

# DDP Enterprise Server - Virtual Edition

Guida introduttiva e Guida all'installazione v9.7



## 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.

© 2017 Dell Inc. Tutti i diritti riservati. Dell, EMC e gli altri marchi sono marchi commerciali di Dell Inc. o delle sue sussidiarie. Gli altri marchi possono essere marchi dei rispettivi proprietari.

Marchi registrati e marchi commerciali utilizzati nella serie di documenti Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise e Dell Data Guardian: Dell™ e il logo Dell, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS® e KACE™ sono marchi commerciali di Dell Inc. Cylance®, CylancePROTECT e il logo Cylance sono marchi registrati di Cylance, Inc. negli Stati Uniti e in altri Paesi. McAfee® e il logo McAfee sono marchi commerciali o marchi registrati di McAfee, Inc. negli Stati Uniti e in altri Paesi. Intel®, Pentium®, Intel Core Inside Duo®, Itanium® e Xeon® sono marchi registrati di Intel Corporation negli Stati Uniti e in altri Paesi. Adobe®, Acrobat® e Flash® sono marchi registrati di Adobe Systems Incorporated. Authen Tec® e Eikon® sono marchi registrati di Authen Tec. AMD® è un marchio registrato di Advanced Micro Devices, Inc. Microsoft®, Windows® e Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista®, MSN®, ActiveX®, Active Directory®, Access®, ActiveSync®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Silverlight®, Outlook®, PowerPoint®, OneDrive®, SQL Server® e Visual C++® sono marchi commerciali o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. VMware® è un marchio registrato o marchio commerciale di VMware, Inc. negli Stati Uniti o in altri Paesi. Box® è un marchio registrato di Box. DropboxSM è un marchio di servizio di Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube® e Google™ Play sono marchi commerciali o marchi registrati di Google Inc. negli Stati Uniti e in altri Paesi. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud@SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari® e Siri® sono marchi di servizio, marchi commerciali o marchi registrati di Apple, Inc. negli Stati Uniti e/o in altri Paesi. GO ID®, RSA® e SecurID® sono marchi registrati di Dell EMC. EnCase™ e Guidance Software® sono marchi commerciali o marchi registrati di Guidance Software. Entrust® è un marchio registrato di Entrust®, Inc. negli Stati Uniti e in altri Paesi. InstallShield® è un marchio registrato di Flexera Software negli Stati Uniti, in Cina, nella Comunità Europea, ad Hong Kong, in Giappone, a Taiwan e nel Regno Unito. Micron® e RealSSD® sono marchi registrati di Micron Technology, Inc. negli Stati Uniti e in altri Paesi. Mozilla® Firefox® è un marchio registrato di Mozilla Foundation negli Stati Uniti e/o in altri Paesi. iOS® è un marchio commerciale o un marchio registrato di Cisco Systems, Inc. negli Stati Uniti e in alcuni altri Paesi ed è concesso in licenza. Oracle® e Java® sono marchi registrati di Oracle e/o suoi affiliate. Altri nomi possono essere marchi commerciali dei rispettivi proprietari. SAMSUNG™ è un marchio commerciale di SAMSUNG negli Stati Uniti o in altri Paesi. Seagate® è un marchio registrato di Seagate Technology LLC negli Stati Uniti e/o in altri Paesi. Travelstar® è un marchio registrato di HGST, Inc. negli Stati Uniti e in altri Paesi. UNIX® è un marchio registrato di The Open Group. VALIDITY™ è un marchio commerciale di Validity Sensors, Inc. negli Stati Uniti e in altri Paesi. VeriSign® e altri marchi correlati sono marchi commerciali o marchi registrati di VeriSign, Inc. o sue affiliate o filiali negli Stati Uniti e in altri Paesi, ed è concesso in licenza a Symantec Corporation. KVM on IP® è un marchio registrato di Video Products. Yahoo!® è un marchio registrato di Yahoo! Inc. In questo prodotto vengono utilizzate parti del programma 7-Zip. Il codice sorgente è disponibile all'indirizzo [7-zip.org](http://7-zip.org). La gestione delle licenze è basata sulla licenza GNU LGPL + restrizioni unRAR ([7-zip.org/license.txt](http://7-zip.org/license.txt)). Virtual Edition usa librerie di terze parti da "urwid" secondo i termini della GNU Lesser General Public License. L'avviso di copyright e la GNU Lesser General Public License sono disponibili nella AdminHelp nella pagina Attributions, Copyrights, and Trademarks (Attribuzioni, copyright e marchi commerciali).

### Guida introduttiva e Guida all'installazione di VE

2017 - 04

Rev. A01

|  |           |
|--|-----------|
| <b>1 Guida introduttiva a Virtual Edition.....</b>                               | <b>5</b>  |
| Installare DDP Enterprise Server - VE.....                                       | 5         |
| Configurare VE.....  | 5         |
| Aprire la Remote Management Console di VE.....                                   | 5         |
| Attività di amministrazione.....   | 6         |
| <b>2 Guida all'installazione di Virtual Edition.....</b>                         | <b>7</b>  |
| Informazioni su DDP Enterprise Server - VE.....                                  | 7         |
| Contattare Dell ProSupport.....  | 7         |
| Requisiti.....   | 7         |
| Prerequisiti di DDP Enterprise Server - VE.....                                  | 7         |
| Prerequisiti della Remote Management Console di VE.....                          | 9         |
| Prerequisiti della modalità proxy.....   | 9         |
| Scaricare DDP Enterprise Server - VE.....  | 10        |
| Installare DDP Enterprise Server - VE.....                                       | 11        |
| Aprire la Remote Management Console di VE.....                                   | 12        |
| Installare e configurare la modalità proxy.....                                  | 12        |
| VE Terminal - Attività di configurazione di base.....                            | 14        |
| Modificare il nome host.....   | 14        |
| Modificare le impostazioni di rete.....  | 14        |
| Impostare il nome host DMZ.....  | 14        |
| Modificare il fuso orario.....   | 15        |
| Aggiornare DDP Enterprise Server - VE.....                                       | 15        |
| Modificare le password utente.....   | 16        |
| Impostare gli utenti File Transfer Protocol (FTP).....                           | 17        |
| Abilitare SSH.....   | 17        |
| Avviare o arrestare i servizi VE.....  | 17        |
| Riavviare VE.....  | 18        |
| Arrestare VE.....  | 18        |
| VE Terminal - Attività di configurazione avanzata.....                           | 18        |
| Impostare o modificare la password del database.....                             | 18        |
| Configurare le impostazioni SMTP.....  | 18        |
| Importare un certificato esistente o registrare un nuovo certificato server..... | 19        |
| Configurare la rotazione del registro.....                                       | 20        |
| Eseguire backup e ripristino.....  | 20        |
| Abilitare l'accesso remoto al database.....                                      | 22        |
| Abilitare il supporto del server DMZ.....  | 22        |
| <b>3 Attività dell'amministratore di DDP Enterprise Server - VE.....</b>         | <b>23</b> |
| Impostare o cambiare la lingua di DDP Enterprise Server - VE Terminal.....       | 23        |
| Verificare lo stato del server.....  | 23        |
| Visualizzare i registri.....   | 24        |
| Aprire l'interfaccia della riga di comando.....                                  | 24        |

|  |           |
|--|-----------|
| Generare un registro snapshot del sistema.....                                   | 24        |
| <b>4 Manutenzione di DDP Enterprise Server - VE.....</b>                         | <b>25</b> |
| <b>5 Risoluzione dei problemi di DDP Enterprise Server - VE.....</b>             | <b>26</b> |
| <b>6 Attività di configurazione di postinstallazione.....</b>                    | <b>27</b> |
| Configurare VE per Data Guardian.....  | 27        |
| Installare e configurare Gestione EAS per Mobile Edition.....                    | 27        |
| Abilitare il controllo della catena di attendibilità di Manager.....             | 29        |
| <b>7 Attività dell'amministratore della Remote Management Console di VE.....</b> | <b>30</b> |
| Assegnare un ruolo amministratore Dell.....                                      | 30        |
| Accedere con ruolo amministratore Dell.....                                      | 30        |
| Eeguire il commit dei criteri.....   | 31        |
| <b>8 Porte delle soluzioni.....</b>  | <b>32</b> |



# Guida introduttiva a Virtual Edition

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

Per istruzioni più dettagliate, consultare la [Guida all'installazione di Virtual Edition](#).

Per informazioni sui prerequisiti di VE, consultare [Prerequisiti di DDP Enterprise Server - VE](#), [Prerequisiti della Remote Management Console di VE](#) e [Prerequisiti della modalità proxy](#).

Per informazioni sulla procedura di aggiornamento di un DDP Enterprise Server - VE esistente, consultare [Aggiornare DDP Enterprise Server - VE](#).

## Installare DDP Enterprise Server - VE

- 1 Individuare la directory in cui sono archiviati i file Dell Data Protection e fare doppio clic per importarli in VMware **DDP Enterprise Server - VE v9.x.x Build x.o.va**.
- 2 Accedere a DDP Enterprise Server - VE.
- 3 Seguire le istruzioni visualizzate.

## Configurare VE

Prima di attivare gli utenti, è necessario completare le seguenti attività di configurazione di DDP Enterprise Server - VE Terminal:

- [Impostare o modificare la password del database](#)
- [Configurare le impostazioni SMTP](#)
- [Importare un certificato esistente o registrare un nuovo certificato server](#)
- [Aggiornare DDP Enterprise Server - VE](#)
- 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](#).

**N.B.:** Se i client di Enterprise Edition dispongono di diritti predefiniti o vengono acquistate licenze dal produttore, impostare l'oggetto criterio di gruppo nel controller di dominio per attivare i diritti (potrebbe non trattarsi dello stesso server in cui è in esecuzione Virtual Edition). Verificare che la porta in uscita 443 sia disponibile per comunicare con il server. Se la porta 443 è bloccata (per qualsiasi motivo), la funzionalità per i diritti non sarà utilizzabile.

## Aprire la Remote Management Console di VE

Aprire la Remote Management Console di VE a questo indirizzo:

<https://server.domain.com:8443/webui/>

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

Per un elenco dei browser Web supportati, consultare [Prerequisiti della Remote Management Console di VE](#).



# Attività di amministrazione

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

Dell consiglia di assegnare i ruoli di amministratore appena possibile. Per completare questa operazione, consultare [Assegnare un ruolo amministratore Dell](#).

Fare clic su "?" nell'angolo in alto a destra della Remote Management Console di VE per avviare la *Guida dell'amministratore di Dell Data Protection*. Viene visualizzata la pagina iniziale. Fare clic su **Aggiungi domini**.

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

- I computer Windows verranno crittografati
- I computer con unità autocrittografanti verranno crittografati
- BitLocker Management non è abilitato
- Advanced Threat Protection non è abilitato
- Threat Protection è abilitato
- I supporti esterni non verranno crittografati
- I dispositivi connessi alle porte non verranno crittografati
- Dell Data Guardian è attivato
- Mobile Edition non è abilitato

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.

# Guida all'installazione di Virtual Edition

La presente Guida all'installazione consente ad utenti meno esperti di installare e configurare DDP Enterprise Server - VE. Come regola generale, Dell consiglia di installare prima DDP Enterprise Server - VE, quindi i client.

Per informazioni sulla procedura di aggiornamento di un DDP Enterprise Server - VE esistente, consultare [Aggiornare DDP Enterprise Server - VE](#).

## Informazioni su DDP Enterprise Server - VE

DDP Enterprise Server - VE è il dispositivo di amministrazione della sicurezza della soluzione Dell. La Remote Management Console di VE 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 DDP Enterprise Server - VE.

DDP Enterprise Server - VE 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

Per assistenza telefonica sui prodotti Dell Data Protection, chiamare il numero +1-877-459-7304, interno 4310039, 24h su 24, 7 giorni su 7.

Inoltre, il supporto online per i prodotti Dell Data Protection è disponibile all'indirizzo [dell.com/support](http://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 servizio per essere messi rapidamente in contatto con l'esperto tecnico più adatto.

Per i numeri di telefono esterni agli Stati Uniti, controllare [Numeri di telefono internazionali di Dell ProSupport](#).

## Requisiti

### Prerequisiti di DDP Enterprise Server - VE

#### Hardware

Lo spazio su disco consigliato per DDP Enterprise Server - VE è di 80 GB.

#### Ambiente virtualizzato



## Ambienti virtualizzati

---

- VMware Workstation 12.5
  - Richiesta CPU a 64 bit
  - 4 GB di RAM consigliati
  - Visitare <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17> 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/workstation-11/index.jsp>
  
- VMware Workstation 11
  - Richiesta CPU a 64 bit
  - 4 GB di RAM consigliati
  - Visitare <http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17> 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/workstation-11/index.jsp>
  
- VMware ESXi 6.0
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Non sono richiesti sistemi operativi
  - 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 5.5
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Non sono richiesti sistemi operativi
  - 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, consultare <http://pubs.vmware.com/vsphere-55/index.jsp>
  
- Hyper-V Server (installazione completa o dei componenti di base)
  - Richiesta CPU x86 a 64 bit
  - Computer host con almeno due core
  - Almeno 8 GB di RAM consigliati
  - Non sono richiesti sistemi operativi
  - L'hardware deve essere conforme ai requisiti minimi di Hyper-V
  - Almeno 4 GB di RAM per la risorsa immagine dedicata



- Deve essere eseguito come macchina virtuale di prima generazione
- Per maggiori informazioni, consultare <https://technet.microsoft.com/en-us/library/hh923062.aspx>

# Prerequisiti della Remote Management Console di VE

## Browser Internet

### **N.B.:**

È necessario che il browser accetti i cookie.

La tabella seguente descrive in dettaglio i browser Internet supportati.

### Browser Internet

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

# Prerequisiti della modalità proxy

## Hardware

La tabella seguente descrive in dettaglio i requisiti hardware *minimi* per la modalità proxy.

### Processore

Core 2 Duo da 2 GHz o superiore

### 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

TCP/IP installato e attivato

## Software

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

### Prerequisiti

---

- **Windows Installer 4.0 o versione successiva**



## Prerequisiti

---

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 4.5**

Microsoft ha pubblicato gli aggiornamenti della sicurezza di .NET Framework versione 4.5

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

**N.B.:**

Disabilitare sempre il controllo dell'account utente quando si utilizza Windows Server 2008. 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.

## Sistema operativo

---

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

- Standard Edition
- Enterprise Edition

- **Windows Server 2008 SP2 a 64 bit**

- Standard Edition
- Enterprise Edition

- **Windows Server 2012 R2**

- Standard Edition
- Datacenter Edition

- **Windows Server 2016**

- Standard Edition
- Datacenter Edition

# Scaricare DDP Enterprise Server - VE

In occasione dell'installazione iniziale, DDP Enterprise Server - VE 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 di DDP Enterprise Server - VE è disponibile all'indirizzo [www.dell.com/support](http://www.dell.com/support), nelle pagine del Supporto dei prodotti per i prodotti Dell Data Protection di seguito elencati:

[Crittografia](#)

Oppure

[Endpoint Security Suite](#)

Oppure

[Endpoint Security Suite Enterprise](#)

Oppure

[Data Guardian](#)

Per scaricare il file OVA:

- 1 Accedere alla pagina di supporto del prodotto per [Encryption](#), [Endpoint Security Suite](#), [Endpoint Security Suite Enterprise](#) o [Data Guardian](#).
- 2 Fare clic su **Driver e download**.
- 3 Accanto a "Visualizza tutti gli aggiornamenti disponibili per <versione SO>", fare clic su **Modifica SO** e selezionare uno dei seguenti: **VMware ESXi 6.0**, **VMware ESXi 5.5** o **VMware ESXi 5.1**.
- 4 In "Visualizza per:" selezionare **Mostra tutti**.
- 5 In Dell Data Protection, selezionare **Scarica**.

## Installare DDP Enterprise Server - VE

Prima di iniziare, verificare che siano soddisfatti tutti i [Requisiti](#) del sistema e dell'ambiente virtuale.

- 1 Individuare i file Dell Data Protection nel supporto di installazione e fare doppio clic per importarli in VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**.
- 2 Accedere a DDP Enterprise Server - VE.
- 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 predefinita** o **Modalità disconnessa**.

### **N.B.:**

Se si seleziona **Modalità disconnessa**, non è possibile attivare Modalità predefinita in VE.

La modalità disconnessa isola VE da Internet e da una LAN non protetta o altra rete. Tutti gli aggiornamenti devono essere eseguiti manualmente. Per ulteriori informazioni sulla funzionalità Modalità disconnessa, fare riferimento alla *guida dell'amministratore*.

- 7 Alla richiesta di modifica della password predefinita, selezionare **Sì**.
- 8 Nella schermata *Imposta password ddpuser* immettere la password corrente (predefinita), ossia **ddpuser**, quindi immettere una password univoca, reinserire la password univoca e selezionare **OK**.

Le password devono includere i seguenti elementi:

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



**i | N.B.:** Quando si usa un IP statico, è necessario creare anche una voce host nel server DNS.

- 11 Nella schermata *Fuso orario*, usare i tasti freccia per evidenziare il fuso orario, quindi selezionare **Invio**.
- 12 Alla richiesta di conferma del fuso orario, selezionare **OK**.
- 13 Quando viene visualizzato il messaggio che indica il completamento della configurazione iniziale, selezionare **OK**.
- 14 [Impostare o modificare la password del database.](#)
- 15 [Configurare le impostazioni SMTP.](#)
- 16 [Importare un certificato esistente o registrare un nuovo certificato server.](#)
- 17 [Aggiornare DDP Enterprise Server - VE.](#)
- 18 Installare un client FTP che supporta SFTP sulla porta 22 e [impostare gli utenti File Transfer Protocol \(FTP\)](#).

Le attività di installazione di DDP Enterprise Server - VE sono state completate.

## Aprire la Remote Management Console di VE

Aprire la Remote Management Console di VE a questo indirizzo:

<https://server.domain.com:8443/webui/>

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

Per un elenco dei browser Web supportati, consultare [Prerequisiti della Remote Management Console di VE](#).

## Installare e configurare la modalità proxy

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

**i | N.B.:** Il servizio beacon è installato come parte dell'installazione per supportare il beacon richiamata di Data Guardian, che inserisce un beacon di richiamata in ogni file protetto da Data Guardian quando è in esecuzione in modalità Office protetto. Ciò consente la comunicazione tra tutti i dispositivi in qualsiasi posizione e il server front-end di Dell. Accertarsi che la sicurezza di rete necessaria sia configurata prima di utilizzare il beacon richiamata. Il criterio Attiva beacon richiamata è abilitato per impostazione predefinita.

Per eseguire l'installazione, è necessario disporre del nome host completo del server DMZ.

- 1 Nel supporto di installazione di Dell, passare alla directory di Dell Enterprise Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Dell Enterprise Server-x64 nella directory principale del server in cui si sta installando VE. **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 finestra di dialogo *Installazione guidata InstallShield*, selezionare la lingua per l'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 Immettere il Product Key.
- 8 Selezionare **Installazione front-end** e fare clic su **Avanti**.
- 9 Per installare un server front-end 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 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 **Sfogli** per immettere il percorso del certificato.

Immettere la password associata al certificato. Il file dell'archivio chiavi deve essere .p12 o pfx.

Fare clic su **Avanti**.

**i** **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**.

**i** **N.B.:**

**Per impostazione predefinita, il certificato scade dopo un anno.**

- 11 Nella finestra di dialogo *Configurazione del server front-end*, immettere il nome host completo o alias DNS del server back-end, selezionare **Enterprise Edition**, 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.

**i** **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 diseleziona un proxy in questa finestra di dialogo, non verrà installato.

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

- Per visualizzare o modificare le porte, nella finestra di dialogo *Configurazione del server front-end* fare clic 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 diseleziona 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**.

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

## VE Terminal - Attività di configurazione di base

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

### Modificare il nome host

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

- 1 Dal menu *Configurazione di base*, selezionare **Nome host**.
- 2 Usare il tasto BACKSPACE per rimuovere il nome host di DDP Enterprise Server - VE 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 ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

- 1 Dal menu *Configurazione di base*, selezionare **Impostazioni di rete**.
- 2 Nella schermata *Configura impostazioni di rete*, scegliere una delle opzioni seguenti, quindi selezionare **OK**.
  - (Impostazione predefinita) Usa DHCP.
  - (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

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

### Impostare il nome host DMZ

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

- 1 Dal menu *Configurazione di base*, selezionare **Nome host DMZ**.
- 2 Immettere il nome di dominio completo del server DMZ e selezionare **OK**.

 **N.B.:** Per usare la modalità proxy (Modalità DMZ), è necessario 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 DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

- 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**.
- 3 Alla richiesta di conferma del fuso orario, selezionare **OK**.

## Aggiornare DDP Enterprise Server - VE

Per informazioni su un aggiornamento specifico, vedere gli avvisi tecnici di VE, disponibili sul sito del supporto Dell all'indirizzo <http://www.dell.com/support>. Per visualizzare la versione e la data di installazione di un aggiornamento già applicato, nel menu **Configurazione di base**, selezionare **Aggiorna DDP Enterprise Server - VE; > Ultimo aggiornamento applicato**.

Per ricevere notifiche tramite posta elettronica quando sono disponibili aggiornamenti di VE, consultare [Configurare le impostazioni SMTP](#).

**i** **N.B.:** In Modalità predefinita, è necessario effettuare un aggiornamento dopo l'installazione iniziale di DDP Enterprise Server - VE e prima dell'attivazione dei client.

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

- 1 Eseguire l'accesso alla Remote 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 Remote Management Console.

## Aggiornare VE (Modalità predefinita)

- 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 **Aggiorna DDP Enterprise Server - VE**.
- 3 Selezionare l'azione desiderata:
  - Imposta server di aggiornamento - Selezionare questa opzione per impostare o modificare il percorso del server dei pacchetti di aggiornamento di DDP Enterprise Server - VE. Nella schermata *Imposta server di aggiornamento*, usare il tasto BACKSPACE per rimuovere il nome host o l'indirizzo IP del server esistente. Immettere il nome di dominio o l'indirizzo IP completo, e selezionare **OK**.

Il server di aggiornamento predefinito è **act.credant.com**.

- 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 gli indirizzi proxy HTTPS, HTTP e FTP. Se è richiesta l'autenticazione firewall, premere la barra spaziatrice per inserire una **X** nel campo Autenticazione richiesta. Immettere nome utente e password, quindi premere **OK**.

**i** **N.B.:** Per eseguire l'aggiornamento da un sito FTP, immettere il nome utente e la password FTP, seguiti dall'URL.

- Verifica aggiornamento - Selezionare questa opzione per verificare la disponibilità di un pacchetto di aggiornamento di DDP Enterprise Server - VE nel server di aggiornamento.
- Scarica aggiornamento - Selezionare questa opzione per scaricare un aggiornamento dopo averlo individuato tramite l'opzione Verifica aggiornamento.



- Applica aggiornamento - Selezionare questa opzione se si desidera applicare un pacchetto di aggiornamento scaricato di DDP Enterprise Server - VE. Nella schermata *Seleziona un file di aggiornamento (.deb)*, selezionare il pacchetto di aggiornamento da installare e premere **Invio**.
- Ultimo aggiornamento applicato - Selezionare questa opzione per visualizzare la versione e la data di installazione della versione corrente di VE.

## Aggiornare VE (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 di VE dal sito del supporto di Dell. I download di VE si trovano nella cartella **Driver e download** all'indirizzo

[www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research](http://www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research)

Oppure

[www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y](http://www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y)

Oppure

[www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research](http://www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research)

Oppure

[www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research](http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research)

- 3 Archiviare il file .deb nella cartella /updates sul server FTP protetto di VE. 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 **Aggiorna DDP Enterprise Server - VE**.
- 5 Selezionare **Applica aggiornamento** e premere **Invio**.  
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**.

## Modificare le password utente

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

È possibile modificare le password dei seguenti utenti:

- ddpuser (Amministratore di DDP Enterprise Server - VE Terminal) - Questo utente ha accesso a VE Terminal e ai suoi menu.
- ddpconsole (accesso alla shell di DDP Enterprise Server - VE) - Questo utente ha accesso alla shell di VE. Un amministratore di rete ha a disposizione l'accesso alla shell per controllare e risolvere i problemi della connettività di rete.
- ddpsupport (Amministratore di Dell ProSupport) - Questo utente esiste esclusivamente per l'utilizzo da parte di Dell ProSupport. 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

## Impostare gli utenti File Transfer Protocol (FTP)

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

È possibile fornire a un massimo di tre utenti l'accesso al server FTP protetto di DDP Enterprise Server - VE per le attività di backup e ripristino. È possibile utilizzare il server FTP di VE anche per archiviare o caricare gli aggiornamenti su DDP Enterprise Server - VE.

- 1 Dal menu *Configurazione di base*, selezionare **Utenti File Transfer Protocol (FTP)**.
- 2 Nella schermata *Configura utenti FTP*, per abilitare un utente FTP premere la barra spaziatrice per inserire una **X** nel campo Stato dell'utente. Per disabilitare un utente FTP, premere la barra spaziatrice per rimuovere la **X** nel campo Stato dell'utente.
- 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 **OK**.

## Abilitare SSH

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

È possibile abilitare SSH per l'accesso come amministratore del supporto, l'accesso alla shell di DDP Enterprise Server - VE e l'interfaccia della riga di comando di VE Terminal.

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

## Avviare o arrestare i servizi VE

Eeguire questa operazione solo se necessario. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

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

 **N.B.:** Il completamento delle modifiche allo stato del server potrebbe richiedere fino a due minuti.



## Riavviare VE

Eeguire questa operazione solo se necessario.

- 1 Dal menu *Configurazione di base*, selezionare **Riavvia applicazione**.
- 2 Al prompt di conferma, selezionare **Si**.
- 3 Dopo il riavvio, accedere a DDP Enterprise Server - VE.

## Arrestare VE

Eeguire 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 **Si**.
- 3 Dopo il riavvio, accedere a DDP Enterprise Server - VE.

## VE Terminal - Attività di configurazione avanzata

Le operazioni di configurazione avanzata sono accessibili dal menu principale.

### Impostare o modificare la password del database

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

- 1 Dal menu *Configurazione avanzata*, selezionare **Password database**.
- 2 Immettere una password per accedere al database e 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.:** Dell consiglia di eseguire il backup delle password al termine dell'installazione.

### Configurare le impostazioni SMTP

Per ricevere notifiche tramite e-mail da DDP Enterprise Server - VE o per usare Data Guardian, attenersi alla procedura descritta in questa sezione per configurare le impostazioni SMTP. Le notifiche tramite posta elettronica da DDP Enterprise Server - VE informano i destinatari su stati di errore del server DDP Enterprise Server - VE, disponibilità di aggiornamenti di DDP Enterprise Server - VE e problemi con licenze 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 Nella schermata *Imposta notifiche tramite posta elettronica*, per abilitare gli avvisi di posta elettronica premere la barra spaziatrice per inserire una **X** nel campo **Abilita avvisi di posta elettronica**.

- 3 Inserire il nome di dominio completo del server SMTP.
- 4 Immettere la porta SMTP.
- 5 Nel campo Da utente, inserire l'ID dell'account di posta elettronica che invierà le notifiche tramite posta elettronica.
- 6 Nel campo Immetti utente, inserire l'ID di un account di posta elettronica per accedere alla modifica delle notifiche di posta elettronica configurate.
- 7 Nel campo Password, inserire la password per accedere alla modifica delle notifiche di posta elettronica configurate.
- 8 Nei campi ID posta elettronica relativi allo stato VE, agli aggiornamenti della password e alla disponibilità di aggiornamenti, inserire gli elenchi dei destinatari per ciascun tipo di notifica. Nella compilazione dell'elenco dei destinatari, seguire le convenzioni riportate di seguito:
  - Il formato dell'indirizzo di posta elettronica è destinatario@dell.com.
  - I destinatari sono separati da virgole o punti e virgola.
- 9 Nel campo Promemoria avviso di servizio, per abilitare i promemoria, premere la barra spaziatrice per immettere una **X** nel campo, quindi impostare l'intervallo di 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.
- 10 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** nel campo.
- 11 Selezionare **OK**.

## Importare un certificato esistente o registrare un nuovo certificato server

I certificati devono essere presenti prima dell'attivazione degli utenti per DDP Enterprise Server - VE.

È possibile importare un certificato esistente o creare una richiesta di certificato tramite DDP Enterprise Server - VE.

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 DDP Enterprise Server - VE.**

- 2 Nel server FTP di DDP Enterprise Server - VE, archiviare il certificato in `/opt/dell/vsftpd/files/certificates`.
- 3 Dal menu *Configurazione avanzata* di DDP Enterprise Server - VE, selezionare **Certificati server**.
- 4 Selezionare **Importa certificato esistente**.
- 5 Selezionare un file di certificato da installare in DDP Enterprise Server - VE.
- 6 Quando richiesto, immettere la password di esportazione del certificato e selezionare **OK**.
- 7 Al termine dell'importazione, selezionare **OK**.

### 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 nella schermata *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 DDP Enterprise Server - VE. 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 nel server FTP di DDP Enterprise Server - VE.
  - 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 in DDP Enterprise Server - VE.
  - 13 Se richiesto, immettere la password del certificato: **changeit**.

Per attivare la convalida dell'attendibilità nei client Encryption basati su Windows, consultare [Abilitare il controllo della catena di attendibilità di Manager](#).

### Creare e installare un certificato autofirmato

- 1 Dal menu *Configurazione avanzata* di DDP Enterprise Server - VE, 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 **SI**.
- 4 Immettere la password del certificato: **changeit**.
- 5 Al termine dell'installazione del nuovo certificato, selezionare **OK** e attendere il riavvio dei servizi.

VE verrà riavviato automaticamente.

## Configurare la rotazione del registro

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

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 o mensile, immettere il giorno appropriato della settimana o del mese sotto forma di numero, dove Lunedì=1.
- 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 e non sono necessari per iniziare ad usare DDP Enterprise Server - VE. Dell consiglia di configurare un processo di backup periodico.

È possibile archiviare i backup in un server FTP protetto esterno (scelta consigliata) o in DDP Enterprise Server - VE. Se archiviati nel server VE, quando la capacità del disco è piena per il 90 per cento non vengono archiviati nuovi backup. L'utente 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 non necessari da DDP Enterprise Server - VE.

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 server VE 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 VE**. 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 **Si**.

VE si riavvia e il backup viene ripristinato.

### 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.:**

Virtual Edition è basata su Debian Ubuntu x64 di Linux.

Accedere a VE come ddpsupport e usare il comando sudo per configurare la soluzione di backup:

```
sudo <istruzioni dal fornitore di soluzioni di backup>
```

Effettuare il backup del contenuto delle seguenti cartelle:

```
/opt/dell/vsftpd/files/backup (obbligatorio)
```



/opt/dell/vsftpd/files/certificates (estremamente consigliato)

/opt/dell/vsftpd/files/support (facoltativo)

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

## Abilitare l'accesso remoto al database

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

**ⓘ | N.B.: Dell consiglia di abilitare l'accesso remoto al database solo se necessario.**

- 1 Dal menu *Configurazione avanzata*, selezionare **Accesso remoto database**.
- 2 Usare la barra spaziatrice per inserire una **X** nel campo Abilita accesso remoto al 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 dell'applicazione DDP si arrestano automaticamente.

## Abilitare il supporto del server DMZ

È possibile completare questa attività in qualsiasi momento. Non è necessaria per iniziare ad usare DDP Enterprise Server - VE. La procedura consigliata è riavviare i servizi ogni qual volta si apporta una modifica alle impostazioni.

- 1 Dal menu *Configurazione avanzata*, selezionare **Abilita supporto server DMZ**.
- 2 Usare la barra spaziatrice per inserire una **X** nel campo Abilita supporto server DMZ e selezionare **OK**.

**ⓘ | N.B.: Per usare la modalità proxy (Modalità DMZ), è necessario [installare e configurare la modalità proxy](#).**

# Attività dell'amministratore di DDP Enterprise Server - VE

## Impostare o cambiare la lingua di DDP Enterprise Server - VE 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.

## Verificare lo stato del server

Per verificare lo stato dei servizi di DDP Enterprise Server - VE, nel menu principale selezionare **Stato server**.

La tabella seguente descrive ciascun servizio e la relativa funzione.

| Nome  | Descrizione   |
|---|---|
| Dell Message Broker   | Bus di Enterprise Server  |
| Dell Identity Server  | Gestisce le richieste di autenticazione del dominio.  |
| Dell Compatibility Server   | Servizio per la gestione dell'architettura aziendale.   |
| Dell Security Server  | Fornisce il meccanismo di controllo dei comandi e della comunicazione con Active Directory. Usato per comunicare con Dell Policy Proxy.                             |
| Dell Compliance Reporter  | Fornisce una visualizzazione completa dell'ambiente per la creazione di rapporti di controllo e conformità.   |
| Dell Core Server  | Servizio per la gestione dell'architettura aziendale.   |
| Dell Core Server HA<br>(High Availability, Elevata disponibilità) | Un servizio ad elevata disponibilità che consente una maggiore sicurezza e migliori prestazioni delle connessioni HTTPS nella gestione dell'architettura aziendale. |
| Dell Inventory Server   | Elabora la coda di inventario.  |
| Dell Forensic Server  | Fornisce servizi Web per l'API Forensic.  |
| Dell Policy Proxy   | Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario.  |

DDP Enterprise Server - VE monitora e riavvia i propri servizi, se necessario.

**i 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**.



# Visualizzare i registri

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

Registro syslog Registro posta Registro autenticazione (SSH) Registro postgres Registro monitoraggio

- Registri di sistema
  - Registro syslog
  - Registro posta
  - Registro autenticazione (SSH)
  - Registro postgres
  - Registro monitoraggio
- Registri dei server
  - Compatibility Server
  - Security Server
  - Message Broker
  - Core Server
  - Core Server HA
  - Compliance Reporter
  - Identity Server
  - Inventory Server
  - Forensic Server
  - Policy Proxy
- Registro databasecustomizer

## Aprire l'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**.

Se l'utente ddpsupport è attivato, Dell ProSupport può recuperare il registro dal server SFTP di DDP Enterprise Server - VE. Se l'utente ddpsupport non è attivato, contattare Dell ProSupport. Per maggiori informazioni, consultare [Contattare Dell ProSupport](#).



# Manutenzione di DDP Enterprise Server - VE

È necessario rimuovere i backup non necessari di DDP Enterprise Server - VE.

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.



# Risoluzione dei problemi di DDP Enterprise Server - VE

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.](#)

# Attività di configurazione di postinstallazione

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

## Configurare VE per Data Guardian

Per configurare VE affinché supporti Data Guardian, nella Remote Management Console di VE impostare su Attivato il criterio Crittografia cloud. Per attivare la modalità Documenti Office protetti di Data Guardian, impostare su Attivato il criterio Documenti Office protetti.

Per le istruzioni di installazione del client Data Guardian, fare riferimento alla *Guida all'installazione avanzata di Enterprise Edition*, *Guida all'installazione di base di Enterprise Edition* o *Guida dell'utente di Data Guardian*.

## Installare e configurare Gestione EAS per Mobile Edition

Per usare Mobile Edition, è necessario installare e configurare Gestione EAS. Se non si intende usare Mobile Edition, ignorare questa sezione.

### Prerequisiti

- L'account di accesso per il servizio EAS Mailbox Manager deve disporre delle autorizzazioni per la creazione/modifica dei criteri di Exchange ActiveSync, l'assegnazione dei criteri alle cassette postali degli utenti e la richiesta di informazioni sui dispositivi ActiveSync.
- Per modificare i file e riavviare i servizi, è necessario eseguire l'Utilità di configurazione EAS con autorizzazioni di amministratore.
- È necessaria la connessione di rete a DDP Enterprise Server - VE.
- Tenere a portata di mano il nome host o l'indirizzo IP di DDP Enterprise Server - VE.
- La funzionalità Accodamento messaggi Microsoft (MSMQ) deve essere già installata/configurata nel server che ospita l'ambiente Exchange. In caso contrario, installare MSMQ 4.0 in Windows Server 2008 o Windows Server 2008 R2 (nel server che ospita l'ambiente Exchange) - <http://msdn.microsoft.com/en-us/library/aa967729.aspx>

### Durante il processo di distribuzione

Se si intende usare Exchange ActiveSync per gestire i dispositivi mobili tramite Mobile Edition, è necessario configurare l'ambiente di Exchange Server.

### Installare EAS Device Manager

- 1 Nel supporto di installazione di mobile Edition, accedere alla cartella Gestione EAS. Nella cartella EAS Device Manager, copiare setup.exe nei propri server *Accesso client di Exchange*.
- 2 Fare doppio clic su **setup.exe** per avviare l'installazione. Se l'ambiente include più di un server *Accesso client di Exchange*, eseguire questo programma di installazione in ciascuno di essi.
- 3 Selezionare la lingua di installazione, quindi fare clic su **OK**.
- 4 Fare clic su **Avanti** quando viene visualizzata la schermata *Introduzione*.
- 5 Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.
- 6 Fare clic su **Avanti** per installare EAS Device Manager nel percorso predefinito **C:\inetpub\wwwroot\Dell\EAS Device Manager\**.



- 7 Fare clic su **Installa** nella schermata *Pronta per l'installazione*.

Viene visualizzata una finestra di stato che mostra l'avanzamento dell'installazione.

- 8 Se lo si desidera, selezionare la casella di controllo per visualizzare il registro di Windows Installer e fare clic su **Fine**.

### Installare EAS Mailbox Manager

- 1 Nel supporto di installazione di mobile Edition, accedere alla cartella Gestione EAS. Nella cartella EAS Mailbox Manager, copiare setup.exe nei server *Cassette postali di Exchange*.
- 2 Fare doppio clic su **setup.exe** per avviare l'installazione. Se l'ambiente include più di un server *Cassette postali di Exchange*, eseguire questo programma di installazione in ciascuno di essi.
- 3 Selezionare la lingua di installazione, quindi fare clic su **OK**.
- 4 Fare clic su **Avanti** quando viene visualizzata la schermata *Introduzione*.
- 5 Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.
- 6 Fare clic su **Avanti** per installare EAS Mailbox Manager nel percorso predefinito **C:\Program Files\Dell\EAS Mailbox Manager\**.
- 7 Quando viene visualizzata la schermata *Informazioni di accesso*, immettere le credenziali dell'account utente che avrà accesso all'utilizzo di questo servizio.

Nome utente: DOMINIO\Nome utente

Password: la password associata al nome utente specificato

Fare clic su **Avanti**.

- 8 Fare clic su **Installa** nella schermata *Pronta per l'installazione*.

Viene visualizzata una finestra di stato che mostra l'avanzamento dell'installazione.

- 9 Se lo si desidera, selezionare la casella di controllo per visualizzare il registro di Windows Installer e fare clic su **Fine**.

### Usare l'utilità di configurazione EAS

- 1 Nello stesso computer, andare a **Start > Dell > Utilità di configurazione EAS > Configurazione EAS** per eseguire l'Utilità di configurazione EAS.
- 2 Fare clic su **Installazione** per configurare le impostazioni di Gestione EAS.
- 3 Immettere le informazioni seguenti:

Nome host di DDP Enterprise Server - VE

Intervallo di polling Dell Policy Proxy (l'impostazione predefinita è 1 minuto)

Selezionare la casella per l'esecuzione di EAS Device Manager in modalità Solo rapporto (procedura consigliata durante la distribuzione).

#### **N.B.:**

La modalità Solo rapporto consente a dispositivi/utenti sconosciuti di accedere a Exchange ActiveSync, ma fornisce comunque all'utente un rapporto sul traffico. Una volta avviata la distribuzione, è possibile modificare questa impostazione per aumentare la sicurezza.

Fare clic su **OK**.

- 4 Viene visualizzato il messaggio di completamento dell'operazione. Fare clic su **Si** per riavviare i servizi IIS e EAS Mailbox Manager.
- 5 Al termine, fare clic su **Esci**.

### Dopo il processo di distribuzione

Una volta avviata la distribuzione e si è pronti per aumentare la sicurezza, attenersi alla procedura riportata di seguito.

## Nei server Cassette postali di Exchange

- 1 Andare a **Start > Dell > Utilità di configurazione EAS > Configurazione EAS** per eseguire l'Utilità di configurazione EAS.
- 2 Fare clic su **Installazione** per configurare le impostazioni di Gestione EAS.
- 3 Immettere le informazioni seguenti:

Nome host di DDP Enterprise Server - VE

Intervallo di polling Dell Policy Proxy (l'impostazione predefinita è 1 minuto)

Selezionare la casella per l'esecuzione di EAS Device Manager in modalità Solo rapporto.

Fare clic su **OK**.

- 4 Viene visualizzato il messaggio di completamento dell'operazione. Fare clic su **SI** per riavviare i servizi IIS e EAS Mailbox Manager.
- 5 Al termine, fare clic su **Esci**.

## Abilitare il controllo della catena di attendibilità di Manager

Se viene usato un certificato autofirmato nel server VE 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 server VE. 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 abilitare la convalida dell'attendibilità SSL/TLS, nel computer client modificare il valore della seguente voce del registro su 0:

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

DisableSSLCertTrust=REG\_DWORD (32-bit):0



# Attività dell'amministratore della Remote Management Console di VE

## Assegnare un ruolo amministratore Dell

- 1 Come amministratore Dell, accedere alla Remote Management Console 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 si desidera 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 Remote Management ConsoleEnterprise Server.
- 2 Accedere alla Remote Management ConsoleEnterprise Server con le credenziali dell'utente di dominio.  
Fare clic su "?" nell'angolo in alto a destra della Remote Management Console per avviare la *Guida dell'amministratore di Dell Data Protection*. Viene visualizzata la pagina iniziale. Fare clic su **Aggiungi domini**.

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

- I computer Windows verranno crittografati
- I computer con unità autocrittografanti verranno crittografati
- I computer Windows con Hardware Crypto Accelerator verranno crittografati
- BitLocker Management non è abilitato
- Advanced Threat Protection non è abilitato
- Threat Protection è abilitato
- I supporti esterni non verranno crittografati

- I dispositivi connessi alle porte non verranno crittografati
- Data Guardian è attivato
- Mobile Edition non è abilitato

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

## Eeguire 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 Immettere una descrizione della modifica nel campo Commento.
- 3 Fare clic su **Commit criteri**.



## Porte delle soluzioni

La tabella seguente descrive ciascun componente e la relativa funzione.

| Nome   | Porta predefinita | Descrizione  | Richiesto per   |
|--|-------------------|--|-----------------|
| Compliance Reporter  | HTTP(S)/8084      | Fornisce una visualizzazione completa dell'ambiente per la creazione di rapporti di controllo e conformità.<br><br>Un componente di DDP Enterprise Server - VE.  | Creare rapporti |
| Remote Management Console                                    | HTTPS/8443        | Console di amministrazione e centro di controllo per la distribuzione a livello aziendale.<br><br>Un componente di DDP Enterprise Server - VE.   | Tutti           |
| Core Server  | HTTPS/8888        | Gestisce il flusso dei criteri, le licenze e la registrazione per l'autenticazione di preavviso, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection. Elabora i dati di inventario utilizzati da Compliance Reporter e dalla Remote Management Console. Raccoglie e archivia i dati di autenticazione. Controlla l'accesso basato sui ruoli.<br><br>Un componente di DDP Enterprise Server - VE. | Tutti           |
| Core Server HA<br>(High Availability, Elevata disponibilità) | HTTPS/8888        | Servizio ad elevata disponibilità che consente una maggiore sicurezza e migliori prestazioni delle connessioni HTTPS con la Remote Management Console, l'autenticazione di preavviso, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection.<br><br>Un componente di DDP Enterprise Server - VE.   | Tutti           |
| Security Server  | HTTPS/8443        | Comunica con Policy Proxy, gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, i prodotti Data Guardian e la comunicazione SED-PBA.<br><br>Un componente di DDP Enterprise Server - VE.  | Tutti           |
| 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 in questo servizio.<br><br>Un componente di DDP Enterprise Server - VE.  | Tutti           |
| Message Broker Service                                       | TCP/61616         | Gestisce la comunicazione tra i servizi di DDP Enterprise Server - VE. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy.   | Tutti           |



| Nome                       | Porta predefinita   | Descrizione  | Richiesto per  |
|----------------------------|---|--|--|
|                            | e STOMP/61613<br>(chiusa o, se configurata per DMZ, 61613 è aperta) | Un componente di DDP Enterprise Server - VE.   |  |
| Identity Server            | HTTPS/8445  | Gestisce le richieste di autenticazione del dominio, inclusa l'autenticazione di SED Manager.<br><br>Richiede un account di Active Directory.<br><br>Un componente di DDP Enterprise Server - VE.  | Tutti  |
| Forensic Server            | HTTPS/8448  | Consente agli amministratori che dispongono dei privilegi appropriati di ottenere dalla Remote Management Console le chiavi di crittografia, da usare per sbloccare i dati o per le attività di decrittografia.<br><br>Un componente di DDP Enterprise Server - VE.  | API Forensic   |
| Inventory Server           | 8887  | Elabora la coda di inventario.<br><br>Un componente di DDP Enterprise Server - VE.   | Tutti  |
| Policy Proxy               | TCP/<br>8000/8090   | Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario.<br><br>Un componente di DDP Enterprise Server - VE.   | Enterprise Edition per Mac<br><br>Enterprise Edition per Windows<br><br>Mobile Edition |
| LDAP                       | 389/636,<br>3268/3269<br><br>RPC - 135, 49125+                      | <b>Porta 3268</b> - 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.<br><br><b>Porta 389</b> - 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. | Tutti  |
| Autenticazione client      | HTTPS/8449  | Consente ai server client di eseguire l'autenticazione a DDP Enterprise Server - VE.   | Crittografia server  |
| Beacon richiamata          | HTTP/8446   | Consente di inserire un beacon richiamata in ciascun file Office protetto, quando si esegue la modalità Office protetto di Data Guardian.  | Data Guardian  |
| Advanced Threat Prevention | HTTPS/TCP/443   | Comunicazione client se si usa Advanced Threat Protection  | Advanced Threat Prevention   |



| Nome                | Porta predefinita | Descrizione   | Richiesto per   |
|---------------------|-------------------|---|---|
| EAS Device Manager  | N/D               | Abilita la funzionalità over-the-air. Installato nel server Accesso client di Exchange. | Gestione di Exchange ActiveSync dei dispositivi mobili. |
| EAS Mailbox Manager | N/D               | L'agente della cassetta postale installato nel server Cassetta postali di Exchange.     | Gestione di Exchange ActiveSync dei dispositivi mobili. |

Sincronizzazione ora NTP: TCP e UDP/123 (per maggiori informazioni, fare riferimento a <https://help.ubuntu.com/its/serverguide/NTP.html>.)

