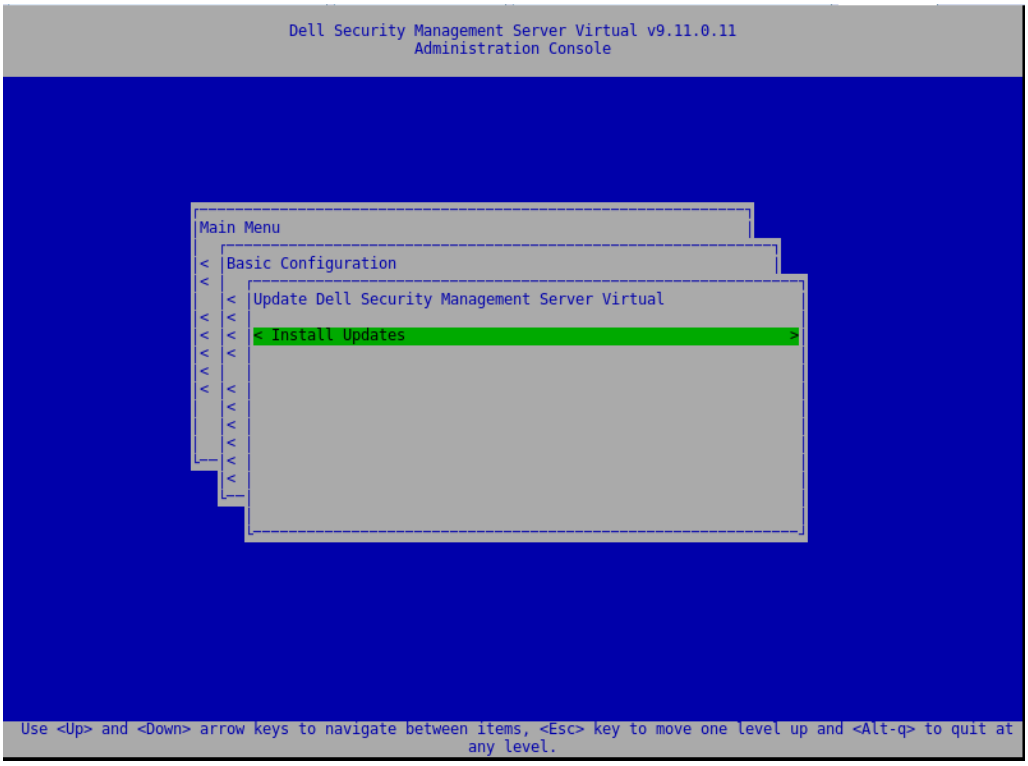
   - Quando si seleziona **Installa aggiornamenti**, Security Management Server Virtual interroga i repository integrati predefiniti di Ubuntu e dist.ddspproduction.com, il repository personalizzato di Dell che contiene gli aggiornamenti dell'applicazione.

     N.B.: Dell interroga dist.ddspproduction.com tramite la porta 443 e la porta 80 per tutti gli aggiornamenti Ubuntu. Vengono scaricati eventuali aggiornamenti disponibili. Le impostazioni proxy definite in Imposta proxy vengono utilizzate per le connessioni della porta 443 e della porta 80 per il download.

Aggiornare Security Management Server Virtual (modalità disconnessa)

1. Dell consiglia di eseguire un backup periodico. Prima dell'aggiornamento, verificare che il processo di backup abbia funzionato correttamente. Consultare Eseguire backup e ripristino.
2. Ottenere il file .deb che contiene l'ultimo aggiornamento del Dell Server dal sito del supporto di Dell.
3. Archiviare il file .deb nella cartella /var/opt/dell/dsmsv/ftp/files/updates sul server FTP protetto del Dell Server.

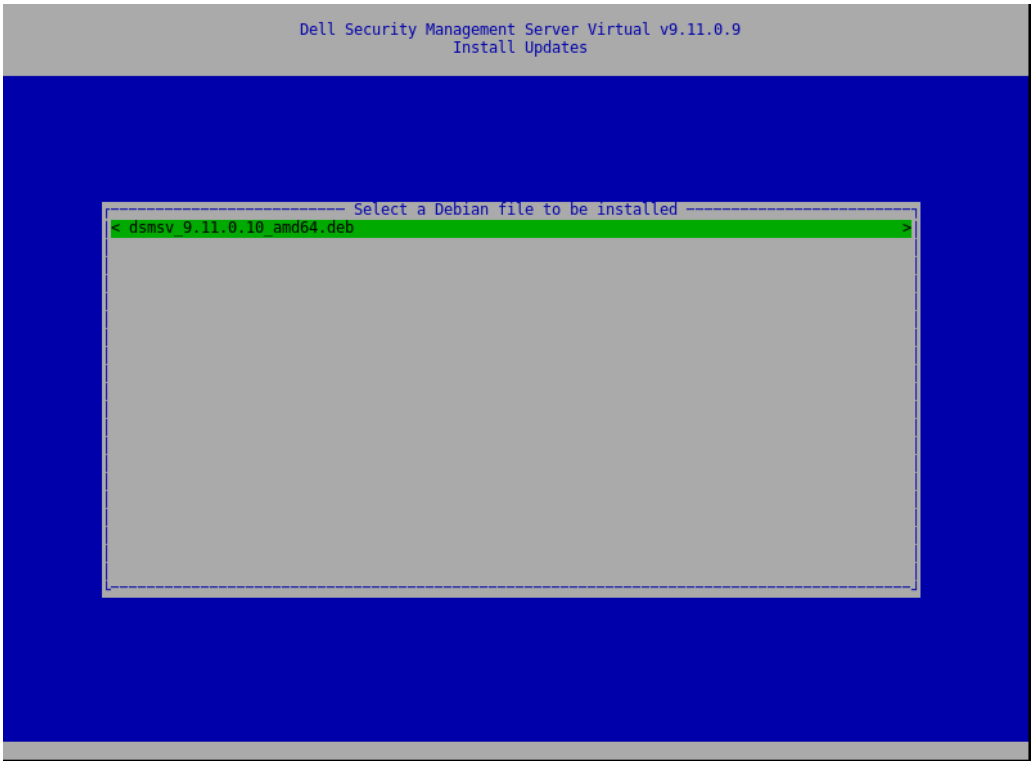
   Accertarsi che il client FTP supporti SFTP sulla porta 22 e che sia configurato un utente FTP. Vedere Impostare gli utenti File Transfer Protocol (FTP).
4. Dal menu **Configurazione di base**, selezionare **Aggiornare Security Management Server Virtual**.
5. Selezionare **Installa aggiornamenti** e premere **Invio**.



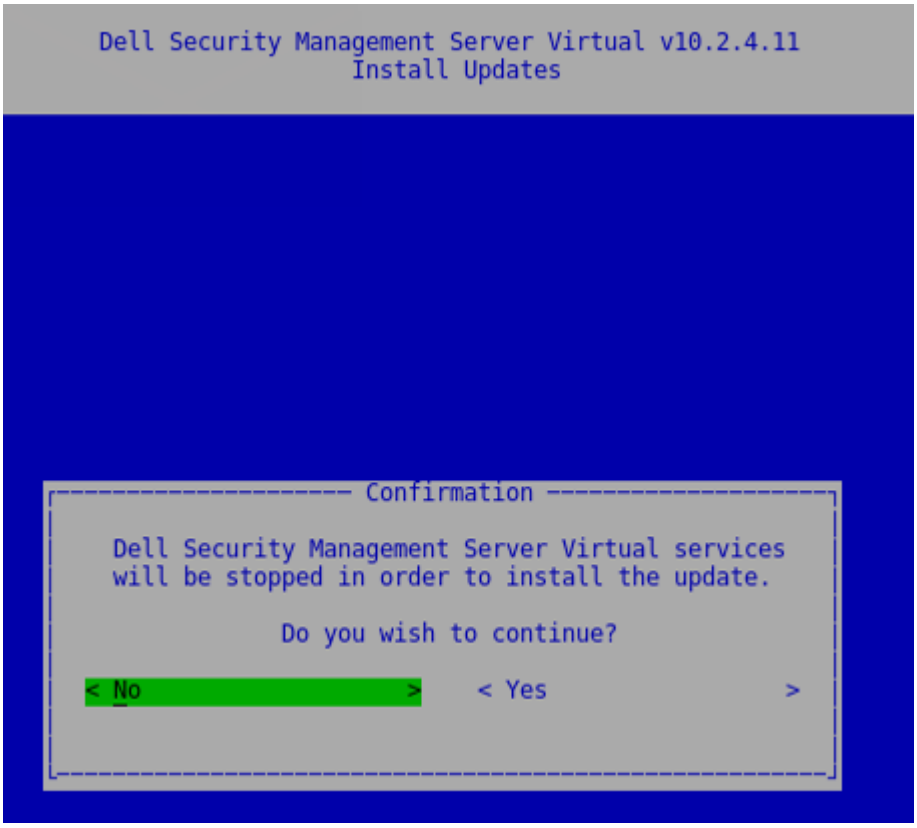
N.B.: Il numero di versione potrebbe essere diverso da quello dell'acquisizione della schermata allegata.

Se il file .deb non viene visualizzato, verificare che sia archiviato nella posizione corretta.

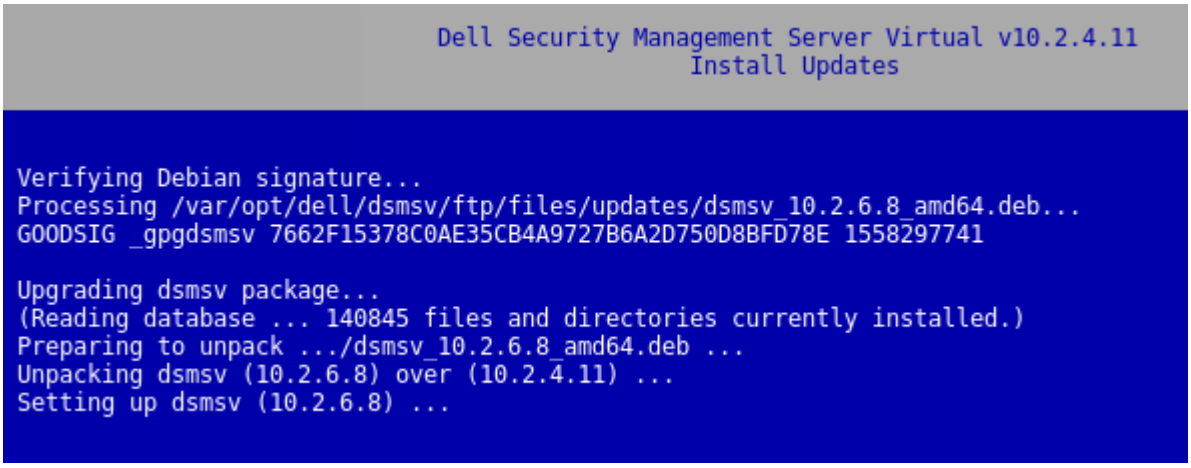
6. Selezionare il file di aggiornamento .deb da installare e premere **Invio**.



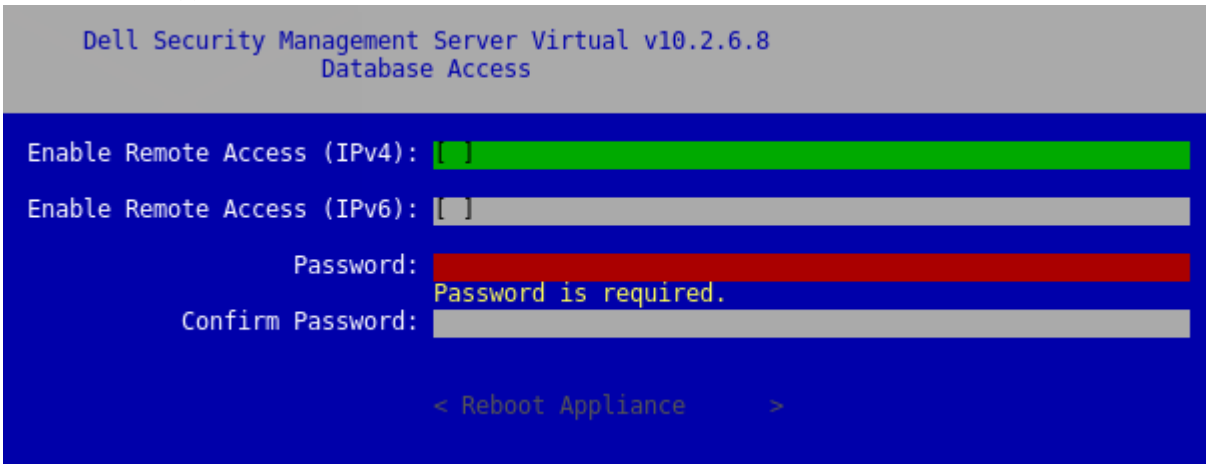
7. Selezionare **Sì** per arrestare i servizi di Security Management Server Virtual.



8. Il pacchetto Debian viene verificato e aggiornato.



9. Al termine dell'aggiornamento, modificare la password del database.



N.B.: Il numero di versione potrebbe essere diverso da quello dell'acquisizione della schermata allegata.

Modificare le password utente

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare Security Management Server Virtual.

È possibile modificare le password dei seguenti utenti:

- delluser (amministratore del terminale) - Questo utente ha accesso al terminale di Dell Server e ai relativi menu.
- dellconsole (accesso alla shell) - Questo utente ha accesso alla shell di Dell Server. Un amministratore di rete ha a disposizione l'accesso alla shell per controllare e risolvere i problemi della connettività di rete.
- dellsupport (amministratore Dell ProSupport) - Questo utente ha diritti "sudo" e deve essere utilizzata con parsimonia. Ai fini della sicurezza, l'utente controlla la password per questo account.

1. Dal menu *Configurazione di base*, selezionare **Modifica password utente**.
2. Nella schermata *Modifica password utente*, selezionare la password utente da modificare e selezionare **Invio**.
3. Nella schermata *Imposta password*, immettere la password corrente, immettere la nuova password, immettere nuovamente la nuova password, quindi selezionare **OK**.

   Le password devono includere i seguenti elementi:

   - Almeno 8 caratteri
   - Almeno 1 lettera maiuscola
   - Almeno 1 cifra
   - Almeno 1 carattere speciale

   N.B.:

Per selezionare diversi account utente, utilizzare il tasto "barra spaziatrice" sulla tastiera per visualizzare l'elenco di selezione.

Impostare gli utenti Secure File Transfer (SFTP)

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare Security Management Server Virtual.

1. Dal menu *Configurazione di base*, selezionare **SFTP**.
2. Nella schermata *SFTP* , per aggiungere un utente SFTP e definire una password, premere **Invio** o il tasto Giù nel campo *Stato* dell'utente. Premendo il tasto della barra spaziatrice, è possibile accedere all'opzione di aggiornamento o eliminazione di un utente esistente. Per disabilitare un utente SFTP, selezionare **Elimina** dopo aver selezionato l'utente, quindi selezionare **Sì** nella schermata di conferma SFTP.
3. Immettere un nome utente e una password per l'utente SFTP.

   Le password devono includere i seguenti elementi:

   - Almeno 8 caratteri
   - Almeno 1 lettera maiuscola
   - Almeno 1 cifra
   - Almeno 1 carattere speciale
4. Una volta inseriti gli utenti SFTP, selezionare **Applica**.

Abilitare SSH

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare a utilizzare Security Management Server Virtual.

È possibile abilitare SSH per l'accesso come amministratore del supporto, l'accesso alla shell e l'interfaccia della riga di comando del terminale.

1. Dal menu *Configurazione di base*, selezionare **SSH**.
2. Evidenziare l'utente per il quale si desidera abilitare l'SSH, premere la barra spaziatrice per inserire una **X** e selezionare **OK**.

Avviare o arrestare i servizi

Eseguire questa operazione solo se necessario.

1. Per avviare o arrestare contemporaneamente tutti i servizi, dal menu *Configurazione di base*, selezionare **Avvia applicazione** o **Interrompi applicazione**.
2. Al prompt di conferma, selezionare **Sì**.

   N.B.:

   Il completamento delle modifiche allo stato del server potrebbe richiedere fino a due minuti.

Riavviare l'applicazione

Eseguire questa operazione solo se necessario.

1. Dal menu *Configurazione di base*, selezionare **Riavvia applicazione**.
2. Al prompt di conferma, selezionare **Sì**.
3. Dopo il riavvio, eseguire l'accesso a Security Management Server Virtual.

Arrestare l'applicazione

Eseguire questa operazione solo se necessario.

1. Dal menu *Configurazione di base*, scorrere verso il basso e selezionare **Arresta applicazione**.
2. Al prompt di conferma, selezionare **Sì**.
3. Dopo il riavvio, eseguire l'accesso a Security Management Server Virtual.

Attività di configurazione del terminale avanzato

Le operazioni di configurazione avanzata sono accessibili dal menu principale.

Configurare la rotazione del registro

N.B.: Le istruzioni riportate di seguito definiscono la rotazione dei log per le applicazioni sui sistemi Dell Security Management Server Virtual che la supportano.

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare Security Management Server Virtual.

La rotazione quotidiana del registro è abilitata per impostazione predefinita. Per modificare la rotazione del registro predefinita, dal menu *Configurazione avanzata*, selezionare **Configurazione rotazione registro.**

Per disabilitare la rotazione del registro, usare la barra spaziatrice per inserire una **X** nel campo *Nessuna rotazione* e selezionare **OK**.

Per abilitare la rotazione del registro, attenersi alla seguente procedura:

1. Per abilitare la rotazione quotidiana, settimanale o mensile, usare la barra spaziatrice per inserire una **X** nel campo appropriato. Per la rotazione settimanale, utilizzare il menu a discesa per selezionare il giorno della settimana appropriato. Per la rotazione mensile, inserire il giorno appropriato del mese.
2. Immettere l'ora della rotazione nel campo *Ora rotazione registro*.
3. Selezionare **OK**.

Eseguire backup e ripristino

È possibile configurare o eseguire i backup in qualsiasi momento, ma non sono necessari per iniziare ad usare Security Management Server Virtual. Dell consiglia di configurare un processo di backup periodico. Per maggiori informazioni, consultare la http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

Se archiviati nel Dell Server, quando la capacità del disco è piena per il 90 per cento, non vengono archiviati nuovi backup. Se sono state configurate le notifiche tramite posta elettronica, si riceverà una notifica tramite posta elettronica, che segnala che lo spazio di allocazione su disco è ridotto.

N.B.:

Per mantenere lo spazio di partizione del disco ed evitare la cancellazione automatica dei backup, rimuovere i backup dal dispositivo di archiviazione.

Per impostazione predefinita i backup vengono eseguiti quotidianamente. Dell consiglia di archiviare i backup in un server FTP protetto esterno con una frequenza che soddisfi i requisiti di un'organizzazione relativi a backup e uso appropriato dello spazio di archiviazione.

Per configurare una pianificazione del backup, dal menu *Configurazione avanzata* selezionare **Backup e ripristino > Configurazione** e seguire la seguente procedura:

1. Per abilitare backup quotidiani, settimanali o mensili, usare la barra spaziatrice per inserire una **X** nel campo appropriato. Per i backup settimanali o mensili, immettere il giorno appropriato della settimana o del mese sotto forma di numerale, dove Lunedì=1. Per disabilitare i backup, usare la barra spaziatrice per inserire una **X** nel campo *Nessun backup* e selezionare **OK**.
2. Immettere l'ora del backup nel campo *Ora backup*.
3. Selezionare **OK**.

Per eseguire un backup immediato, dal menu *Configurazione avanzata* selezionare **Backup e ripristino > Esegui backup ora.** Quando viene visualizzata la conferma del backup, selezionare **OK**.

N.B.:

Prima di iniziare un'operazione di ripristino, tutti i servizi del Dell Server devono essere in esecuzione. Verificare lo stato del server. Se tutti i servizi non sono in esecuzione, riavviarli. Per ulteriori informazioni, consultare Avviare o arrestare i servizi. Iniziare il ripristino ***solo*** quando ***tutti*** i servizi sono in esecuzione.

Per eseguire il ripristino da un backup, dal menu *Configurazione avanzata*, selezionare **Backup e ripristino > Ripristina** e selezionare il file di backup da ripristinare. Nella schermata di conferma selezionare **Sì.**

Il backup viene ripristinato dopo il riavvio.

Archiviare i backup in un server FTP protetto

Per archiviare i backup in un server FTP protetto, il client FTP deve supportare SFTP sulla porta 22.

Secondo i requisiti di backup dell'organizzazione, è possibile scaricare i backup nei seguenti modi:

- Manualmente
- Attraverso uno script automatizzato
- Attraverso una soluzione di backup approvata dall'organizzazione

Per scaricare i backup utilizzando la soluzione di backup dell'organizzazione, ottenere istruzioni dettagliate dal proprio fornitore di soluzioni di backup.

N.B.:

Il Dell Server è basato su Debian Ubuntu x64 di Linux.

Accedere al Dell Server come dellsupport e usare il comando **sudo** per configurare la soluzione di backup:

sudo <istruzioni del fornitore di soluzioni di backup>

Effettuare il backup del contenuto delle seguenti cartelle:

/backup (obbligatorio)

/certificates (vivamente consigliato)

/support (opzionale)

Al completamento del processo sudo, digitare **exit** e premere **Invio** fino alla visualizzazione della richiesta di accesso.

Configurare le impostazioni SMTP

Per ricevere notifiche tramite e-mail, attenersi alla procedura descritta in questa sezione per configurare le impostazioni SMTP. Le notifiche tramite posta elettronica informano i destinatari in merito a stati di errore del Dell Server, aggiornamenti della password, disponibilità di aggiornamenti per il Dell Server e problemi relativi alla licenza client.

La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

Per configurare le impostazioni SMTP, attenersi alla seguente procedura:

1. Dal menu *Configurazione avanzata*, selezionare **Notifiche tramite posta elettronica**.
2. Per abilitare gli avvisi di posta elettronica, premere la barra spaziatrice per immettere una **X** nel campo *Abilita avvisi di posta elettronica* sulla schermata Notifiche tramite posta elettronica.
3. Inserire il nome di dominio completo del server SMTP.
4. Immettere la porta SMTP.
5. Immettere la porta SMTP.
6. Immetti la password amministratore
7. Nel campo *Invia notifiche da*, immettere l'ID dell'account di posta elettronica per inviare le notifiche tramite posta elettronica.
8. Nel campo *Invia stato del server a*, immettere un ID dell'account di posta elettronica per inviare le notifiche sullo stato del server. I destinatari sono separati da virgole o punti e virgola.
9. Nel campo *Invia modifiche della password a*, immettere un ID dell'account di posta elettronica per inviare notifiche di modifica della password.
10. Nel campo *Invia aggiornamenti del software a*, immettere un ID dell'account di posta elettronica per inviare notifiche di aggiornamento del software.

11. Nel campo *Promemoria avviso di servizio*, per abilitare i promemoria, premere la barra spaziatrice per immettere una **X**, quindi impostare l'intervallo del promemoria in minuti. Un Promemoria avviso di servizio viene attivato quando l'intervallo del promemoria è trascorso dopo l'invio di una notifica relativa ad un problema dello stato del sistema e l'host o il servizio rimane nello stesso stato.
12. Nel campo *Rapporto di riepilogo*, per abilitare i rapporti delle notifiche, selezionare l'intervallo desiderato (Ogni giorno, Ogni settimana oppure Ogni mese), quindi premere la barra spaziatrice per immettere una **X**.
13. Selezionare **OK**.

Importare un certificato esistente o registrare un nuovo certificato server

È possibile importare un certificato esistente o creare una richiesta di certificato tramite Security Management Server Virtual.

La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

Importare un certificato server esistente

1. Esportare il certificato esistente e la relativa catena di attendibilità completa dal rispettivo archivio chiavi.

   N.B.: Conservare la password di esportazione, in quanto sarà necessario immetterla al momento dell'importazione del certificato in Security Management Server Virtual.
2. Nel server FTP Dell Server archiviare il certificato in **/certificates**.
3. Dal menu *Configurazione avanzata*, selezionare **Certificati server**.
4. Selezionare **Importa certificato esistente**.
5. Selezionare un file di certificato da installare Dell Server.
6. Quando richiesto, immettere la password di esportazione del certificato e selezionare **OK**.
7. Al termine dell'importazione, selezionare **OK**.

   N.B.: Per maggiori informazioni, fare riferimento a http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en

Registrare un nuovo certificato server

1. Dal menu *Configurazione avanzata*, selezionare **Certificati server**.
2. Selezionare **Nuovo certificato server.**
3. Selezionare **Crea richiesta certificato.**
4. Compilare i campi *Genera richiesta certificato*:
   - Nome paese: codice paese di due lettere.
   - *Stato/provincia*: immettere il nome esteso dello stato o della provincia (ad esempio Italia).
   - *Nome località/Città:* immettere il valore appropriato (ad esempio Roma).
   - *Organizzazione*: immettere il valore appropriato (ad esempio Dell).
   - *Unità organizzativa*: immettere il valore appropriato (ad esempio Sicurezza).
   - *Nome comune*: immettere il nome di dominio completo del server in cui è installato Dell Server. Questo nome completo include il nome host e il nome di dominio (ad esempio, server.dominio.com).
   - *ID posta elettronica*: immettere l'indirizzo di posta elettronica a cui verrà inviato il CSR.
5. Seguire la procedura organizzativa per acquisire un certificato server SSL da un'autorità di certificazione. Inviare il contenuto del file CSR per la firma.
6. Quando si riceve il certificato firmato, esportare il certificato come file .p7b e scaricare la catena di attendibilità completa in formato .der.
7. Creare copie di backup del certificato e della catena di attendibilità.
8. Caricare il file del certificato e la relativa catena di attendibilità Dell Server.
9. Dal menu *Configurazione avanzata*, selezionare **Certificati server**.

10. Selezionare **Nuovo certificato server.**
11. Selezionare **`Completa registrazione certificato.`**
12. Selezionare il file di certificato da installare Dell Server.
13. Se richiesto, immettere la password del certificato: **changeit**.

Per attivare la convalida dell'attendibilità nei client Encryption basati su Windows, consultare la sezione Abilitare il controllo della catena di attendibilità di Manager.

Creare e installare un certificato autofirmato

N.B.: I certificati autofirmati generati per impostazione predefinita vengono generati per 10 anni.

1. Dal menu *Configurazione avanzata* Dell Server, selezionare **Certificati server**.
2. Selezionare **Crea e installa un certificato autofirmato**.
3. Per confermare di voler sostituire il certificato preinstallato con un nuovo certificato, fare clic su **Sì**.
4. Immettere la password del certificato: **changeit**.
5. Al termine dell'installazione del nuovo certificato, selezionare **OK** e attendere il riavvio dei servizi.

I servizi verranno riavviati automaticamente.

Abilitare l'accesso al database

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare Security Management Server Virtual.

N.B.: Dell consiglia di abilitare l'accesso al database solo se necessario e disabilitarlo quando non è più necessario.

1. Dal menu *Configurazione avanzata*, selezionare **Accesso database**.
2. Usare la barra spaziatrice per inserire una **X** nel campo *Abilita accesso database* e selezionare **OK**. Se non è stata ancora configurata la password database, viene visualizzata una richiesta per immetterla.
3. Immettere la password del database.
4. Immettere nuovamente la password del database.

   I componenti applicativi di Dell Data Security si interrompono automaticamente.

Impostare o cambiare la lingua del Terminal

La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

1. Nel menu principale, selezionare **Imposta lingua.**
2. Utilizzare i tasti freccia per selezionare la lingua preferita.

Visualizzare i registri

Per controllare i registri seguenti, nel menu principale selezionare **Visualizza registri.**

- Registri di sistema
  - Registro syslog
  - Registro posta
  - Registro autenticazione (SSH)
  - Registro postgres
  - Registro monitoraggio
- Registri dei server
  - Message Broker
  - Identity Server

    - Compatibility Server
    - Security Server
    - Core Server
    - Core Server HA
    - Inventory Server
    - Forensic Server
    - Policy Proxy
- Console di amministrazione
    - pybackup.log
    - pyconsole.log
    - pydatabase.log
    - update.log
- Registro databasecustomizer

N.B.: Per spostarsi attraverso questa schermata, utilizzare i seguenti dati:

- Per passare alla fine del log è possibile tenere premuto il tasto Alt e premere il tasto destro " /" tasto sulla tastiera
- Per uscire dalla finestra registro, tenere premuto a sinistra controllo e premere "x" sulla tastiera.
- I tasti di direzione per una navigazione.
- Pagina su e Pagina giù scorrono le pagine in alto e in basso una alla volta.
- La barra spaziatrice allunga i registri da una pagina.

Apertura dell'interfaccia della riga di comando

Per aprire l'interfaccia della riga di comando, nel menu principale selezionare **Avvia shell.**

Per uscire dall'interfaccia della riga di comando, digitare **exit** e premere **Invio**.

Generare un registro snapshot del sistema

Per generare un registro snapshot del sistema per Dell ProSupport, nel menu principale selezionare **Strumenti supporto.**

1. Dal menu *Strumenti supporto*, selezionare **Genera registro snapshot sistema.**
2. All'indicazione della creazione del file, selezionare **OK**.

3

Manutenzione di

Rimuovere backup inutili di Security Management Server Virtual.

Vengono conservati solo i dieci backup più recenti. Se lo spazio di partizione del disco è uguale o inferiore al dieci per cento, non vengono archiviati altri backup. Se si verifica questa condizione, si riceve una notifica tramite posta elettronica, che segnala che lo spazio di allocazione su disco è ridotto.

4

Risoluzione dei problemi

Se si verifica un errore e sono state configurate le notifiche tramite posta elettronica, l'utente riceverà una notifica tramite posta elettronica. In base alle informazioni contenute nella notifica tramite posta elettronica, attenersi alla seguente procedura:

1. Verificare i file di registro applicabili.
2. Riavviare i servizi, se necessario. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.
3. Generare un registro snapshot del sistema.
4. Contattare Dell ProSupport. Per maggiori informazioni, consultare Contattare Dell ProSupport.

5

Configurazione di postinstallazione

Dopo l'installazione, potrebbe essere necessario configurare alcuni componenti dell'ambiente in base alla soluzione Dell Data Security utilizzata dall'organizzazione.

Dopo aver installato Security Management Server Virtual, modificare i seguenti parametri predefiniti:

- Modificare la password del server back-end nel seguente percorso:

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`

- Modificare la password per ogni server front-end presente nell'ambiente nel seguente percorso:

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

La password verrà visualizzata come segue: `proxy-server.password=ENC(<texthere>)`

Per modificare la password:

1. Selezionare: `ENC(<texthere>)`
2. Modificare il testo selezionato in: `CLR(<newpasswordhere>)`

   Una volta riavviato il servizio, la riga modificata cambia in `ENC` da `CLR` e la password viene crittografata.

NOTA: è possibile modificare anche proxy-server.username purché corrisponda al file application.properties di Message Broker e a tutti i server front-end attivi.

Convalidare il controllo della catena di attendibilità di Manager

Se viene usato un certificato autofirmato nel Security Management Server Virtual per SED o BitLocker Manager, la convalida dell'attendibilità SSL/TLS deve rimanere ***disabilitata*** nel computer client. Prima di abilitare la convalida dell'attendibilità SSL/TLS nel computer client, devono essere soddisfatti i seguenti requisiti:

- Un certificato firmato da un'autorità radice (ad esempio Entrust o Verisign) deve essere importato nel Dell Server. Consultare Importare un certificato esistente o registrare un nuovo certificato server.
- La catena di attendibilità completa del certificato deve essere archiviata nell'archivio chiavi Microsoft nel computer client.

Per disabilitare la convalida dell'attendibilità SSL/TLS, nel computer client modificare il valore della seguente voce del registro in 1:

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):1

Proprietà di timeout per la console di gestione

Per modificare la proprietà di timeout per la console di gestione, ndare al file application.properties e modificare i valori predefiniti:

- `idle.warn.seconds=1080`
- `idle.timeout.seconds=1200`

6

Attività dell'amministratore della Management Console

Assegnare un ruolo amministratore Dell

1. In qualità di amministratore server Security Management, accedere alla console di gestione all'indirizzo https://server.domain.com:8443/webui/. Le credenziali predefinite sono **superadmin/changeit.**
2. Nel riquadro sinistro cliccare su **Popolamenti** > **Domini**.
3. Cliccare su un dominio al quale aggiungere un utente.
4. Nella pagina Dettagli dominio, cliccare sulla scheda **Membri**.
5. Cliccare 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. Cliccare su **Aggiungi**.
9. Dalla barra del menu, cliccare 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. Cliccare su **Salva**.

Accedere con ruolo amministratore Dell

1. Disconnettersi dalla Management Console.
2. Accedere alla Management Console con le credenziali dell'utente di dominio.

   Fare clic su "?" nell'angolo in alto a destra della Management Console per avviare la *guida dell'amministratore.* Viene visualizzata la pagina iniziale. Fare clic su **Aggiungi domini**.

   Per ogni organizzazione vengono impostati dei criteri di base; tuttavia, è necessario modificare tali criteri in base alle specifiche esigenze, come illustrato di seguito (tutte le attivazioni prevedono licenze e diritti):

   - La Crittografia basata su criteri verrà attivata con la crittografia Common-Key
   - I computer con unità autocrittografanti verranno crittografati
   - BitLocker Management non è abilitato
   - Advanced Threat Prevention non è abilitato
   - Threat Protection è disabilitato
   - I supporti esterni non verranno crittografati
   - Le porte non saranno gestite da Controllo porte
   - I dispositivi con Full Disk Encryption installato non verranno crittografati

   Vedere l'argomento *Gestione dei criteri* nella guida dell'amministratore per le descrizioni dei criteri.

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**.

7

Porte

La tabella seguente descrive ciascun componente e la relativa funzione.

Nome	Porta predefinita	Descrizione
Servizio gruppo di accesso	TCP/ 8006	Gestisce autorizzazioni e gruppi di accesso per diversi prodotti Dell Security. **N.B.:** La porta 8006 non è attualmente protetta. Verificare che la porta sia correttamente filtrata attraverso un firewall. Questa porta è solo interna.
Console di gestione	HTTPS/ 8443	Console di amministrazione e centro di controllo per la distribuzione a livello aziendale.
Core Server	HTTPS/ 8887 (chiuso)	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 dalla console di gestione. Raccoglie e archivia i dati di autenticazione. Controlla l'accesso basato sui ruoli.
Core Server HA (elevata disponibilità)	HTTPS/ 8888	Servizio ad elevata disponibilità che consente una maggiore sicurezza e migliori prestazioni delle connessioni HTTPS con la console di gestione, l'autenticazione di preavvio, SED Management, FDE, BitLocker Manager, Threat Protection e Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Comunica con Policy Proxy e gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, e la comunicazione SED-PBA e Full Disk Encryption-PBA.
Compatibility Server	TCP/ 1099 (chiusa)	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. **N.B.:** La porta 1099 deve essere filtrata attraverso un firewall. Dell consiglia che questa porta sia solo interna.

Nome	Porta predefinita	Descrizione
Message Broker Service	TCP/ 61616 (chiuso) e STOMP/ 61613 (chiusa o, se configurata per DMZ, 61613 è aperta)	Gestisce la comunicazione tra i servizi di Dell Server. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy. **N.B.:** La porta 61616 deve essere filtrata attraverso un firewall. Dell consiglia che questa porta sia solo interna. **N.B.:** La porta 61613 deve essere aperta solo ai Security Management Server configurati in modalità front-end.
Identity Server	8445 (chiuso)	Gestisce le richieste di autenticazione del dominio, inclusa l'autenticazione per la gestione SED.
Forensic Server	HTTPS/ 8448	Consente agli amministratori che dispongono dei privilegi appropriati di ottenere dalla console di gestione le chiavi di crittografia, da usare per sbloccare i dati o per le attività di decrittografia. Richiesto per le API Forensic.
Inventory Server	8887	Elabora la coda di inventario.
Policy Proxy	TCP/ 8000	Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario. Richiesto per Encryption Enterprise (Windows e Mac)
PostGres	TCP/ 5432	Database locale utilizzato per i dati di eventi. **N.B.:** La porta 5432 deve essere filtrata attraverso un firewall. Dell consiglia che questa porta sia solo interna.
LDAP	389/636, 3268/3269 RPC - 135, 49125+	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

Nome	Porta predefinita	Descrizione
		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.
Autenticazione client	HTTPS/ 8449	Consente ai server client di eseguire l'autenticazione a Dell Server. Richiesto per Server Encryption