

Dell Data Protection

Guida alla migrazione e all'installazione di Enterprise
Server 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.

I marchi registrati e i marchi commerciali utilizzati nella suite 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. La gestione delle licenze è basata sulla licenza GNU LGPL + restrizioni unRAR (7-zip.org/license.txt).

Guida alla migrazione e all'installazione di Enterprise Server

2017 - 04

Rev. A01

1 Introduzione a Dell Enterprise Server.....	5
Informazioni su Dell Enterprise Server.....	5
Contattare Dell ProSupport.....	5
2 Requisiti e architettura per Dell Enterprise Server.....	6
Requisiti di Dell Enterprise Server.....	6
Prerequisiti di Dell Enterprise Server.....	6
Hardware di Dell Enterprise Server.....	6
Software di Dell Enterprise Server.....	7
Supporto lingue di Dell Enterprise Server.....	9
Progettazione dell'architettura di Dell Enterprise Server.....	9
3 Configurazione di preinstallazione.....	15
Configurazione.....	15
4 Installazione o aggiornamento/migrazione.....	21
Prima di iniziare l'installazione o l'aggiornamento/migrazione.....	21
Nuova installazione.....	22
Installare un server back-end e un nuovo database.....	22
Installare un server back-end con un database esistente.....	26
Installare server front-end.....	30
Aggiornamento/migrazione.....	32
Prima di iniziare l'aggiornamento/migrazione.....	32
Eseguire l'aggiornamento/la migrazione dei server back-end.....	34
Eseguire l'aggiornamento/la migrazione dei server front-end.....	36
Installazione in modalità disconnessa.....	36
Installare Enterprise Server in modalità disconnessa.....	39
Disinstallare Dell Enterprise Server.....	40
5 Configurazione di postinstallazione.....	41
Installazione e configurazione di Gestione EAS.....	41
Installare EAS Device Manager.....	41
Installare EAS Mailbox Manager.....	42
Usare l'utilità di configurazione EAS.....	42
Configurare le impostazioni di Gestione EAS.....	42
Dell Security Server nella configurazione in modalità DMZ.....	43
Usare Keytool per importare il certificato di dominio DMZ.....	43
Modificare il file application.properties.....	44
Registrazione dell'APNs.....	44
Server Configuration Tool.....	45
Aggiungere certificati nuovi o aggiornati.....	45
Importare un certificato di Dell Manager.....	48
Importare un certificato di identità.....	49

Configurare le impostazioni per il Certificato SSL server o Mobile Edition.....	49
Configurare le impostazioni SMTP per Data Guardian o servizi e-mail.....	49
Modificare nome del database, percorso o credenziali.....	50
Migrare il database.....	51
6 Attività di amministrazione.....	52
Assegnare un ruolo amministratore Dell.....	52
Accedere con ruolo amministratore Dell.....	52
Caricare la licenza di accesso client.....	52
Eseguire il commit dei criteri.....	52
Configurare Dell Compliance Reporter.....	53
Configurare l'autenticazione SQL con Compliance Reporter.....	53
Configurare l'autenticazione di Windows con Compliance Reporter.....	53
Eseguire i backup.....	54
Backup di Enterprise Server.....	54
Backup di SQL Server.....	54
Backup di PostgreSQL Server.....	54
7 Descrizioni dei componenti Dell.....	55
8 Procedure consigliate per SQL Server.....	57
9 Certificati.....	58
Creare un certificato autofirmato e generare una richiesta di firma del certificato.....	58
Generare una nuova coppia di chiavi e un certificato autofirmato.....	58
Richiedere un certificato firmato da un'Autorità di certificazione.....	59
Importare un certificato radice.....	60
Metodo di esempio per richiedere un certificato.....	60
Esportare un certificato in .PFX usando la console di gestione dei certificati.....	61
Aggiungere un certificato attendibile per la firma al Security Server quando è stato usato un certificato non attendibile per SSL.....	62



Introduzione a Dell Enterprise Server

Informazioni su Dell Enterprise Server

Enterprise Server rappresenta la parte di amministrazione della sicurezza della soluzione Dell. La Remote Management Console consente agli amministratori di monitorare lo stato degli endpoint, l'applicazione dei criteri e la protezione in tutta l'azienda.

Enterprise Server ha le seguenti funzioni:

- Gestione centralizzata dei 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

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. 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 e architettura per Dell Enterprise Server

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

Requisiti di Dell Enterprise Server

I componenti di Dell Enterprise Server hanno altri requisiti hardware e software, oltre al software fornito nel supporto di installazione Dell. Prima di continuare con le attività di installazione o aggiornamento/migrazione, accertarsi che l'ambiente di installazione soddisfi i requisiti.

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

Prerequisiti di Dell Enterprise Server

La tabella seguente descrive in dettaglio il software che deve essere presente prima di installare Dell Enterprise Server. I collegamenti e le istruzioni per installare questi prerequisiti sono descritti in dettaglio in [Configurazione di preinstallazione](#).

Ciascun software applicabile deve essere installato prima di avviare l'installazione, a meno che l'elemento venga installato dal programma di installazione. In caso contrario, l'installazione non andrà a buon fine.

Hardware di Dell Enterprise Server

Prerequisiti

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

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

- **Visual C++ 2013 Redistributable Package**

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

- **Visual C++ 2015 Redistributable Package**

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

- **.NET Framework versione 3.5 SP1**

- **.NET Framework versione 4.5**

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

- **SQL Native Client 2012**

Se si utilizza SQL Server 2012 o SQL Server 2016.

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

La tabella seguente descrive in dettaglio i requisiti hardware *minimi* per Dell Enterprise Server. Consultare [Progettazione dell'architettura di Dell Enterprise Server](#) per ulteriori informazioni sulla scalabilità in base alle dimensioni della propria distribuzione.

Requisiti hardware

Processore

CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

CPU Quad-Core moderna (2 GHz+) per configurazione con server singolo

RAM

8 GB minimo, a seconda della configurazione

16 GB per configurazione con server singolo

Spazio libero su disco

+/- 1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale)

20 GB o più di spazio libero su disco (oltre allo spazio per il paging virtuale) per configurazione con server singolo

Scheda di rete

Scheda di interfaccia di rete 10/100/1000

Varie

TCP/IPv4 installato e attivato

Software di Dell Enterprise Server

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

- i** **N.B.:** Prima dell'installazione, disabilitare il controllo dell'account utente ed è necessario riavviare il server per rendere effettiva tale modifica. In Windows Server 2012 R2 e Windows Server 2016, il programma di installazione disabilita il controllo dell'account utente.
- i** **N.B.:** I percorsi dei registri di sistema di Dell Policy Proxy (se installato): HKLM\SOFTWARE\Wow6432Node\Dell
- i** **N.B.:** Percorso del registro di sistema per i Windows Server: HKLM\SOFTWARE\Dell.

Dell Enterprise Server - Server back-end e server front-end Dell

- **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



Server Exchange ActiveSync

Se si intende usare Mobile Edition, sono supportati i seguenti server Exchange ActiveSync. Questo componente è installato nel server Exchange front-end.

- Exchange ActiveSync 12.0 - componente di Exchange Server 2007
- Exchange ActiveSync 12.1 - componente di Exchange Server 2007 SP1
- Exchange ActiveSync 14.0 - componente di Exchange Server 2010
- Exchange ActiveSync 14.1 - componente di Exchange Server 2010 SP1

Accodamento messaggi Microsoft (MSMQ) deve essere installato/configurato nel server Exchange.

Archivio LDAP

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

Ambienti virtuali consigliati per i componenti di Dell Enterprise Server

Dell Enterprise Server può essere facoltativamente installato in un ambiente virtuale. Si consigliano solo i seguenti ambienti.

Dell Enterprise Server v9.7 è stato convalidato con server Hyper-V (installazione completa o base), e come ruolo in Windows Server 2012 R2 o Windows Server 2016.

- Server Hyper-V (installazione completa o 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 Hyper-V
 - Almeno 4 GB di RAM per la risorsa immagine dedicata
 - Deve essere eseguito come macchina virtuale di Generazione 1
 - Per maggiori informazioni, consultare <https://technet.microsoft.com/en-us/library/hh923062.aspx>

Dell Enterprise Server v9.7 è stato convalidato con VMware ESXi 5.5 e VMware ESXi 6.0. Accertarsi che tutte le patch e gli aggiornamenti siano applicati immediatamente a VMware ESXi al fine di affrontare potenziali vulnerabilità.

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

- VMware ESXi 5.5
 - Richiesta CPU x86 a 64 bit
 - Computer host con almeno due core
 - Almeno 8 GB di RAM consigliati
 - 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>
- 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>

ⓘ | N.B.: Il database di SQL Server che ospita Dell Enterprise Server deve essere eseguito in un computer separato.

Database

- **SQL Server 2008 e SQL Server 2008 R2** - Standard Edition/Enterprise Edition
- **SQL Server 2008 SP4 (con KB3045311)** - Standard Edition/Enterprise Edition
- **SQL Server 2012** - Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2014** - Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2016** - Standard Edition/Enterprise Edition

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

Compliance Reporter e Remote Management Console di Dell Data Protection

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

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

Supporto lingue di Dell Enterprise Server

La Remote Management Console dispone dell'interfaccia utente multilingue (MUI, Multilingual User Interface) e supporta le seguenti lingue:

Supporto lingue

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

Progettazione dell'architettura di Dell Enterprise Server

Le soluzioni Dell Encryption, Endpoint Security Suite ed Endpoint Security Suite Enterprise sono prodotti altamente scalabili e vengono scalate in base alle dimensioni della propria organizzazione e al numero di endpoint destinati alla crittografia. La presente sezione offre una serie di linee guida per scalare l'architettura per 5.000-60.000 endpoint.

ⓘ | N.B.: Se l'organizzazione dispone di oltre 50.000 endpoint, contattare Dell ProSupport per assistenza.



i N.B.:

Tutti i componenti elencati in tutte le sezioni includono le specifiche hardware minime necessarie per garantire prestazioni ottimali nella maggior parte degli ambienti. Non allocando le risorse adeguate ad uno qualsiasi dei componenti elencati, si potrebbe causare la riduzione delle prestazioni o problemi di funzionalità dell'applicazione.

Fino a 5.000 endpoint

Questa architettura è adatta per la maggior parte delle aziende medio-piccole con un numero di endpoint compreso tra 1 e 5.000. Tutti i componenti di Dell Enterprise Server possono essere installati in un unico server. Facoltativamente, è possibile posizionare un server front-end nella DMZ per la pubblicazione dei criteri e/o per l'attivazione degli endpoint tramite Internet.

Componenti dell'architettura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard o Enterprise Edition

Windows Server 2012 R2 - Standard o Datacenter Edition

Windows Server 2016 - Standard o Datacenter Edition

Configurazione con server singolo

16 GB; 20 GB o più di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Quad-Core moderna (2 GHz+)

Configurazione del server quando usata per server front-end

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

Server front-end esterno Dell

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard o Enterprise Edition

Windows Server 2012 R2 - Standard o Datacenter Edition

Windows Server 2016 - Standard o Datacenter Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (con KB3045311) Standard Edition / Enterprise Edition

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

Da 5.000 a 20.000 endpoint

Questa architettura è adatta per ambienti con un numero di endpoint compreso tra 5.000 e 20.000. Per distribuire il carico aggiuntivo, viene aggiunto un server front-end progettato per gestire circa 15.000 - 20.000 endpoint. Facoltativamente, è possibile posizionare un server front-end nella DMZ per la pubblicazione dei criteri e/o per l'attivazione degli endpoint tramite Internet.

Componenti dell'architettura



Dell Enterprise Server

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

Server front-end interno Dell (1) e server front-end esterno Dell (1)

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard o Enterprise Edition

Windows Server 2012 R2 - Standard o Datacenter Edition

Windows Server 2016 - Standard o Datacenter Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (con KB3045311) Standard Edition / Enterprise Edition

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

Da 20.000 a 40.000 endpoint

Questa architettura è adatta per ambienti con un numero di endpoint compreso tra 20.000 e 40.000. Viene aggiunto un altro server front-end per distribuire il carico aggiuntivo. Ogni server front-end è progettato per gestire circa 15.000 - 20.000 endpoint. Facoltativamente, è possibile posizionare un server front-end nella DMZ per l'attivazione degli endpoint e/o la pubblicazione dei criteri negli endpoint in Internet.

Componenti dell'architettura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard o Enterprise Edition

Windows Server 2012 R2 - Standard o Datacenter Edition

Windows Server 2016 - Standard o Datacenter Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

Server front-end interni Dell (2) e server front-end esterno Dell (1)

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard o Enterprise Edition

Windows Server 2012 R2 - Standard o Datacenter Edition

Windows Server 2016 - Standard o Datacenter Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (con KB3045311) Standard Edition / Enterprise Edition



SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

Da 40.000 a 60.000 endpoint

Questa architettura è adatta per ambienti con un numero di endpoint compreso tra 40.000 e 60.000. Viene aggiunto un altro server front-end per distribuire il carico aggiuntivo. Ogni server front-end è progettato per gestire circa 15.000 - 20.000 endpoint. Facoltativamente, è possibile posizionare un server front-end nella DMZ per l'attivazione degli endpoint e/o la pubblicazione dei criteri negli endpoint in Internet.

i N.B.:

Se l'organizzazione dispone di oltre 50.000 endpoint, contattare Dell ProSupport per assistenza.

Componenti dell'architettura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard o Enterprise Edition

Windows Server 2012 R2 - Standard o Datacenter Edition

Windows Server 2016 - Standard o Datacenter Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

Server front-end interni Dell (2) e server front-end esterno Dell (1)

Windows Server 2008 R2 SP0-SP1 64-bit/Windows Server 2008 SP2 64-bit - Standard o Enterprise Edition

Windows Server 2012 R2 - Standard o Datacenter Edition

Windows Server 2016 - Standard o Datacenter Edition

8 GB minimo in base alla configurazione; +-1,5 GB di spazio libero su disco (oltre allo spazio per il paging virtuale); CPU Dual-Core moderna minima (2 GHz+), inclusi Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium o AMD equivalente

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (con KB3045311) Standard Edition / Enterprise Edition

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

Considerazioni sulla disponibilità elevata

Questa architettura rappresenta un'architettura a disponibilità elevata che supporta fino a 60.000 endpoint. In una configurazione attiva/passiva, sono installati due Dell Enterprise Server. Per eseguire il failover al secondo Dell Enterprise Server, arrestare i servizi sul nodo primario e indirizzare l'alias DNS (CNAME) al secondo nodo. Avviare i servizi sul secondo nodo e la Remote Management Console per accertarsi che l'applicazione funzioni correttamente. I servizi sul secondo nodo (passivo) devono essere configurati come "Manuale" al fine di prevenirne l'avvio accidentale durante le regolari operazioni di manutenzione e applicazione delle patch.

L'organizzazione può inoltre scegliere di avere un server database del cluster SQL. In questa configurazione, il Dell Enterprise Server deve essere configurato in modo da usare l'IP o il nome host del cluster.

N.B.:
La replica del database non è supportata.

Il traffico dei client è distribuito su tre server front-end interni. Facoltativamente, è possibile posizionare più server front-end nella DMZ per l'attivazione degli endpoint e/o per la pubblicazione dei criteri negli endpoint in Internet.

Virtualizzazione

Dell Enterprise Server può essere facoltativamente installato in un ambiente virtuale. Si consigliano solo i seguenti ambienti.

Dell Enterprise Server v9.7 è stato convalidato con server Hyper-V (installazione completa o base), e come ruolo in Windows Server 2012 R2 o Windows Server 2016.

- Server Hyper-V (installazione completa o 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 Hyper-V
 - Almeno 4 GB di RAM per la risorsa immagine dedicata
 - Deve essere eseguito come macchina virtuale di Generazione 1
 - Per maggiori informazioni, consultare <https://technet.microsoft.com/en-us/library/hh923062.aspx>

Dell Enterprise Server v9.7 è stato convalidato con VMware ESXi 5.5 e VMware ESXi 6.0. Accertarsi che tutte le patch e gli aggiornamenti siano applicati immediatamente a VMware ESXi al fine di affrontare potenziali vulnerabilità.

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

- VMware ESXi 5.5
 - Richiesta CPU x86 a 64 bit
 - Computer host con almeno due core
 - Almeno 8 GB di RAM consigliati
 - 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>
- 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>

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

SQL Server



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

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



Configurazione di preinstallazione

Prima di iniziare, leggere le *Consulenze tecniche di Enterprise Server* per eventuali soluzioni alternative correnti o problemi noti che riguardano Dell Enterprise Server.

La configurazione di preinstallazione del/i server in cui si intende installare Dell Enterprise Server è molto importante. Prestare attenzione a questa sezione per garantire l'installazione corretta di Dell Enterprise Server.

Configurazione

- 1 Se abilitata, disattivare Protezione avanzata (ESC, Enhanced Security Configuration) di Internet Explorer. Aggiungere l'URL del server ai siti attendibili dalle opzioni di sicurezza del browser. Riavviare il server.
- 2 Aprire le seguenti porte per ciascun componente:

Interna:

Comunicazione Active Directory: TCP/389

Comunicazione tramite posta elettronica (opzionale): 25

Su front-end (se necessario):

Comunicazione da Dell Policy Proxy esterno a Dell Message Broker: TCP/61616 e STOMP/61613

Comunicazione a Dell Security Server back-end: HTTPS/8443

Comunicazione a Dell Core Server back-end: HTTPS/8888 e 9000

Comunicazione alle porte RMI - 1099

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

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

Esterna (se necessario):

Database SQL: TCP/1433

Remote Management Console: HTTPS/8443

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

Dell Compatibility Server: TCP/1099

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

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 e 9000 (8888 configurata automaticamente all'installazione)



Dell Device Server: HTTP(S)/8443 (Dell Enterprise Server v7.7 o successiva) o HTTP(S)/8081 (Dell Enterprise Server precedente alla v7.7)

Dell Key Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell Security Server: HTTPS/8443

Autenticazione client: HTTPS/8449 (se si usa Server Encryption)

Comunicazione client, se si utilizza Advanced Threat Prevention: HTTPS/TCP/443

N.B.:

Se i client 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 (è possibile che non si tratti del server in cui è in esecuzione Enterprise 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 dei diritti non sarà utilizzabile. Per maggiori informazioni, consultare la [Guida all'installazione avanzata di Enterprise Edition](#).

Creare un database Dell

- 3 Se non si dispone ancora di un database SQL configurato per Dell Enterprise Server, il programma di installazione crea il database durante l'installazione. Se si preferisce impostare un database prima di installare Dell Enterprise Server, seguire le istruzioni seguenti per creare sia il database che l'utente SQL in SQL Management Studio. **Queste istruzioni sono facoltative in quanto il programma di installazione creerà un database per l'utente solo se non è già esistente.**

Quando si installa Dell Enterprise Server, seguire le istruzioni in [Installare un server back-end con un database esistente](#).

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

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

Quando si utilizza un'istanza SQL Server non predefinita, dopo l'installazione di Dell Enterprise Server occorre specificare la porta dinamica di tale istanza nella scheda Database del Server Configuration Tool. Per ulteriori informazioni, consultare [Server Configuration Tool](#). In alternativa, abilitare il servizio SQL Server Browser e accertarsi che la porta UDP 1434 sia aperta. Per maggiori informazioni, consultare [https://msdn.microsoft.com/en-us/library/510203\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/510203(v=sql.120).aspx).

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

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

Creare un nuovo database di Windows SQL Server usando l'Autenticazione di Windows:

- a Fare clic su **Start > Tutti i programmi > Microsoft SQL Server > Management Studio**.
- b Fare clic con il pulsante destro del mouse sulla cartella Database, quindi fare clic su Nuovo database. Viene visualizzata la finestra di dialogo Proprietà database.
- c Immettere il Nome database e fare clic su **OK**.
- d Espandere la cartella *Sicurezza*, quindi fare clic con il pulsante destro del mouse su **Account di accesso**.
- e Fare clic su **Nuovo account accesso** per creare un proprietario del nuovo database.
- f Immettere un nome utente nel campo *Nome*.
- g Selezionare l'opzione di autenticazione *Autenticazione di Windows*.

- h Selezionare **Mapping utenti**, quindi evidenziare il nuovo database.
- i Selezionare il ruolo del database (db_owner) e fare clic su **OK**.

OPPURE

Creare un nuovo database di SQL Server usando Autenticazione di SQL Server:

- a Fare clic su **Start > Tutti i programmi > Microsoft SQL Server > Management Studio**.
- b Fare clic con il pulsante destro del mouse sulla cartella *Database*, quindi fare clic su **Nuovo database**. Viene visualizzata la finestra di dialogo *Proprietà database*.
- c Immettere il Nome database e fare clic su **OK**.
- d Espandere la cartella *Sicurezza*, quindi fare clic con il pulsante destro del mouse su **Account di accesso**.
- e Fare clic su **Nuovo account accesso** per creare un proprietario del nuovo database.
- f Immettere un nome utente nel campo *Nome*.
- g Selezionare l'opzione di autenticazione *Autenticazione di SQL Server*. Immettere e confermare la password.
- h Deselezionare **Imponi scadenza password**.
- i Selezionare **Mapping utenti** quindi evidenziare il nuovo database.
- j Selezionare il ruolo del database (db_owner) e fare clic su **OK**.

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

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

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

Installare .NET Framework 4.5

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

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

Installare SQL Native Client 2012

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

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

Configurare Microsoft CA (MSCEP)

È necessario completare questa procedura nel server in cui è in esecuzione MSCEP solo se si intende usare iOS con Mobile Edition.

- 7 Configurare MSCEP.

Windows Server 2008 R2 deve essere Enterprise Edition. **Standard Edition non consente l'installazione del ruolo MSCEP.**

- a Aprire Server Manager. Nel menu a sinistra, selezionare **Ruoli server** e selezionare la casella di controllo **Servizi certificati Active Directory**. Fare clic su **Avanti**. L'Aggiunta guidata ruoli prosegue con le fasi successive.

In *AD CS > Servizi ruolo*, selezionare le caselle di controllo per i servizi ruolo **Autorità di certificazione** e **Registrazione Web Autorità di certificazione**. Selezionare **Aggiungi servizi ruolo necessari per Server Web (IIS)** (se richiesto). Fare clic su **Avanti**.

In *AD CS > Tipo di installazione*, selezionare **Autonomo**. Fare clic su **Avanti**.

In *AD CS > Tipo di CA*, selezionare **CA subordinata**. Fare clic su **Avanti**.

In *AD CS > Chiave privata*, selezionare **Crea una nuova chiave privata**. Fare clic su **Avanti**.



In *AD CS > Chiave privata > Crittografia*, mantenere le impostazioni predefinite di **N. RSA del provider di archiviazione chiavi del software Microsoft, 2048 e SHA1**. Fare clic su **Avanti**.

In *AD CS > Chiave privata > Nome CA*, lasciare tutti i valori predefiniti. Fare clic su **Avanti**.

In *AD CS > Chiave privata > Richiesta certificato*, selezionare **Invia una richiesta di certificato a una CA padre**. Selezionare **Sfoggia per: Nome CA**. Sfogliare e selezionare **CA padre**. Fare clic su **Avanti**.

In *AD CS > Database certificati*, lasciare i valori predefiniti. Fare clic su **Avanti**.

In *Server Web (IIS)*, fare clic su **Avanti**.

In *Server Web (IIS) > Servizi ruolo*, lasciare i valori predefiniti. Fare clic su **Avanti**.

In *Conferma*, fare clic su **Installa**.

In *Risultati*, esaminarli e fare clic su **Chiudi**.

In *Server Manager > Ruoli*, selezionare **Aggiungi servizi ruolo** in *Servizi certificati Active Directory*.

Quando viene visualizzata la finestra *Seleziona servizi ruolo*, selezionare la casella di controllo per **Servizio Registrazione dispositivi di rete**. Fare clic su **Avanti**.

Aggiungere l'account utente che *Servizio Registrazione dispositivi di rete* deve usare quando autorizza le richieste di certificati al Gruppo utenti di IIS_IUSRS del server locale. Il formato è Dominio\Nome utente. Fare clic su **OK**.

Nella finestra *Specifica account utente*, selezionare l'utente che è stato appena aggiunto al gruppo IIS_IUSRS. Fare clic su **Avanti**.

Nella finestra *Indicazione delle informazioni sull'Autorità registrazione*, lasciare i valori predefiniti per *Informazioni necessarie e Aggiungi informazioni facoltative* se lo si desidera. Fare clic su **Avanti**.

Nella finestra *Configurazione della crittografia per l'Autorità registrazione*, lasciare i valori predefiniti. Fare clic su **Avanti**.

Nella finestra *Conferma selezioni per l'installazione*, fare clic su **Installa**.

Nella finestra *Risultati installazione*, rivedere i risultati e fare clic su **Chiudi**.

Chiudere Server Manager.

- b Modificare la chiave di registro come segue:

```
HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword
```

```
"EnforcePassword"=dword:00000000
```

- c Aprire Gestione IIS. Andare a **\<ServerName> \Sites\Default Web Site\CertSrv\mscep_admin**.

Aprire *Autenticazione* e abilitare **Autenticazione anonima**.

- d Fare clic su **Start > Esegui**. Digitare *certsrv.msc* e fare clic su **Invio**.

Quando viene visualizzata la finestra *certsrv*, fare clic con il pulsante destro del mouse sul nome del server, selezionare **Proprietà** e fare clic sulla scheda **Modulo criterio**.

Fare clic su **Proprietà** e selezionare **Utilizza le impostazioni contenute nel modello di certificato. Altrimenti, emetti automaticamente il certificato**. Fare clic su **OK**.

- e Chiudere Gestione IIS.

- f Riavviare il server. Per verificare, aprire Internet Explorer e nella barra degli indirizzi, immettere

```
http://server.domain.com/certsrv/mscep_admin/.
```

L'installazione di MSCEP Windows Server 2008 R2 è completata.

Windows Server 2012 R2 o Windows Server 2016:

- a Seguire le istruzioni di installazione nell'articolo: [Network Device Enrollment Service \(NDES\) in Active Directory Certificate Services \(AD CS\)](#) (Servizio Registrazione dispositivi di rete nei Servizi certificati Active Directory).
- b Modificare la chiave di registro come segue:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000
- c Aprire Gestione IIS. Andare a `\<Nome server>\Sites\Default Web Site\CertSrv\mscep_admin`.

Aprire *Autenticazione* e abilitare **Autenticazione anonima**.
- d Fare clic su **Start > Esegui**. Digitare `certsrv.msc` e fare clic su **Invio**.

Quando viene visualizzata la finestra `certsrv`, fare clic con il pulsante destro del mouse sul nome del server, selezionare **Proprietà** e fare clic sulla scheda **Modulo criterio**.

Fare clic su **Proprietà** e selezionare **Utilizza le impostazioni contenute nel modello di certificato. Altrimenti, emetti automaticamente il certificato**. Fare clic su **OK**.
- e Chiudere Gestione IIS.
- f Riavviare il server. Per verificare, aprire Internet Explorer e nella barra degli indirizzi, immettere

`http://server.domain.com/certsrv/mscep_admin/`.

L'installazione di MSCEP Windows Server 2012 R2/Windows Server 2016 è completata.

Installare/Configurare Accodamento messaggi Microsoft (MSMQ)

Questa fase deve essere completata solo se si intende usare Mobile Edition. Si tratta di un prerequisito affinché EAS Device Manager ed EAS Mailbox Manager siano in grado di comunicare.

- 8 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>

OPPURE

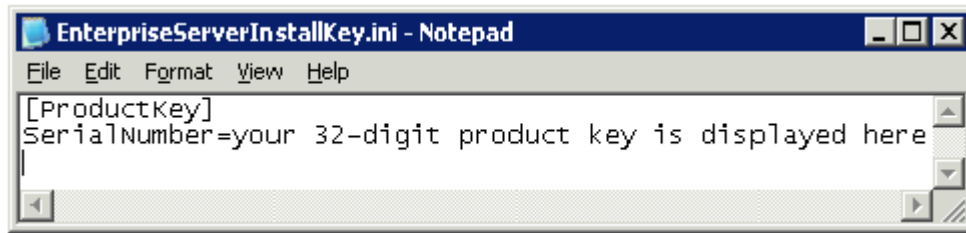
In Windows Server 2012 R2:

- a Aprire Server Manager.
- b Passare a **Gestisci > Aggiungi ruoli e funzionalità**.
- c Nella schermata Prima di iniziare, fare clic su **Avanti**.
- d Selezionare **Installazione basata su ruoli o basata su funzionalità** e fare clic su **Avanti**.
- e Selezionare il server in cui installare la funzionalità e fare clic su **Avanti**.
- f Non selezionare ruoli server. Fare clic su **Avanti**.
- g In Funzionalità, selezionare **Accodamento messaggi** e fare clic su **Installa**.

Facoltativo

- 9 **Per una nuova installazione:** copiare il Product Key (il nome del file è `EnterpriseServerInstallKey.ini`) in `C:\Windows` per popolare automaticamente il Product Key di 32 caratteri nel programma di installazione di Dell Enterprise Server.





La configurazione di preinstallazione del server è completa. Continuare con [Installare o aggiornare/migrare](#).

Installazione o aggiornamento/migrazione

Questo capitolo fornisce le istruzioni per quanto segue:

- [Nuova installazione](#) - Per installare un nuovo Dell Enterprise Server.
- [Aggiornamento/migrazione](#) - Per eseguire l'aggiornamento da un Dell Enterprise Server v8.0, o successiva, esistente e funzionale.
- [Disinstallare Dell Enterprise Server](#) - Per rimuovere l'installazione in uso, se necessario.

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

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

Prima di iniziare, accertarsi di aver completato la procedura appropriata di [Configurazione di preinstallazione](#).

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

Se il controllo dell'account utente (UAC) è abilitato, è necessario disabilitarlo. In Windows Server 2012 R2, il programma di installazione disabilita il controllo dell'account utente ed è necessario riavviare il server per rendere effettiva tale modifica.

Durante l'installazione, per impostare il database sono richieste le credenziali di Autenticazione di Windows o SQL. Se si seleziona l'Autenticazione di Windows, vengono usate le credenziali dell'utente connesso. L'utente deve disporre dei diritti di amministratore del sistema e dei diritti per creare e gestire il database SQL (creare il database, aggiungere utenti e assegnare autorizzazioni). Per l'Autenticazione SQL, l'account usato deve disporre degli stessi diritti. Tali credenziali vengono usate solo durante l'installazione. Il prodotto installato non utilizza tali credenziali.

Durante l'installazione, inoltre, è necessario specificare le credenziali di autenticazione del runtime del servizio che i servizi Dell possono usare per accedere al server SQL. L'account utente deve disporre dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza al ruolo del database: dbo_owner, public.

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

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

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

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

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

I file di registro per l'installazione si trovano in questa directory: **C:\ProgramData\Dell\Dell Data Protection\Installer Logs**



Nuova installazione

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

- [Installare un server back-end e un nuovo database](#) - Per installare un nuovo Dell Enterprise Server e un nuovo database.
- [Installare un server back-end con un database esistente](#) - Per installare un nuovo Dell Enterprise Server e connetterlo a un database SQL creato durante la [Configurazione di preinstallazione](#) o ad un database SQL esistente che sia v9.x o successiva, quando la versione di schema corrisponde alla versione di Dell Enterprise Server da installare. È necessario migrare un database v8.x o successiva allo schema più recente con la versione più recente del Server Configuration Tool. Per istruzioni sulla migrazione dei database con il Server Configuration Tool, consultare [Migrare il database](#). Per ottenere il Server Configuration Tool più recente o migrare a una versione di database precedente alla v8.0, contattare Dell ProSupport per assistenza.

❗ N.B.:

Se l'utente dispone di un Dell Enterprise Server v8.x funzionale, o versione successiva, fare riferimento alle istruzioni contenute in [Aggiornare/migrare server back-end](#).

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

- [Installare un server front-end](#) - Per installare un server front-end in modo che comunichi con un server back-end.

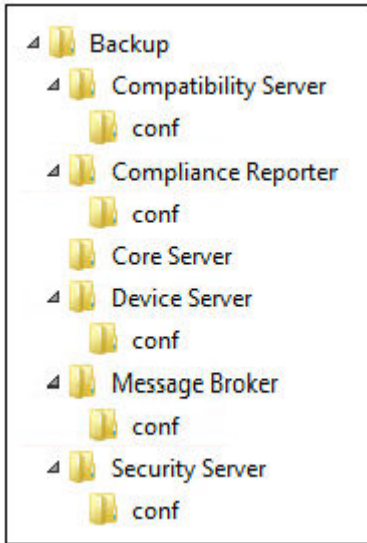
Installare un server back-end e un nuovo database

- 1 Nel supporto di installazione di Dell, passare alla directory di Dell Enterprise Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Enterprise Server-x64 nella directory principale del server in cui si sta installando Enterprise Server. **Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.**
- 2 Fare doppio clic su **setup.exe**.
- 3 Nella 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 Se il [punto 9](#) (facoltativo) in [Configurazione di preinstallazione](#) è stato completato, fare clic su **Avanti**. Altrimenti, immettere il Product Key da 32 caratteri e fare clic su **Avanti**. Il Product Key si trova nel file "EnterpriseServerInstallKey.ini".
- 8 Selezionare **Installazione back-end** e fare clic su **Avanti**.
- 9 Per installare Dell Enterprise Server nel percorso predefinito C:\Program Files\Dell, fare clic su **Avanti**. Altrimenti, fare clic su **Modifica** per selezionare un percorso diverso, quindi fare clic su **Avanti**.
- 10 Per selezionare un percorso in cui archiviare i file di configurazione del backup, fare clic su **Modifica**, passare alla cartella desiderata, quindi fare clic su **Avanti**.

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

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

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



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

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

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

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

Fare clic su **Avanti**.

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

OPPURE

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

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

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

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.



N.B.:

Per impostazione predefinita, il certificato scade dopo un anno.

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

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

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

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

Fare clic su **Avanti**.

N.B.:

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

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

OPPURE

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

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

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

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.

N.B.:

Per impostazione predefinita, il certificato scade dopo un anno.

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

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

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

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

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

- a Fare clic su **Sfogli** per selezionare il server in cui installare il database.
- b Selezionare il metodo di autenticazione che deve usare il programma di installazione per configurare il database di Dell Data Protection. Dopo l'installazione, il prodotto installato non utilizza le credenziali specificate qui.

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

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

OPPURE

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

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

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

- c Identificare il catalogo del database:
Immettere il nome del catalogo di un nuovo database. Nella schermata successiva verrà richiesto di creare il nuovo catalogo.
- d Fare clic su **Avanti**.
- e Per confermare che si desidera far creare un database al programma di installazione, fare clic su **Sì**. Per tornare alla schermata precedente per apportare modifiche, fare clic su **No**.

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

- **Autenticazione di Windows**

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

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

Tali credenziali vengono anche utilizzate dai servizi Dell che gestiscono Dell Enterprise Server.

OPPURE

- **Autenticazione di SQL Server**

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

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

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

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

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

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

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



Installare un server back-end con un database esistente

❗ N.B.:

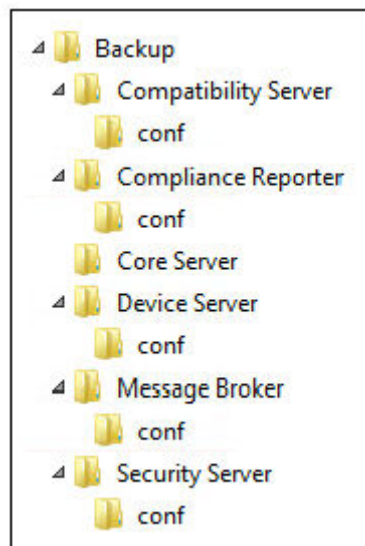
Se l'utente dispone di un Dell Enterprise Server v8.x funzionale, o versione successiva, fare riferimento alle istruzioni contenute in [Aggiornare/migrare server back-end](#).

È possibile installare un nuovo Dell Enterprise Server e connetterlo ad un database SQL creato durante la [Configurazione di preinstallazione](#) o ad un database SQL esistente che sia v9.x o successiva, quando la versione di schema corrisponde alla versione di Dell Enterprise Server da installare.

È necessario migrare un database v8.x o successiva allo schema più recente con la versione più recente del Server Configuration Tool. Per istruzioni sulla migrazione dei database con il Server Configuration Tool, consultare [Migrare il database](#). Per ottenere il Server Configuration Tool più recente o **migrare a una versione di database precedente alla v8.0**, contattare Dell ProSupport per assistenza.

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

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



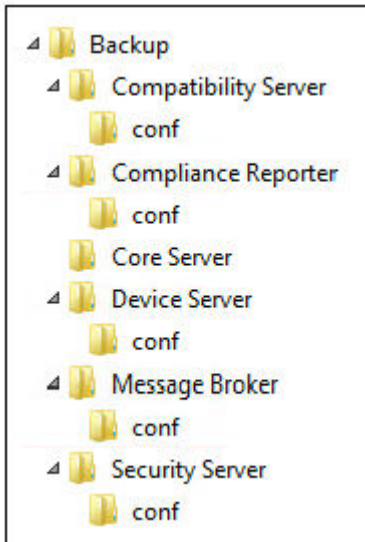
- 1 Nel supporto di installazione di Dell, passare alla directory di Dell Enterprise Server. **Decomprimere** (NON copiare/incollare o trascinare la selezione) Enterprise Server-x64 nella directory principale del server in cui si sta installando Enterprise Server. **Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.**
- 2 Fare doppio clic su **setup.exe**.
- 3 Nella 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 Se il [punto 9](#) (facoltativo) in [Configurazione di preinstallazione](#) è stato completato, fare clic su **Avanti**. Altrimenti, immettere il Product Key da 32 caratteri e fare clic su **Avanti**. Il Product Key si trova nel file "EnterpriseServerInstallKey.ini".
- 8 Selezionare **Installazione back-end** e **Installazione di ripristino**, quindi fare clic su **Avanti**.

- 9 Per installare Dell Enterprise Server nel percorso predefinito C:\Program Files\Dell, fare clic su **Avanti**. Altrimenti, fare clic su **Modifica** per selezionare un percorso diverso, quindi fare clic su **Avanti**.
- 10 Per selezionare un percorso in cui archiviare i file di configurazione del backup, fare clic su **Modifica**, passare alla cartella desiderata, quindi fare clic su **Avanti**.

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

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

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



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

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

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

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

Fare clic su **Avanti**.

N.B.:

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

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

OPPURE

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

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



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

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.



N.B.:

Per impostazione predefinita, il certificato scade dopo un anno.

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

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

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

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

Fare clic su **Avanti**.



N.B.:

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

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

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

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

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

Organizzazione

Unità organizzativa (ad esempio Sicurezza)

Città

Stato (nome completo)

Paese: Abbreviazione di due lettere del Paese

Fare clic su **Avanti**.

N.B.:

Per impostazione predefinita, il certificato scade dopo un anno.

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

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

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

- Per visualizzare o modificare le porte, fare clic su **Modifica porte**. Modificare le porte solo se necessario. Dell consiglia di usare le impostazioni predefinite. Al termine, fare clic su **OK**.
- 14 Specificare il metodo di autenticazione per il programma di installazione da usare.
- a Fare clic su **Sfogli** per selezionare il server in cui si trova il database.
 - b Selezionare il tipo di autenticazione.
 - **Credenziali di autenticazione di Windows dell'utente corrente**

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

OPPURE

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

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

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

- c Fare clic su **Sfogli** per selezionare il nome di catalogo del database esistente.
 - d Fare clic su **Avanti**.
- 15 Selezionare il metodo di autenticazione per il prodotto da usare. Questo è l'account che il prodotto usa per gestire il database e i servizi Dell.

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

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

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

OPPURE

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

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

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



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

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

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

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

- L'opzione **Migra questo database allo schema corrente** viene usata per ripristinare un buon database da un'implementazione del server non riuscita. Questa opzione usa i file di ripristino nella cartella \Backup per riconnetterli al database, quindi migra il database allo schema corrente. Questa opzione deve essere usata *solo* dopo aver provato prima a reinstallare la versione corretta di Enterprise Server, quindi eseguendo il programma di installazione più recente per l'aggiornamento.
 - L'opzione **Procedi senza migrare il database** installa i file di Enterprise Server senza configurare completamente il database. La configurazione del database deve essere completata manualmente in un secondo momento usando il Server Configuration Tool e sarà necessario apportare altre modifiche manualmente.
- b Quando lo schema del database dispone già dello schema della versione in uso ma non è connesso al back-end di Dell Enterprise Server è considerato un *Ripristino*. Viene visualizzata questa finestra di dialogo:
- Selezionare **Modalità di installazione di ripristino** per proseguire l'installazione con il database selezionato.
 - Selezionare **Seleziona un nuovo database** per sceglierne uno diverso.
 - Selezionare **Esci dal programma di installazione per terminare l'installazione**.
- c Fare clic su **Avanti**.

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

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

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

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

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

Installare server front-end

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

❗ N.B.: Il servizio beacon è installato come parte 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 Enterprise Server. **Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.**
- 2 Fare doppio clic su **setup.exe**.
- 3 Nella 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 **Sfoglia** per immettere il percorso del certificato.

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

Fare clic su **Avanti**.

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.





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**.
Una finestra di dialogo di stato visualizza lo stato del processo di installazione.
- 14 Al completamento dell'installazione, fare clic su **Fine**.
Le attività di installazione del server front-end sono state completate.

Aggiornamento/migrazione

È possibile aggiornare Dell Enterprise Server v8.0 e versioni successive a Dell Enterprise Server v9.x. Se la versione server è precedente alla v8.0, è necessario prima eseguire l'aggiornamento alla v8.0, quindi alla v9.x.

Prima di iniziare l'aggiornamento/migrazione

Prima di iniziare, accertarsi che la [Configurazione di preinstallazione](#) sia stata completata. È particolarmente importante se si sta distribuendo Mobile Edition.

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

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

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

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

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

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

Dell Enterprise Server v9.x supporta:

- Enterprise Edition:
 - Client Windows v7.x/8.x
 - Client Mac v7.x/8.x
 - Client SED v8.x
 - Authentication v8.x



- BitLocker Manager v7.2x+ e v8.x
- Data Guardian v1.x
- Endpoint Security Suite v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Aggiornamento/migrazione da Dell Enterprise Server v8.x o successiva (quando si esegue la migrazione di Dell Enterprise Server da una versione precedente alla v8.x, contattare Dell ProSupport per assistenza).

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

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

Applicare le modifiche ai criteri

- 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.

Accertarsi che i servizi Dell siano in esecuzione

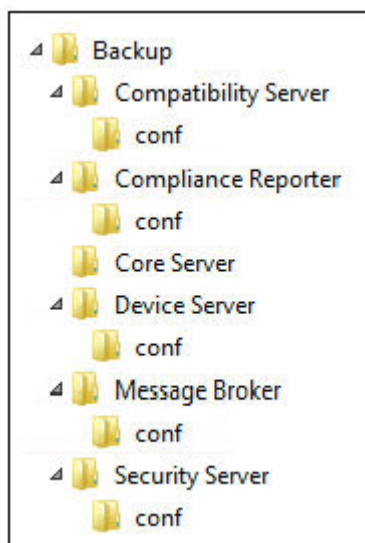
- 6 Dal menu *Start* di Windows, fare clic su **Start > Esegui**. Digitare *services.msc* e fare clic su **OK**. Quando *Servizi* si apre, passare a ciascun servizio Dell e, se necessario, fare clic su **Avvia il servizio**.

Eseguire il backup dell'installazione esistente

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

N.B.:

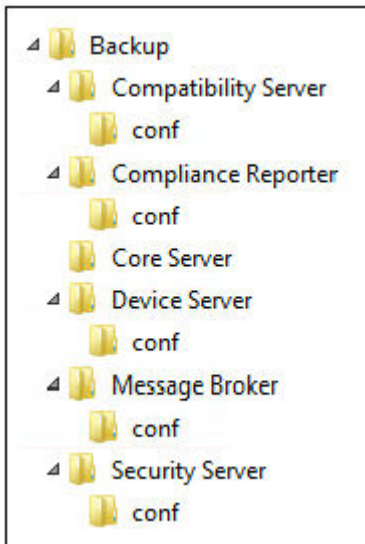
La struttura di cartelle creata dal programma di installazione durante l'installazione (esempio mostrato qui di seguito) deve rimanere invariata



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

- 1 Nel supporto di installazione di Dell, passare alla directory di 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 Enterprise Server. **Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.**
- 2 Fare doppio clic su **setup.exe**.
- 3 Nella finestra di dialogo *Installazione guidata InstallShield*, selezionare la lingua per l'installazione, quindi fare clic su **OK**.
- 4 Nella schermata iniziale, fare clic su **Avanti**.
- 5 Leggere il contratto di licenza, accettare i termini, quindi fare clic su **Avanti**.
- 6 Per selezionare un percorso in cui archiviare i file di configurazione del backup, fare clic su **Modifica**, passare alla cartella desiderata e fare clic su **Avanti**.
Dell consiglia di selezionare, per il backup, un percorso di rete remoto o un'unità esterna.

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



- 7 Quando il programma di installazione salva correttamente il database esistente, la finestra di dialogo viene precompilata. Per connettere il database esistente, specificare il metodo di autenticazione da usare. Dopo l'installazione, il prodotto installato non utilizza le credenziali specificate qui.
 - a Selezionare il tipo di autenticazione del database:
 - **Credenziali di autenticazione di Windows dell'utente corrente**

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

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

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

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

- b Fare clic su **Avanti**.
- 8 Se la finestra di dialogo Informazioni sull'account del runtime del servizio non viene pre-popolata, specificare il metodo di autenticazione che il prodotto può usare dopo l'installazione.
 - a Selezionare il tipo di autenticazione.
 - b Immettere nome utente e password dell'account di servizio del dominio che i servizi Dell useranno per accedere all'SQL Server e fare clic su **Avanti**.

L'account utente deve essere nel formato DOMINIO\Nomeutente ed essere dotato dello Schema predefinito delle autorizzazioni dell'SQL Server: dbo e Appartenenza a ruoli del database per: dbo_owner, public.
- 9 Se non è stato eseguito il backup del database, è **necessario** eseguirlo prima di continuare l'installazione. **Non sarà possibile ripristinare l'aggiornamento del database**. Solo dopo aver eseguito il backup del database, selezionare **Sì, il backup del database è stato eseguito**, quindi fare clic su **Avanti**.
- 10 Fare clic su **Installa** per avviare l'installazione.

Una finestra di dialogo di stato visualizza lo stato del processo di aggiornamento.
- 11 Al completamento dell'installazione, fare clic su **Fine**.

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

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

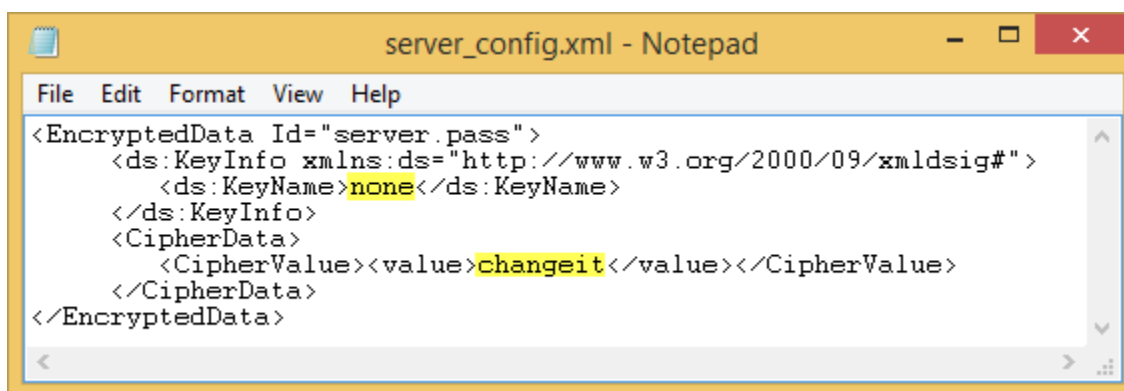
- 12 Nel backup dell'installazione, copiare/incollare: <directory installazione Compatibility Server>\conf\secretKeyStore nella nuova installazione:
<directory installazione Compatibility Server>\conf\secretKeyStore
- 13 Nella nuova installazione, aprire <directory installazione Compatibility Server>\conf\server_config.xml e sostituire il valore **server.pass** con il valore del backup di <directory installazione Compatibility Server>\conf\server_config.xml, come segue:

Istruzioni per server.pass:

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

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

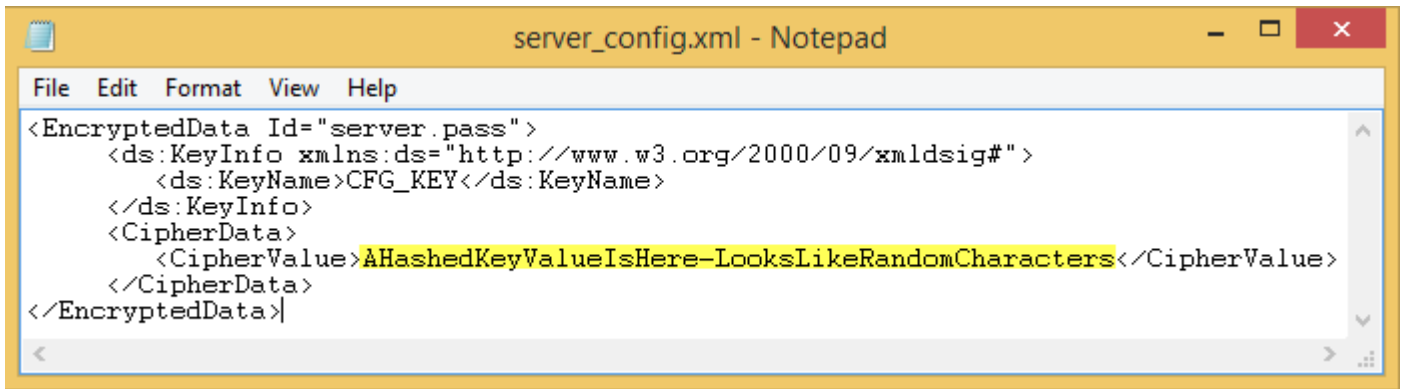
Password nota



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

Password sconosciuta





```
<EncryptedData Id="server.pass">
  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:KeyName>CFG_KEY</ds:KeyName>
  </ds:KeyInfo>
  <CipherData>
    <CipherValue>AHashedKeyValueIsHere-LooksLikeRandomCharacters</CipherValue>
  </CipherData>
</EncryptedData>
```

Salvare e chiudere i file.

① N.B.:

Mai provare a modificare la password di **Dell Enterprise Server** modificando il valore `server.pass` in `server_config.xml`. Se si modifica questo valore, si perde l'accesso al database.

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

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

① N.B.: A partire dalla versione 9.5, il servizio beacon viene installato come parte di questo aggiornamento utilizzando il nome host predefinito e la porta 8446. Il servizio beacon supporta il beacon 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. Il criterio Attiva beacon richiamata è abilitato per impostazione predefinita. Accertarsi che la sicurezza di rete necessaria sia configurata prima di utilizzare il beacon richiamata.

- 1 Nel supporto di installazione di Dell, passare alla directory di 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 Enterprise Server. **Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.**
- 2 Fare doppio clic su **setup.exe**.
- 3 Nella 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 Nella finestra di dialogo *Installazione del programma*, fare clic su **Installa**.
Una finestra di dialogo di stato visualizza lo stato del processo di installazione.
- 8 Al completamento dell'installazione, fare clic su **Fine**.
- 9 Impostare il server back-end in modo che comunichi con il server front-end.
 - a Nel server back-end, andare a <directory installazione Security Server>\conf\ e aprire il file `application.properties`.
 - b Individuare `publicdns.server.host` e impostare il nome su un nome host risolvibile dall'esterno.
 - c Individuare `publicdns.server.port` e impostare la porta (quella predefinita è 8443).Al termine dell'installazione i servizi Dell verranno riavviati. Non sarà necessario riavviare il server finché le attività di Configurazione di postinstallazione saranno state completate.

Installazione in modalità disconnessa

La modalità disconnessa isola Enterprise Server da Internet e da una LAN non protetta o altra rete. Dopo aver installato Enterprise Server in modalità disconnessa, rimane in modalità disconnessa e non può essere modificato nuovamente in modalità connessa.



Enterprise Server è installato in modalità disconnessa tramite di comando.

La seguente tabella elenca gli switch disponibili.

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

La tabella seguente elenca le opzioni disponibili per la visualizzazione.

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

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

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

Parametri

AGREE_TO_LICENSE=Si - Questo valore deve essere "Si."

PRODUCT_SN=xxxxx - Opzionale se si è in possesso delle informazioni di licenza nella posizione standard; in caso contrario, immetterlo qui.

INSTALLDIR=<path> - Opzionale.

BACKUPDIR=<path> - Questa è la posizione in cui verranno archiviati i file di ripristino.

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

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

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

Sono necessari i seguenti requisiti con SSL_TYPE=1:

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

Sono necessari i seguenti requisiti con SSL_TYPE=2:

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY - Facoltativo, impostazione predefinita = "USA"



Parametri

SSL_STATENAME

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

Sono necessari i seguenti requisiti con SSOS_TYPE=1:

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

Sono necessari i seguenti requisiti con SSOS_TYPE=2:

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY - Facoltativo, impostazione predefinita = "USA"

SSOS_STATENAME

DISPLAY_SQLSERVER - Questo valore sarà analizzato per ottenere le informazioni su Server, Istanza e porta.

Esempio:

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

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

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

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

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

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

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

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

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

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

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

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

Parametri

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

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

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

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

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

CORESERVERHOST - Opzionale. Nome host Core Server.

RMIHOST - Opzionale. Nome host server compatibilità.

REPORTERHOST - Opzionale. Nome host Compliance Reporter.

DEVICEHOST - Opzionale. Nome host Device Server.

KEYSERVERHOST - Opzionale. Nome host chiave server.

TIGAHOST - Opzionale. Nome host server di sicurezza.

SMTP_HOST - Opzionale. Nome host SMTP.

ACTIVEMQHOST - Opzionale. Nome host Message Broker.

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

SERVERPORT_CLIENTAUTH - Opzionale.

REPORTERPORT - Opzionale.

DEVICEPORT - Opzionale.

KEYSERVERPORT - Opzionale.

GKPORT - Opzionale.

TIGAPORT - Opzionale.

SMTP_PORT - Opzionale.

ACTIVEMQ_TCP - Opzionale.

ACTIVEMQ_STOMP - Opzionale.

Installare Enterprise Server in modalità disconnessa

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

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



Disinstallare Dell Enterprise Server

- 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 disinstallando Enterprise Edition. **Le operazioni di copia/incolla o trascinamento della selezione provocano errori che non permettono di effettuare l'installazione.**
- 2 Fare doppio clic su **setup.exe**.
- 3 Nella schermata iniziale, fare clic su **Avanti**.
- 4 Nella finestra di dialogo *Rimuovere il programma*, fare clic su **Rimuovi**.
Una finestra di dialogo di stato visualizza lo stato del processo di disinstallazione.
- 5 Al completamento della disinstallazione, fare clic su **Fine**.

Configurazione di postinstallazione

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

Sia se si sta effettuando la prima installazione di Dell Enterprise Server o se si sta aggiornando un'installazione esistente, sarà necessario configurare alcuni componenti dell'ambiente.

Installazione e configurazione di Gestione EAS

È necessario completare questa sezione se si intende usare Mobile Edition. In caso contrario, tralasciare questa sezione e continuare con [Dell Security Server nella configurazione in modalità DMZ](#).

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 Dell Policy Proxy.
- Tenere l'FQDN di Dell Policy Proxy a portata di mano.
- Tenere il numero di porta di Dell Policy Proxy a portata di mano.
- La funzionalità Accodamento messaggi Microsoft (MSMQ) deve essere già installata/configurata nel server che ospita l'ambiente Exchange. In caso contrario, consultare [Installare/Configurare Accodamento messaggi Microsoft \(MSMQ\)](#).

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 Dell, 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 Dell, 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 Nella 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:
FQDN di Dell Policy Proxy

Porta Dell Policy Proxy (la porta predefinita è 8090)

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

Selezionare la casella per eseguire EAS Device Manager in modalità Solo rapporto (procedura consigliata durante la distribuzione)

① 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**.

Configurare le impostazioni di Gestione EAS

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

- 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:
FQDN di Dell Policy Proxy

Porta Dell Policy Proxy (la porta predefinita è 8090)

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

Deselezionare la casella per eseguire 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**.

Dell Security Server nella configurazione in modalità DMZ

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

Se si usa un certificato attendibile, ignorare questa sezione e continuare con [Registrazione dell'APNs](#).

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

Usare Keytool per importare il certificato di dominio DMZ

❗ IMPORTANTE:

Eseguire il backup dei file dell'Autorità di certificazione Dell Security Server esistenti prima di continuare con le istruzioni di Keytool. In caso di errore di configurazione, è possibile ripristinare il file salvato.

Presupposti

- Dell Security Server è stato installato con un certificato non attendibile.
- Dell Security Server in Modalità DMZ è stato installato usando un certificato firmato (Entrust, Verisign, ecc.)
- È disponibile un file di certificato .pfx. Se è necessario convertire il certificato in .pfx, consultare Esportazione di un certificato in .PFX usando la console di gestione dei certificati.

Procedura

- 1 Aggiungere Keytool al percorso di sistema.

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

- 2 Usare Keytool per elencare il contenuto del certificato di dominio attendibile che si desidera importare. Prendere nota del Nome alias elencato.

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

- 3 Usare Keytool per importare il contenuto del certificato firmato nel file dell'Autorità di certificazione di Dell Security Server:

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

Per -sralias, è necessario ottenere queste informazioni dal contenuto esportato del certificato firmato.

Per -destalias, può essere il percorso desiderato.



- 4 Eseguire il backup e sostituire il file dell'Autorità di certificazione corrente nella directory <directory installazione Security Server>\conf \ con il file dell'Autorità di certificazione appena creato in Dell Security Server.

Modificare il file application.properties

Modificare il file application.properties per specificare l'alias del certificato per la firma.

- 1 Andare a <directory di installazione di Security Server>\conf\application.properties
- 2 Modificare le seguenti informazioni:
keystore.alias.signing=<modificare questo valore con il valore al [punto 3](#) precedente per -destAlias>
- 3 Riavviare il servizio Dell Security Server.

Registrazione dell'APNs

Se si intende usare Mobile Edition for Mobile Device Security con dispositivi iOS, è necessario usare la Registrazione APN guidata per:

- Creare un CSR
- Creare un certificato push Apple
- Caricare un certificato push

Se non si intende usare Mobile Edition for Mobile Device Security con dispositivi iOS, ignorare questa sezione e continuare con [Server Configuration Tool](#).

Il servizio di notifica push di Apple (APNs, Apple Push Notification service) consente la comunicazione protetta dei dispositivi iOS over-the-air. L'APNs è usato per inviare la notifica affinché un dispositivo iOS comunichi con Dell Enterprise Server. L'APNs invia solo la notifica al dispositivo, non i dati.

Procedura

- 1 Aprire un browser e andare a <https://<FQDN server sicurezza>:8443/csrweb>.
- 2 Nella finestra di dialogo di accesso Registrazione APNs guidata, immettere le credenziali amministratore Dell e fare clic su **Accedi**.
- 3 Viene visualizzata una finestra di dialogo che descrive le fasi da effettuare. Fare clic su **Avanti**.

Fase I: Creare un CSR

- 4 Immettere le informazioni seguenti:

E-mail: L'indirizzo di posta elettronica può essere qualsiasi UPN, ma si consiglia di usare un account per l'amministratore che conserverà il certificato dell'APNs.

Nome comune: Immettere il nome comune associato a questo indirizzo di posta elettronica.

Fare clic su **Genera CSR**.

- 5 Dopo aver generato un CSR, salvare il file in un percorso facilmente accessibile.
- 6 Fare clic su **Avanti**.

Fase II: Creare un certificato push di Apple

- 7 Fare clic sul collegamento del **Portale dei certificati push di Apple**. Accedere con il proprio ID e password Apple.
- 8 Leggere le Condizioni per l'utilizzo, indicarne l'accettazione e fare clic su **Accetto**.
- 9 Fare clic su **Sfogli** quindi **caricare** il CSR appena creato.
- 10 Nella pagina *Certificati per server di terze parti*, fare clic su **Scarica**. Salvare il file in un percorso facilmente accessibile.
- 11 Tornare alla Registrazione APNs guidata e fare clic su **Avanti**.

Fase III: Caricare il certificato push

12 Immettere le seguenti informazioni (usare le stesse credenziali usate nella [Fase I: Creare un CSR](#)).

E-mail:

Nome comune:

File certificato push: fare clic su **Sfoglia** per individuare il file salvato al [punto 7](#). Fare clic su **Carica**.

13 Viene visualizzato il messaggio di completamento dell'operazione. Fare clic su **Fine**.

La registrazione del certificato dell'APNs con Dell Enterprise Server è stata completata.

Server Configuration Tool

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

Il Dell Server Configuration Tool consente di:

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

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

Per avviare Dell Server Configuration Tool, andare a **Start > Programmi > Dell > Enterprise Edition > Server Configuration Tool > Esegui Server Configuration Tool**.

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

Aggiungere certificati nuovi o aggiornati

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

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

I componenti interessati dalla configurazione del certificato sono:

- Servizi Java (per esempio Dell Device Server e così via)
- Applicazioni .NET (Dell Core Server)
- Convalida di smart card usate per l'autenticazione di preavviso (Dell Security Server)
- Importazione di chiavi di crittografia private da usare per firmare i bundle dei criteri inviati a Dell Manager. Dell Manager esegue la convalida SSL per i client Enterprise Edition gestiti in remoto con unità autocrittografanti o BitLocker Manager.



- Workstation client:
 - Workstation su cui è in esecuzione BitLocker Manager
 - Workstation su cui è in esecuzione Enterprise Edition (client Windows)
 - Workstation su cui è in esecuzione Endpoint Security Suite
 - Workstation su cui è in esecuzione Endpoint Security Suite Enterprise

Informazioni sul tipo di certificati da usare:

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

- Convalida di smart card usate per l'autenticazione di preavvio:
 - Importazione del certificato di firma dell'"Agenzia principale" e della catena di attendibilità completa nell'archivio chiavi Java di Dell Security Server. Per maggiori informazioni, consultare Creare un certificato autofirmato e generare una richiesta di firma del certificato. È necessario importare la catena di attendibilità completa.

Dell Manager:

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

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

Scegliere **un** metodo:

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

Rapido

- 1 Dal menu principale, selezionare **Azioni > Configura i certificati**.
- 2 All'avvio della configurazione guidata, selezionare **Rapido** e fare clic su **Avanti**. Se disponibili, verranno usate le informazioni del certificato autofirmato creato durante l'installazione di Enterprise Server.
- 3 Dal menu principale, selezionare **Configurazione > Salva**. Se richiesto, confermare il salvataggio.

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

Avanzato

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

- [Percorso 1 - Genera certificato autofirmato](#)
- [Percorso 2 - Utilizza impostazioni correnti](#)

Percorso 1 - Genera certificato autofirmato

- 1 Dal menu principale, selezionare **Azioni > Configura i certificati**.
- 2 All'avvio della configurazione guidata, selezionare **Avanzato** e fare clic su **Avanti**.

- 3 Selezionare **Genera certificato autofirmato** e fare clic su **Avanti**. Se disponibili, verranno usate le informazioni del certificato autofirmato creato durante l'installazione di Enterprise Server.
- 4 Dal menu principale, selezionare **Configurazione > Salva**. Se richiesto, confermare il salvataggio.

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

Percorso 2 - Utilizza impostazioni correnti

- 1 Dal menu principale, selezionare **Azioni > Configura i certificati**.
- 2 All'avvio della configurazione guidata, selezionare **Avanzato** e fare clic su **Avanti**.
- 3 Selezionare **Utilizza impostazioni correnti** e fare clic su **Avanti**.
- 4 Nella finestra *Certificato SSL per Compatibility Server*, selezionare **Genera certificato autofirmato** e fare clic su **Avanti**. Se disponibili, verranno usate le informazioni del certificato autofirmato creato durante l'installazione di Enterprise Server.

Fare clic su **Avanti**.

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

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

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

Al termine fare clic su **Fine**.

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

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

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

Al termine fare clic su **Fine**.

- *Utilizza impostazioni correnti* - Selezionare questa opzione per cambiare l'impostazione di un certificato in qualsiasi momento dopo la configurazione iniziale di Dell Enterprise Server. Selezionare questa opzione per mantenere il certificato già configurato. Dopo aver selezionato questa opzione verrà visualizzata la finestra Certificato di sicurezza messaggi.

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

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

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

Al termine fare clic su **Fine**.

- *Genera certificato autofirmato* - Se disponibili, verranno usate le informazioni del certificato autofirmato creato durante l'installazione di Enterprise Server.

Fare clic su **Avanti**.

Al termine fare clic su **Fine**.

La configurazione del certificato è completa.

Al completamento delle modifiche:



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

Importare un certificato di Dell Manager

Se la distribuzione include client Enterprise Edition gestiti in remoto con unità autocrittografanti o BitLocker Manager, è necessario importare il certificato appena creato (o esistente). Il certificato di Dell Manager è usato come veicolo per proteggere la chiave privata usata per firmare i bundle dei criteri inviati ai client Enterprise Edition gestiti in remoto e a BitLocker Manager. Questo certificato può essere indipendente da tutti gli altri certificati. Inoltre, se questa chiave è compromessa può essere sostituita con una nuova e Dell Manager richiederà una nuova chiave pubblica se non è in grado di decrittografare i bundle dei criteri.

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

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

Al completamento delle modifiche:

- 1 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.
- 2 Chiudere Dell Server Configuration Tool.

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

Importare un certificato di identità

Se la distribuzione include Server Encryption, è necessario importare il certificato appena creato (o esistente). Il certificato di identità protegge la chiave privata usata per firmare i bundle dei criteri inviati ai server client. Questo certificato può essere indipendente da tutti gli altri certificati.

- 1 Dal menu principale, selezionare **Azioni** > **Importa certificato di identità**.
- 2 Sfogliare per selezionare un certificato e fare clic su **Avanti**.
- 3 Quando viene richiesta la password del certificato, immettere la password associata al certificato esistente.
- 4 Nella finestra di dialogo Account di Windows, selezionare un'opzione:
 - a Per modificare le credenziali associate al certificato di identità, selezionare **Utilizza credenziali diverse per l'account di Windows con il certificato di identità**.
 - b Per continuare ad usare le credenziali dell'account che ha effettuato l'accesso, fare clic su **Avanti**.
- 5 Dal menu principale, selezionare **Configurazione** > **Salva**. Se richiesto, confermare il salvataggio.

Configurare le impostazioni per il Certificato SSL server o Mobile Edition

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

Dell Manager:

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

SCEP:

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

Al completamento delle modifiche:

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

Configurare le impostazioni SMTP per Data Guardian o servizi e-mail

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

Questa scheda conferma le impostazioni SMTP per Data Guardian. Se è necessario configurare le impostazioni SMTP per scopi diversi dall'uso di Data Guardian, consultare l'argomento della guida dell'amministratore "Abilitare il server SMTP per le notifiche e-mail sulle licenze".

Immettere le informazioni seguenti:

- 1 Nel campo Nome host: immettere l'FQDN del server SMTP, come *smtpnomeserver.dominio.com*.



- 2 Nel campo *Nome utente*: immettere il nome dell'utente che accederà al server di posta. Il formato può essere `DOMINIO\mrossi`, `mrossi` o qualsiasi forma richiesta dalla propria organizzazione.
- 3 Nel campo *Password*: immettere la password associata al nome utente.
- 4 Nel campo *Indirizzo origine*: immettere l'indirizzo di posta elettronica che originerà l'e-mail. È possibile utilizzare l'account del nome utente (`mrossi@dominio.com`), ma anche un altro account a cui il nome utente specificato è in grado di accedere per inviare le e-mail (`RegistrazioneCloud@dominio.com`).
- 5 Nel campo *Porta*: immettere il numero di porta (tipicamente 25).
- 6 Nel menu *Autenticazione*: selezionare *Vero* o *Falso*.

Al completamento delle modifiche:

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

Modificare nome del database, percorso o credenziali

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

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

Dell consiglia di usare un nome di dominio completo, benché sia possibile utilizzare un indirizzo IP.
- 2 Nel campo *Porta server*: immettere il numero di porta.

Quando si utilizza un'istanza SQL Server non predefinita, occorre specificare la porta dinamica di tale istanza nel campo *Porta*. In alternativa, abilitare il servizio SQL Server Browser e accertarsi che la porta UDP 1434 sia aperta. Per maggiori informazioni, consultare [https://msdn.microsoft.com/en-us/library/hh510203\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx).
- 3 Nel campo *Database*: immettere il nome del database.
- 4 Nel campo *Autenticazione*: selezionare **Autenticazione di Windows** o **Autenticazione di SQL Server**. Se si sceglie l'Autenticazione di Windows, per l'autenticazione verranno utilizzate le stesse credenziali utilizzate per accedere a Windows (i campi *Nome utente* e *Password* non saranno modificabili).
- 5 Nel campo *Nome utente*: immettere il nome utente appropriato associato al database.
- 6 Nel campo *Password*: immettere la password del nome utente elencato nel campo *Nome utente*.
- 7 Dal menu principale, selezionare **Configurazione > Salva**. Se richiesto, confermare il salvataggio.
- 8 Per testare la configurazione del database, dal menu principale selezionare **Azioni > Testa la configurazione del database**. Viene avviata la configurazione guidata.
- 9 Nella finestra *Test della configurazione* leggere le informazioni sul test e fare clic su **Avanti**.
- 10 Se nella scheda *Database* è stata selezionata la voce *Autenticazione di Windows*, è possibile immettere facoltativamente delle credenziali alternative per consentire l'uso delle stesse credenziali che verranno utilizzate per eseguire Dell Enterprise Server. Fare clic su **Avanti**.
- 11 Nella finestra *Testa la configurazione*, vengono visualizzati i risultati di Testa le impostazioni di connessione, Test di compatibilità e Test database migrato.
- 12 Fare clic su **Fine**.

N.B.:

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

Al completamento delle modifiche:

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

Migrare il database


È possibile migrare un database v8.x allo schema più recente con la versione più recente del Server Configuration Tool. Per ottenere il Server Configuration Tool più recente o migrare a una versione di database precedente alla v8.0, contattare Dell ProSupport per assistenza.

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

- 1 Se non si è ancora effettuato il backup del database Dell esistente, **farlo adesso**.
- 2 Dal menu principale, selezionare **Azioni > Migra il database**. Viene avviata la configurazione guidata.
- 3 Nella finestra *Migra il database Enterprise*, viene visualizzato un avviso. Confermare che è stato eseguito il backup dell'intero database o che non è necessario eseguire il backup del database esistente. Fare clic su **Avanti**.

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

Al termine, verificare l'eventuale presenza di errori.

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

- 4 Fare clic su **Fine**.

Al completamento della migrazione:

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

Attività di amministrazione

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.

Caricare la licenza di accesso client

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

- 1 Nel riquadro sinistro fare clic su **Gestione**.
- 2 Fare clic su **Gestione licenza**.
- 3 Fare clic su **Scegli file** per individuare e selezionare il file Licenza client.

Eseguire il commit dei criteri

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

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

- 1 Nel riquadro sinistro fare clic su **Gestione > Esegui commit**.
- 2 Immettere una descrizione della modifica nel campo Commento.
- 3 Fare clic su **Commit criteri**.

Configurare Dell Compliance Reporter

- 1 Nel riquadro sinistro fare clic su **Compliance Reporter**.
- 2 Quando si avvia Dell Compliance Reporter, accedere usando le credenziali predefinite *superadmin/changeit*.
- 3 Sono supportati due diversi metodi di autenticazione. Per configurare, selezionare:
 - [Configurare l'autenticazione SQL con Compliance Reporter](#)
 - [Configurare l'autenticazione di Windows con Compliance Reporter](#)

Configurare l'autenticazione SQL con Compliance Reporter

A partire dalla v8.1, l'Origine dati ha la preconfigurazione di tipo out-of-the-box. Non è necessaria alcuna configurazione. Usare la procedura seguente per modificare l'Origine dati, se necessario.

- 1 Per impostare l'Origine dati, nel menu principale fare clic su **Impostazioni**. Nel menu a sinistra, fare clic su **Origine dati**.
- 2 Immettere il nome utente per accedere al database Dell.
- 3 Immettere la password per accedere al database Dell.
- 4 Immettere il nome host per accedere al database Dell.
- 5 Immettere il nome database per accedere al database Dell.
- 6 Immettere il numero massimo di connessioni inattive consentite. L'impostazione predefinita è 2.
- 7 Immettere il numero massimo di connessioni (attive) consentite. L'impostazione predefinita è 10.
- 8 Immettere il Tempo max attesa (numero massimo di millisecondi di attesa per una connessione). -1 è sempre.
- 9 Per verificare l'URL del database e testare la connettività tra Dell Compliance Reporter e il database Dell, fare clic su **Test connessione**.
- 10 Fare clic su **Aggiorna**. Per eliminare le informazioni, fare clic su **Annulla**.

Le attività di amministrazione sono state completate. Il resto del capitolo tratta l'Autenticazione di Windows e può essere ignorato se per Dell Compliance Reporter viene usata l'Autenticazione SQL.

Se necessario, continuare con [Creare un certificato autofirmato e generare una richiesta di firma del certificato](#) oppure [Esportare un certificato in .PFX usando la console di gestione dei certificati](#).

Configurare l'autenticazione di Windows con Compliance Reporter

A partire dalla v8.1, l'Origine dati ha la preconfigurazione di tipo out-of-the-box. Non è necessaria alcuna configurazione. Usare la procedura seguente per modificare l'Origine dati, se necessario.

- 1 Immettere il nome utente per accedere al database Dell.
- 2 Lasciare vuoto il campo password. Quando l'utente di dominio effettua l'accesso, la password passerà al database.
- 3 Immettere il nome host per accedere al database Dell.
- 4 Immettere il nome database per accedere al database Dell.
- 5 Immettere il numero massimo di connessioni inattive consentite. L'impostazione predefinita è 2.
- 6 Immettere il numero massimo di connessioni (attive) consentite. L'impostazione predefinita è 10.
- 7 Immettere il Tempo max attesa (numero massimo di millisecondi di attesa per una connessione). -1 è sempre.



- 8 Per verificare l'URL del database e testare la connettività tra Dell Compliance Reporter e il database Dell, fare clic su **Test connessione**.
- 9 Fare clic su **Aggiorna**. Per eliminare le informazioni, fare clic su Annulla.

Le attività di amministrazione sono state completate. **Se necessario**, continuare con [Creare un certificato autofirmato e generare una richiesta di firma del certificato](#) oppure [Esportare un certificato in .PFX usando la console di gestione dei certificati](#).

Eseguire i backup

Ai fini del ripristino d'emergenza, assicurarsi che venga eseguito il backup dei seguenti percorsi ogni settimana, con differenziali notturni.

Backup di Enterprise Server

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

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

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

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

Backup di SQL Server

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

Per ulteriori informazioni sulle procedure consigliate di SQL Server, consultare [L'elenco seguente illustra le procedure consigliate per SQL Server da implementare durante l'installazione di Dell Data Protection, se non ancora implementate](#).

Backup di PostgreSQL Server

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

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

Descrizioni dei componenti Dell

La tabella seguente descrive ciascun componente e la relativa funzione.

Nome	Descrizione	Richiesto per
Compliance Reporter	Fornisce una visualizzazione completa dell'ambiente tramite la creazione di rapporti di controllo e conformità. Componente di Dell Enterprise Server.	Creare rapporti
Key Server	Negozia, autentica e crittografa una connessione client tramite le API Kerberos. Richiede l'accesso al database SQL per estrarre i dati della chiave. Componente di Dell Enterprise Server.	Utilità di amministrazione Dell
Server Configuration Tool	Configura la comunicazione del database con Core Server e Compatibility Server/ Security Server. Usato per inizializzare il database in seguito all'installazione o per migrare il database ad un nuovo schema. Usato per controllare Dell Services. Componente di Dell Enterprise Server.	Tutti
Remote Management Console Enterprise Server Console	Console di amministrazione e centro di controllo per la distribuzione a livello aziendale. Componente di Dell Enterprise Server.	Tutti
Core Server	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. Componente di Dell Enterprise Server.	Tutti
Security Server	Comunica con Policy Proxy e gestisce i recuperi delle chiavi Forensic, le attivazioni dei client, i prodotti Data Guardian, la comunicazione SED-PBA e la comunicazione di Active Directory per l'autenticazione o la riconciliazione, inclusa la convalida dell'identità per l'autenticazione nella Remote Management Console. Richiede l'accesso al database SQL.	Tutti



Nome	Descrizione	Richiesto per
	Componente di Dell Enterprise Server.	
Compatibility Server	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.	Tutti
	Componente di Dell Enterprise Server.	
Message Broker Service	Gestisce la comunicazione tra i servizi di Enterprise Server. Organizza le informazioni sui criteri create dal Compatibility Server per l'accodamento del Policy Proxy	Tutti
	Richiede l'accesso al database SQL.	
	Componente di Dell Enterprise Server.	
Device Server	Supporta le attivazioni e il recupero delle password.	Enterprise Edition per Mac
	Componente di Dell Enterprise Server.	Enterprise Edition per Windows
		Shield palmari
		CREDActivate
Device Server Plug-ins	Fornisce supporto per vari componenti.	Tutti
	Componente di Dell Enterprise Server.	
Identity Server	Gestisce le richieste di autenticazione del dominio.	Tutti
	Richiede un account di Active Directory.	
	Deve essere l'account usato per accedere a SQL quando viene usata l'Autenticazione di Windows.	
	Componente di Dell Enterprise Server.	
Policy Proxy	Fornisce un percorso di comunicazione di rete per fornire gli aggiornamenti dei criteri di protezione e dell'inventario.	Enterprise Edition per Mac
	Componente di Dell Enterprise Server.	Enterprise Edition per Windows
		Mobile Edition for Mobile Device Security
Security Token Services (STS)	Usati per contribuire a creare un canale di autenticazione protetta tra l'interfaccia utente di Dell Enterprise Server e i servizi di back-end Dell.	Tutti
EAS Device Manager	Abilita la funzionalità over-the-air. Installato nel server Accesso client di Exchange.	Gestione di Exchange ActiveSync dei dispositivi mobili.
EAS Mailbox Manager	L'agente della cassetta postale installato nel server Cassetta postali di Exchange.	Gestione di Exchange ActiveSync dei dispositivi mobili.



Procedure consigliate per SQL Server

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

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

Per maggiori informazioni, cercare gli articoli TechNet di Microsoft sulle "Informazioni su pagine ed extent".

- Microsoft SQL Server 2008 - <http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29>
- Microsoft SQL Server 2008 R2 - [http://technet.microsoft.com/en-us/library/ms190969\(v=sql.105\).aspx](http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx)

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

Per maggiori informazioni, cercare gli articoli TechNet di Microsoft sulle "Opzioni di configurazione del server Server Memory".

- Microsoft SQL Server 2008 - <http://technet.microsoft.com/en-us/library/ms178067%28v=sql.100%29>
- Microsoft SQL Server 2008 R2 - <http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29>
- Microsoft SQL Server 2012 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.110\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.110))
- Microsoft SQL Server 2014 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.120\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.120))
- Microsoft SQL Server 2016 - [https://technet.microsoft.com/en-us/library/ms178067\(v=sql.130\)](https://technet.microsoft.com/en-us/library/ms178067(v=sql.130))

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

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

- Microsoft SQL Server 2008 - <http://technet.microsoft.com/en-us/library/ms188396%28v=sql.100%29>
- Microsoft SQL Server 2008 R2 - <http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29>
- Microsoft SQL Server 2012 - <https://msdn.microsoft.com/en-us/library/ms188396.aspx>
- Microsoft SQL Server 2014 - <https://msdn.microsoft.com/en-us/library/ms188396.aspx>
- Microsoft SQL Server 2016 - <https://msdn.microsoft.com/en-us/library/ms188396.aspx>

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



Certificati

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

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

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

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

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

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

Generare una nuova coppia di chiavi e un certificato autofirmato

- 1 Passare alla directory **conf** di Dell Compliance Reporter, Dell Security Server o Dell Device Server.
- 2 Eseguire il backup del database di certificati predefinito:

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

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

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

- 4 Per generare un certificato, eseguire Keytool come mostrato:

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

- 5 Immettere le seguenti informazioni quando richiesto da Keytool.

N.B.:

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

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

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

<directory installazione Device Server>\conf\eserver.properties. Set the value eserver.keystore.password =

<directory installazione Security Server>\conf\eserver.properties. Set the value eserver.keystore.password =

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

Se no, digitare *no*. Keytool visualizza ciascun valore immesso in precedenza. Fare clic su **Invio** per accettare o modificare il valore, e fare clic su **Invio**.

- *Password della chiave per l'alias*: se non si immette un'altra password qui, verrà utilizzata la password Keystore.

Richiedere un certificato firmato da un'Autorità di certificazione

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

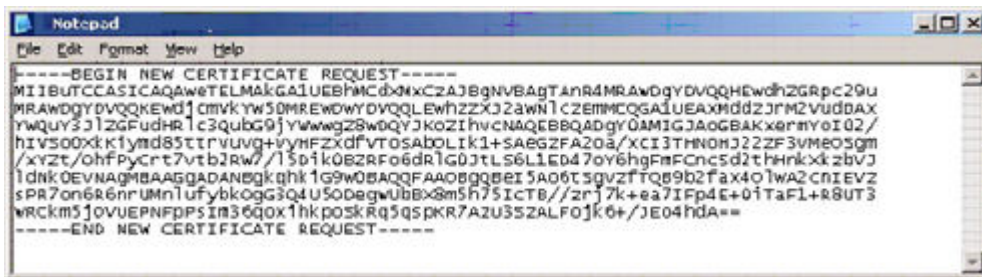
- 1 Sostituire lo stesso valore usato in precedenza per **<certificatealias>**:

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

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

Il file .csr conterrà una coppia BEGIN/END che verrà utilizzata durante la creazione del certificato nella CA.

File .CSR di esempio



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

N.B.:

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

- 3 Alla ricezione del certificato firmato, archivarlo in un file.
- 4 La procedura consigliata è quella di eseguire il backup del certificato in caso di errore durante il processo di importazione, onde evitare di dover ripetere per intero la procedura.



Importare un certificato radice

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

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

1 Effettuare **una** delle seguenti operazioni:

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

2 Effettuare **una** delle seguenti operazioni:

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

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

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

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

Metodo di esempio per richiedere un certificato

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

- 1 Passare al server Microsoft CA. L'indirizzo IP verrà fornito dall'organizzazione.
- 2 Selezionare **Richiedi certificato** e fare clic su **Avanti**.

Servizi certificati Microsoft

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

Scegli tipo di richiesta

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

Richiesta certificato avanzata

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

Invia una richiesta salvata

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

Scarica certificato CA

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

Scarica percorso certificato CA

- 8 Importare il certificato dell'autorità di firma convertito. Tornare alla finestra DOS. Tipo:

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

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

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

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

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

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

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

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

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

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



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

- 1 Interrompere il servizio Security Server, se in esecuzione.
- 2 Eseguire il backup del file dell'Autorità di certificazione in <directory installazione Security Server>\conf\
Usare Keytool per completare le operazioni seguenti:
- 3 Esportare il PFX attendibile in un file di testo e documentare l'Alias:

```
keytool -list -v -keystore "
```
- 4 Importare il PFX nel file dell'Autorità di certificazione in <directory installazione Security Server>\conf\

```
keytool -importkeystore -v -srckeystore "
```
- 5 Modificare il valore keystore.alias.signing in <directory installazione Security Server>\conf\application.properties.

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

Avviare il servizio Security Server.