

Dell Data Protection

Enterprise Server Installation and Migration Guide v9.6



Legend

 **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

 **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

 **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

© 2016 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in the Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, Dell Data Protection | Security Tools, and Dell Data Protection | Secure Lifecycle suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen Tec® and Eikon® are registered trademarks of Authen Tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and 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®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, YouTube®, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, Aperture®, App StoreSM, Apple Remote Desktop™, Apple TV®, Boot Camp™, FileVault™, iCloud®SM, iPad®, iPhone®, iPhoto®, iTunes Music Store®, Macintosh®, Safari®, and Siri® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. GO ID®, RSA®, and SecurID® are registered trademarks of Dell EMC. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. InstallShield® is a registered trademark of Flexera Software in the United States, China, European Community, Hong Kong, Japan, Taiwan, and United Kingdom. Micron® and RealSSD® are registered trademarks of Micron Technology, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners. SAMSUNG™ is a trademark of SAMSUNG in the United States or other countries. Seagate® is a registered trademark of Seagate Technology LLC in the United States and/or other countries. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. This product uses parts of the 7-Zip program. The source code can be found at 7-zip.org. Licensing is under the GNU LGPL license + unRAR restrictions (7-zip.org/license.txt).

Enterprise Server Installation and Migration Guide

2017 - 02

Rev. A01

1 Dell Enterprise Server Introduction.....	5
About Dell Enterprise Server.....	5
Contact Dell ProSupport.....	5
2 Dell Enterprise Server Requirements and Architecture.....	6
Dell Enterprise Server Requirements.....	6
Dell Enterprise Server Prerequisites.....	6
Dell Enterprise Server Hardware.....	6
Dell Enterprise Server Software.....	7
Dell Enterprise Server Language Support.....	9
Dell Enterprise Server Architecture Design.....	9
3 Pre-Installation Configuration.....	15
Configuration.....	15
4 Install or Upgrade/Migrate.....	20
Before You Begin Installation or Upgrade/Migration.....	20
New Installation.....	20
Install Back End Server and New Database.....	21
Install Back End Server with Existing Database.....	34
Install Front End Server.....	48
Upgrade/Migration.....	57
Before You Begin Upgrade/Migration.....	57
Upgrade/Migrate Back End Server(s).....	59
Upgrade/Migrate Front End Server(s).....	65
Disconnected Mode Installation.....	68
Install Enterprise Server in Disconnected Mode.....	71
Uninstall Dell Enterprise Server.....	72
5 Post-Installation Configuration.....	74
EAS Management Installation and Configuration.....	74
Install EAS Device Manager.....	74
Install EAS Mailbox Manager.....	75
Use the EAS Configuration Utility.....	75
Configure EAS Management Settings.....	75
Dell Security Server in DMZ Mode Configuration.....	76
Use Keytool to Import the DMZ Domain Certificate.....	76
Modify application.properties File.....	77
APNs Enrollment.....	77
Server Configuration Tool.....	78
Add New or Updated Certificates.....	78
Import Dell Manager Certificate.....	80
Import Identity Certificate.....	81



Configure settings for Server SSL Certificate or Mobile Edition.....	82
Configure SMTP settings for Secure Lifecycle or Email Services.....	82
Change Database Name, Location, or Credentials.....	83
Migrate the Database.....	83
6 Administrative Tasks.....	85
Assign Dell Administrator Role.....	85
Log in with Dell Administrator Role.....	85
Upload Client Access License.....	85
Commit Policies.....	85
Configure Dell Compliance Reporter.....	86
Configure SQL Authentication with Compliance Reporter.....	86
Configure Windows Authentication with Compliance Reporter.....	86
Perform Back ups.....	87
Enterprise Server Backups.....	87
SQL Server Backups.....	87
PostgreSQL Server Backups.....	87
7 Dell Component Descriptions.....	88
8 SQL Server Best Practices.....	90
9 Certificates.....	91
Create a Self-Signed Certificate and Generate a Certificate Signing Request.....	91
Generate a New Key Pair and a Self-Signed Certificate.....	91
Request a Signed Certificate from a Certificate Authority.....	92
Import a Root Certificate.....	92
Example Method to Request a Certificate.....	93
Export a Certificate to .PFX Using the Certificate Management Console.....	96
Add a Trusted Signing Cert to the Security Server when an Untrusted Certificate was used for SSL.....	97



Dell Enterprise Server Introduction

About Dell Enterprise Server

The Enterprise Server is the security administration piece of Dell's solution. The Remote Management Console allows administrators to monitor the state of endpoints, policy enforcement, and protection across the enterprise.

The Enterprise Server has the following features:

- Centralized management of devices
- Role-based security policy creation and management
- Administrator-assisted device recovery
- Separation of administrative duties
- Automatic distribution of security policies
- Trusted paths for communication between components
- Unique encryption key generation and automatic secure key escrow
- Centralized compliance auditing and reporting

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell Data Protection product.

Additionally, online support for Dell Data Protection products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Code available when you call.

For phone numbers outside of the United States, check [Dell ProSupport International Phone Numbers](#).



Dell Enterprise Server Requirements and Architecture

This section details hardware and software requirements and architecture design recommendations for Dell Data Protection implementation.

Dell Enterprise Server Requirements

The Dell Enterprise Server components have hardware and software requirements in addition to the software provided on the Dell installation media. Ensure that the installation environment meets the requirements before continuing with installation or upgrade/migration tasks.

Before beginning installation, ensure that all patches and updates are applied to the servers used for installation.

Dell Enterprise Server Prerequisites

The following table details the software that must be in place before installing the Dell Enterprise Server. Links and directions to install these prerequisites are detailed in [Pre-Installation Configuration](#).

Each applicable software item must be installed before installation begins, unless it is noted that the installer installs the item. Otherwise, the installation fails.

Dell Enterprise Server Hardware

Prerequisites

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

If not installed, the installer will install it for you.

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

If not installed, the installer will install it for you.

- **.NET Framework Version 3.5 SP1**

- **.NET Framework Version 4.5**

Microsoft has published security updates for .NET Framework Version 4.5.

- **SQL Native Client 2012**

If using SQL Server 2012 or SQL Server 2016.

The following table details the *minimum* hardware requirements for Dell Enterprise Server. See [Dell Enterprise Server Architecture Design](#) for additional information about scaling based on the size of your deployment.

Hardware Requirements

Processor

Modern Dual-Core CPU minimum (2 GHz+), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent
Modern Quad-Core CPU (2 GHz+) for single-server configuration

RAM

8GB minimum, depending on configuration
16GB for single-server configuration

Free Disk Space

+1.5 GB free disk space (plus virtual paging space)
20GB or more free disk space (plus virtual paging space) for single-server configuration

Network Card

10/100/1000 network interface card

Miscellaneous

TCP/IPv4 installed and activated

Dell Enterprise Server Software

The following table details the software requirements for the Dell Enterprise Server and Proxy Server.

- NOTE:** UAC must be disabled before installation. The server must be rebooted for this change to take effect. On Windows Server 2012 R2 and Windows Server 2016, the installer disables UAC.
- NOTE:** Registry locations for Dell Policy Proxy (if installed): HKLM\SOFTWARE\Wow6432Node\Dell
- NOTE:** Registry location for Windows Servers: HKLM\SOFTWARE\Dell

Dell Enterprise Server - Back End Server and Dell Front End Server

- **Windows Server 2008 R2 SP0-SP1 64-bit**
 - Standard Edition
 - Enterprise Edition
- **Windows Server 2008 SP2 64-bit**
 - Standard Edition
 - Enterprise Edition
- **Windows Server 2012 R2**
 - Standard Edition
 - Datacenter Edition
- **Windows Server 2016**
 - Standard Edition



Exchange ActiveSync Servers

If you intend to use Mobile Edition, the following Exchange ActiveSync Servers are supported. This component is installed on your front-end Exchange Server.

- Exchange ActiveSync 12.0 - a component of Exchange Server 2007
- Exchange ActiveSync 12.1 - a component of Exchange Server 2007 SP1
- Exchange ActiveSync 14.0 - a component of Exchange Server 2010
- Exchange ActiveSync 14.1 - a component of Exchange Server 2010 SP1

Microsoft Message Queuing (MSMQ) must be installed/configured on the Exchange Server.

LDAP Repository

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

Recommended Virtual Environments for Dell Enterprise Server Components

The Dell Enterprise Server can optionally be installed in a virtual environment. Only certain environments are recommended and there may be performance considerations as described below.

- Dell Enterprise Server v9.6 has been validated with VMware ESXi 5.5 and VMware ESXi 6.0. Ensure that all patches and updates are immediately applied to VMware ESXi to address potential vulnerabilities.

NOTE: When running VMware ESXi and Windows Server 2012 R2 or Windows Server 2016, VMXNET3 Ethernet Adapters are recommended.

Dell Enterprise Server Performance in a Virtual Environment

- Dell has observed up to a 50% performance impact, depending on environment. The impact is most noticeable during activation, inventory processing, and triage. If performance is a concern, we recommend deploying to a non-virtual server environment.
- The SQL Server database hosting the Dell Enterprise Server should be run on a separate computer and on physical hardware.

Database

- **SQL Server 2008 and SQL Server 2008 R2** - Standard Edition / Enterprise Edition
- **SQL Server 2008 SP4 (with 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

NOTE: Express Editions are not supported for production environments. Express Editions may be used in POC and evaluations only.

Dell Data Protection Remote Management Console and Compliance Reporter

- Internet Explorer 11.x or later
- Mozilla Firefox 41.x or later
- Google Chrome 46.x or later

NOTE: Your browser must accept cookies.

Dell Enterprise Server Language Support

The Remote Management Console is Multilingual User Interface (MUI) compliant and support the following languages:

Language Support

EN - English	JA - Japanese
ES - Spanish	KO - Korean
FR - French	PT-BR - Portuguese, Brazilian
IT - Italian	PT-PT - Portuguese, Portugal (Iberian)
DE - German	

Dell Enterprise Server Architecture Design

The Dell Data Protection Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise, and Secure Lifecycle solutions are highly scalable products, scaled on the size of your organization and the number of endpoints targeted for encryption. This section provides a set of guidelines for scaling the architecture for 5,000 to 60,000 endpoints.

NOTE: If the organization has more than 50,000 endpoints, please contact Dell ProSupport for assistance.

NOTE:

Each of the components listed in each section include the minimum hardware specifications, which are required to ensure optimal performance in most environments. Failing to allocate adequate resources to any of these components may result in performance degradation or functional problems with the application.

Up to 5,000 Endpoints

This architecture accommodates most small to medium size businesses ranging between 1 and 5,000 endpoints. All Dell Enterprise Server components can be installed on a single server. Optionally, a front-end server can be placed in the DMZ for publishing policies and/or activating endpoints over the Internet.

Architecture Components

Dell Enterprise Server

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

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

Single-Server Configuration

16GB; 20GB or more free disk space (plus virtual paging space); Modern Quad-Core CPU (2 GHz+)

Server configuration when used with Front-End Server

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell External Front-End Server

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



Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

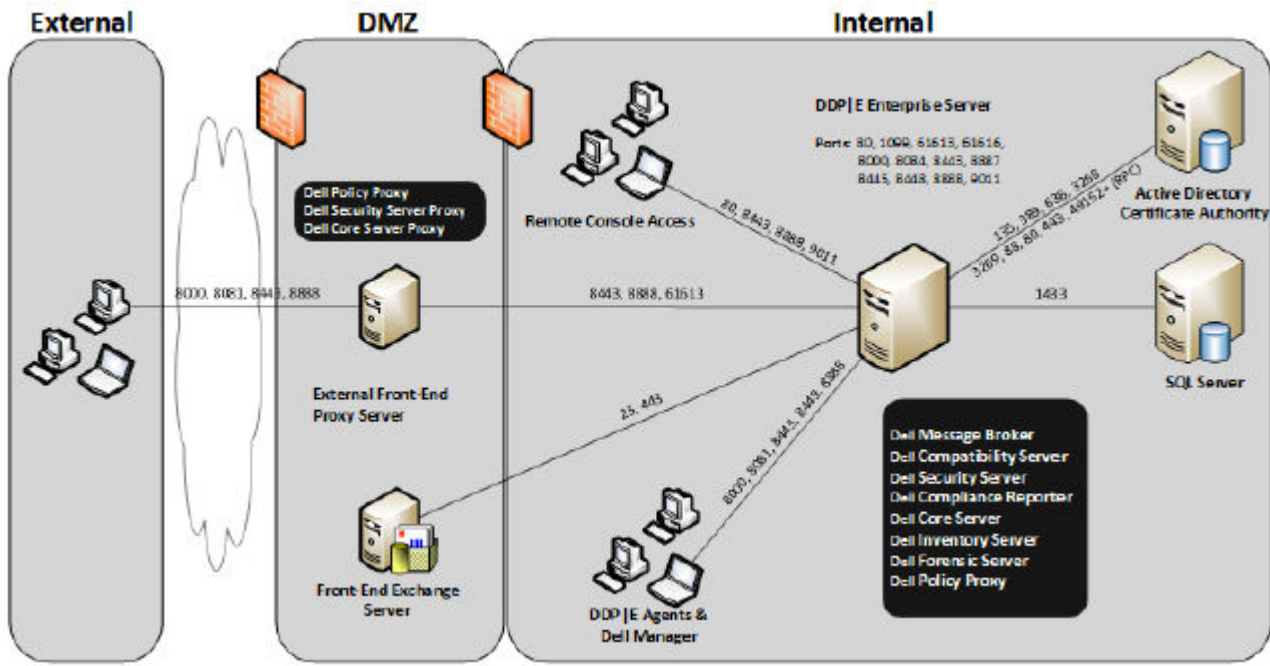
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with 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



5,000 - 20,000 Endpoints

This architecture accommodates environments ranging between 5,000 and 20,000 endpoints. A front-end server is added to distribute the additional load and is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for publishing policies and/or activating endpoints over the Internet.

Architecture Components

Dell Enterprise Server

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell Internal Front-End Server (1) and Dell External Front-End Server (1)

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

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition



8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

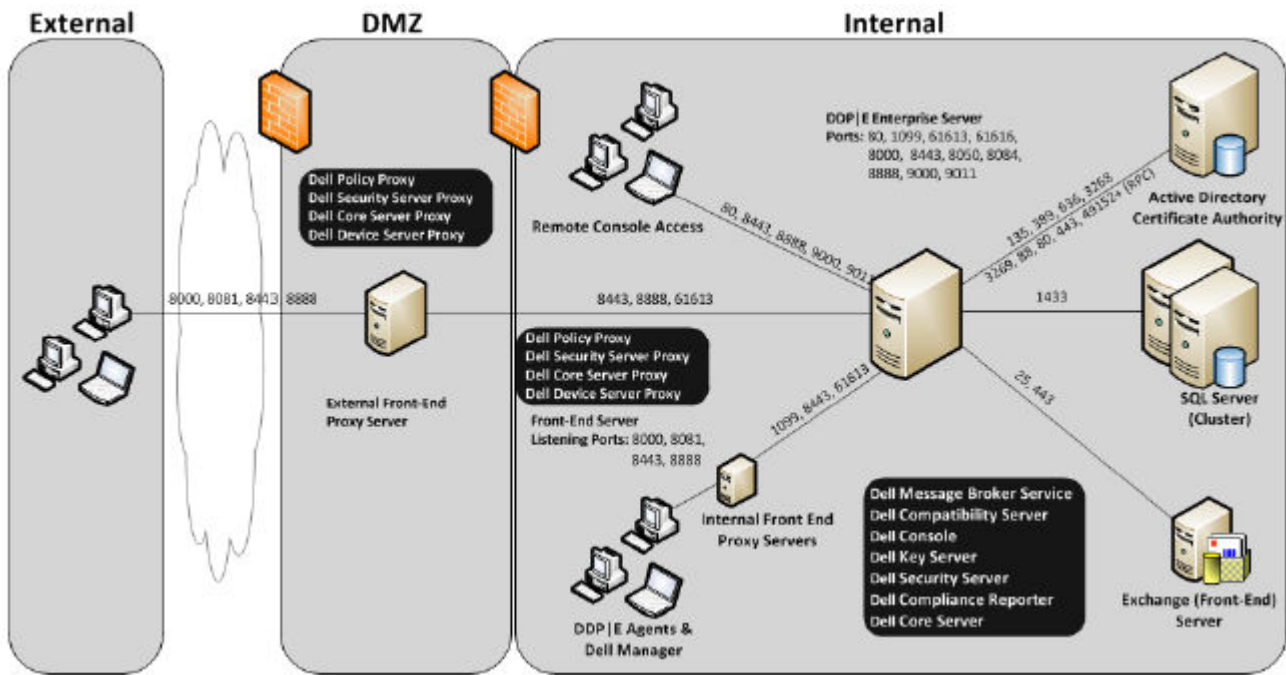
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with 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



20,000 - 40,000 Endpoints

This architecture accommodates environments ranging between 20,000 and 40,000 endpoints. An additional front-end server is added to distribute the additional load. Each front-end server is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.

Architecture Components

Dell Enterprise Server

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

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell Internal Front-End Servers (2) and Dell External Front-End Server (1)

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

Windows Server 2012 R2 - Standard or Datacenter Edition



Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

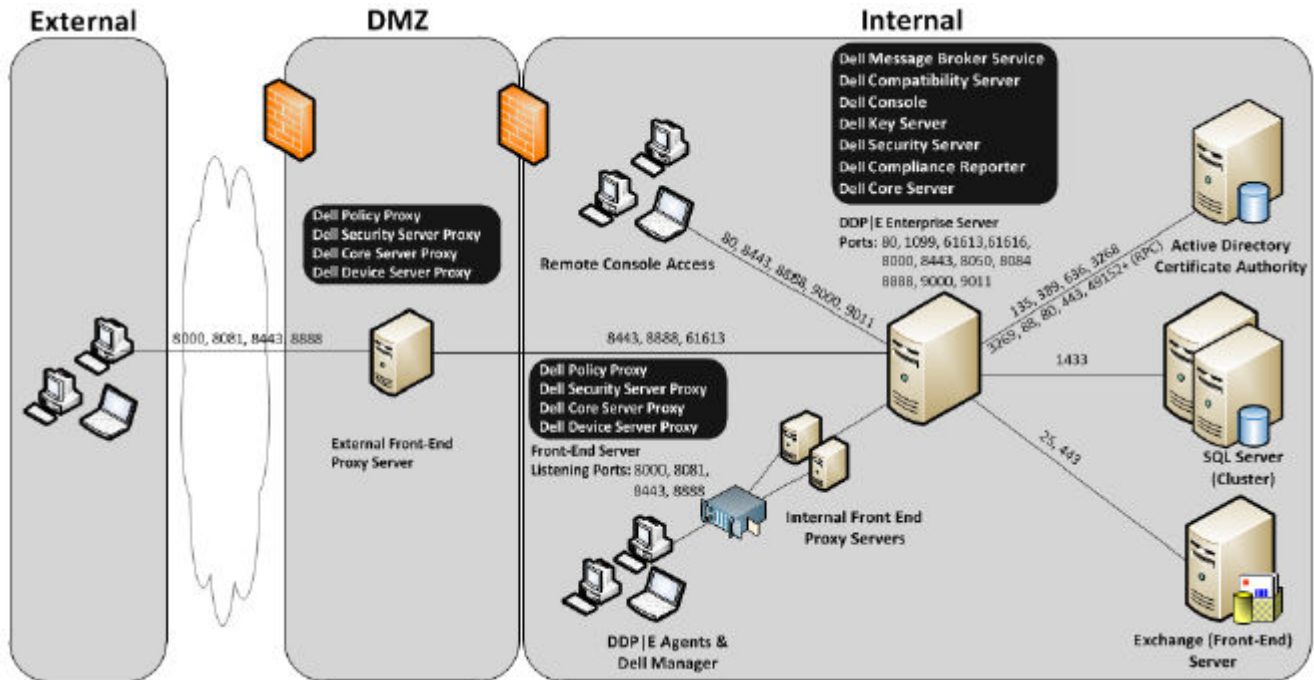
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with 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



40,000 - 60,000 Endpoints

This architecture accommodates environments ranging between 40,000 and 60,000 endpoints. An additional front-end server is added to distribute the additional load. Each front-end server is designed to handle approximately 15,000 - 20,000 endpoints. Optionally, a front-end server can be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.

NOTE:

If the organization has more than 50,000 endpoints, please contact Dell ProSupport for assistance.

Architecture Components

Dell Enterprise Server

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

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition



8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

Dell Internal Front-End Servers (2) and Dell External Front-End Server (1)

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

Windows Server 2012 R2 - Standard or Datacenter Edition

Windows Server 2016 - Standard or Datacenter Edition

8GB minimum, depending on configuration; +-1.5 GB free disk space (plus virtual paging space); Modern Dual-Core CPU minimum (2 GHz +), including Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium, or AMD equivalent

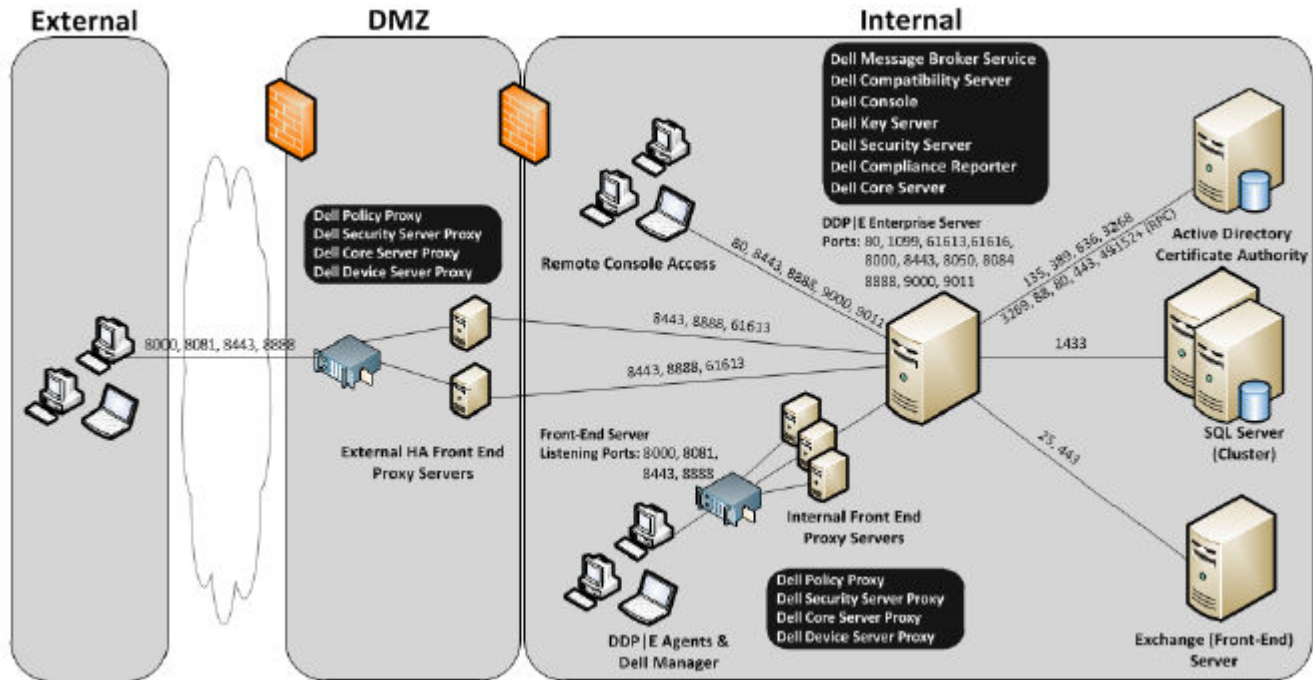
SQL Server

SQL Server 2008, SQL Server 2008 R2, and SQL Server 2008 SP4 (with 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



High Availability Considerations

This architecture depicts a highly available architecture supporting up to 60,000 endpoints. There are two Dell Enterprise Servers set up in an active/passive configuration. To failover to the second Dell Enterprise Server, stop the services on the primary node and point the DNS Alias (CNAME) to the second node. Start the services on the second node and launch the Remote Management Console to ensure the application is working properly. Services on the second (passive) node should be configured as "Manual" in order to prevent those services from accidentally starting during regular maintenance and patching.

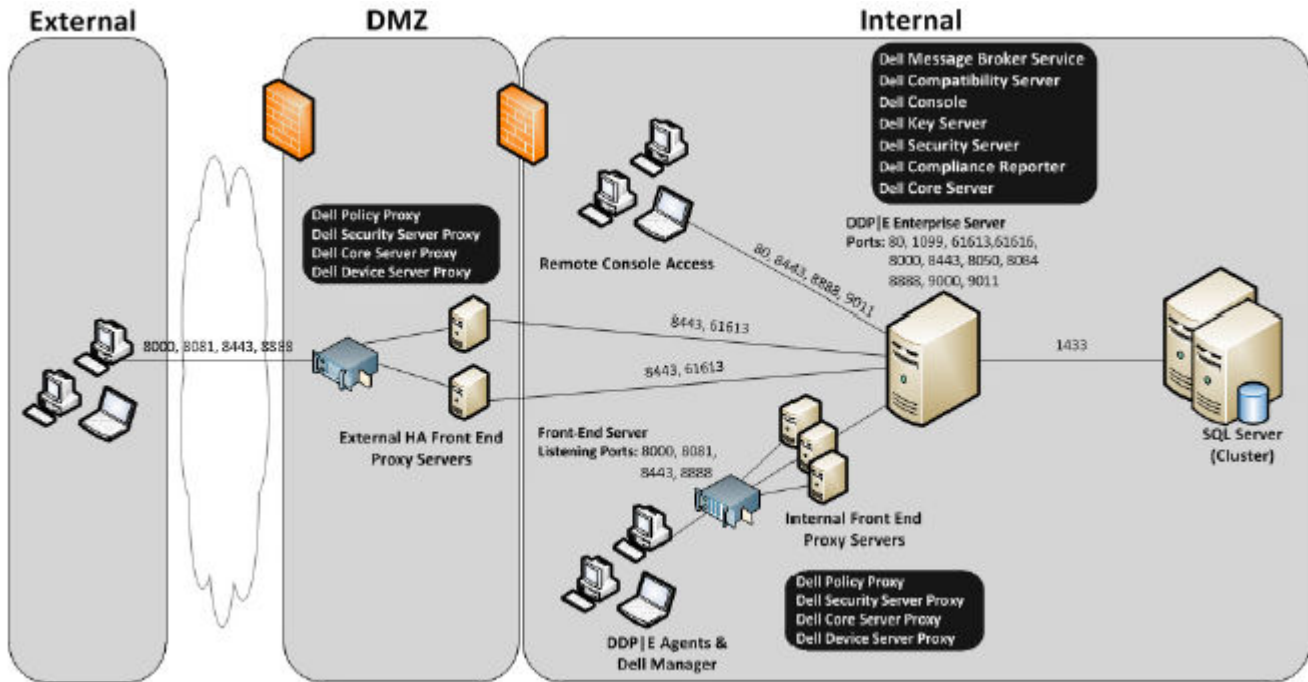
An organization can also choose to have an SQL Cluster database server. In this configuration, the Dell Enterprise Server should be configured to use the cluster IP or hostname.



NOTE:

Database replication is not supported.

Client traffic is distributed across three internal front-end servers. Optionally, multiple front-end servers can also be placed in the DMZ for activating endpoints and/or publishing policies to endpoints over the Internet.



Virtualization

Dell Data Protection Application Servers

Disk speed on the hardware that hosts the virtual server, RAM allocation to the guest, and storage configuration may cause significant performance impact. The impact is most noticeable during activation, policy and inventory processing, and triage. Dell recommends reserving as much RAM as possible for the virtual host, and giving the virtual host priority in resource allocation. If performance is a concern, Dell recommends deploying to a non-virtual server environment.

SQL Server

In larger environments, it is highly recommended that the SQL Database server run on physical hardware and on a redundant system, such as a SQL Cluster, to ensure availability and data continuity. It is also recommended to perform daily full backups with transactional logging enabled to ensure that any newly generated keys through user/device activation are recoverable.

Database maintenance tasks should include rebuilding of all databases indexes and collecting statistics.



Pre-Installation Configuration

Before you begin, read the *Enterprise Server Technical Advisories* for any current workarounds or known issues related to Dell Enterprise Server.

The pre-installation configuration of the server(s) where you intend to install the Dell Enterprise Server is very important. Pay special attention to this section to ensure a smooth installation of the Dell Enterprise Server.

Configuration

- 1 If enabled, turn off Internet Explorer Enhanced Security Configuration (ESC). Add the Server URL to Trusted Sites in the browser security options. Reboot the server.
- 2 Open the following ports for each component:

Internal:

Active Directory communication: TCP/389

Email communication (optional): 25

To Front End (if needed):

Communication from external Dell Policy Proxy to Dell Message Broker: TCP/61616 and STOMP/61613

Communication to Back End Dell Security Server: HTTPS/8443

Communication to Back End Dell Core Server: HTTPS/8888 and 9000

Communication to RMI ports - 1099

Communication to Back End Dell Device Server: HTTP(S)/8443 - If your Dell Enterprise Server is v7.7 or later. If your Dell Enterprise Server is pre-v7.7, HTTP(S)/8081.

External (if needed):

SQL Database: TCP/1433

Remote Management Console: HTTPS/8443

LDAP: TCP/389/636 (local domain controller), TCP/3268/3269 (global catalog), TCP/135/49125+ (RPC)

Dell Compatibility Server: TCP/1099

Dell Compliance Reporter: HTTP(S)/8084 (automatically configured at installation)

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 and 9000 (8888 is automatically configured at installation)

Dell Device Server: HTTP(S)/8443 (Dell Enterprise Server v7.7 or later) or HTTP(S)/8081 (Pre-v7.7 Dell Enterprise Server)



Dell Key Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell Security Server: HTTPS/8443

Client Authentication: HTTPS/8449 (If using Server Encryption)

Beacon server: HTTP/8446 (If using Secure Lifecycle)



NOTE:

If your Enterprise Edition clients will be entitled from the factory or you purchase licenses from the factory, set the GPO on the domain controller to enable entitlements (this may not be the server running Enterprise Edition). Ensure that outbound port 443 is available to communicate with the Server. If port 443 is blocked for any reason, the entitlement functionality will not work. For more information, see [Enterprise Edition Advanced Installation Guide](#).

Create Dell Database

- 3 If you do not yet have a SQL database configured for Dell Enterprise Server, the installer creates the database for you during installation. If you would prefer to set up a database before you install Dell Enterprise Server, follow the instructions below to create the SQL database and SQL user in SQL Management Studio. **These instructions are optional, because the installer will create a database for you if one does not already exist.**

When you install Dell Enterprise Server, follow the instructions in [Install Back End Server with Existing Database](#).

The Dell Enterprise Server is prepared for both SQL and Windows Authentication. The default authentication method is SQL Authentication.

After you create the database, create a Dell database user with db_owner rights. The db_owner may assign permissions, back up and restore the database, create and delete objects, and manage user accounts and roles without any restrictions. Additionally, ensure that this user has permissions/privileges to run stored procedures.

When using a non-default SQL Server instance, after Dell Enterprise Server installation, you must specify the dynamic port of the instance on the Database tab of the Server Configuration Tool. For more information, see [Server Configuration Tool](#). As an alternative, enable the SQL Server Browser service and ensure that UDP port 1434 is open. For more information, see [https://msdn.microsoft.com/en-us/library/hh510203\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx).

If either the SQL database or SQL instance is configured with a non-default collation, the non-default collation must be case-insensitive. For a list of collations and case sensitivity, see [https://msdn.microsoft.com/en-us/library/ms144250\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx).

To create the SQL database and SQL user in SQL Management Studio, choose one:

Create a New Windows SQL Server Database using Windows Authentication:

- a Click **Start > All Programs > Microsoft SQL Server > Management Studio**.
- b Right-click the Databases folder, and then click New Database. The Database Properties dialog displays.
- c Enter the Database Name and click **OK**.
- d Expand the *Security* folder, and right-click **Logins**.
- e Click **New Login** to create an owner for the new database.
- f Enter a username in the *Name* field.
- g Select the Authentication option *Windows Authentication*.
- h Select **User Mapping** and then highlight the new database.
- i Select the database role (db_owner), and click **OK**.

OR



Create a New SQL Server Database using SQL Server Authentication:

- a Click **Start > All Programs > Microsoft SQL Server > Management Studio**.
- b Right-click the *Databases* folder, and then click **New Database**. The *Database Properties* dialog displays.
- c Enter the Database Name and click **OK**.
- d Expand the *Security* folder, and right-click **Logins**.
- e Click **New Login** to create an owner for the new database.
- f Enter a username in the *Name* field.
- g Select the Authentication option *SQL Server Authentication*. Enter and confirm the password.
- h Deselect **Enforce Password Expiration**.
- i Select **User Mapping** and then highlight the new database.
- j Select the database role (db_owner), and click **OK**.

Install Visual C++ 2010/2013 Redistributable Package

- 4 *If not already installed*, install Visual C++ 2010 and 2013 Redistributable Packages. If desired, you can allow the Dell Enterprise Server installer to install these components.

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

Install .NET Framework 4.5

- 5 *If not already installed*, install .NET Framework 4.5.

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

Install SQL Native Client 2012

- 6 *If using SQL Server 2012 or SQL Server 2016*, install SQL Native Client 2012.

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

Configure Microsoft CA (MSCEP)

This step only needs to be completed on your server running MSCEP if you intend to use iOS with Mobile Edition.

- 7 Configure MSCEP.

Windows Server 2008 R2 must be Enterprise Edition. ***Standard Edition will not allow the MSCEP role to be installed.***

- a Open Server Manager. In the left menu, select **Server Roles** and check the box for **Active Directory Certificate Services**. Click **Next**. The Add Roles Wizard advances you to the next steps.

In *AD CS > Role Services*, check the boxes for **Certification Authority** and **Certification Authority Web Enrollment** role services. Select **Add Required Role Services for Web Server IIS** (if prompted). Click **Next**.

In *AD CS > Setup Type*, select **Standalone**. Click **Next**.

In *AD CS > CA Type*, select **Subordinate CA**. Click **Next**.

In *AD CS > Private Key*, select **Create a new private key**. Click **Next**.

In *AD CS > Private Key > Cryptography*., keep the defaults of **RSA#Microsoft Software Key Storage Provider, 2048** and **SHA1**. Click **Next**.

In *AD CS > Private Key > CA Name*, keep all of the default values. Click **Next**.



In *AD CS > Private Key > Certificate Request.*, select **Send a certificate request to a parent: CA**. Select **Browse by: CA name**. Browse to and select **Parent CA**. Click **Next**.

In *AD CS > Certificate Database*, keep the default values. Click **Next**.

In *Web Server (IIS)*, click **Next**.

In *Web Server (IIS) > Role Services*, keep the default values. Click **Next**.

In *Confirmation*, click **Install**.

In *Results*, review the results and click **Close**.

In *Server Manager > Roles*, select **Add Role Services** under *Active Directory Certificate Services*.

When the *Select Role Services* window displays, check the box for **Network Device Enrollment Service**. Click **Next**.

Add the user account that *Network Device Enrollment Service* should use when authorizing certificate requests to the Users Group of IIS_IUSRS of the local server. The format is Domain\UserName. Click **OK**.

At the *Specify User Account* windows, select the user that was just added to the IIS_IUSRS group. Click **Next**.

At the *Specify Registration Authority Information* window, keep the default values for *Required Information* and *Add Optional Information* as desired. Click **Next**.

At the *Configure Cryptography for Registration Authority* window, keep the default values. Click **Next**.

At the *Confirm Installation Selections* window, click **Install**.

At the *Installation Results* window, review the results and click **Close**.

Close Server Manager.

- b Modify Registry Key as follows:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

- c Open IIS Manager. Drill into **\<ServerName> \Sites\Default Web Site\CertSrv\mscep_admin**.

Open *Authentication* and enable **Anonymous Authentication**.

- d Click **Start > Run**. Type *certsrv.msc* and click **Enter**.

When the *certsrv* window displays, right-click the server name, select **Properties** and click the **Policy Module** tab.

Click **Properties** and select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**. Click **OK**.

- e Close IIS Manager.

- f Restart the server. To verify, open Internet Explorer and in the address bar, enter

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

End of MSCEP Windows Server 2008 R2 setup.

Windows Server 2012 R2 or Windows Server 2016:

- a Follow Setup instructions in the article, [Network Device Enrollment Service \(NDES\) in Active Directory Certificate Services \(AD CS\)](#)."

- b Modify Registry Key as follows:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

- c Open IIS Manager. Drill into `\<ServerName>\Sites\Default Web Site\CertSrv\mscep_admin`.

Open *Authentication* and enable **Anonymous Authentication**.

- d Click **Start > Run**. Type `certsrv.msc` and click **Enter**.

When the `certsrv` window displays, right-click the server name, select **Properties** and click the **Policy Module** tab.

Click **Properties** and select **Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate**. Click **OK**.

- e Close IIS Manager.
- f Restart the server. To verify, open Internet Explorer and in the address bar, enter

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

End of MSCEP Windows Server 2012 R2/Windows Server 2016 setup.

Install/Configure Microsoft Message Queuing (MSMQ)

This step only needs to be completed if you intend to use Mobile Edition. This is a prerequisite for the EAS Device Manager and EAS Mailbox Manager to be able to communicate.

- 8 On Windows Server 2008 or Windows Server 2008 R2 (on the server hosting the Exchange environment): <http://msdn.microsoft.com/en-us/library/aa967729.aspx>

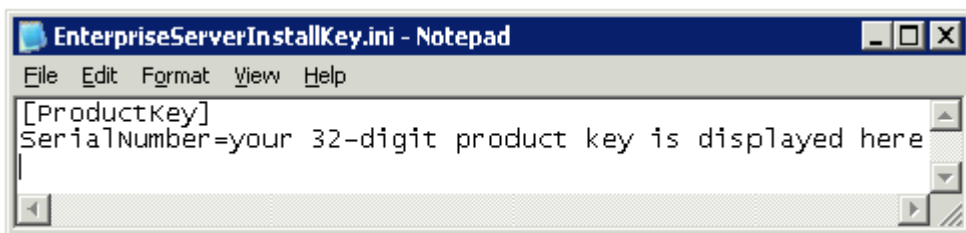
OR

On Windows Server 2012 R2:

- a Open Server Manager.
- b Navigate to **Manage > Add Roles and Features**.
- c In the Before You Begin screen, click **Next**.
- d Select **Role-based or feature-based installation**, and click **Next**.
- e Select the server on which to install the feature, and click **Next**.
- f Do not select any server roles. Click **Next**.
- g In Features, select **Message Queuing**, and click **Install**.

Optional

- 9 **For a new installation** - copy your Product Key (the name of the file is `EnterpriseServerInstallKey.ini`) to `C:\Windows` to automatically populate the 32-character Product Key in the Dell Enterprise Server installer.



The pre-installation configuration of the server is complete. Continue to [Install or Upgrade/Migrate](#).

Install or Upgrade/Migrate

The chapter provides instructions for the following:

- [New Installation](#) - To install a new Dell Enterprise Server.
- [Upgrade/Migration](#) - To upgrade from an existing, functional Dell Enterprise Server v8.0 or later.
- [Uninstall Dell Enterprise Server](#) - To remove the current installation, if necessary.

If your installation must include more than one Main Server (Back End), contact your Dell ProSupport representative.

Before You Begin Installation or Upgrade/Migration

Before you begin, ensure that applicable [Pre-Installation Configuration](#) steps are complete.

Read the *Enterprise Server Technical Advisories* for any current workarounds or known issues related to Dell Enterprise Server installation.

If User Account Control (UAC) is enabled, you must disable it. On Windows Server 2012 R2, the installer disables UAC. The server must be rebooted for this change to take effect.

During installation, Windows or SQL Authentication credentials are required to set up the database. If you select Windows Authentication, the logged on user credentials are used. The user must have system administrator rights and rights to create and manage the SQL database (create database, add user, and assign permissions). For SQL Authentication, the account used must have these same rights. These credentials are used only during installation. The installed product does not use these credentials.

Also during installation, service runtime authentication credentials must be specified for Dell services to use to access the SQL server. The user account must have the SQL server permissions Default Schema: dbo and Database Role Membership: db_owner, public.

If you are uncertain about access privileges or connectivity to the database, ask your database administrator to confirm these before you begin installation.

Dell recommends that database best practices are used for the Dell database and that Dell software is included in your organization's disaster recovery plan.

If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

For production, Dell strongly recommends installing the SQL Server on a dedicated server.

It is best practice to install the Back End Server before installing and configuring a Front End Server.

Installation log files are located in this directory: `C:\ProgramData\Dell\Dell Data Protection\Installer Logs`

New Installation

Choose one of two options for Back End Server installation:

- [Install Back End Server and New Database](#) - To install a new Dell Enterprise Server and a new database.
- [Install Back End Server with Existing Database](#) - To install a new Dell Enterprise Server and connect to a SQL database created during [Pre-Installation Configuration](#) or an existing SQL database that is v9.x or later, when the schema version matches the Dell Enterprise Server version to be installed. A v8.x or later database must be migrated to the latest schema with the latest version of Server

Configuration Tool. For instructions on database migration with the Server Configuration Tool, see [Migrate the Database](#). To obtain the latest Server Configuration Tool, or to migrate a pre-v8.0 database, contact Dell ProSupport for assistance.

NOTE:

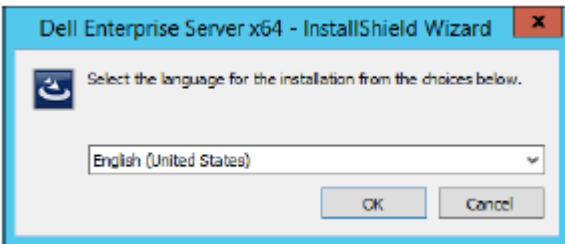
If you have a functional Dell Enterprise Server v8.x or later, refer to instructions in [Upgrade/Migrate Back End Server\(s\)](#).

If you install a Front End Server, perform this installation after Back End Server installation:

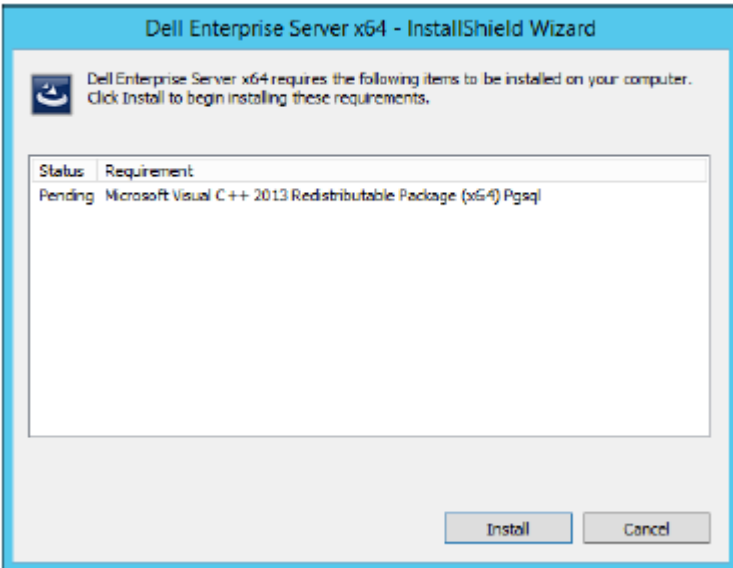
- [Install Front End Server](#) - To install a Front End Server to communicate with a Back End Server.

Install Back End Server and New Database

- 1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (DO NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Enterprise Server. **Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.**
- 2 Double-click **setup.exe**.
- 3 In the *InstallShield Wizard* dialog, select the language for installation, then click **OK**.

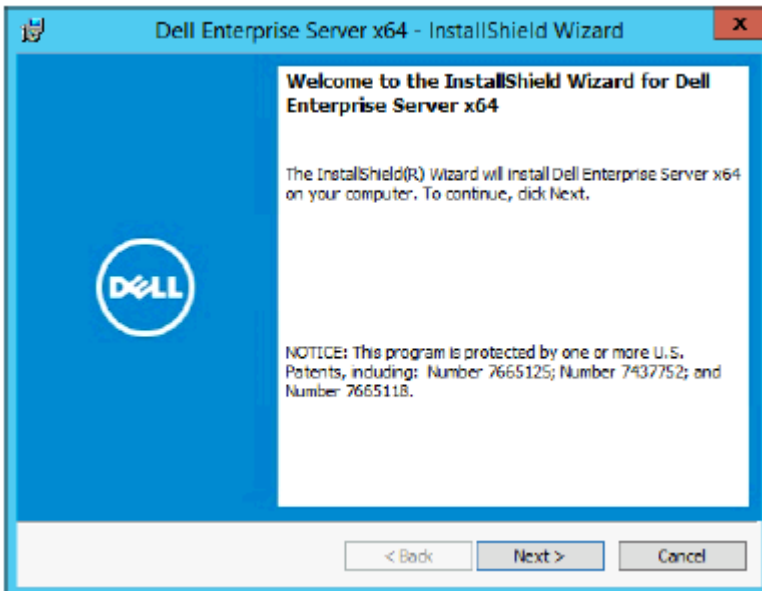


- 4 If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.

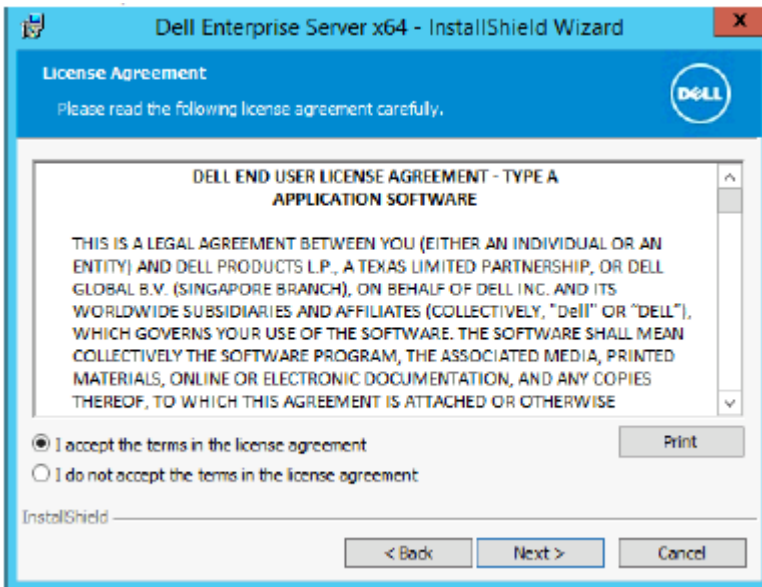


- 5 In the *Welcome* dialog, click **Next**.



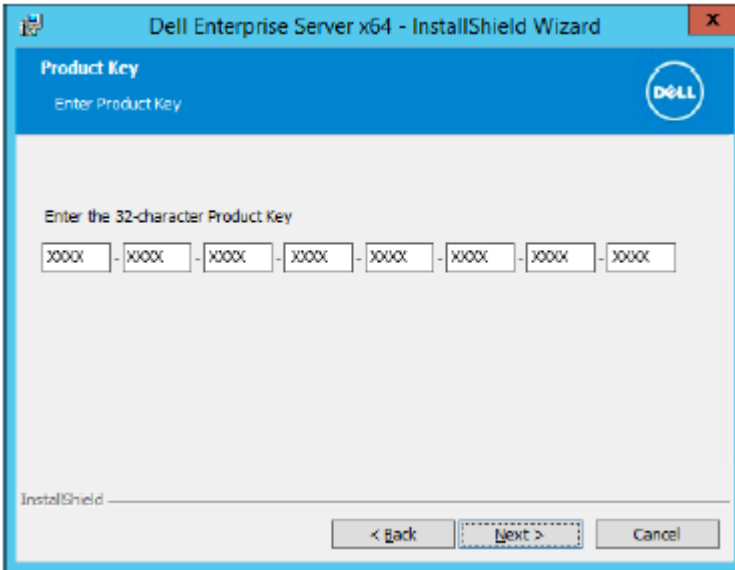


- 6 Read the license agreement, accept the terms, then click **Next**.

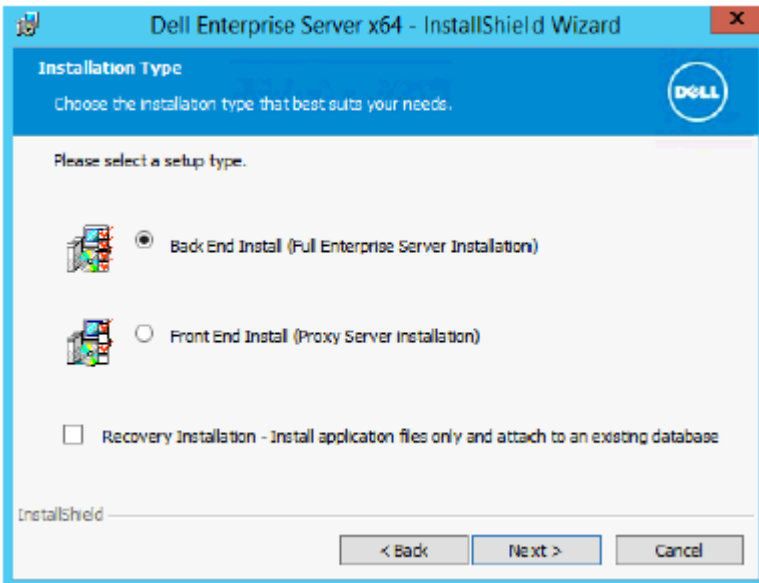


- 7 If you optionally completed [step 9 in Pre-Installation Configuration](#), click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is located in the file "*EnterpriseServerInstallKey.ini*".



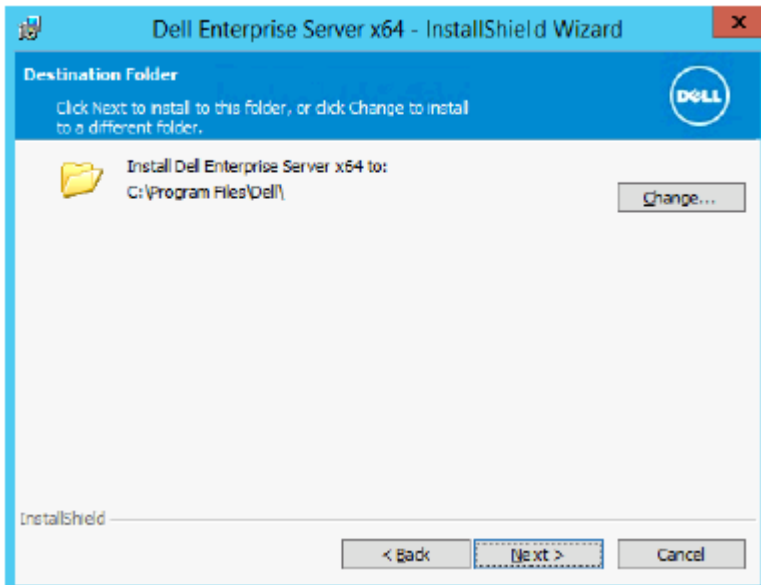


- 8 Select **Back End Install** and click **Next**.

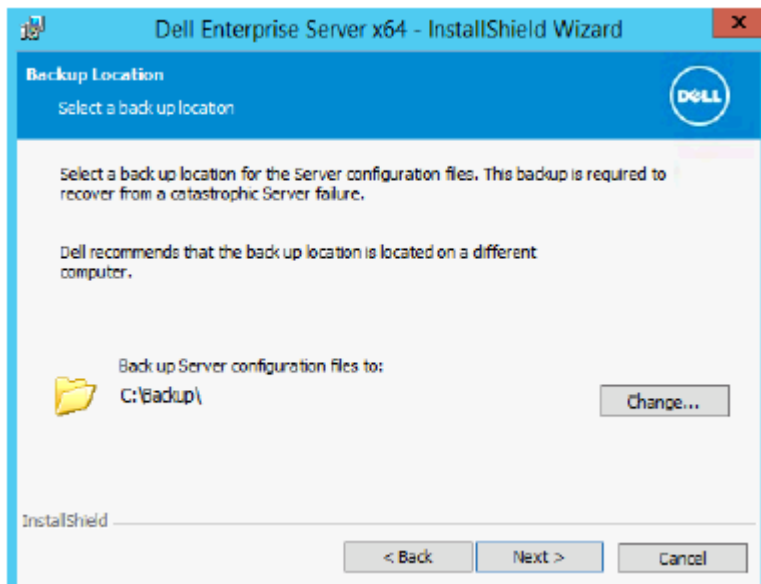


- 9 To install the Dell Enterprise Server to the default location of C:\Program Files\Dell, click **Next**. Otherwise, click **Change** to select a different location, then click **Next**.



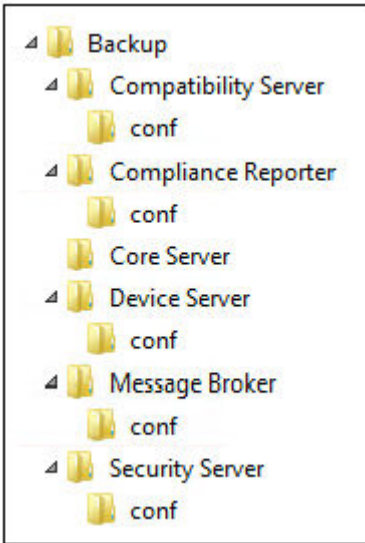


- 10 To select a location for backup configuration files to be stored, click **Change**, navigate to the desired folder, then click **Next**. **Dell recommends that you select a remote network location or external drive for backup.**



After installation, any changes to configuration files, including changes made with the Server Configuration Tool, must be manually backed up in these folders. Configuration files are an important part of the total information used to manually restore the server.

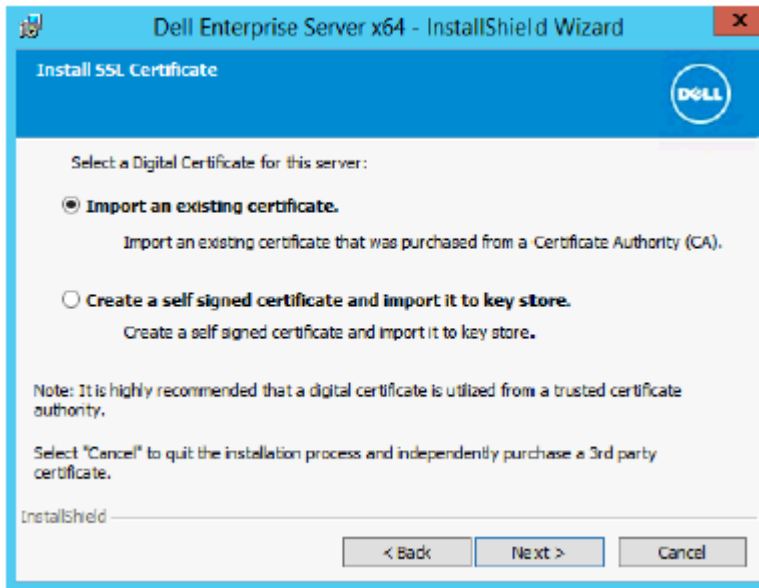
NOTE: The folder structure created by the installer during this installation step (example shown below) must remain unchanged.



11 You have a choice of digital certificate types to use. **It is highly recommended that you use a digital certificate from a trusted certificate authority.**

Select option "a" or "b" below:

- a To use an existing certificate that was purchased from a CA authority, select **Import an existing certificate** and click **Next**.



Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See [Exporting a Certificate to .PFX Using the Certificate Management Console](#) for instructions.

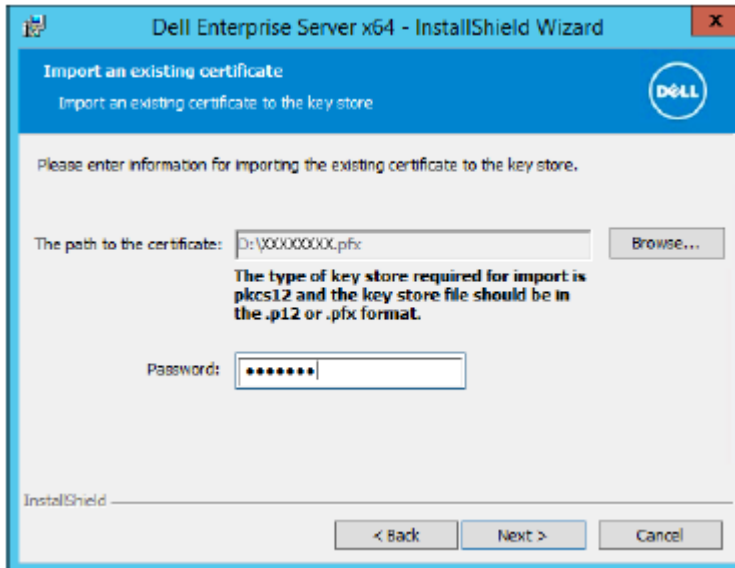
Click **Next**.



NOTE:

To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":

- Personal Information Exchange - PKCS#12 (.PFX)
- Include all certificates in the certification path if possible
- Export all extended properties



OR

- b To create a self-signed certificate, select **Create a self signed certificate and import it to key store and click Next.**

At the *Create Self-Signed Certificate* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organization

Organizational Unit (example: Security)

City

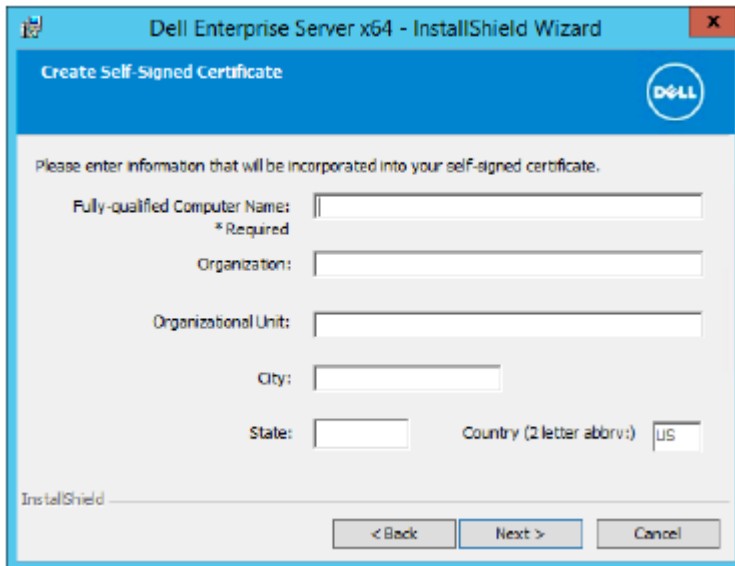
State (full name)

Country: Two-letter country abbreviation

Click **Next**.

NOTE:

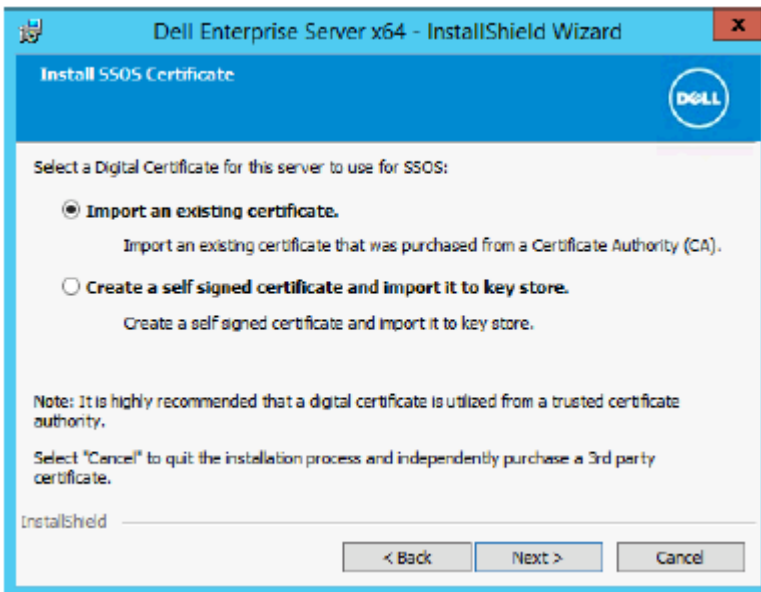
The certificate expires in one year, by default.



12 For Server Encryption (SE), you have a choice of digital certificate types to use. It is highly recommended that you use a digital certificate from a trusted certificate authority.

Select option "a" or "b" below:

- a To use an existing certificate that was purchased from a CA authority, select **Import an existing certificate** and click **Next**.



Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See [Exporting a Certificate to .PFX Using the Certificate Management Console](#) for instructions.

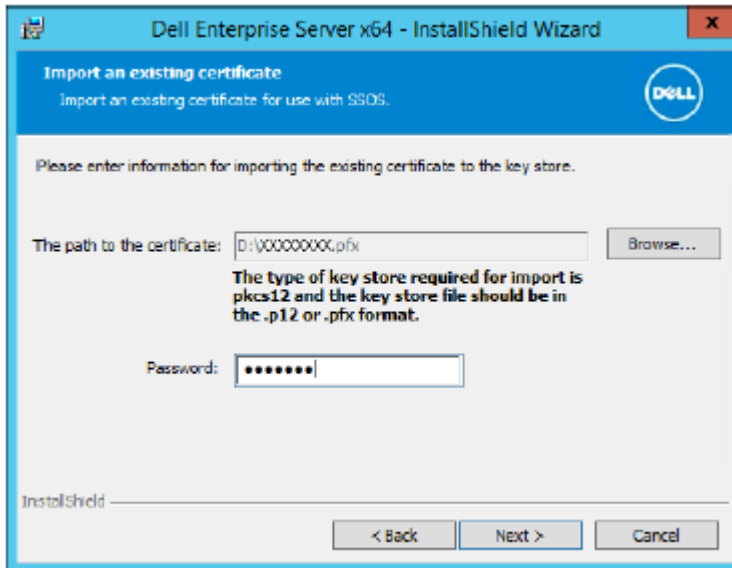
Click **Next**.



NOTE:

To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":

- Personal Information Exchange - PKCS#12 (.PFX)
- Include all certificates in the certification path if possible
- Export all extended properties



OR

- b To create a self-signed certificate, select **Create a self signed certificate and import it to key store and click Next.**

At the *Create Self-Signed Certificate* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organization

Organizational Unit (example: Security)

City

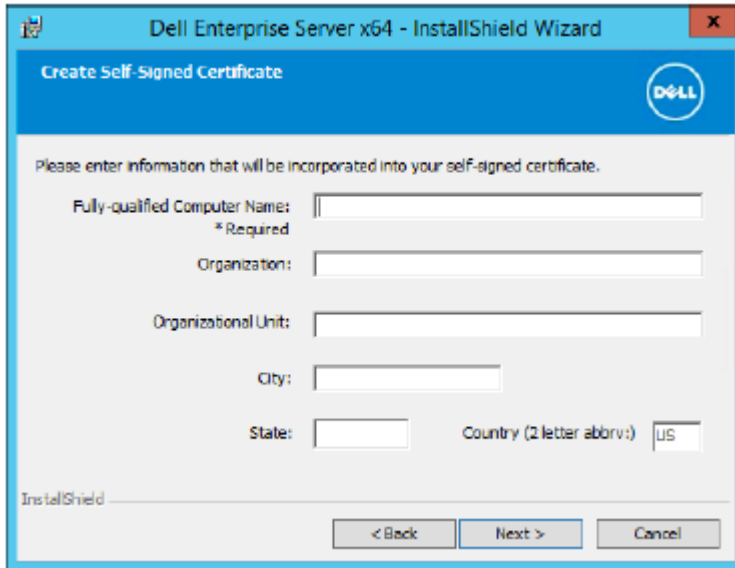
State (full name)

Country: Two-letter country abbreviation

Click **Next**.

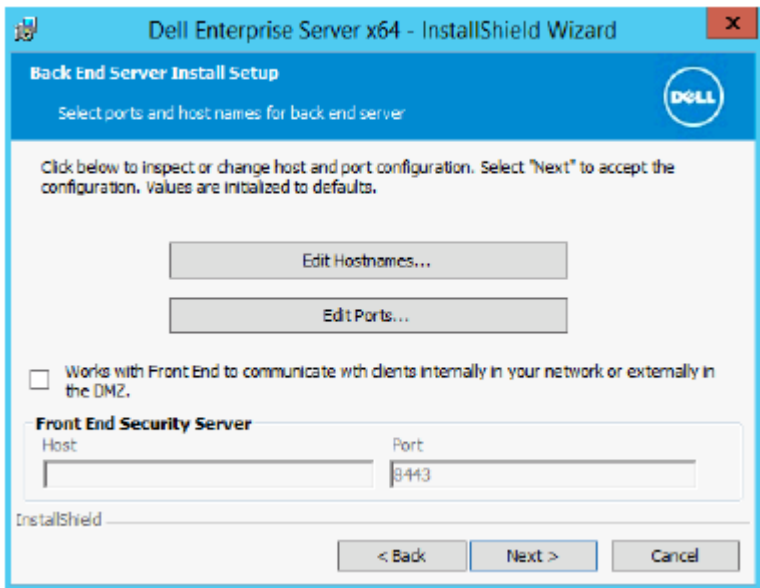
NOTE:

The certificate expires in one year, by default.



13 From the *Back End Server Install Setup* dialog, you can view or edit hostnames and ports.

- To accept the default hostnames and ports, in the *Back End Server Install Setup* dialog, click **Next**.
- If you are using a Front End Server, select **Works with Front End to communicate with clients internally in your network or externally in the DMZ** and enter the Front End Security Server hostname (for example, server.domain.com).

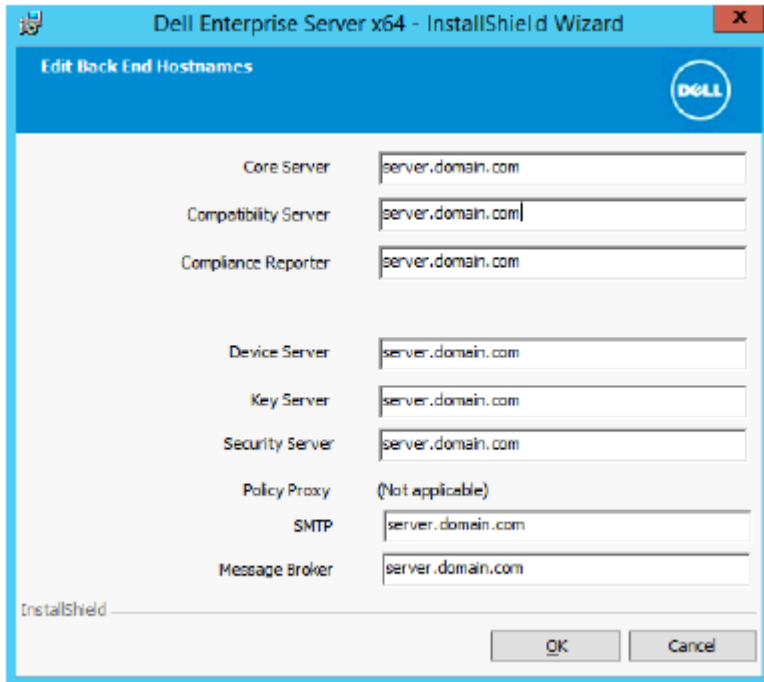


- To view or edit hostnames, click **Edit Hostnames**. Edit hostnames only if necessary. Dell recommends using the defaults.

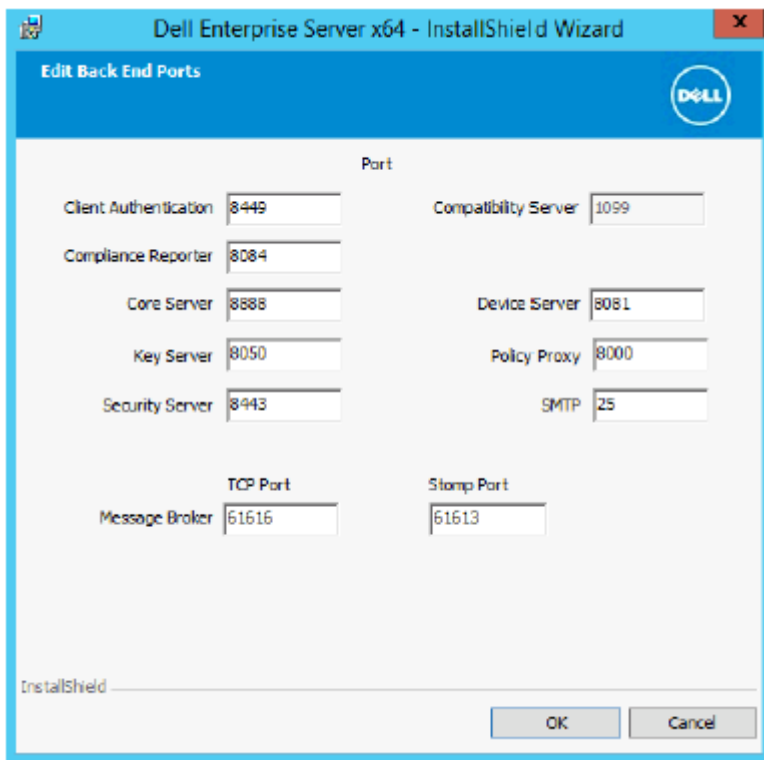
NOTE: A hostname cannot contain an underscore character ("_").

When finished, click **OK**.





To view or edit Ports, click **Edit Ports**. Edit ports only if necessary. Dell recommends using the defaults. When finished, click **OK**.

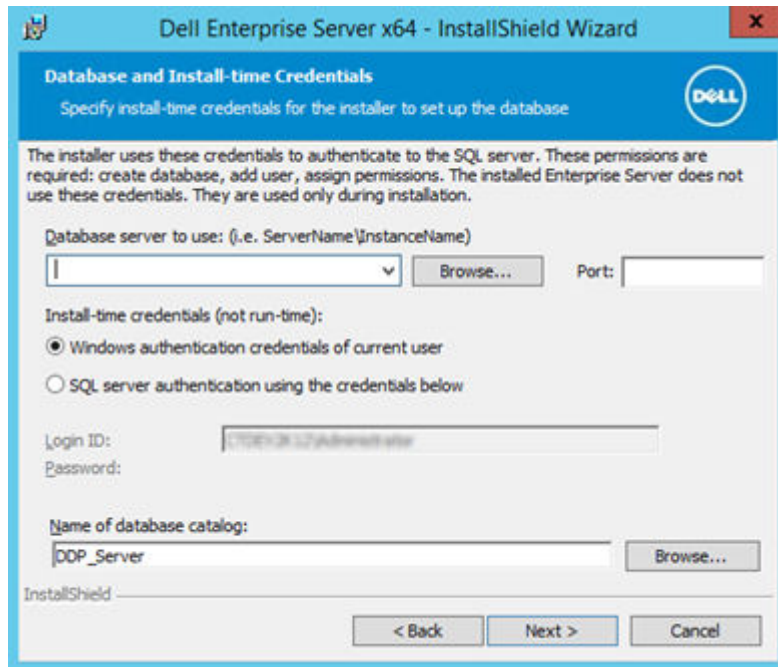


14 To create a new database, follow these steps:

- a Click **Browse** to select the server on which to install the database.
- b Select the authentication method for the installer to use to set up the Dell Data Protection database. After installation, the installed product does not use the credentials specified here.
 - **Windows authentication credentials of current user**



If you choose Windows Authentication, the same credentials that were used to log in to Windows will be used for authentication (User Name and Password fields will not be editable). Ensure that the account has system administrator rights and the ability to manage the SQL Server.



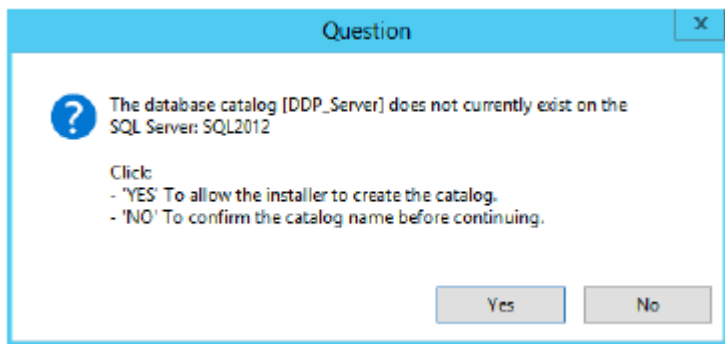
OR

- **SQL server authentication using the credentials below**

If you use SQL authentication, the SQL account used must have system administrator rights on the SQL Server.

The installer must authenticate to the SQL Server with these permissions: create database, add user, assign permissions.

- c Identify the database catalog:
Enter the name for a new database catalog. You are prompted in the next dialog to create the new catalog.
- d Click **Next**.
- e To confirm that you want the installer to create a database, click **Yes**. To return to the previous screen to make changes, click **No**.



- 15 Select the authentication method for the product to use. This step connects an account to the product.

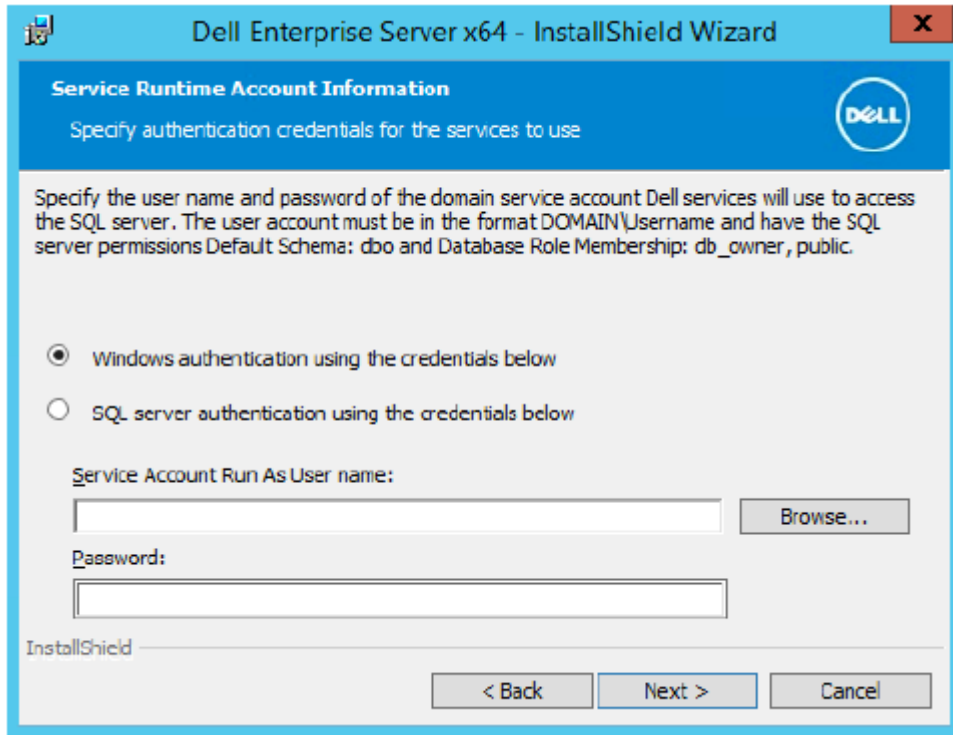
- **Windows authentication**

Select **Windows authentication using the credentials below**, enter the credentials for the product to use, and click **Next**.

Ensure that the account has system administrator rights and the ability to manage the SQL Server. The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.



These credentials are also used by Dell services as they work with the Dell Enterprise Server.

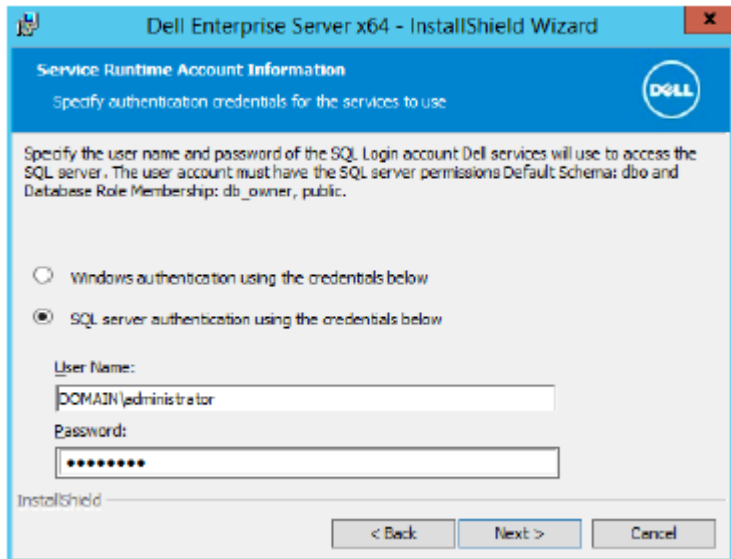


OR

SQL Server authentication

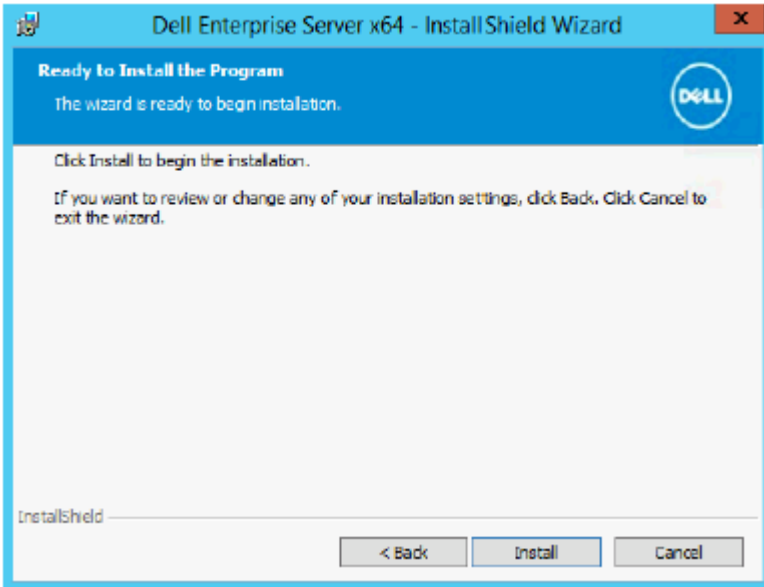
Select **SQL server authentication using the credentials below**, enter the SQL Server credentials for the Dell services to use as they work with the Dell Enterprise Server, and click **Next**.

The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

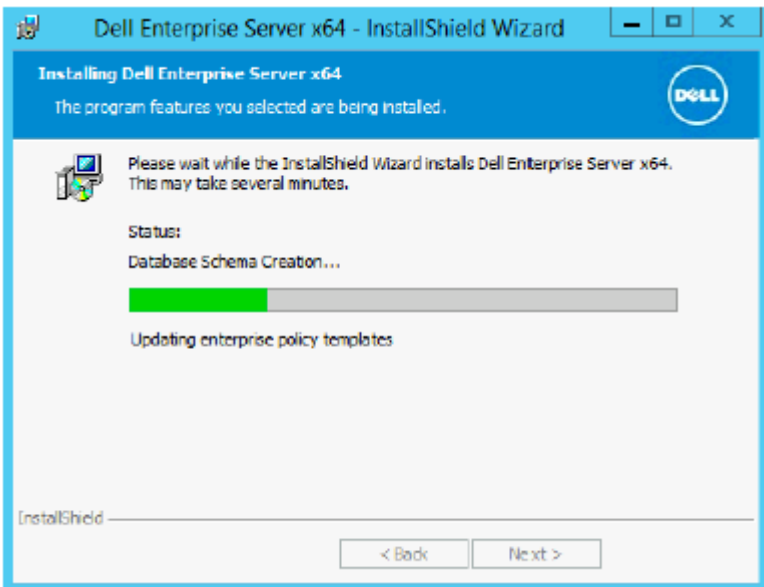


16 In the *Ready to Install the Program* dialog, click **Install**.



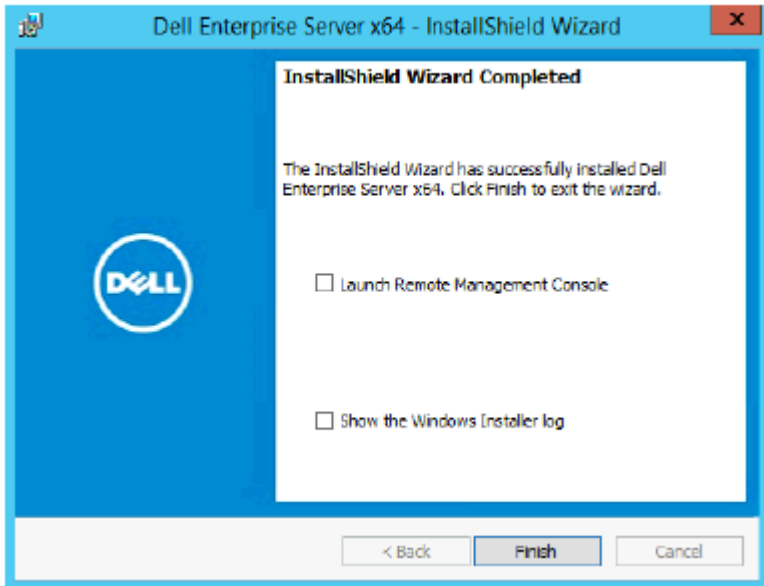


A progress dialog displays status throughout the installation process.



17 When the installation is completed, click **Finish**.





Back End Server installation tasks are complete.

Dell Services are restarted at the end of installation. It is not necessary to reboot the Server.

Install Back End Server with Existing Database

NOTE:

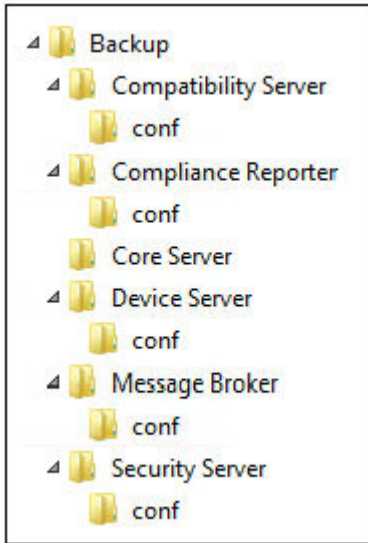
If you have a functional Dell Enterprise Server v8.x or later, refer to instructions in Upgrade/Migrate Back End Server(s).

You can install a new Dell Enterprise Server and connect to a SQL database created during [Pre-Installation Configuration](#) or an existing SQL database that is v9.x or later, when the schema version matches the Dell Enterprise Server version to be installed.

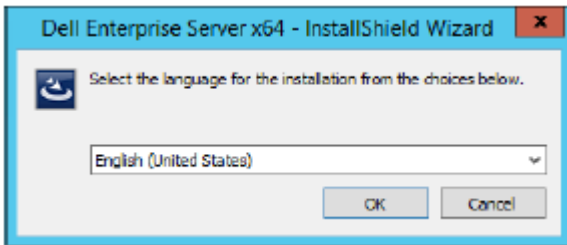
A v8.x or later database must be migrated to the latest schema with the latest version of Server Configuration Tool. For instructions on database migration with the Server Configuration Tool, see [Migrate the Database](#). To obtain the latest Server Configuration Tool, or **to migrate a pre-v8.0 database**, contact Dell ProSupport for assistance.

The user account from which the installation is performed must have database owner privileges for the SQL database. If you are uncertain about access privileges or connectivity to the database, ask your database administrator to confirm these before you begin installation.

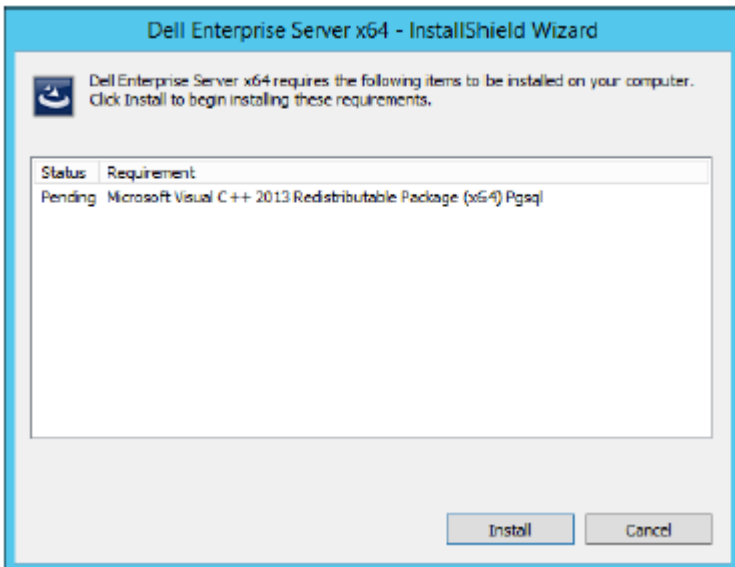
If the existing database has previously been installed with Dell Enterprise Server, before you begin installation, ensure that the database, configuration files, and the secretKeyStore are backed up and accessible from the server on which you are installing Dell Enterprise Server. Access to these files is necessary to configure Dell Enterprise Server and the existing database. The folder structure created by the installer during installation (example shown below) must remain unchanged.



- 1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (DO NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Enterprise Server. **Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.**
- 2 Double-click **setup.exe**.
- 3 In the *InstallShield Wizard* dialog, select the language for installation, then click **OK**.

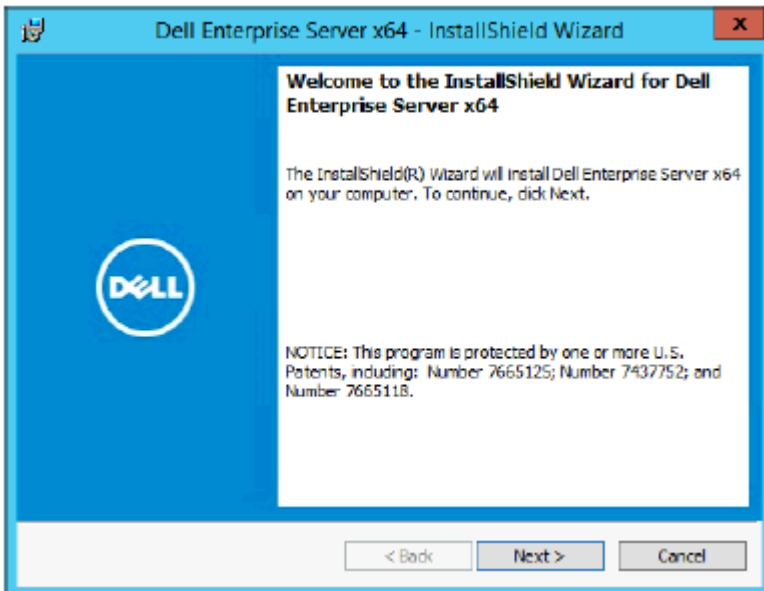


- 4 If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.

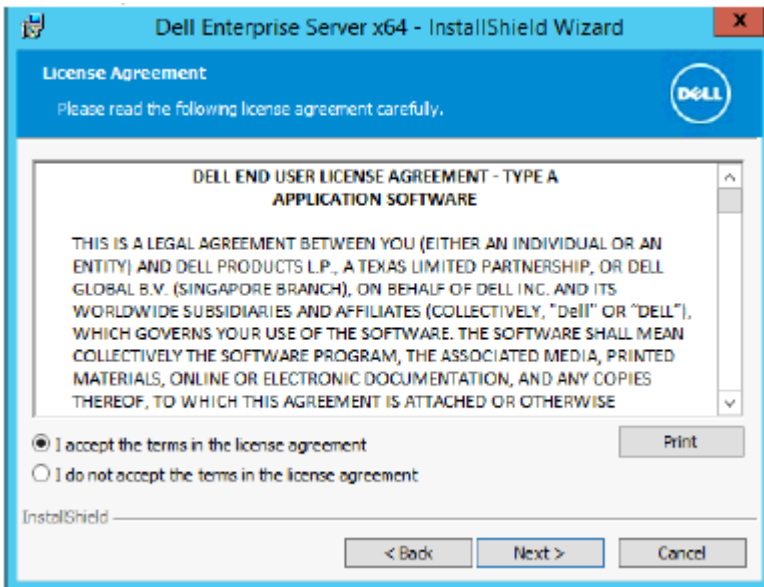


- 5 In the *Welcome* dialog, click **Next**.



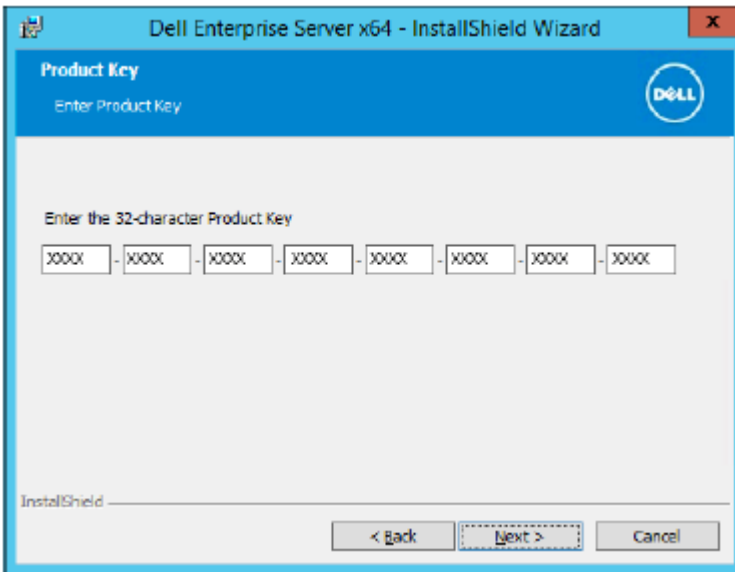


- 6 Read the license agreement, accept the terms, then click **Next**.

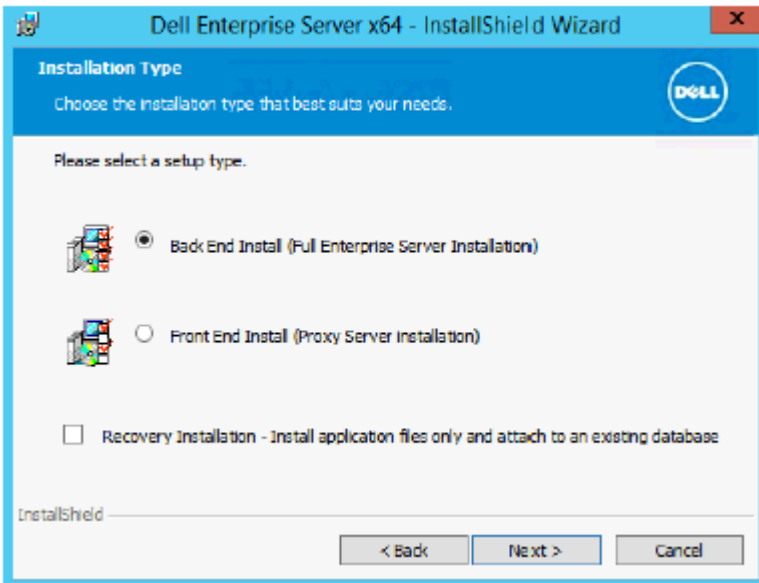


- 7 If you optionally completed [step 9 in Pre-Installation Configuration](#), click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is located in the file "*EnterpriseServerInstallKey.ini*."



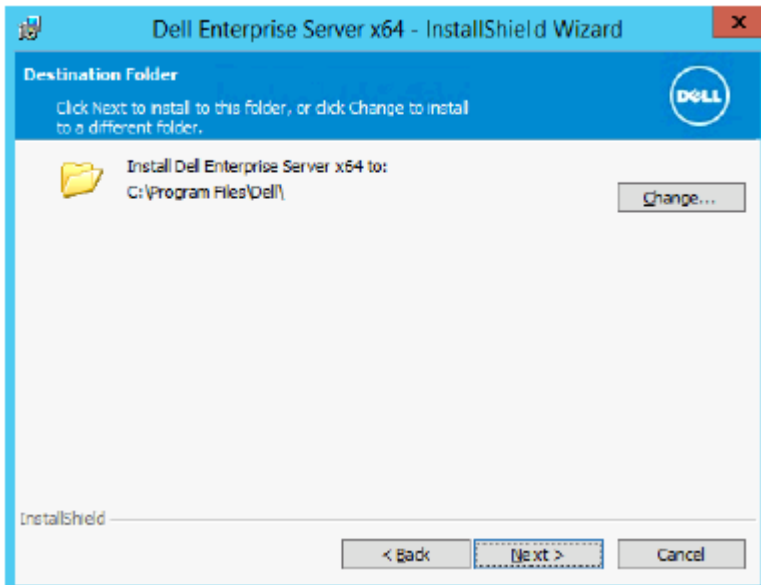


- 8 Select **Back End Install** and **Recovery Installation**, and click **Next**.

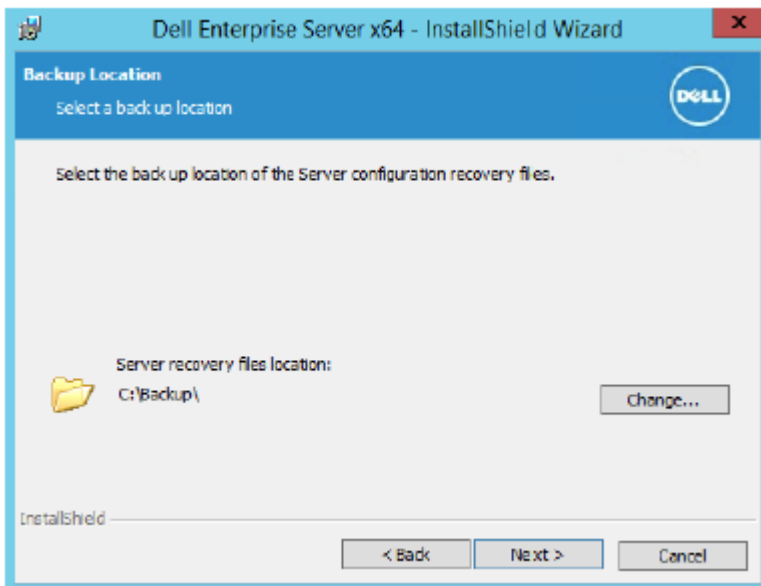


- 9 To install the Dell Enterprise Server to the default location of C:\Program Files\Dell, click **Next**. Otherwise, click **Change** to select a different location, then click **Next**.



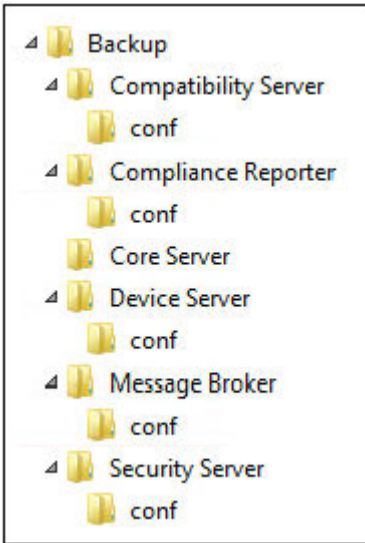


- 10 To select a location for backup configuration files to be stored, click **Change**, navigate to the desired folder, then click **Next**. **Dell recommends that you select a remote network location or external drive for backup.**



After installation, any changes to configuration files, including changes made with the Server Configuration Tool, must be manually backed up in these folders. Configuration files are an important part of the total information used to manually restore the server.

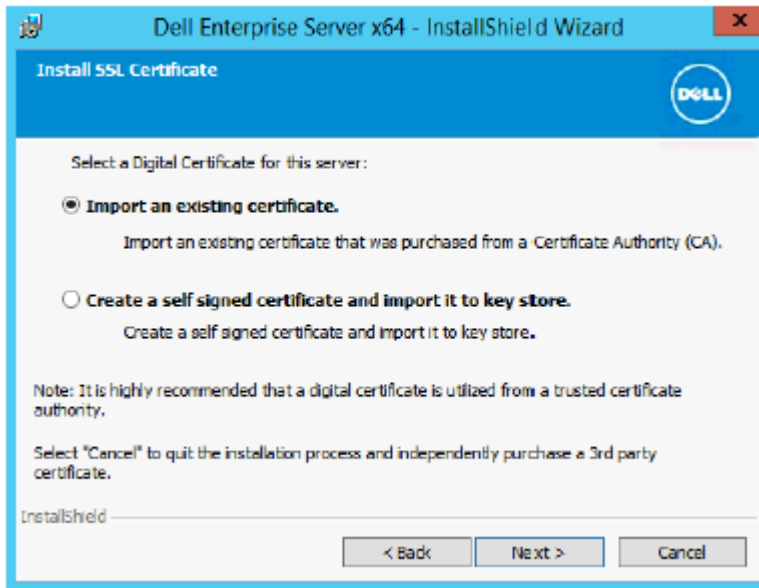
NOTE: The folder structure created by the installer during installation (example shown below) must remain unchanged.



11 You have a choice of digital certificate types to use. **It is highly recommended that you use a digital certificate from a trusted certificate authority.**

Select option "a" or "b" below:

- a To use an existing certificate that was purchased from a CA authority, select **Import an existing certificate** and click **Next**.



Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See [Exporting a Certificate to .PFX Using the Certificate Management Console](#) for instructions.

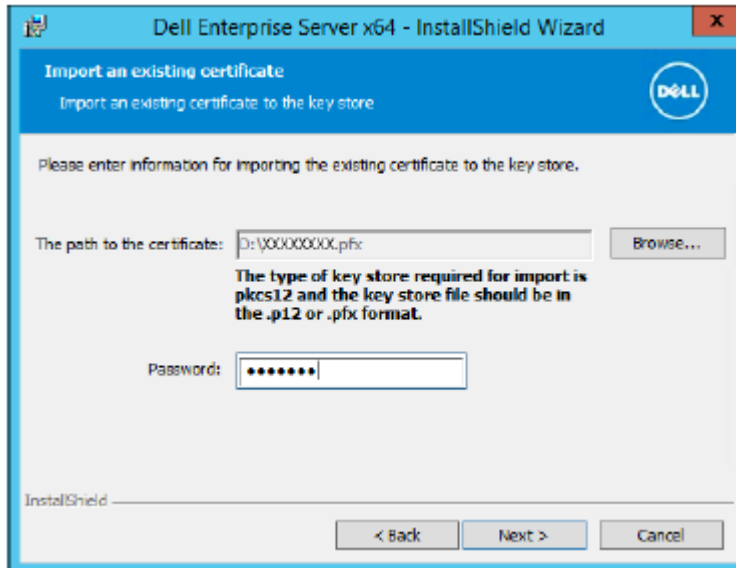
Click **Next**.



NOTE:

To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":

- Personal Information Exchange - PKCS#12 (.PFX)
- Include all certificates in the certification path if possible
- Export all extended properties



OR

- b To create a self-signed certificate, select **Create a self signed certificate and import it to key store and click Next.**

At the *Create Self-Signed Certificate* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organization

Organizational Unit (example: Security)

City

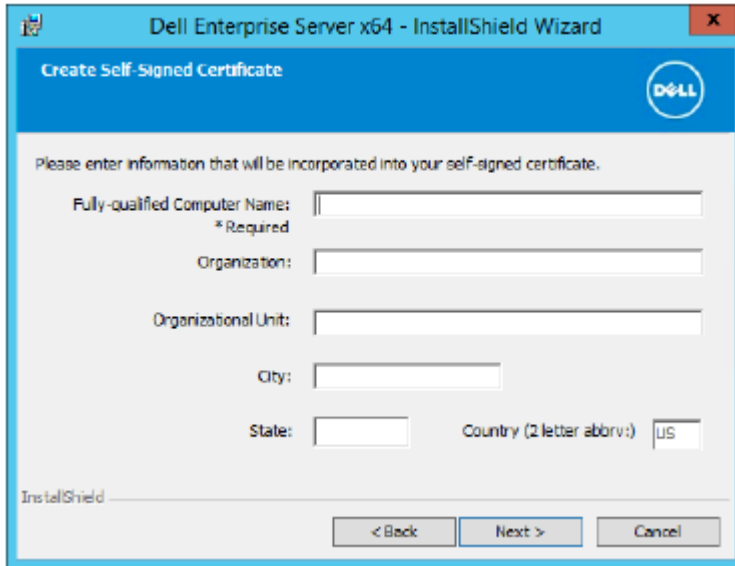
State (full name)

Country: Two-letter country abbreviation

Click **Next**.

NOTE:

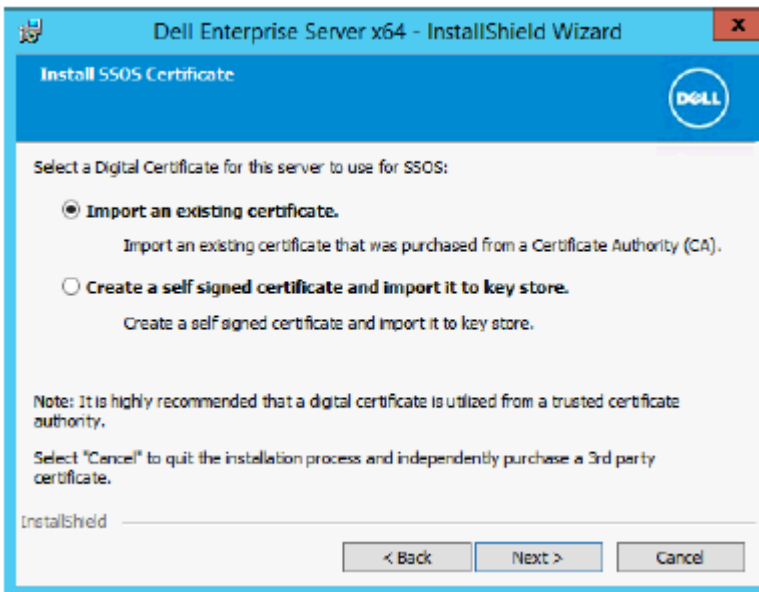
The certificate expires in one year, by default.



12 For Server Encryption (SE), you have a choice of digital certificate types to use. It is highly recommended that you use a digital certificate from a trusted certificate authority.

Select option "a" or "b" below:

- a To use an existing certificate that was purchased from a CA authority, select **Import an existing certificate** and click **Next**.



Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx. See [Exporting a Certificate to .PFX Using the Certificate Management Console](#) for instructions.

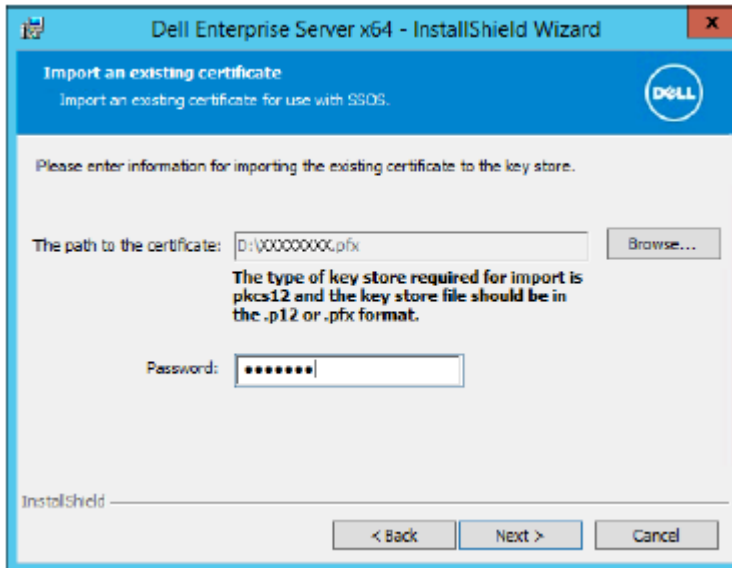
Click **Next**.



NOTE:

To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":

- Personal Information Exchange - PKCS#12 (.PFX)
- Include all certificates in the certification path if possible
- Export all extended properties



- b To create a self-signed certificate, select **Create a self signed certificate and import it to key store and click Next.**

At the *Create Self-Signed Certificate* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organization

Organizational Unit (example: Security)

City

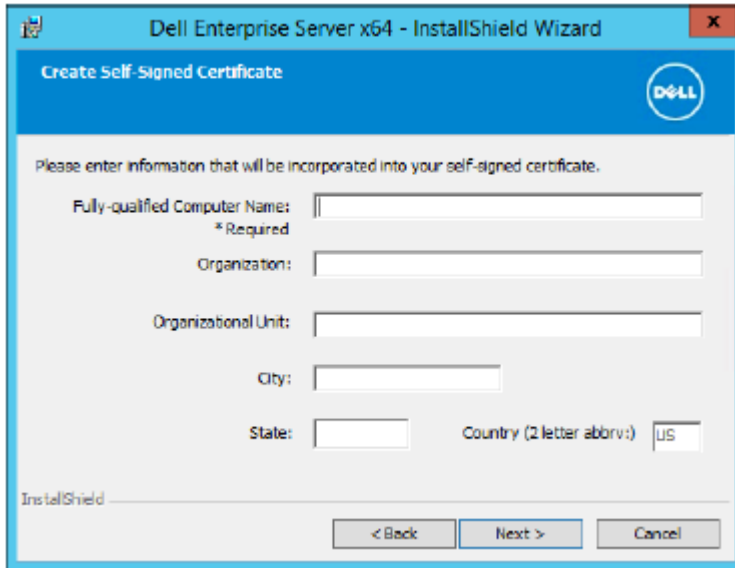
State (full name)

Country: Two-letter country abbreviation

Click **Next**.

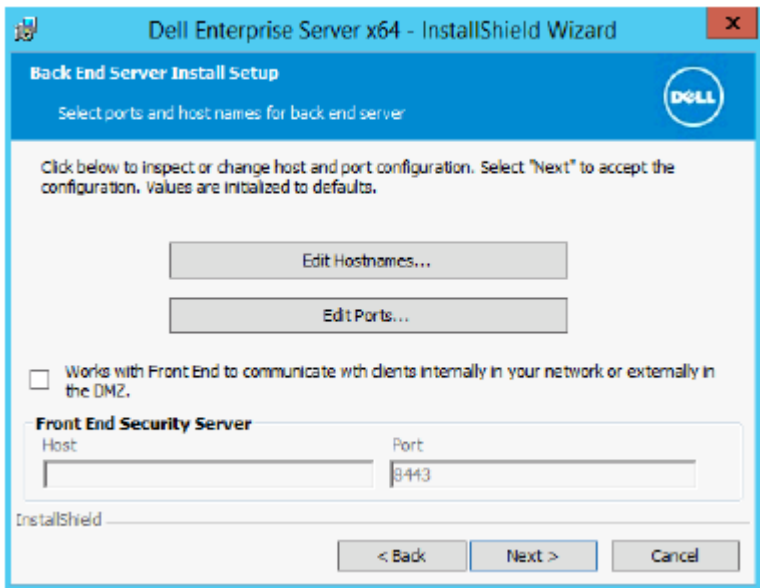
NOTE:

The certificate expires in one year, by default.



13 From the *Back End Server Install Setup* dialog, you can view or edit hostnames and ports.

- To accept the default hostnames and ports, in the *Back End Server Install Setup* dialog, click **Next**.
- If you are using a Front End Server, select **Works with Front End to communicate with clients internally in your network or externally in the DMZ** and enter the Front End Security Server hostname (for example, server.domain.com).

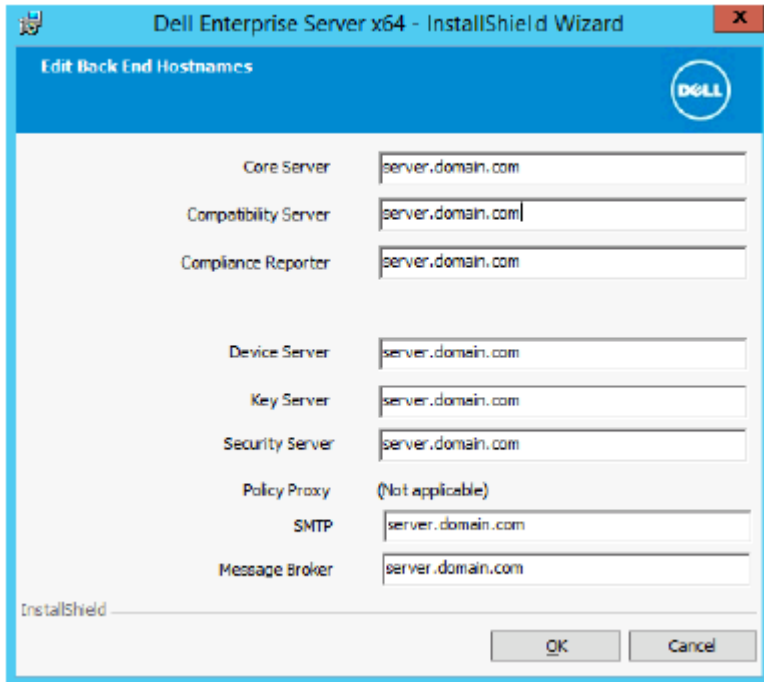


- To view or edit hostnames, click **Edit Hostnames**. Edit hostnames only if necessary. Dell recommends using the defaults.

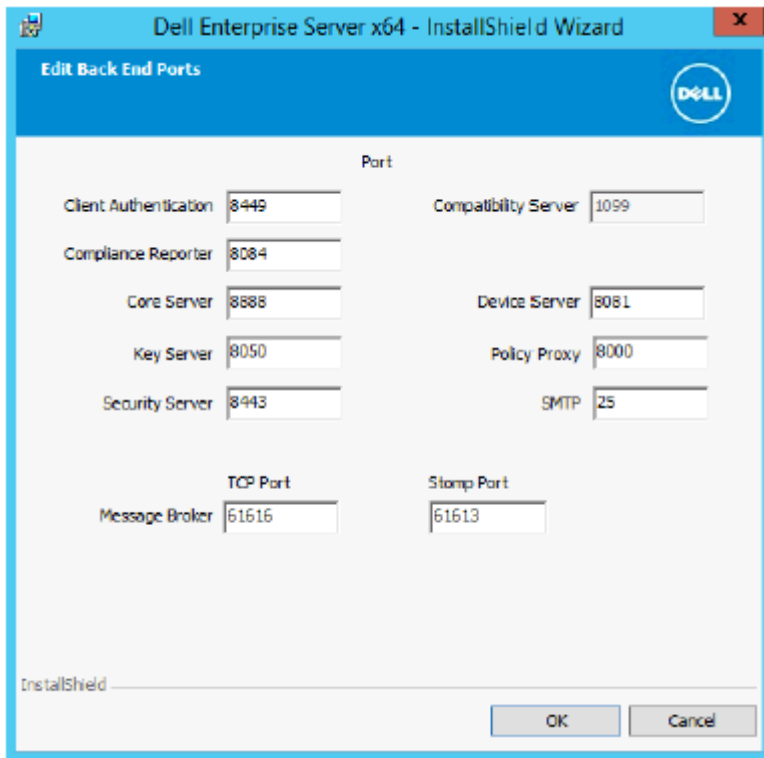
NOTE: A hostname cannot contain an underscore character ("_").

When finished, click **OK**.





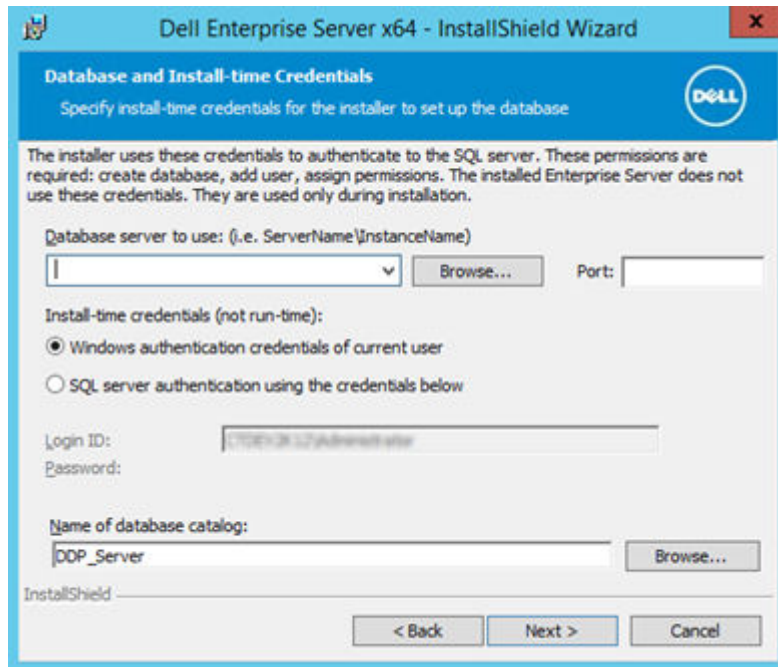
- To view or edit Ports, click **Edit Ports**. Edit ports only if necessary. Dell recommends using the defaults. When finished, click **OK**.



- 14 Specify the authentication method for the installer to use.
 - a Click **Browse** to select the server where the database resides.
 - b Select the authentication type.
 - **Windows authentication credentials of current user**



If you choose Windows Authentication, the same credentials that were used to log in to Windows will be used for authentication (User Name and Password fields will not be editable). Ensure that the account has system administrator rights and the ability to manage the SQL Server.



OR

- **SQL server authentication using the credentials below**

If you use SQL authentication, the SQL account used must have system administrator rights on the SQL Server.

The installer must authenticate to the SQL Server with these permissions: create database, add user, assign permissions.

- c Click **Browse** to select the name of the existing database catalog.
- d Click **Next**.

15 Select the authentication method for the product to use. This is the account that the product uses to work with the database and Dell services.

- **To use Windows authentication**

Select **Windows authentication using the credentials below**, enter the credentials for the account that the product can use, then click **Next**.

Ensure that the account has system administrator rights and the ability to manage the SQL Server. The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

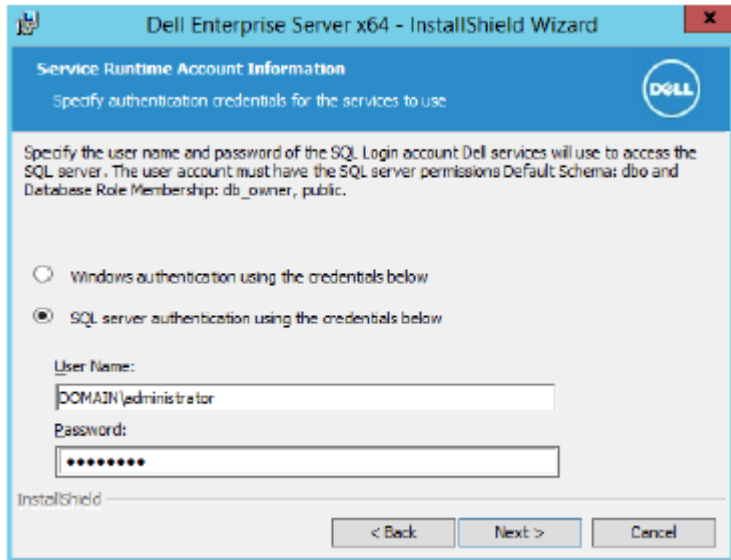
OR

- **To use SQL Server authentication**

Select **SQL server authentication using the credentials below**, enter the SQL Server credentials, then click **Next**.

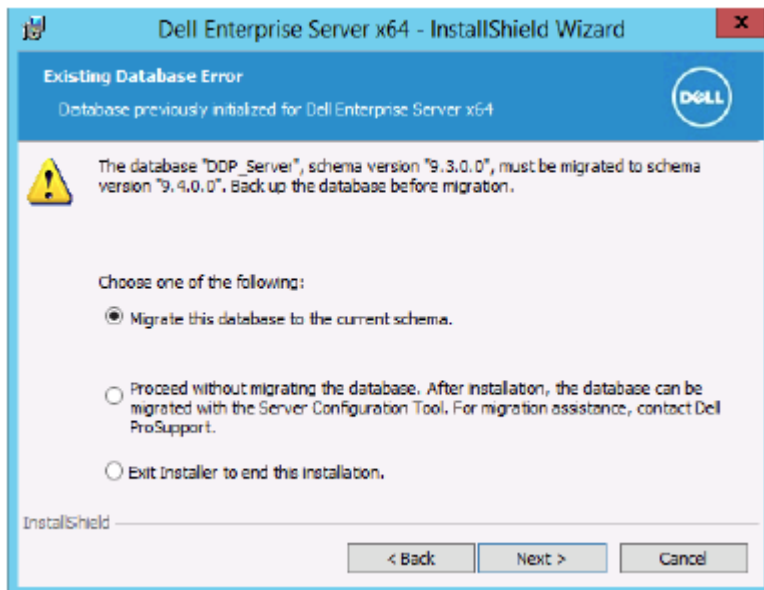
The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.





If the installer detects a problem with the database, an Existing Database Error dialog displays. The options in the dialog depend on the circumstances:

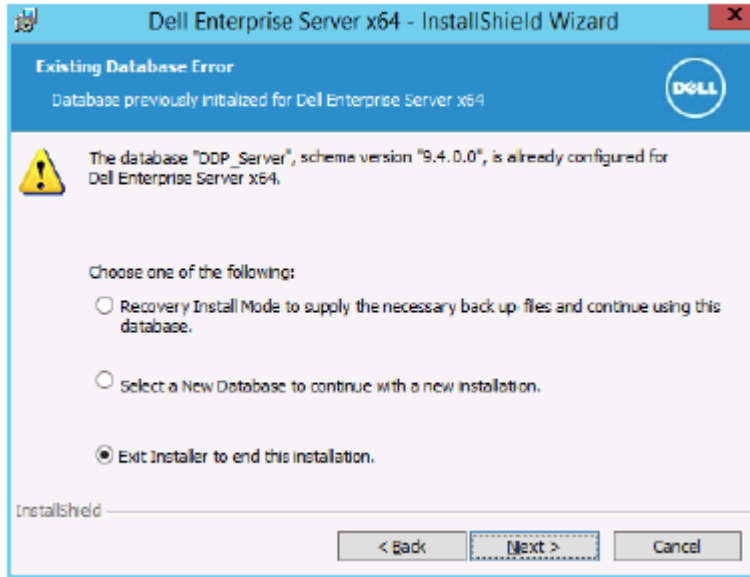
- The database schema is from a previous version. (Refer to step a.)
 - The database already has a database schema that matches the version currently being installed. (Refer to step b.)
- a When the database schema is from a previous version, select **Exit Installer to end this installation**. Next, you must back up the database.



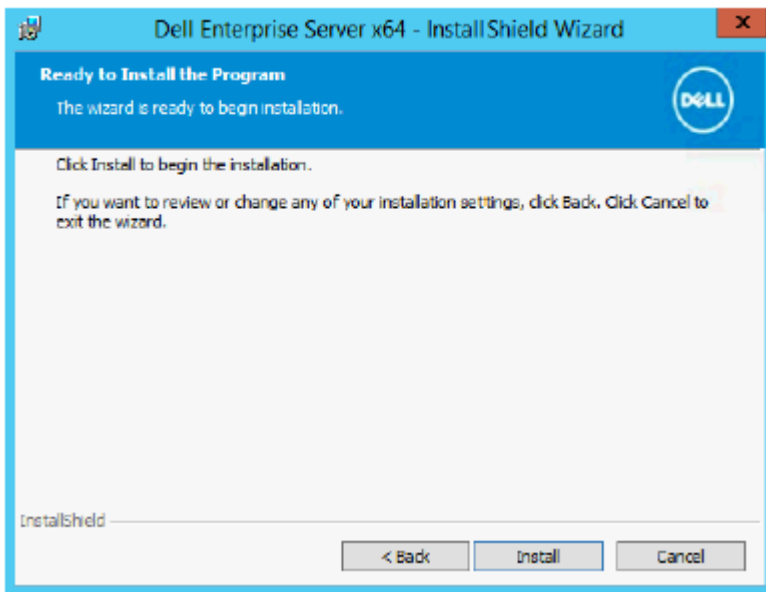
The following options **MUST** be used only with the help of Dell ProSupport:

- The **Migrate this database to the current schema** option is used to recover a good database from a failed server implementation. This option uses the recovery files in the \Backup folder to reconnect to the database, and then migrates the database to the current schema. This option should *only* be used after first trying to re-install the correct version of Enterprise Server, then running the latest installer to upgrade.
 - The **Proceed without migrating the database** option installs the Enterprise Server files without completely configuring the database. Database configuration must be completed later, manually, using the Server Configuration tool and requires further manual changes.
- b When the database schema already has the current version's schema, but is not connected to a Dell Enterprise Server backend, it is considered a *Recovery*. This dialog appears:
- Select **Recovery Install Mode** to continue the installation with the selected database.

- Select **Select a New Database** to choose a different database.
 - Select **Exit Installer to end this installation.**
- c. Click **Next**.

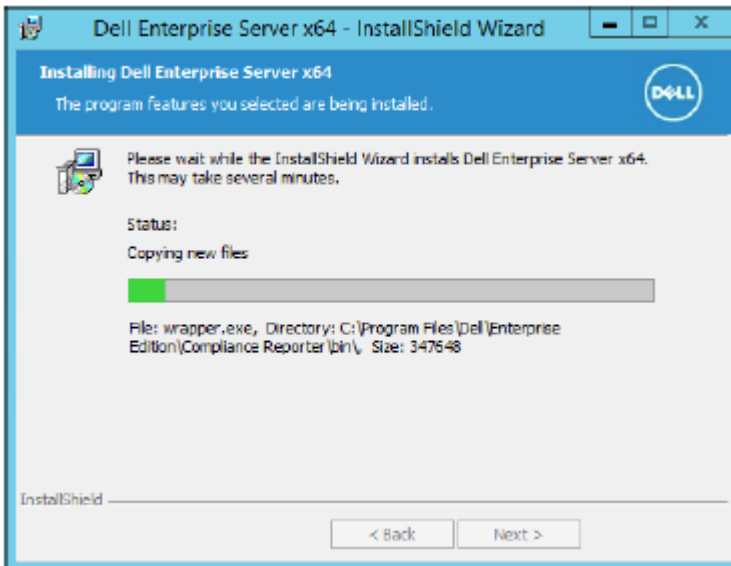


- 16 In the *Ready to Install the Program* dialog, click **Install**.

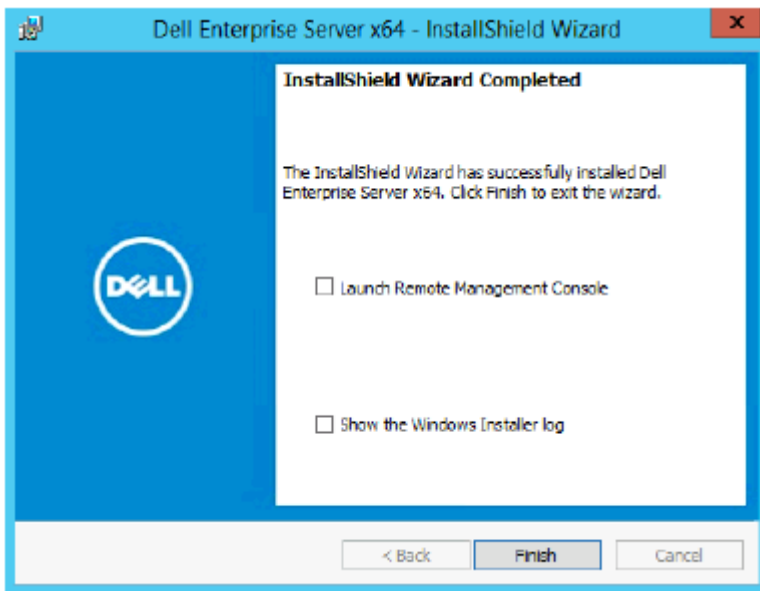


A progress dialog displays status throughout the installation process.





When the installation is completed, click **Finish**.



Back End Server installation tasks are complete.

Dell Services are restarted at the end of installation. It is not necessary to reboot the Server.

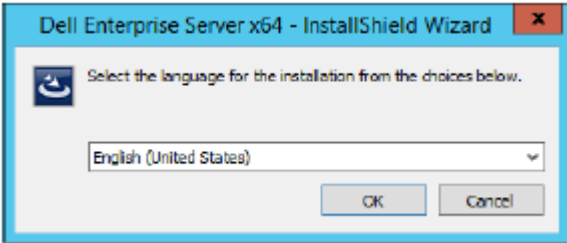
Install Front End Server

Front End Server installation provides a front-end (DMZ Mode) option for use with Dell Enterprise Server. If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

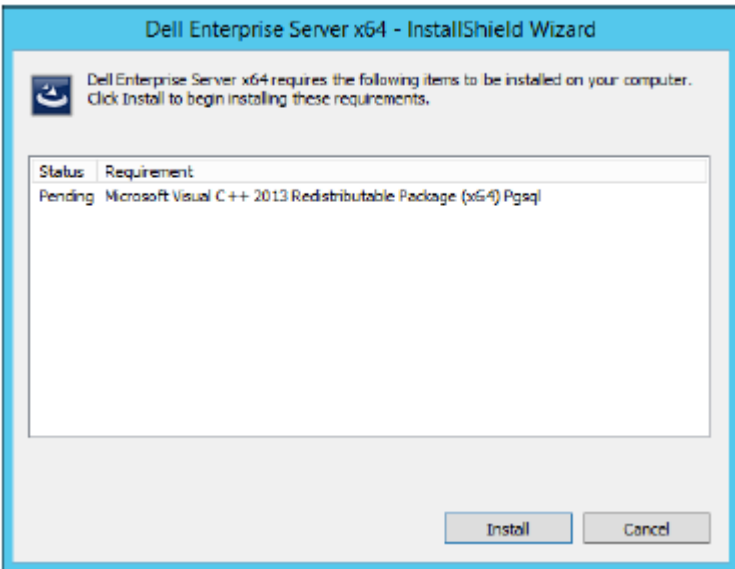
NOTE: The Beacon Service is installed as part of this installation to support Secure Lifecycle callback beacon, which inserts a callback beacon into every file protected by Secure Lifecycle when running Protected Office mode. This allows communication between any device in any location and the Dell Front End Server. Ensure that necessary network security is configured before using the callback beacon. The Enable Callback Beacon policy is enabled by default.

To perform this installation, you will need the fully-qualified hostname of the DMZ server.

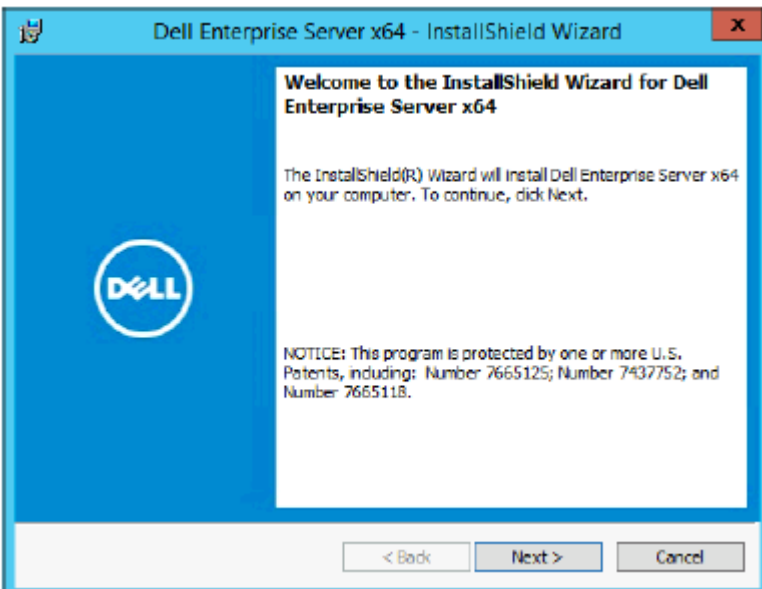
- 1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (DO NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Enterprise Server. **Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.**
- 2 Double-click **setup.exe**.
- 3 In the *InstallShield Wizard* dialog, select the language for installation, then click **OK**.



- 4 If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.

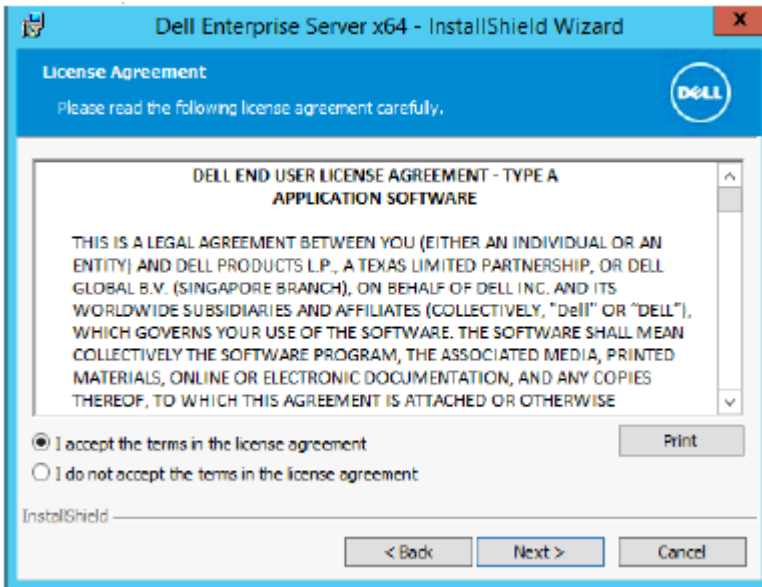


- 5 In the *Welcome* dialog, click **Next**.

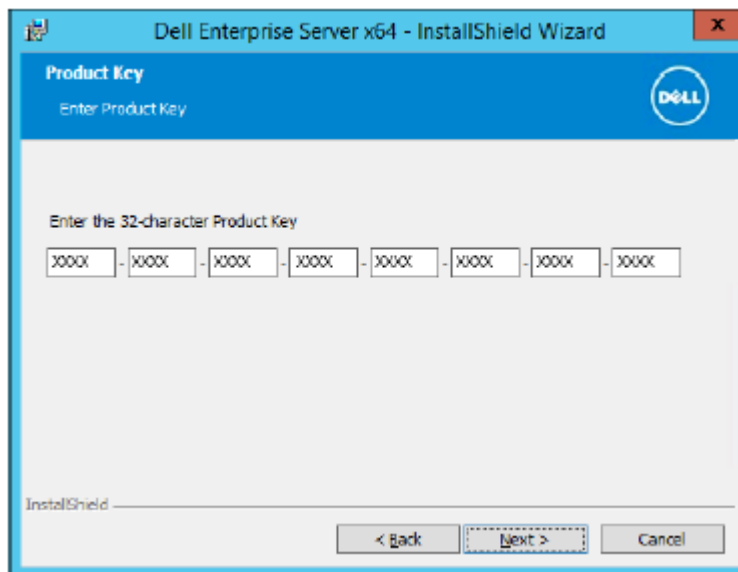


- 6 Read the license agreement, accept the terms, then click **Next**.



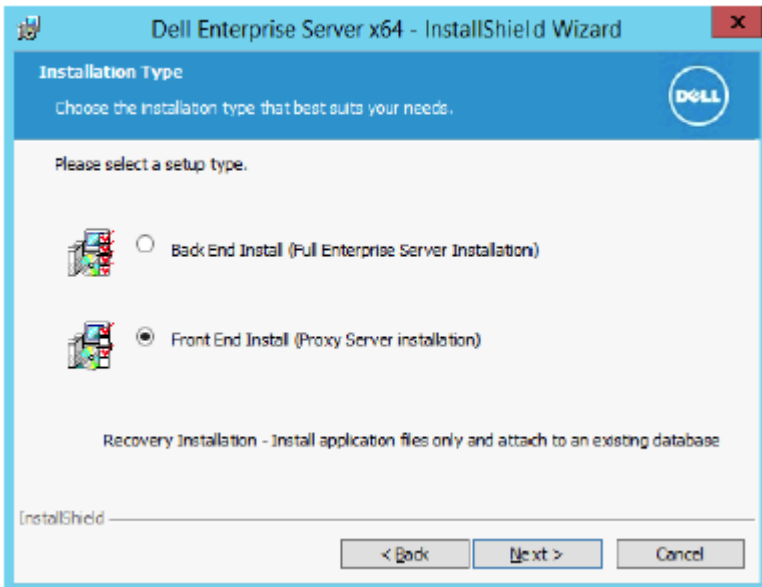


7 Enter the Product Key.

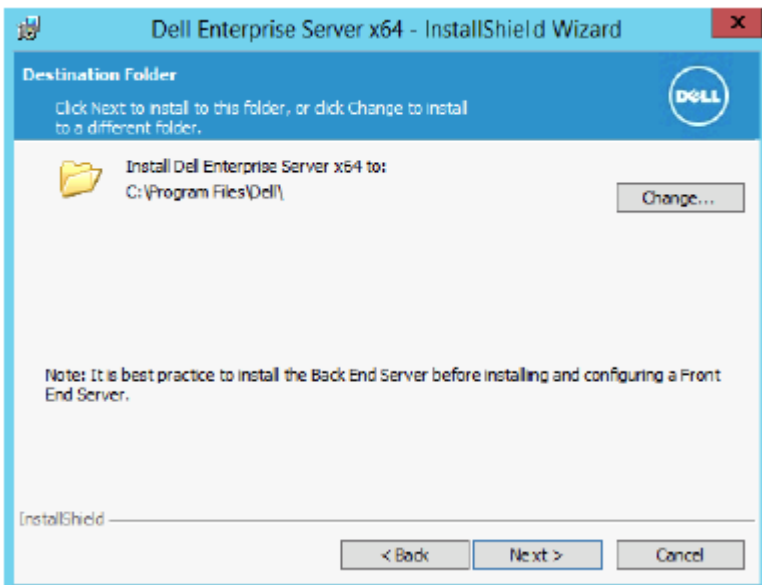


8 Select **Front End Install** and click **Next**.





- 9 To install the Front End Server to the default location of C:\Program Files\Dell, click **Next**. Otherwise, click **Change** to select a different location, then click **Next**.

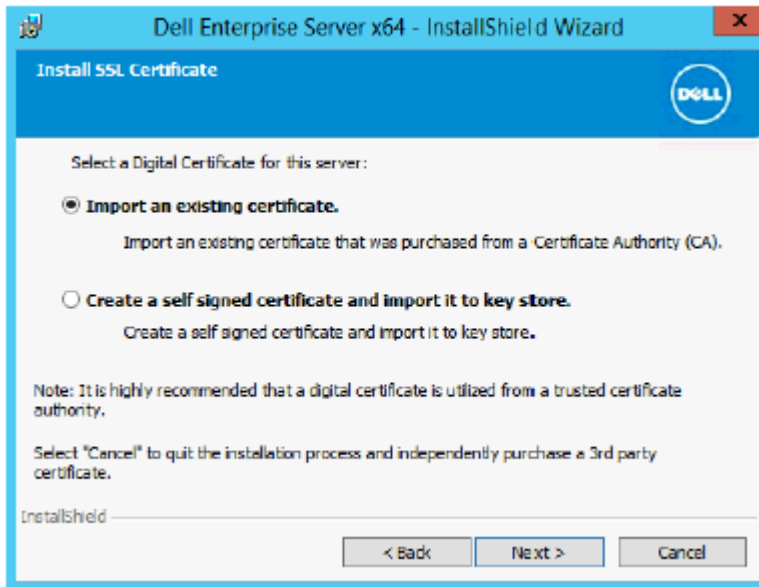


- 10 You have a choice of digital certificate types to use. **It is highly recommended that you use a digital certificate from a trusted certificate authority.**

Select option "a" or "b" below:

- a To use an existing certificate that was purchased from a CA authority, select **Import an existing certificate** and click **Next**.





Click **Browse** to enter the path to the certificate.

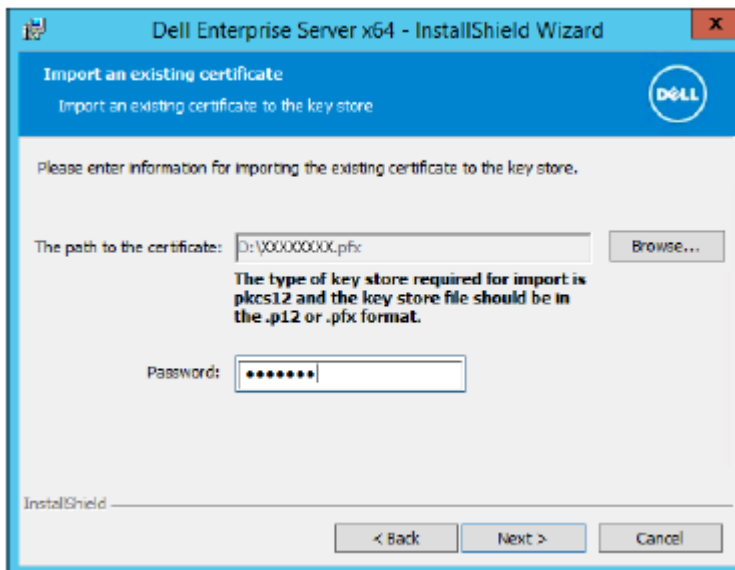
Enter the password associated with this certificate. The key store file must be .p12 or pfx. See [Exporting a Certificate to .PFX Using the Certificate Management Console](#) for instructions.

Click **Next**.

NOTE:

To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":

- Personal Information Exchange - PKCS#12 (.PFX)
- Include all certificates in the certification path if possible
- Export all extended properties



- b To create a self-signed certificate, select **Create a self signed certificate and import it to key store** and click **Next**. At the *Create Self-Signed Certificate* dialog, enter the following information:



Fully qualified computer name (example: computername.domain.com)

Organization

Organizational Unit (example: Security)

City

State (full name)

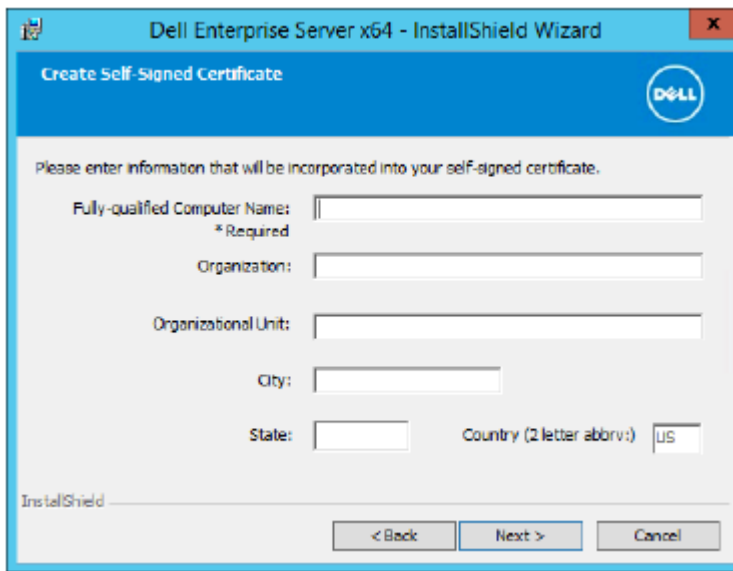
Country: Two-letter country abbreviation

Click **Next**.



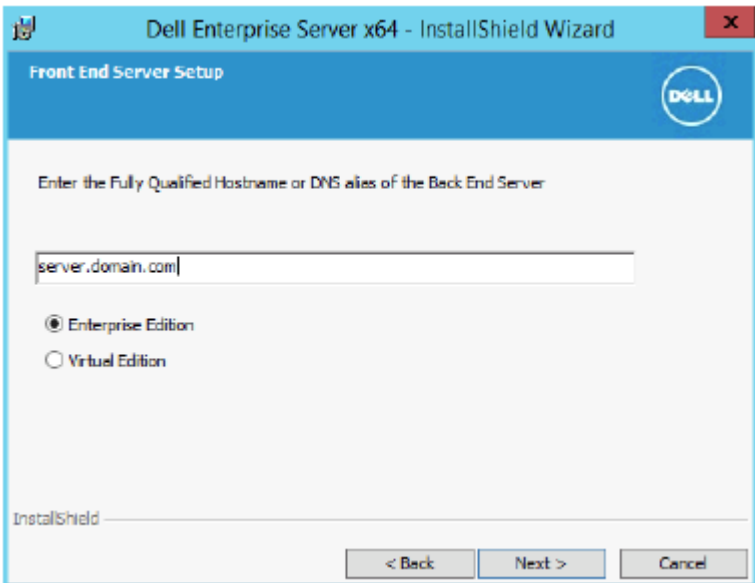
NOTE:

The certificate expires in one year, by default.



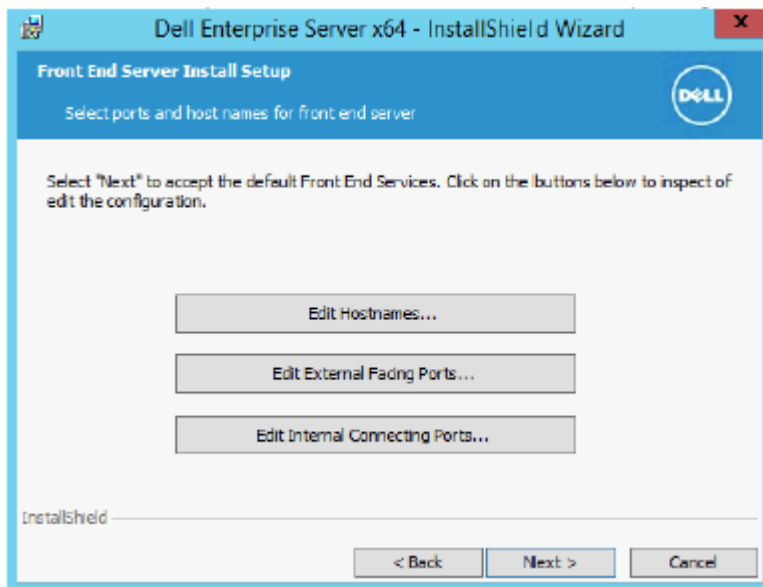
- 11 In the *Front End Server Setup* dialog, enter the fully qualified hostname or DNS alias of the Back End Server, select **Enterprise Edition**, and click **Next**.





12 From the *Front End Server Install Setup* dialog, you can view or edit hostnames and ports.

- To accept the default hostnames and ports, in the *Front End Server Install Setup* dialog, click **Next**.



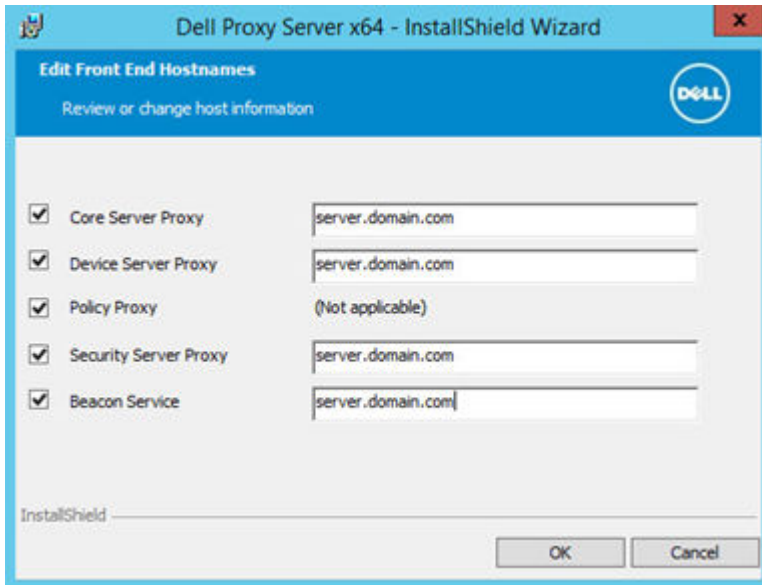
- To view or edit hostnames, in the *Front End Server Setup* dialog, click **Edit Hostnames**. Edit hostnames only if necessary. Dell recommends using the defaults.

NOTE:
A hostname cannot contain an underscore character ("_").

Deselect a proxy only if you are certain that you do not want to configure it for installation. If you deselect a proxy in this dialog, it will not be installed.

When finished, click **OK**.

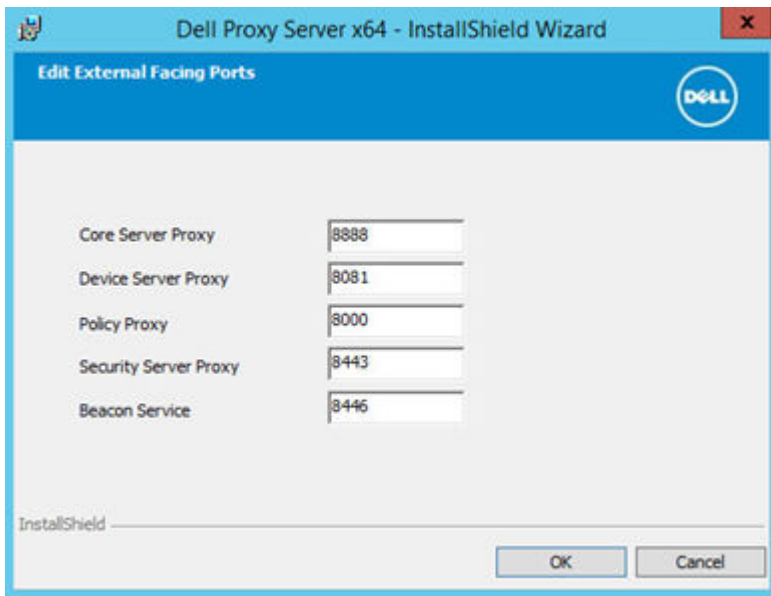


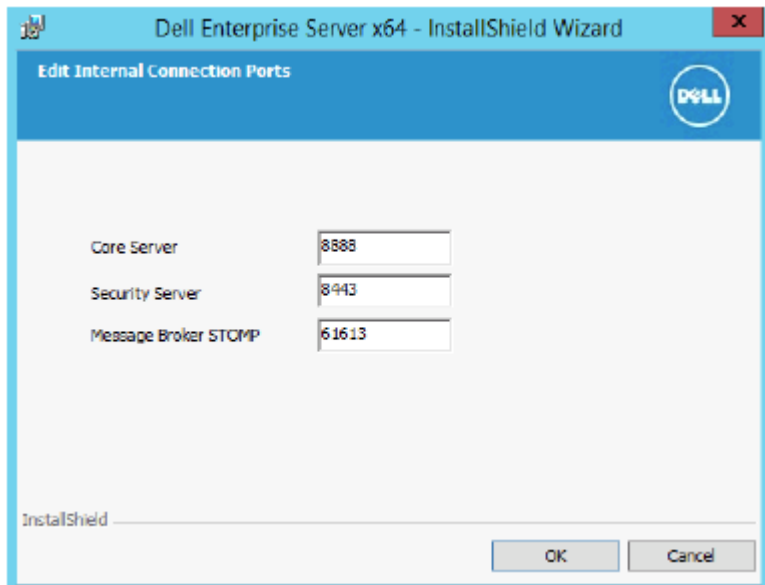


- To view or edit Ports, in the *Front End Server Setup* dialog, click either **Edit External Facing Ports** or **Edit Internal Connecting Ports**. Edit ports only if necessary. Dell recommends using the defaults.

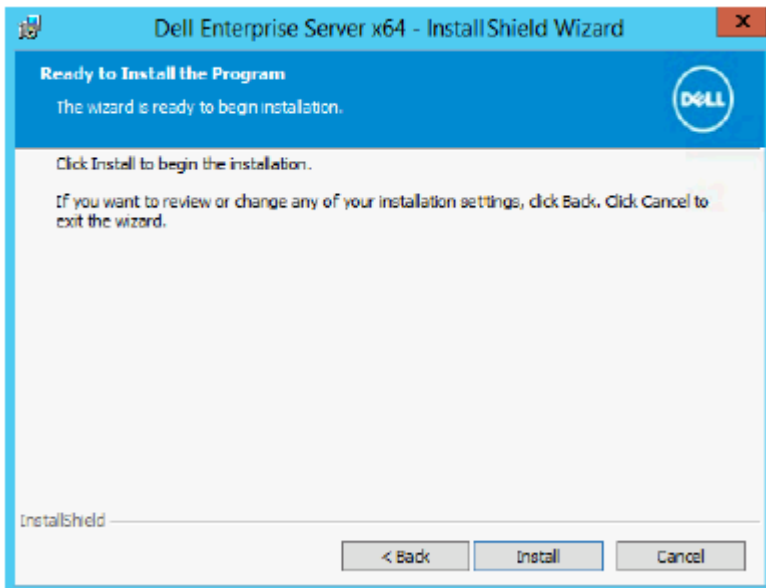
If you deselect a proxy in the *Edit Front End Host Names* dialog, its port does not display in the External Ports or Internal Ports dialogs.

When finished, click **OK**.



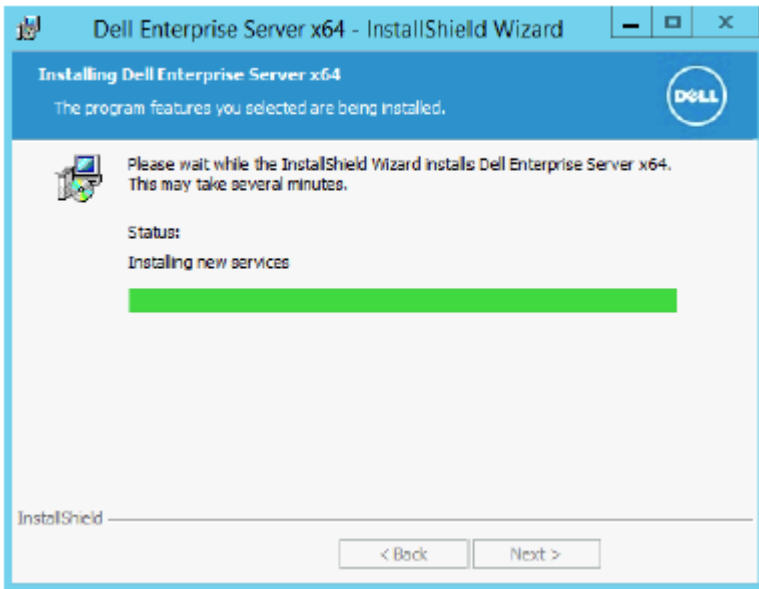


13 In the *Ready to Install the Program* dialog, click **Install**.

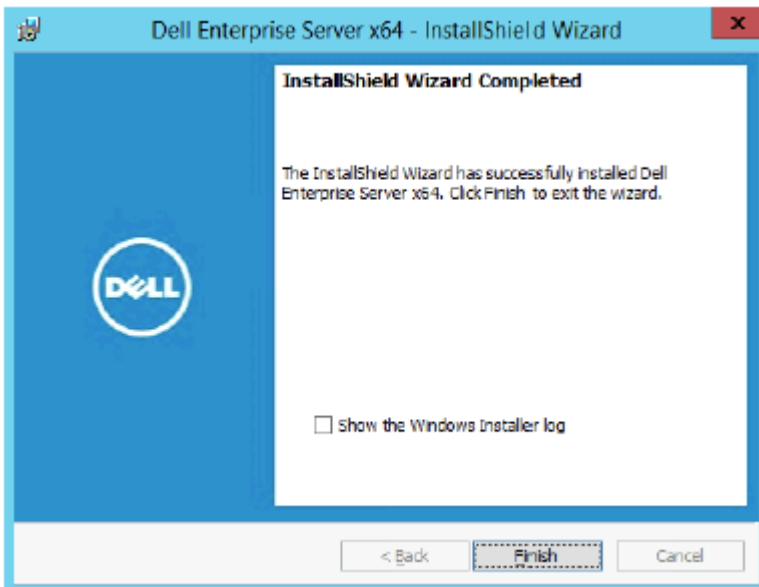


A progress dialog displays status throughout the installation process.





- 14 When the installation is completed, click **Finish**.



Front End Server installation tasks are complete.

Upgrade/Migration

You can upgrade Dell Enterprise Server v8.0 and later to Dell Enterprise Server v9.x. If your Server version is older than v8.0, you must first upgrade to v8.0 then upgrade to v9.x.

Before You Begin Upgrade/Migration

Before you begin, ensure that all [Pre-Installation Configuration](#) is complete. This is of particular importance if you are deploying Mobile Edition.

Read the *Enterprise Server Technical Advisories* for any current workarounds or known issues related to Dell Enterprise Server installation.



The user account from which the installation is performed must have database owner privileges for the SQL database. If you are uncertain about access privileges or connectivity to the database, ask your database administrator to confirm these before you begin installation.

Dell recommends that database best practices are used for the Dell database and that Dell software is included in your organization's disaster recovery plan.

If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

For production, Dell recommends installing the SQL Server on a dedicated server.

To leverage full capabilities of policies, we recommend updating to the most current versions of both the Dell Enterprise Server and Clients.

Dell Enterprise Server v9.x supports:

- Enterprise Edition:
 - Windows clients v7.x/8.x
 - Mac clients v7.x/8.x
 - SED clients v8.x
 - Authentication v8.x
 - BitLocker Manager v7.2x+ and v8.x
 - Secure Lifecycle v1.x
- Endpoint Security Suite v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Upgrade/Migration from Dell Enterprise Server v8.x or later. (When migrating from pre-v8.x Dell Enterprise Server, contact Dell ProSupport for assistance.)

When upgrading/migrating your Dell Enterprise Server to a version that includes new policies that are introduced in that version, commit updated policy after upgrade/migration, to ensure that your preferred policy settings are implemented for the new policies, rather than default values.

In general, our recommended upgrade path is to upgrade/migrate the Dell Enterprise Server and its components, followed by Client installation/upgrade.

Apply Policy Changes

- 1 As a Dell Administrator, log in to the Remote Management Console.
- 2 In the left menu, click **Management > Commit**.
- 3 Enter a description of the change in the Comment field.
- 4 Click **Commit Policies**.
- 5 When the commit is complete, log off the Remote Management Console.

Ensure that Dell Services are running

- 6 From the Windows *Start* menu, click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and, if necessary, click **Start the service**.

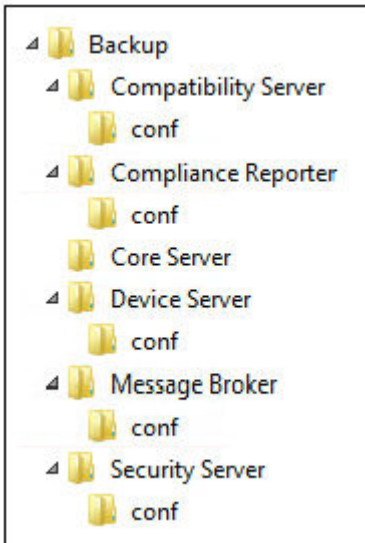
Back Up the Existing Installation

- 7 Back up your entire existing installation to an alternate location. The backup should include the SQL database, secretKeyStore, and configuration files. Several files from your existing installation will be needed after the upgrade/migration process is complete.



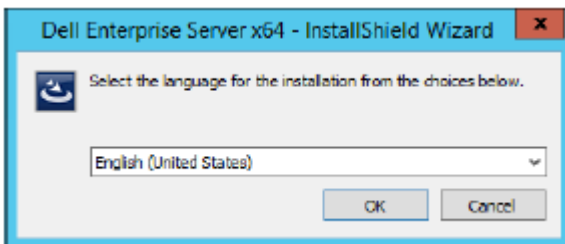
NOTE:

The folder structure created by the installer during installation (example shown below) must remain unchanged

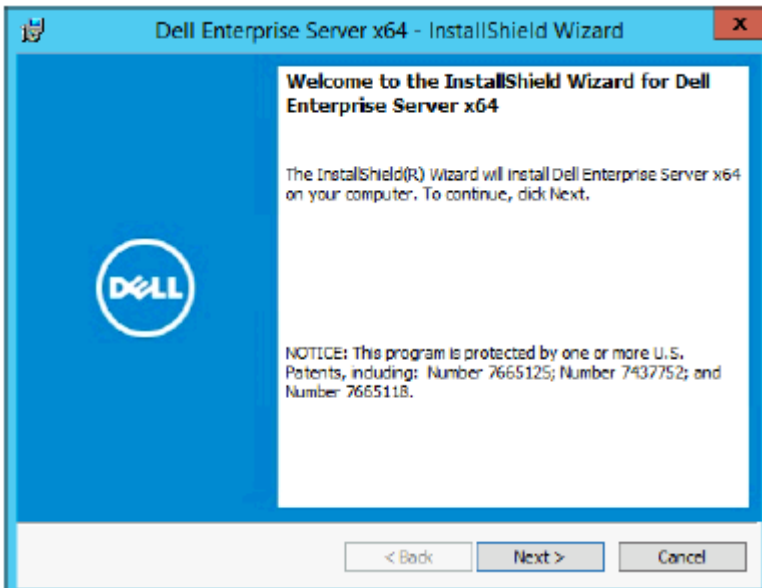


Upgrade/Migrate Back End Server(s)

- 1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Enterprise Server. **Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.**
- 2 Double-click **setup.exe**.
- 3 In the *InstallShield Wizard* dialog, select the language for installation, then click **OK**.

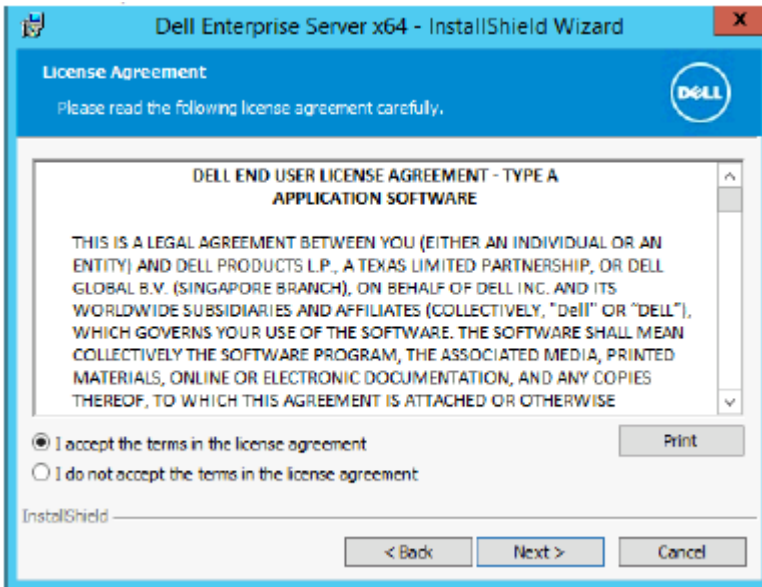


- 4 In the *Welcome* dialog, click **Next**.

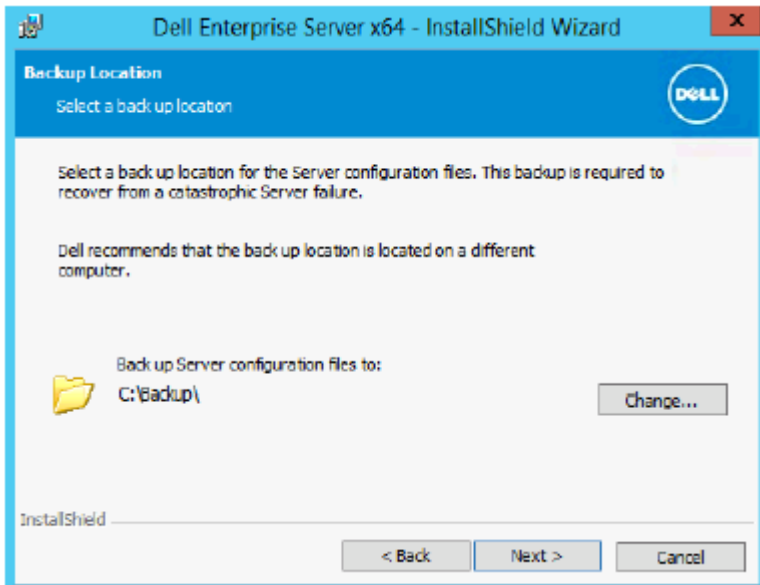


- 5 Read the license agreement, accept the terms, then click **Next**.

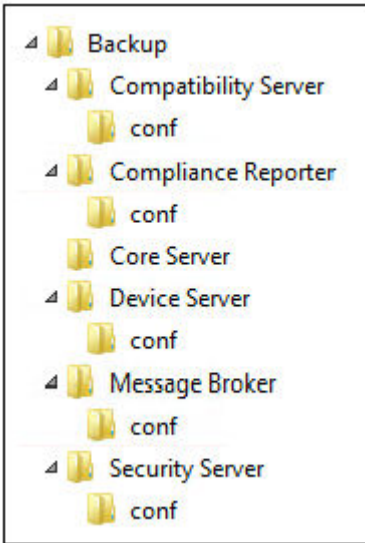




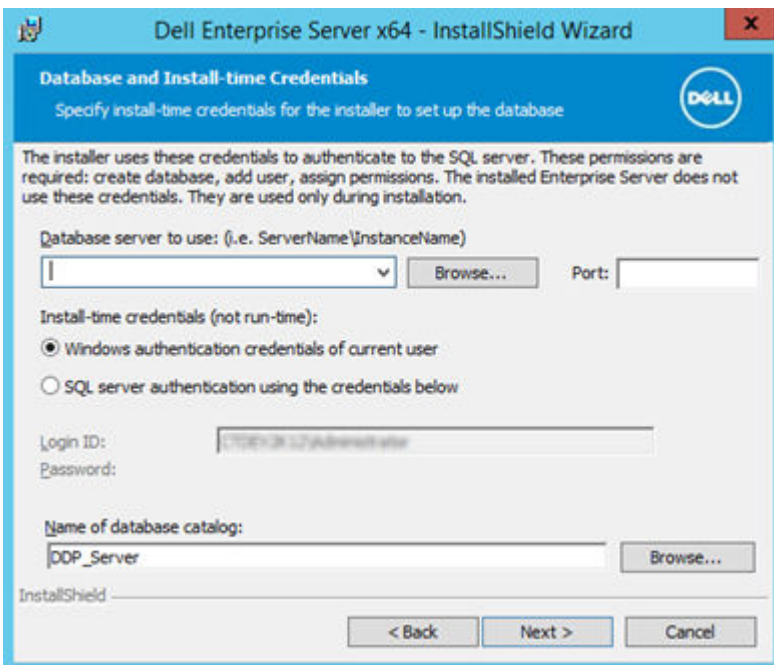
- To select a location for backup configuration files to be stored, click **Change**, navigate to the desired folder, and click **Next**. Dell recommends that you select a remote network location or external drive for backup.



The folder structure created by the installer during installation (example shown below) must remain unchanged.



7 When the installer properly locates the existing database, the dialog is filled out for you.



To connect to the existing database, specify the authentication method to use. After installation, the installed product does not use credentials specified here.

- a Select the database authentication type:
 - **Windows authentication credentials of current user**

If you choose Windows Authentication, the same credentials that were used to log in to Windows will be used for authentication (User Name and Password fields will not be editable).

Ensure that the account has system administrator rights and the ability to manage the SQL Server. The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

OR

- **SQL server authentication using the credentials below**

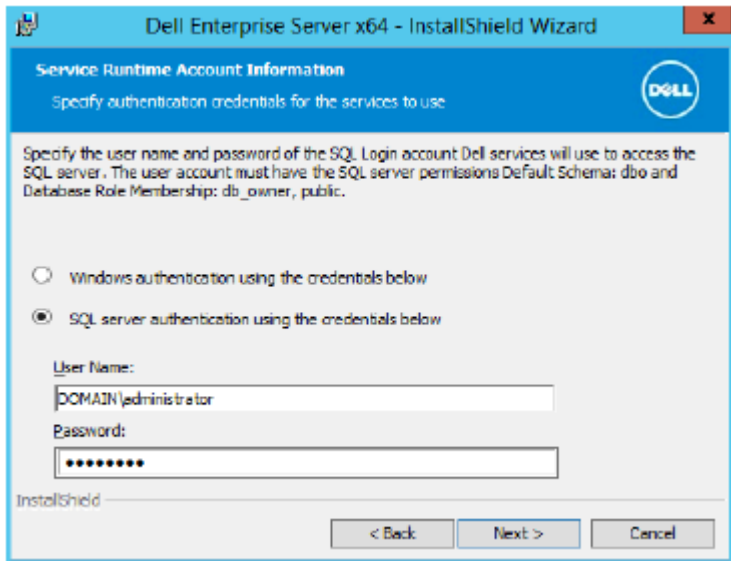


If you use SQL authentication, the SQL account used must have system administrator rights on the SQL Server.

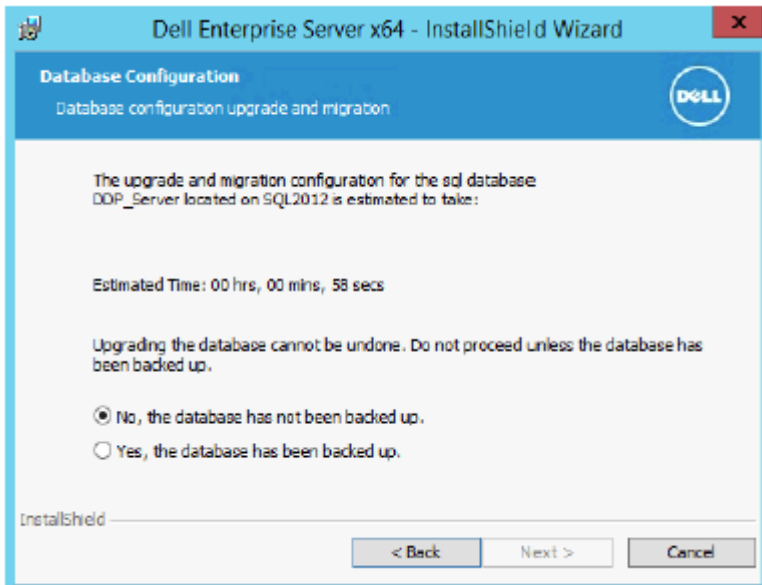
The installer must authenticate to the SQL Server with these permissions: create database, add user, assign permissions.

- b Click **Next**.
- 8 If the Service Runtime Account Information dialog is not pre-populated, specify the authentication method for the product to use after installation.
- a Select the authentication type.
 - b Enter the user name and password of the domain service account that Dell services will use to access the SQL Server, and click **Next**.

The user account must be in the format DOMAIN\Username and have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

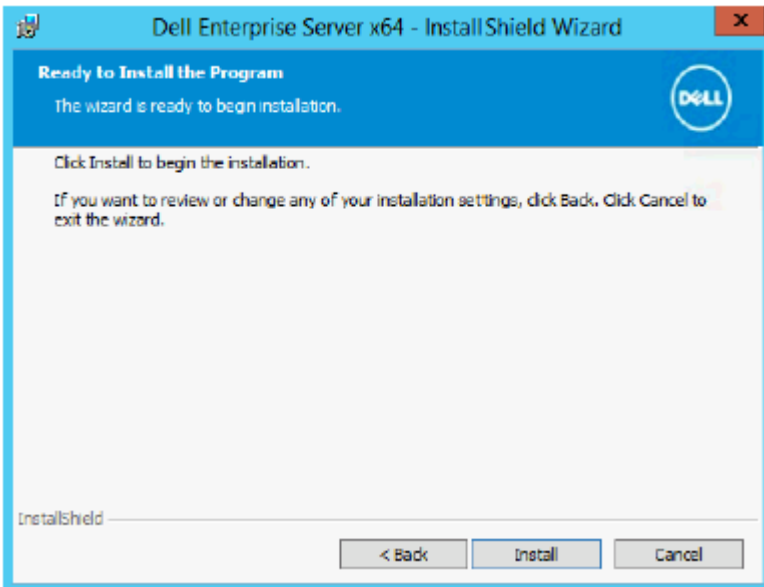


- 9 If the database is not backed up, you **must** back it up before continuing the installation. ***Database upgrade cannot be rolled back.*** Only after the database is backed up, select **Yes, the database has been backed up**, and click **Next**.

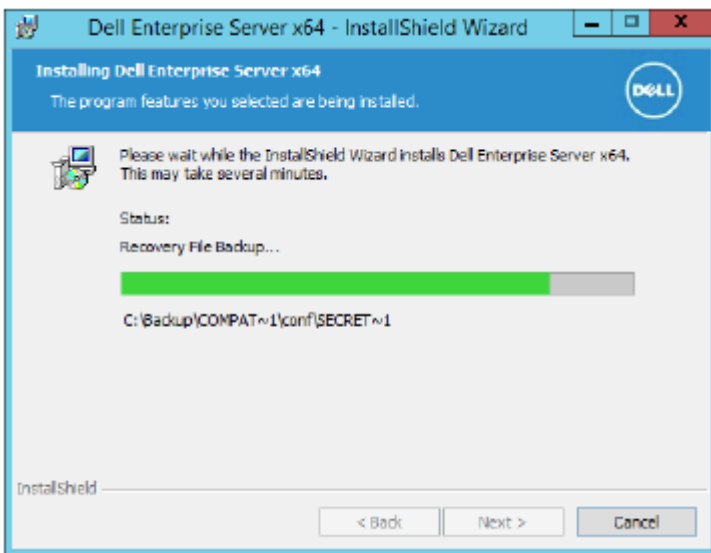


- 10 Click **Install** to begin the installation.



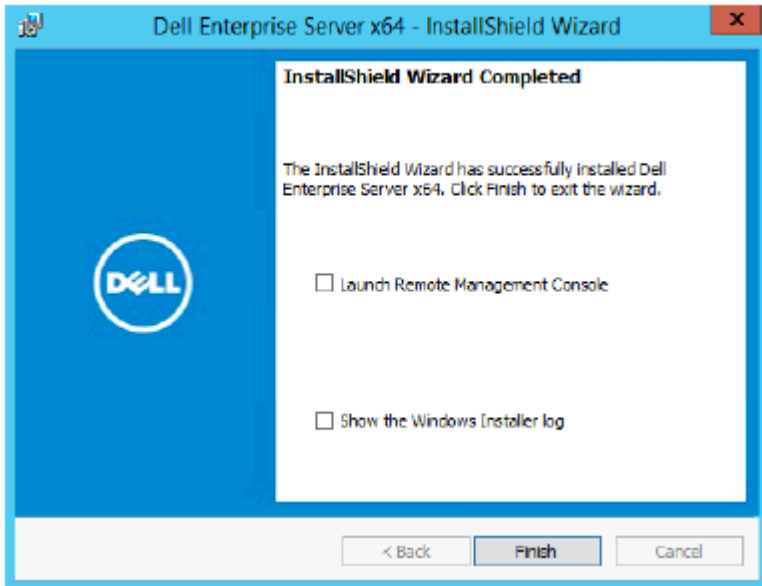


A progress dialog displays status throughout the upgrade process.



- 11 When the installation is completed, click **Finish**.





Dell Services are restarted at the end of migration. It is not necessary to reboot the Server.

The installer performs steps 12-13 for you. It is a Best Practice to check these values to ensure the changes have been made properly.

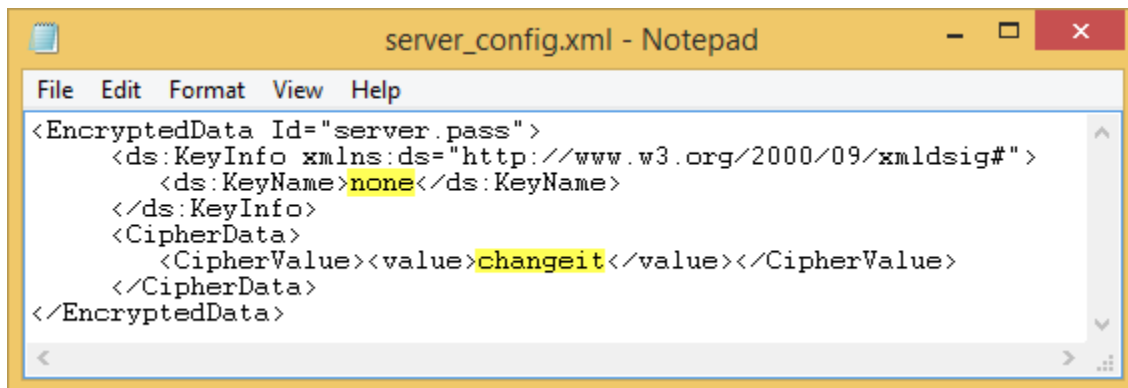
- 12 In your backed up installation, copy/paste: <Compatibility Server install dir>\conf\secretKeyStore to the new installation:
<Compatibility Server install dir>\conf\secretKeyStore
- 13 In the new installation, open <Compatibility Server install dir>\conf\server_config.xml and replace the **server.pass** value with the value from the backed up <Compatibility Server install dir>\conf\server_config.xml, as follows:

Instructions for server.pass:

If you know the password, refer to the example server_config.xml file and make the following changes:

- Edit the *KeyName* from **CFG_KEY** value to **none**.
- Enter the plain text password and enclose it between <value> </value>, which in this example is <value>changeit</value>
- When the Dell Enterprise Server starts, the plain text password is hashed, and the hashed value replaces the plain text.

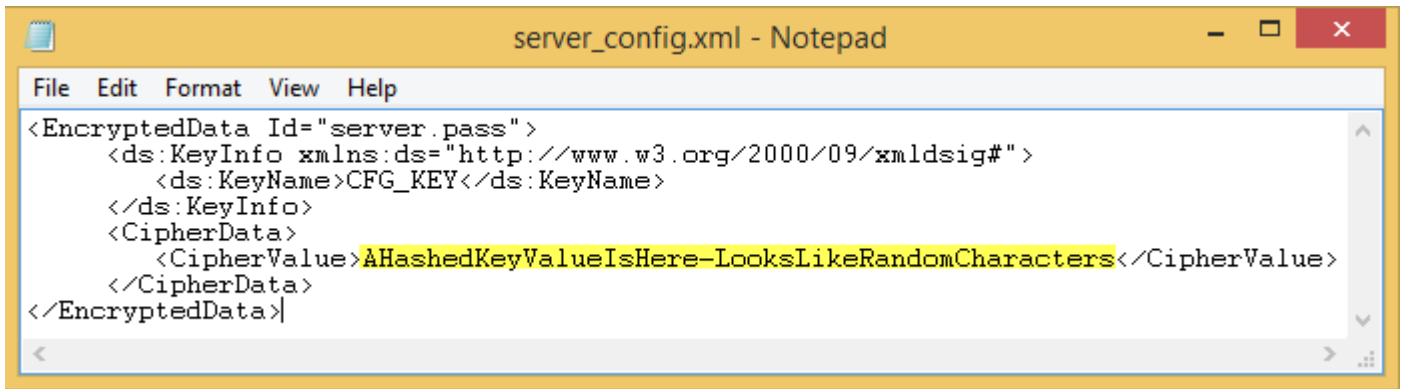
Known Password



If you do not know the password, cut and paste the section similar to the section shown in [Figure 4-2](#) from the backed up <Compatibility Server install dir>\conf\server_config.xml file into the corresponding section in the new server_config.xml file.

Unknown Password





```
server_config.xml - Notepad
File Edit Format View Help
<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>
```

Save and close the file.

NOTE:

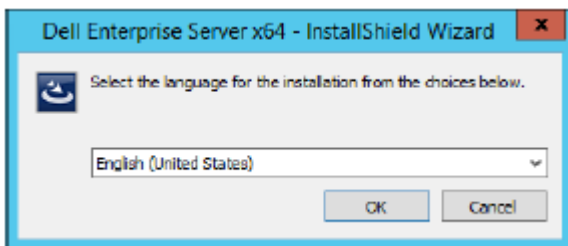
Do not attempt to change the **Dell** Enterprise Server password by editing the server.pass value in server_config.xml at any other time. If you change this value, you lose access to the database.

Back End Server migration tasks are complete.

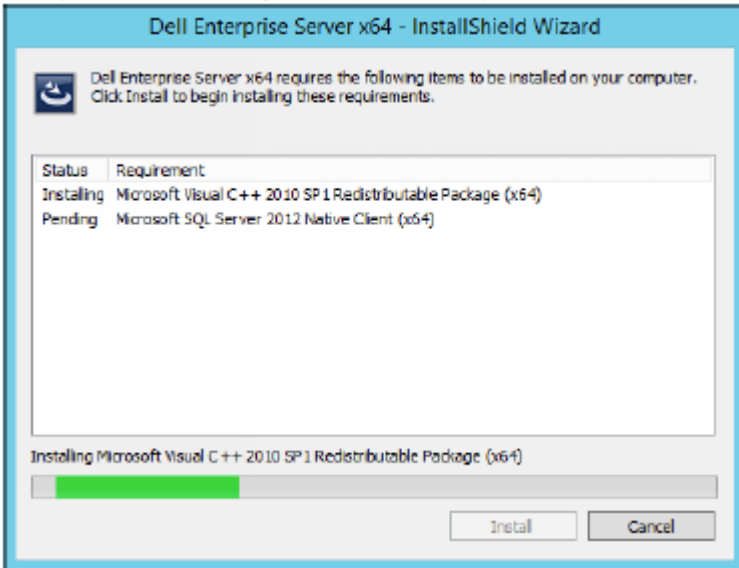
Upgrade/Migrate Front End Server(s)

NOTE: Beginning with v9.5, the Beacon Service is installed as part of this upgrade using the default hostname and port 8446. The Beacon Service supports Secure Lifecycle callback beacon, which inserts a callback beacon into every file protected by Secure Lifecycle when running Protected Office mode. This allows communication between any device in any location and the Dell Front End Server. The Enable Callback Beacon policy is enabled by default. Ensure that necessary network security is configured before using the callback beacon.

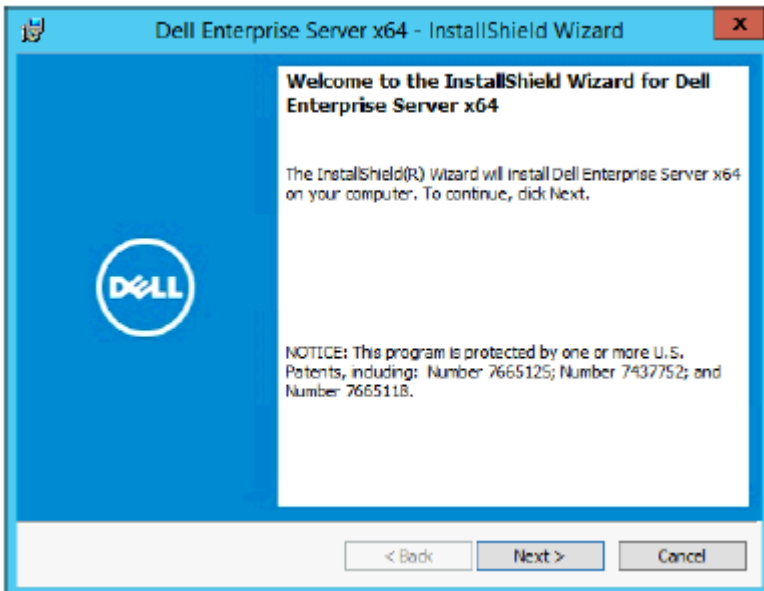
- 1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing Enterprise Server. **Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.**
- 2 Double-click **setup.exe**.
- 3 In the *InstallShield Wizard* dialog, select the language for installation, then click **OK**.



- 4 If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.

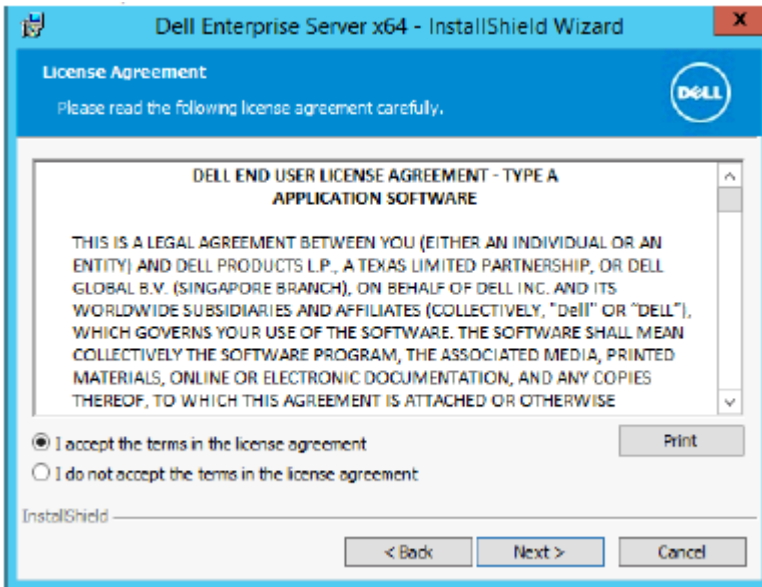


- 5 In the *Welcome* dialog, click **Next**.

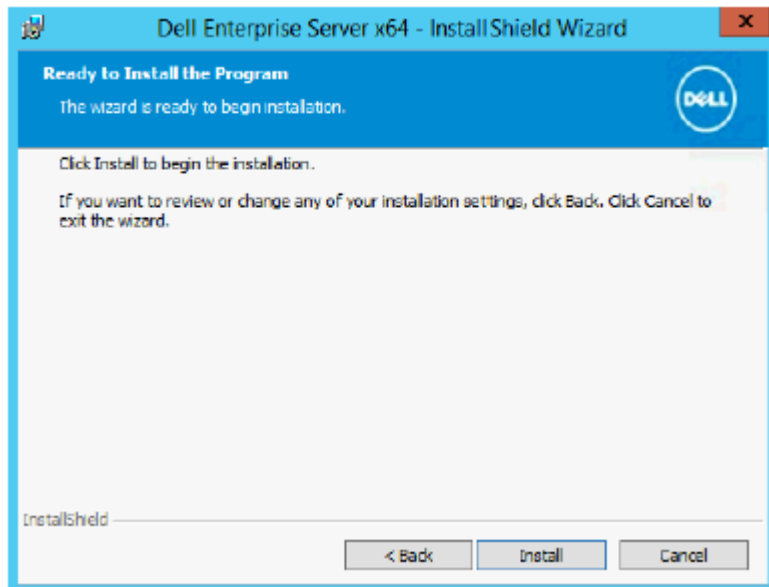


- 6 Read the license agreement, accept the terms, then click **Next**.

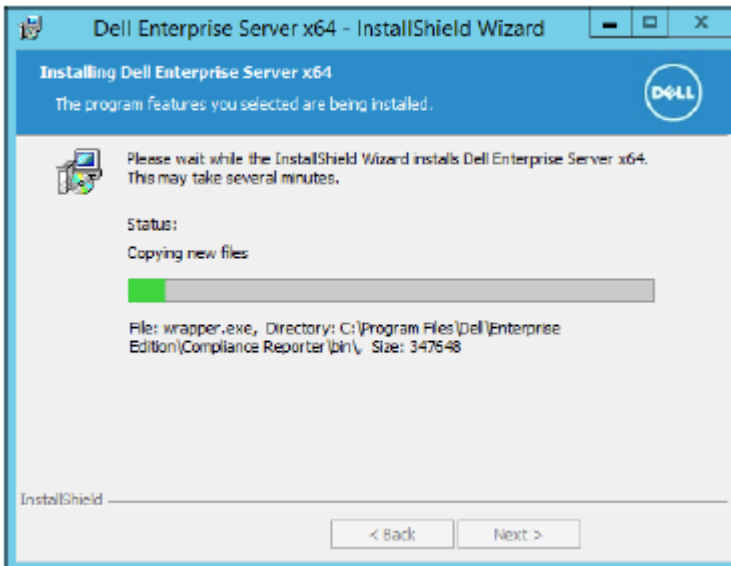




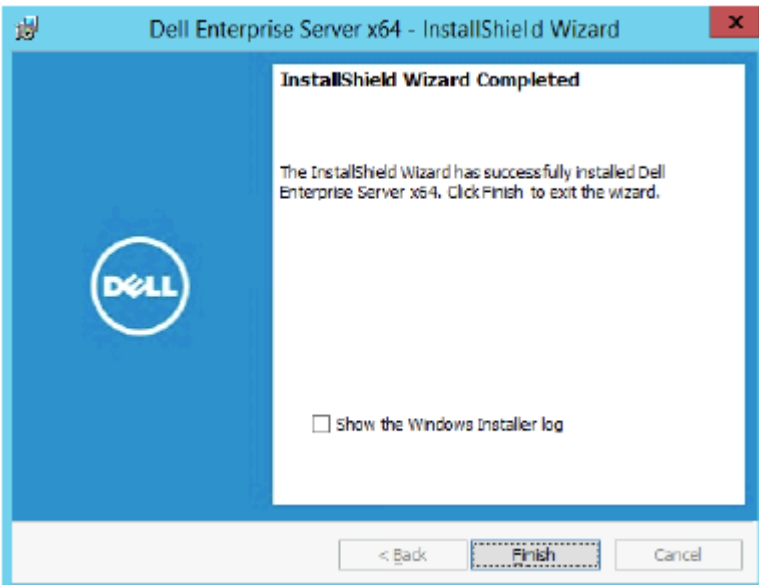
- 7 In the *Ready to Install the Program* dialog, click **Install**.



A progress dialog displays status throughout the installation process.



8 When the installation is completed, click **Finish**.



- 9 Set up the back end server to communicate with the front end server.
- On the back end server, go to <Security Server install dir>\conf\ and open the application.properties file.
 - Locate publicdns.server.host and set the name to an externally resolvable host name.
 - Locate publicdns.server.port and set the port (the default is 8443).

Dell Services are restarted at the end of installation. It is not necessary to reboot the Server until Post-Installation Configuration tasks are complete.

Disconnected Mode Installation

Disconnected mode isolates Enterprise Server from the Internet and an unsecured LAN or other network. After Enterprise Server is installed in Disconnected Mode, it will remain in Disconnected Mode and cannot be changed back to Connected Mode.

Enterprise Server is installed in Disconnected Mode at the command line.

The following table lists the available switches.

Switch	Meaning
/v	Pass variables to the .msi inside the *.exe
/s	Silent mode

The following table lists available display options.

Option	Meaning
/q	No Progress dialog, restarts itself after process completion
/qb	Progress dialog with Cancel button
/qn	No user interface

The following table details the parameters available for the installation. These parameters can be specified at the command line or called from a file by using the property:

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

Parameters

AGREE_TO_LICENSE=Yes - This value must be "Yes."

PRODUCT_SN=xxxxx - Optional if you have the license information in the standard location; otherwise, enter it here.

INSTALLDIR=<path> - Optional.

BACKUPDIR=<path> - This is where the recovery files will be stored.

NOTE: The folder structure created by the installer during this installation step (example shown below) must remain unchanged.

AIRGAP=1 - This value must be "1" to install Enterprise Server in Disconnected Mode.

SSL_TYPE=n - Where n is 1 to import an existing certificate that was purchased from a CA authority and 2 to create a self-signed certificate. The SSL_TYPE value determines which SSL properties are required.

The following are required with SSL_TYPE=1:

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

The following are required with SSL_TYPE=2:

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY - Optional, default = "US"

SSL_STATENAME

SSOS_TYPE=n - Where n is 1 to import an existing certificate that was purchased from a CA authority and 2 to create a self-signed certificate. The SSOS_TYPE value determines which SSOS properties are required.



Parameters

The following are required with SSOS_TYPE=1:

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

The following are required with SSOS_TYPE=2:

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY - Optional, default = "US"

SSOS_STATENAME

DISPLAY_SQLSERVER - This value will be parsed to get Server, Instance and port information.

Example:

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE - Optional. The default value is FALSE, which means that the database is not created. The database must already exist on server.

To create a new database, set this value to TRUE.

IS_SQLSERVER_AUTHENTICATION=0 - Optional. The default value is 0, which specifies that Windows authentication credentials of the current logged on user are used to authenticate to the SQL server. To use SQL authentication, set this value to 1.

NOTE: The installer must authenticate to the SQL server with these permissions: create database, add user, assign permissions. The credentials are install-time credentials, not run-time credentials.

If SQL authentication is used, the following are required:

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION - Required. Specify the authentication method for the product to use. This step connects an account to the product. These credentials are also used by Dell services as they work with the Enterprise Server. To use Windows authentication, set this value to 0. To use SQL authentication, set the value to 1.

NOTE: Ensure that the account has system administrator rights and the ability to manage the SQL server. The user account must have the SQL server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

SQL_EE_USERNAME - Required. With Windows authentication, use this format: DOMAIN\username. With SQL authentication, specify the user name.

SQL_EE_PASSWORD - Required. Specify the password associated with the Windows or SQL user name.

If SQL authentication is used (EE_SQLSERVER_AUTHENTICATION=1) the following are valid:

RUNAS_KEYSERVER_USER - Set the Key Server "run as" Windows username in this format: Domain\user. This must be a Windows user account.

RUNAS_KEYSERVER_PSWD - Set Key Server "run as" Windows password associated with the Windows user account.

Parameters

SQL_ADD_LOGIN=T - Optional. The default is null (this login is not added). When the value is set to T, if the SQL_EE_USERNAME is not a login or user for the database, the installer will attempt to add the user's SQL authentication credentials and set privileges to allow the credentials to be used by the product.

Following are hostname parameters. Edit hostnames only if necessary. Dell recommends using the defaults. Format must be `server.domain.com`.

 **NOTE: A hostname cannot contain an underscore character ("_").**

CORESERVERHOST - Optional. Core Server Hostname.

RMIHOST - Optional. Compatibility Server Hostname.

REPORTERHOST - Optional. Compliance Reporter Hostname.

DEVICEHOST - Optional. Device Server Hostname.

KEYSERVERHOST - Optional. Key Server Hostname.

TIGAHOST - Optional. Security Server Hostname.

SMTP_HOST - Optional. SMTP Hostname.

ACTIVEMQHOST - Optional. Message Broker Hostname.

Following are port parameters. Edit ports only if necessary. Dell recommends using the defaults

SERVERPORT_CLIENTAUTH - Optional.

REPORTERPORT - Optional.

DEVICEPORT - Optional.

KEYSERVERPORT - Optional.

GKPORT - Optional.

TIGAPORT - Optional.

SMTP_PORT - Optional.

ACTIVEMQ_TCP - Optional.

ACTIVEMQ_STOMP - Optional.

Install Enterprise Server in Disconnected Mode

The following example installs Enterprise Server in silent mode with a progress dialog, using installation parameters listed in the file, C :

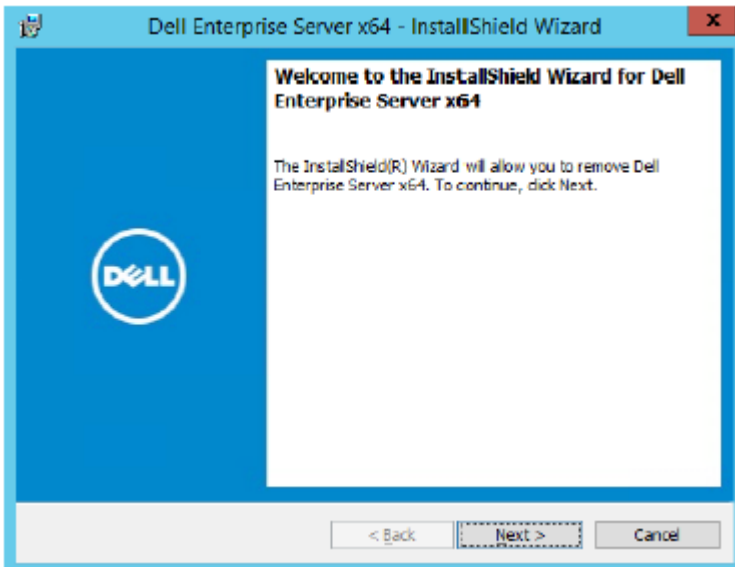
```
\mysetups\eeoptions.txt\" "
```

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

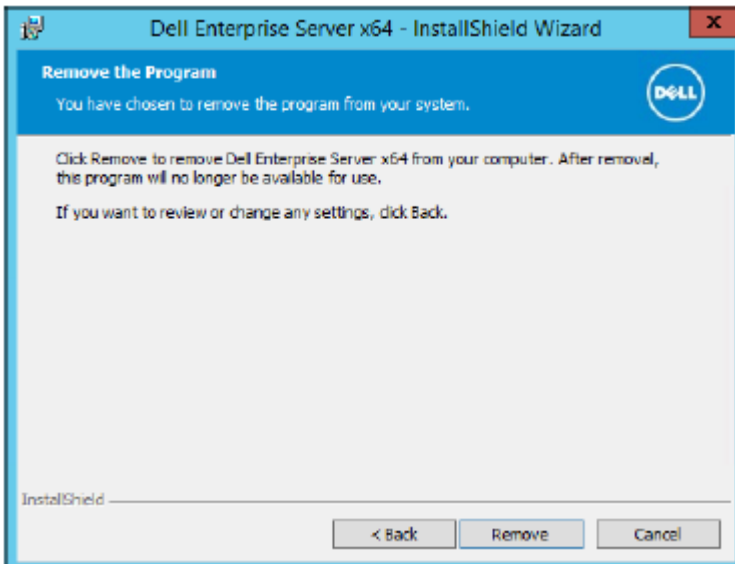


Uninstall Dell Enterprise Server

- 1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (DO NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are uninstalling Enterprise Server. ***Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.***
- 2 Double-click **setup.exe**.
- 3 In the *Welcome* dialog, click **Next**.

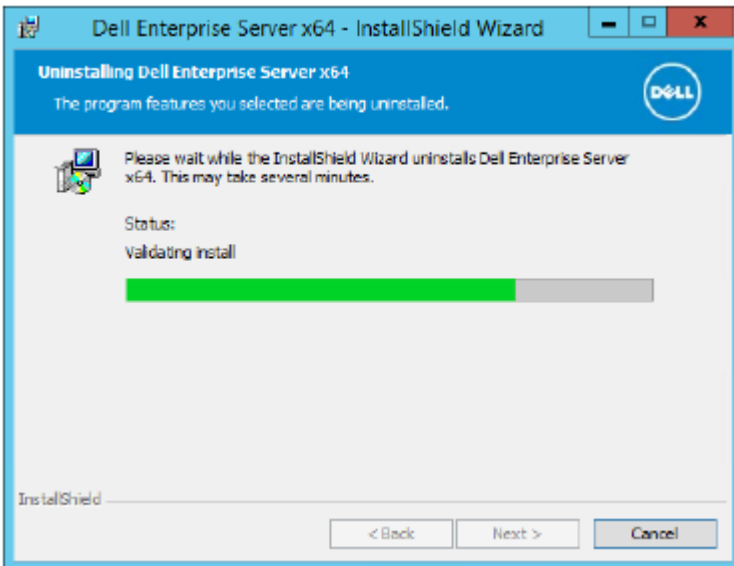


- 4 In the *Remove the Program* dialog, click **Remove**.

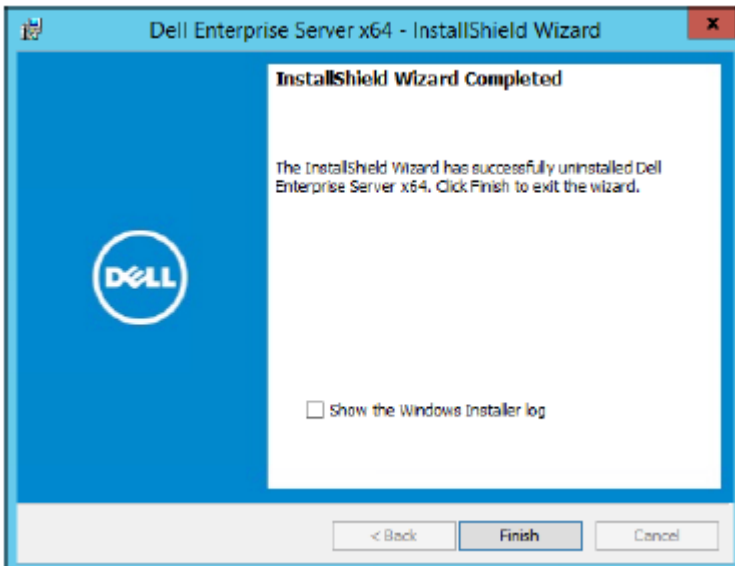


A progress dialog displays status throughout the uninstallation process.





- 5 When the uninstallation is completed, click **Finish**.



Post-Installation Configuration

Read the *Enterprise Server Technical Advisories* for current workarounds or known issues related to Dell Enterprise Server configuration.

Whether you are installing the Dell Enterprise Server for the first time or are upgrading an existing installation, some components of your environment must be configured.

EAS Management Installation and Configuration

This section needs to be completed if you intend to use Mobile Edition. If not, omit this section and continue to [Dell Security Server in DMZ Mode Configuration](#).

Prerequisites

- The logon account for the EAS Mailbox Manager Service must be an account with permissions to create/modify Exchange ActiveSync policy, assign policies to user mailboxes, and query information about ActiveSync devices.
- The EAS Configuration Utility must be run with Admin permissions to modify files and restart Services.
- Network connection to the Dell Policy Proxy is required.
- Have the FQDN of the Dell Policy Proxy available.
- Have the Dell Policy Proxy port number available.
- Microsoft Message Queuing (MSMQ) must already be installed/configured on the server hosting the Exchange environment. If not, see [Install/Configure Microsoft Message Queuing \(MSMQ\)](#).

During the Deployment Process

If you intend to use Exchange ActiveSync to manage mobile devices through Mobile Edition, your Exchange Server environment must be configured.

Install EAS Device Manager

- 1 In the Dell installation media, navigate to the EAS Management folder. In the EAS Device Manager folder, copy setup.exe to your *Exchange Client Access Server(s)*.
- 2 Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Client Access Server*, run this installer on each one.
- 3 Select the language for installation, then click **OK**.
- 4 Click **Next** when the *Welcome* screen displays.
- 5 Read the license agreement, agree to the terms, and click **Next**.
- 6 Click **Next** to install EAS Device Manager in the default location of `C:\inetpub\wwwroot\Dell\EAS Device Manager\`.
- 7 Click **Install** at the *Ready to Begin Installation* screen.
A status window displays the installation progress.
- 8 If desired, check the box to show the Windows Installer log and click **Finish**.

Install EAS Mailbox Manager

- 1 In the Dell installation media, navigate to the EAS Management folder. In the EAS Mailbox Manager folder, copy setup.exe to your *Exchange Mailbox Server(s)*.
- 2 Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Mailbox Server*, run this installer on each one.
- 3 Select the language for installation, then click **OK**.
- 4 Click **Next** when the *Welcome* screen displays.
- 5 Read the license agreement, agree to the terms, and click **Next**.
- 6 Click **Next** to install EAS Mailbox Manager in the default location of `C:\Program Files\Dell\EAS Mailbox Manager\`.
- 7 At the Logon Information screen, enter the credentials of the user account that will logon to use this Service.
User Name: DOMAIN\Username

Password: password associated with this user name

Click **Next**.
- 8 Click **Install** at the *Ready to Begin Installation* screen.
A status window displays the installation progress.
- 9 If desired, check the box to show the Windows Installer log and click **Finish**.

Use the EAS Configuration Utility

- 1 On the same computer, go to **Start > Dell > EAS Configuration Utility > EAS Configuration** to run the EAS Configuration Utility.
- 2 Click **Setup** to configure EAS Management Settings.
- 3 Enter the following information:
FQDN of the Dell Policy Proxy

Dell Policy Proxy Port (the default port is 8090)

Dell Policy Proxy Polling Interval (the default is 1 minute)

Select the box to run EAS Device Manager in report-only mode (recommended during deployment)

NOTE:

The Report-only mode allows unknown devices/users to have access to Exchange ActiveSync, but still reports the traffic to you. Once your deployment is up and running, you can change this setting to tighten security.

- Click **OK**.
- 4 A success message displays. Click **Yes** to re-start IIS and EAS Mailbox Manager Services.
 - 5 Click **Quit** when finished.

Configure EAS Management Settings

Once your deployment is up and running, and you are ready to tighten security, follow the steps below.

- 1 Go to **Start > Dell > EAS Configuration Utility > EAS Configuration** to run the EAS Configuration Utility.
- 2 Click **Setup** to configure EAS Management Settings.
- 3 Enter the following information:



FQDN of the Dell Policy Proxy

Dell Policy Proxy Port (the default port is 8090)

Dell Policy Proxy Polling Interval (the default is 1 minute)

De-select the box to run EAS Device Manager in report-only mode

Click **OK**.

4 A success message displays. Click **Yes** to re-start IIS and EAS Mailbox Manager Services.

5 Click **Quit** when finished.

Dell Security Server in DMZ Mode Configuration

If the Dell Security Server is deployed in a DMZ and a private network, and only the DMZ server has a domain certificate from a trusted Certificate Authority (CA), some manual steps are needed to add the trusted certificate into the Java keystore of the private network Dell Security Server.

If a trusted certificate is being used, omit this section and continue to [APNs Enrollment](#).

NOTE: We highly recommend the use of domain certificates from a trusted Certificate Authority for both DMZ and private network servers.

Use Keytool to Import the DMZ Domain Certificate

IMPORTANT:

Back up the existing Dell Security Server cacerts before continuing with the Keytool instructions. If a configuration error is made, you can revert back to the saved file.

Assumptions

- Dell Security Server was installed with an untrusted certificate.
- Dell Security Server in DMZ Mode was installed using a signed certificate (Entrust, Verisign, etc.)
- A .pfx certificate file is available. If your certificate needs to be converted to .pfx, see [Exporting a Certificate to .PFX Using the Certificate Management Console](#).

Process

1 Add Keytool to the system path.

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

2 Use Keytool to list the contents of the trusted domain certificate that you want to import. Take note of the Alias Name listed.

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

3 Use Keytool to import the contents of the signed certificate into the Dell Security Server's cacerts file:

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

For -sralias, you will need to gather this information from the exported contents of the signed certificate.

For -destalias, this can be any location you choose.

4 Backup and replace the current cacerts file in the <Security Server install dir>\conf\ directory with this newly created cacerts file on the Dell Security Server.

Modify application.properties File

Modify the application.properties file to specify the alias of the signing cert.

- 1 Go to <Security Server install dir>\conf\application.properties
- 2 Modify the following information:
keystore.alias.signing=<Change this value to the value of [step 3](#) above for -destalias>
- 3 Restart the Dell Security Server Service.

APNs Enrollment

If you intend to use Mobile Edition for Mobile Device Security with iOS devices, the APNs Enrollment wizard must be used to:

- Create a CSR
- Create an Apple Push Certificate
- Upload a Push Certificate

If you do not intend to use Mobile Edition for Mobile Device Security with iOS devices, omit this section and continue to [Server Configuration Tool](#).

The Apple Push Notification service (APNs) enables secure communication to iOS devices over-the-air. APNs is used to send notification for an iOS device to check in with the Dell Enterprise Server. The APNs only sends notification to the device, no data is sent.

Process

- 1 Open a browser and go to <https://<FQDN-of-security-server>:8443/csrweb>.
- 2 On the APNs Enrollment Wizard Login dialog, enter your Dell Administrator credentials and click **Login**.
- 3 A dialog displays that describes the steps you are about to take. Click **Next**.

Step I: Create CSR

- 4 Enter the following information:

Email: The email address can be any UPN, but we recommend using an account for the administrator that will be maintaining the APNs certificate.

Common Name: Enter the Common Name associated with this email address.

Click **Generate CSR**.

- 5 After you generate a CSR, save the file to an easily accessible location.
- 6 Click **Next**.

Step II: Create Apple Push Certificate

- 7 Click the link for the **Apple Push Certificate Portal**. Login with your Apple ID and password.
- 8 Read the Terms of Use, indicate acceptance, and click **Accept**.
- 9 Click **Browse** and then **Upload** the CSR you just created.
- 10 On the *Certificates for Third-Party Servers* page, click **Download**. Save the file to an easily accessible location.
- 11 Return to the APNs Enrollment Wizard and click **Next**.

Step III: Upload Push Certificate

- 12 Enter the following information (use the same credentials that were used in [Step I: Create CSR](#)).

Email:



Common Name:

Push Cert File: Click **Browse** to locate the file saved in [step 7](#). Click **Upload**.

13 A success message displays. Click **Finish**.

Enrollment of the APNs Certificate with the Dell Enterprise Server is complete.

Server Configuration Tool

When configurations to your environment become necessary after you've completed your installation, use the Dell Server Configuration Tool to make the changes.

The Dell Server Configuration Tool allows you to:

- [Add New or Updated Certificates](#)
- [Import Dell Manager Certificate](#)
- [Import Identity Certificate](#)
- [Configure settings for Server SSL Certificate or Mobile Edition](#)
- [Configure SMTP settings for Secure Lifecycle or Email Services](#)
- [Change Database Name, Location, or Credentials](#)
- [Migrate the Database](#)

The Dell Core Server and Dell Compatibility Server cannot run simultaneously with the Dell Server Configuration Tool. Stop the Dell Core Server Service and Dell Compatibility Server Service in *Services* (**Start > Run**. Type *services.msc*) prior to starting the Dell Server Configuration Tool.

To launch the Dell Server Configuration Tool, go to **Start > Programs > Dell > Enterprise Edition > Server Configuration Tool > Run Server Configuration Tool**.

The Dell Server Configuration Tool logs to `C:\Program Files\Dell\Enterprise Edition\Configuration Tool\Logs`.

Add New or Updated Certificates

You have a choice of which type of certificates to use - self-signed or signed:

- **Self-signed** certificates are signed by their own creator. Self-signed certificates are appropriate for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.
- **Signed** (public CA-signed or domain-signed) certificates are signed by a public CA or a domain. In the case of certificates that are signed by a public certificate authority (CA), the certificate of the signing CA will, usually, already exist in the Microsoft certificate store and therefore, the chain of trust will be automatically established. For domain CA-signed certificates, if the workstation has been joined to the domain, the signing CA certificate from the domain will have been added to the workstation's Microsoft certificate store, thereby also creating a chain of trust.

The components that are affected by certificate configuration:

- Java Services (for instance, Dell Device Server, and so on)
- .NET Applications (Dell Core Server)
- Validation of smart cards used for Preboot Authentication (Dell Security Server)
- Importing of private encryption keys to be used for signing policy bundles being sent to Dell Manager. Dell Manager performs SSL validation for remotely-managed Enterprise Edition clients with self-encrypting drives, or BitLocker Manager.
- Client Workstations:
 - Workstations running BitLocker Manager
 - Workstations running Enterprise Edition (Windows clients)



- Workstations running Endpoint Security Suite
- Workstations running Endpoint Security Suite Enterprise

Information regarding which type of certificates to use:

Preboot Authentication using smart cards requires SSL validation with the Dell Security Server. Dell Manager performs SSL validation when connecting to the Dell Core Server. For these types of connections, the signing CA will need to be in the keystore (either the Java keystore or the Microsoft keystore, depending on which Dell Server component is being discussed). If self-signed certificates are chosen, the following options are available:

- Validation of smart cards used for Preboot Authentication:
 - Import the "Root Agency" signing certificate and full chain of trust into the Dell Security Server Java keystore. For more information, see [Create a Self-Signed Certificate and Generate a Certificate Signing Request](#). The full chain of trust must be imported.

Dell Manager:

- Insert the "Root Agency" signing certificate (from the self-signed certificate generated) into the workstation's "Trusted Root Certification Authorities" (for "local computer") in the Microsoft keystore.
- Modify the behavior of Server-side SSL validation. To turn off Server-side SSL trust validation, check **Disable Trust Chain Check** on the Settings tab.

There are two methods to create a certificate - *Express* and *Advanced*.

Choose **one** method:

- [Express](#) - Choose this method to generate a self-signed certificate for all components. This is the easiest method, but self-signed certificates are appropriate only for pilots, POCs, etc. For a production environment, Dell recommends public CA-signed or domain-signed certificates.
- [Advanced](#) - Choose this method to configure each component separately.

Express

- 1 From the top menu, select **Actions > Configure Certificates**.
- 2 When the Configuration Wizard launches, select **Express** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.
- 3 From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Certificate set up is complete. The rest of this section details the Advanced method of creating a certificate.

Advanced

There are two paths to create a certificate - *Generate Self-Signed Certificate* and *Use Current Settings*. Choose **one** path:

- [Path 1 - Generate Self-Signed Certificate](#)
- [Path 2 - Use Current Settings](#)

Path 1 - Generate Self-Signed Certificate

- 1 From the top menu, select **Actions > Configure Certificates**.
- 2 When the Configuration Wizard launches, select **Advanced** and click **Next**.
- 3 Select **Generate Self-Signed Certificate** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.
- 4 From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Certificate set up is complete. The rest of this section details the other method of creating a certificate.

Path 2 - Use Current Settings



- 1 From the top menu, select **Actions > Configure Certificates**.
- 2 When the Configuration Wizard launches, select **Advanced** and click **Next**.
- 3 Select **Use Current Settings** and click **Next**.
- 4 At the *Compatibility Server SSL Certificate* window, select **Generate Self-Signed Certificate** and click **Next**. The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

Click **Next**.

- 5 At the *Core Server SSL Certificate* window, select one of the following:

- *Select Certificate* - Select this option to use an existing certificate. Click **Next**.

Browse to the location of the existing certificate, enter the password associated with the existing certificate, and click **Next**.

Click **Finish** when complete.

- *Generate Self-Signed Certificate* - The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available. If you select this option, the Message Security Certificate window does not display (the window does display if you select option *Use Current Settings*) and the certificate created for the Dell Compatibility Server is used.

Verify that the fully qualified computer name is correct. Click **Next**.

A warning message displays, telling you that a certificate by the same name already exists. When asked if you would like to use it, click **Yes**.

Click **Finish** when complete.

- *Use Current Settings* - Select this option to change a setting on a certificate anytime after the initial configuration of the Dell Enterprise Server. Selecting this option leaves your already configured certificate in place. Selecting this option advances you to the Message Security Certificate window.

At the Message Security Certificate, select **one** of the following:

- *Select Certificate* - Select this option to use an existing certificate. Click **Next**.

Browse to the location of the existing certificate, enter the password associated with the existing certificate, and click **Next**.

Click **Finish** when complete.

- *Generate Self-Signed Certificate* - The information from the self-signed certificate that was created when installing the Enterprise Server will be used, if available.

Click **Next**.

Click **Finish** when complete.

Certificate set up is complete.

When changes are complete:

- 1 From the top menu, select **Configuration > Save**. If prompted, confirm the save.
- 2 Close the Dell Server Configuration Tool.
- 3 Click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Start the service**.

Import Dell Manager Certificate

If your deployment includes Enterprise Edition remotely-managed clients with self-encrypting drives, or BitLocker Manager, you must import your newly created (or existing) certificate. The Dell Manager certificate is used as a vehicle to protect the private key which is used to sign the policy bundles being sent to Enterprise Edition remotely-managed clients and BitLocker Manager. This certificate can be

independent of any of the other certificates. Additionally, if this key is compromised it can be replaced with a new key, and Dell Manager will request a new public key if it cannot decrypt the policy bundles.

- 1 Open the Microsoft Management Console.
- 2 Click **File** > **Add/Remove Snap-in**.
- 3 Click **Add**.
- 4 At the *Add Standalone Snap-in* window, select **Certificates** and click **Add**.
- 5 Select **Computer Account** and click **Next**.
- 6 At the *Select Computer* window, select **Local computer (the computer this console is running on)** and click **Finish**.
- 7 Click **Close**.
- 8 Click **OK**.
- 9 In the *Console Root* folder, expand *Certificates (Local Computer)*.
- 10 Go to the *Personal* folder and locate the desired certificate.
- 11 Highlight the desired certificate, right-click **All Tasks** > **Export**.
- 12 When the Certificate Export wizard opens, click **Next**.
- 13 Select **Yes, export the private key** and click **Next**.
- 14 Select **Personal Information Exchange - PKCS #12 (.PFX)** and then select the sub-options **Include all certificates in the certification path if possible** and **Export all extended properties**. Click **Next**.
- 15 Enter and confirm a password. This can be any password of your choosing. Choose a password that is easy for you to remember, but no one else. Click **Next**.
- 16 Click **Browse** to browse to the location of where you would like to save the file.
- 17 In the *File Name* field, enter a name to save the file as. Click **Save**.
- 18 Click **Next**.
- 19 Click **Finish**.
- 20 A message stating that the export was successful displays. Close the MMC.
- 21 Go back to the Dell Server Configuration Tool.
- 22 From the top menu, select **Actions** > **Import Manager Certificate**.
- 23 Navigate to the location where the exported file was saved. Select the file and click **Open**.
- 24 Enter the password associated with this file and click **OK**.

The Dell Manager certificate import is now complete.

When changes are complete:

- 1 From the top menu, select **Configuration** > **Save**. If prompted, confirm the save.
- 2 Close the Dell Server Configuration Tool.
- 3 Click **Start** > **Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Start the service**.

Import Identity Certificate

If your deployment includes Server Encryption, you must import your newly created (or existing) certificate. The identity certificate protects the private key which is used to sign the policy bundles being sent to client servers. This certificate can be independent of any of the other certificates.

- 1 From the top menu, select **Actions** > **Import Identity Certificate**.
- 2 Browse to select a certificate and click **Next**.
- 3 At the Certificate Password prompt, enter the password associated with the existing certificate.



- 4 In the Windows Account Dialog, choose one option:
 - a To change the credentials associated with the identity certificate, select **Use different Windows account credentials with the identity certificate**.
 - b To continue using the credentials of the account that is logged on, click **Next**.
- 5 From the top menu, select **Configuration > Save**. If prompted, confirm the save.

Configure settings for Server SSL Certificate or Mobile Edition

In the Server Configuration Tool, click the **Settings** tab.

Dell Manager:

To turn off Server-side Dell Manager SSL trust validation, check **Disable Trust Chain Check**.

SCEP:

If using Mobile Edition, enter the URL of the server hosting SCEP.

When changes are complete:

- 1 From the top menu, select **Configuration > Save**. If prompted, confirm the save.
- 2 Close the Dell Server Configuration Tool.
- 3 Click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Start the service**.

Configure SMTP settings for Secure Lifecycle or Email Services

In the Server Configuration Tool, click the **SMTP** tab.

This tab configures SMTP settings for Secure Lifecycle. If SMTP settings need to be configured for other purposes outside of Secure Lifecycle, see the AdminHelp topic "Enable SMTP Server for License Email Notifications".

Enter the following information:

- 1 In the Host Name: field, enter the FQDN of your SMTP server, such as smtpservername.domain.com.
- 2 In the User Name: field, enter the User Name that will log in to the mail server. The format can be DOMAIN\jdoe, jdoe, or whatever form your organization requires.
- 3 In the Password: field, enter the Password associated with this User Name.
- 4 In the From Address: field, enter the email address that the email will originate from. This may be the same as the account for the User Name (jdoe@domain.com), but it can also be another account that the specified User Name has access to send email for (CloudRegistration@domain.com).
- 5 In the Port: field, enter the Port number (typically 25).
- 6 In the Authentication: menu, select either True or False.

When changes are complete:

- 1 From the top menu, select **Configuration > Save**. If prompted, confirm the save.
- 2 Close the Dell Server Configuration Tool.
- 3 Click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Start the service**.

Change Database Name, Location, or Credentials

In the Server Configuration Tool, click the **Database** tab.

- 1 In the *Server Name*: field, enter the fully qualified domain name (if there is an instance name, include it) of the server hosting the database. For example, SQLTest.domain.com\DellDB.

Dell recommends using a fully qualified domain name, although an IP address may be used.

- 2 In the *Server Port*: field, enter the port number.

When using a non-default SQL Server instance, you must specify the dynamic port of the instance in the *Port*: field. As an alternative, enable the SQL Server Browser service and ensure that UDP port 1434 is open. For more information, see [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 In the *Database*: field, enter the name of the database.
- 4 In the *Authentication*: field, select either **Windows Authentication** or **SQL Server Authentication**. If you choose Windows Authentication, the same credentials that were used to log in to Windows will be used for authentication (User Name and Password fields will not be editable).
- 5 In the *User Name*: field, enter the appropriate username associated with this database.
- 6 In the *Password*: field, enter the password for the username listed in the UserName field.
- 7 From the top menu, select **Configuration > Save**. If prompted, confirm the save.
- 8 To test the database configuration, from the top menu, select **Actions > Test Database Configuration**. The Configuration Wizard launches.
- 9 At the *Configuration Test* window, read the test information and click **Next**.
- 10 If you chose Windows Authentication in the *Database* tab, you can optionally enter alternate credentials to allow the use of the same credentials that will be used to run the Dell Enterprise Server. Click **Next**.
- 11 At the *Test Configuration* window, the results of the Test Connection Settings, Compatibility Test, and the Database Migrated Test display.
- 12 Click **Finish**.

NOTE:

If either the SQL database or SQL instance is configured with a non-default collation, the non-default collation must be case-insensitive. For a list of collations and case sensitivity, see [https://msdn.microsoft.com/en-us/library/ms144250\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx).

When changes are complete:

- 1 From the top menu, select **Configuration > Save**. If prompted, confirm the save.
- 2 Close the Dell Server Configuration Tool.
- 3 Click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Start the service**.

Migrate the Database

You can migrate a v8.x database to the latest schema with the latest version of the Server Configuration Tool. To obtain the latest Server Configuration Tool, or to migrate a pre-v8.0 database, contact Dell ProSupport for assistance.

In the Server Configuration Tool, click the **Database** tab.

- 1 If you have not yet backed up your existing Dell database, **do so now**.
- 2 From the top menu, select **Actions > Migrate Database**. The Configuration Wizard launches.



- 3 At the *Migrate Enterprise Database* window, a warning displays. Confirm that you have either backed up the entire database or confirm that a backup does not need to be made of your existing database. Click **Next**.

At the *Migrating Database* window, informational messages display the status of the migration.

When complete, check for errors.

 **NOTE:** An error message identified by , signifies that a database task has failed and corrective action needs to be taken before the database can be properly migrated. Click **Finish**, correct the database errors, and reinitiate the instructions in this section.

- 4 Click **Finish**.

When migration is complete:

- 1 From the top menu, select **Configuration > Save**. If prompted, confirm the save.
- 2 Close the Dell Server Configuration Tool.
- 3 Click **Start > Run**. Type *services.msc* and click **OK**. When *Services* opens, navigate to each Dell Service and click **Start the service**.

Administrative Tasks

Assign Dell Administrator Role

- 1 As a Dell Administrator, log in to the Remote Management Console at this address: <https://server.domain.com:8443/webui/> The default credentials are **superadmin/changeit**.
- 2 In the left pane, click **Populations > Domains**.
- 3 Click a domain that you want to add a user to.
- 4 On the Domain Detail page, click the **Members** tab.
- 5 Click **Add User**.
- 6 Enter a filter to search the User Name by Common Name, Universal Principal Name, or sAMAccountName. The wild card character is *****.
A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not appear in the Domain or Group Members list in the Management, ensure that all three names are properly defined for the user in the enterprise directory server.

The query will automatically search by common name, then UPN, and then sAMAccount name until a match is found.
- 7 Select users from the *Directory User List* to add to the Domain. Use <Shift><click> or <Ctrl><click> to select multiple users.
- 8 Click **Add**.
- 9 From the menu bar, click the **Details & Actions** tab of the specified user.
- 10 Scroll across the menu bar, and select the **Admin** tab.
- 11 Select the administrator roles to add to this user.
- 12 Click **Save**.

Log in with Dell Administrator Role

- 1 Log out of the Remote Management ConsoleEnterprise Server.
- 2 Log in to the Remote Management ConsoleEnterprise Server and login with Domain user credentials.

Upload Client Access License

You received Client Access Licenses separately from the installation files, either at the initial purchase or later if you added additional Client Access Licenses.

- 1 In the left pane, click **Management**.
- 2 Click **License Management**.
- 3 Click **Choose File** to locate and select the Client License file.

Commit Policies

Commit policies when installation is completed.

To commit polices after installation or, later, after policy modifications are saved, follow these steps:

- 1 In the left pane, click **Management > Commit**.
- 2 Enter a description of the change in the Comment field.



- 3 Click **Commit Policies**.

Configure Dell Compliance Reporter

- 1 In the left pane, click **Compliance Reporter**.
- 2 When Dell Compliance Reporter launches, log in using the default credentials of *superadmin/changeit*.
- 3 Two different authentication methods are supported. To configure, select either:
 - [Configure SQL Authentication with Compliance Reporter](#)
 - [Configure Windows Authentication with Compliance Reporter](#)

Configure SQL Authentication with Compliance Reporter

As of v8.1, the Data Source is pre-configured out-of-the-box. No configuration is needed. Use the steps below to change the Data Source, if needed.

- 1 To set the Data Source, on the top menu, click **Settings**. In the left menu, click **Data Source**.
 - 2 Type the Username to log in to the Dell database.
 - 3 Type the Password to log in to the Dell database.
 - 4 Type the Hostname to log in to the Dell database.
 - 5 Type the Database Name to log in to the Dell database.
 - 6 Type the Max Idle connections allowed. The default is 2.
 - 7 Type the Max Connections (active) allowed. The default is 10.
 - 8 Type the Max Wait (maximum number of milliseconds to wait for a connection). -1 is indefinitely.
 - 9 To verify the database URL and test the connectivity between the Dell Compliance Reporter and the Dell database, click **Test Connection**.
 - 10 Click **Update**. To discard the information, click Cancel.
- Administrative tasks are complete. The rest of this chapter discusses Windows Authentication and may be ignored if SQL Authentication is used for Dell Compliance Reporter.

If needed, continue to [Create a Self-Signed Certificate and Generate a Certificate Signing Request](#), or [Export a Certificate to .PFX Using the Certificate Management Console](#).

Configure Windows Authentication with Compliance Reporter

As of v8.1, the Data Source is pre-configured out-of-the-box. No configuration is needed. Use the steps below to change the Data Source, if needed.

- 1 Type the Username to log in to the Dell database.
 - 2 Leave the password blank. When the domain user logs in, their password will be passed to the database.
 - 3 Type the Hostname to log in to the Dell database.
 - 4 Type the Database Name to log in to the Dell database.
 - 5 Type the Max Idle connections allowed. The default is 2.
 - 6 Type the Max Connections (active) allowed. The default is 10.
 - 7 Type the Max Wait (maximum number of milliseconds to wait for a connection). -1 is indefinitely.
 - 8 To verify the database URL and test the connectivity between the Dell Compliance Reporter and the Dell database, click **Test Connection**.
 - 9 Click **Update**. To discard the information, click Cancel.
- Administrative tasks are complete. **If needed**, continue to [Create a Self-Signed Certificate and Generate a Certificate Signing Request](#), or [Export a Certificate to .PFX Using the Certificate Management Console](#).



Perform Back ups

For the purposes of Disaster Recovery, ensure the following locations are backed up weekly, with nightly differentials.

Enterprise Server Backups

On a regular basis, back up the files that are stored in the location you selected for configuration file backup during installation ([step 10 on page 27](#)) or upgrade/migration ([step 6 on page 68](#)). Weekly backups of this data are acceptable, since it should rarely change and can be manually reconfigured if needed. The most critical files store information necessary to connect to the database:

<Installation folder>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<Installation folder>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<Installation folder>\Enterprise Edition\Compatibility Server\conf\gkresource.xml

SQL Server Backups

Perform nightly full backups with transactional logging enabled, and perform differential database backups every 3-4 hours. If a backup database is available, then the recommendation would be that transaction logs and/or log shipping tasks be performed in 15-minute intervals (or shorter intervals if possible). As always, we recommend database best practices are used for the Dell database and that Dell software is included in your organization's disaster recovery plan.

For additional information on SQL Server best practices, please see [The following list explains SQL server best practices, which should be implemented when Dell Data Protection is installed if not already implemented..](#)

PostgreSQL Server Backups

Audit events are stored in the PostgreSQL server, which should be routinely backed up. For backup instructions, refer to <https://www.postgresql.org/docs/9.5/static/backup.html>.

Dell recommends that database best practices are used for the PostgreSQL database and that Dell software is included in your organization's disaster recovery plan.



Dell Component Descriptions

The following table describes each component and its function.

Name	Description	Required For
Compliance Reporter	Provides an extensive view of the environment through auditing and compliance reporting. A component of the Dell Enterprise Server.	Reporting
Key Server	Negotiates, authenticates, and encrypts a client connection using Kerberos APIs. Requires SQL database access to pull the key data. A component of the Dell Enterprise Server.	Dell Admin Utilities
Server Configuration Tool	Configures database communication with the Core Server and Compatibility Server/ Security Server. Used to initialize the database upon installation or to migrate the database to a newer schema. Used to control Dell Services. A component of the Dell Enterprise Server.	All
Remote Management Console Enterprise Server Console	Administration console and control center for the entire enterprise deployment. A component of the Dell Enterprise Server.	All
Core Server	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Protection. Processes inventory data for use by Compliance Reporter and the Remote Management Console. Collects and stores authentication data. Controls role-based access. A component of the Dell Enterprise Server.	All
Security Server	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, Secure Lifecycle products, SED-PBA communication., and Active Directory communication for authentication or reconciliation, including identity validation for authentication into the Remote Management Console. Requires SQL database access. A component of the Dell Enterprise Server.	All

Name	Description	Required For
Compatibility Server	<p>A service for managing the enterprise architecture. Collects and stores initial inventory data during activation and policy data during migrations. Processes data based on user groups in this service.</p> <p>A component of the Dell Enterprise Server.</p>	All
Message Broker Service	<p>Handles communication between services of the Enterprise Server. Stages policy information created by the Compatibility Server for policy proxy queuing</p> <p>Requires SQL database access.</p> <p>A component of the Dell Enterprise Server.</p>	All
Device Server	<p>Supports activations and password recovery.</p> <p>A component of the Dell Enterprise Server.</p>	<p>Enterprise Edition for Mac</p> <p>Enterprise Edition for Windows</p> <p>Handheld Shields</p> <p>CREDActivate</p>
Device Server Plug-ins	<p>Provides support for various components.</p> <p>A component of the Dell Enterprise Server.</p>	All
Identity Server	<p>Handles domain authentication requests.</p> <p>Requires an Active Directory account.</p> <p>Must be the account used to access SQL when Windows Authentication is used.</p> <p>A component of the Dell Enterprise Server.</p>	All
Policy Proxy	<p>Provides a network-based communication path to deliver security policy updates and inventory updates.</p> <p>A component of the Dell Enterprise Server.</p>	<p>Enterprise Edition for Mac</p> <p>Enterprise Edition for Windows</p> <p>Mobile Edition for Mobile Device Security</p>
Security Token Services (STS)	<p>Used to help create a secure authentication channel between the Dell Enterprise Server User Interface and Dell Back End Services.</p>	All
EAS Device Manager	<p>Enables over-the-air functionality. Installed on the Exchange Client Access Server.</p>	Exchange ActiveSync Management of mobile devices.
EAS Mailbox Manager	<p>The mailbox agent that is installed on the Exchange Mailbox Server.</p>	Exchange ActiveSync Management of mobile devices.



SQL Server Best Practices

The following list explains SQL server best practices, which should be implemented when Dell Data Protection is installed if not already implemented.

- 1 Ensure the NTFS block size where the data file and log file reside is 64 KB. SQL Server extents (basic unit of SQL Storage) are 64 KB.

For more information, search Microsoft's TechNet articles for "Understanding Pages and Extents."

- 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 As a general guideline, set the maximum amount of SQL Server memory to 80 percent of the installed memory.

For more information, search Microsoft's TechNet articles for "Server Memory Server Configuration Options."

- 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 Set -t1222 on the instance startup properties to ensure deadlock information is captured if one occurs.

For more information, search Microsoft's TechNet articles for "Trace Flags (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 Ensure that all indexes are covered by a weekly maintenance job to rebuild the indexes.

Certificates

Create a Self-Signed Certificate and Generate a Certificate Signing Request

This section details the steps to create a self-signed certificate for the Java-based components. This process **cannot** be used to create a self-signed certificate for .NET-based components.

We recommend a self-signed certificate *only* in a non-production environment.

If your organization requires an SSL server certificate, or you need to create a certificate for other reasons, this section describes the process to create a java keystore using Keytool.

If your organization plans to use smart cards for authentication, you will need to use Keytool to import the full certificate chain of trust that are used in the smart card user's certificate.

Keytool creates private keys that are passed in the format of a Certificate Signing Request (CSR) to a Certificate Authority (CA), such as VeriSign® or Entrust®. The CA will then, based on this CSR, create a server certificate that it signs. The server certificate is then downloaded to a file along with the signing authority certificate. The certificates are then imported into the cacerts file.

Generate a New Key Pair and a Self-Signed Certificate

- 1 Navigate to the **conf** directory of Dell Compliance Reporter, Dell Security Server, or Dell Device Server.
- 2 Back up the default certificate database:

Click **Start > Run**, and type `move cacerts cacerts.old`.

- 3 Add Keytool to the system path. Type the following command in a command prompt:

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

- 4 To generate a certificate, run Keytool as shown:

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

- 5 Enter the following information as the Keytool prompts for it.

NOTE:

Back up configuration files before editing them. Only change the specified parameters. Changing other data in these files, including tags, can cause system corruption and failure. **Dell** cannot guarantee that problems resulting from unauthorized changes to these files can be solved without reinstalling the **Dell** Enterprise Server.

- *Keystore password*: Enter a password (unsupported characters are <>:&" '), and set the variable in the component **conf** file to the same value, as follows:

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

<Device Server install dir>\conf\eserver.properties. Set the value `eserver.keystore.password =`

<Security Server install dir>\conf\eserver.properties. Set the value `eserver.keystore.password =`



- *Fully Qualified Server Name*: Enter the fully qualified name of the server where the component you are working with is installed. This fully qualified name includes the host name and the domain name (example, server.domain.com).
- *Organizational unit*: Enter the appropriate value (example, Security).
- *Organization*: Enter the appropriate value (example, Dell).
- *City or locality*: Enter the appropriate value (example, Dallas).
- *State or province*: Enter the unabbreviated state or province name (example, Texas).
- Two-letter country code.
- The utility prompts for confirmation that the information is correct. If so, type `yes`.

If not, type `no`. The Keytool displays each value entered previously. Click **Enter** to accept the value or change the value and click **Enter**.

- *Key password for alias*: If you do not enter another password here, this password defaults to the Keystore password.

Request a Signed Certificate from a Certificate Authority

Use this procedure to generate a Certificate Signing Request (CSR) for the self-signed certificate created in [Generate a New Key Pair and a Self-Signed Certificate](#).

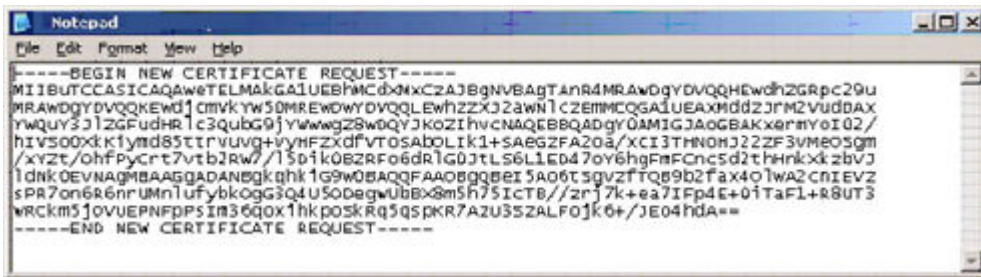
- 1 Substitute the same value used previously for `<certificatealias>`:

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

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

The `.csr` file will contain a BEGIN/END pair that will be used during the creation of the certificate on the CA.

Example .CSR File



- 2 Follow your organizational process for acquiring an SSL server certificate from a Certificate Authority. Send the contents of the `<csr-filename>` for signing.



NOTE:

There are several methods to request a valid certificate. An example method is shown in [Example Method to Request a Certificate](#).

- 3 When the signed certificate is received, store it in a file.
- 4 As a best practice, back up this certificate in case an error occurs during the import process. This backup will prevent having to start the process over.

Import a Root Certificate

If the root certificate Certificate Authority is Verisign (but not Verisign Test), skip to the next procedure and import the signed certificate.

The Certificate Authority root certificate validates signed certificates.

1 Do **one** of the following:

- Download the Certificate Authority root certificate, and store it in a file.
- Obtain the enterprise directory server root certificate.

2 Do **one** of the following:

- If you are enabling SSL for Dell Compliance Reporter, Dell Security Server, or Dell Device Server, change to the component **conf** directory.
- If you are enabling SSL between the Dell Enterprise Server and the enterprise directory server, change to **<Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (the default password for JRE cacerts is **changeit**).

3 Run Keytool as follows to install the root certificate:

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

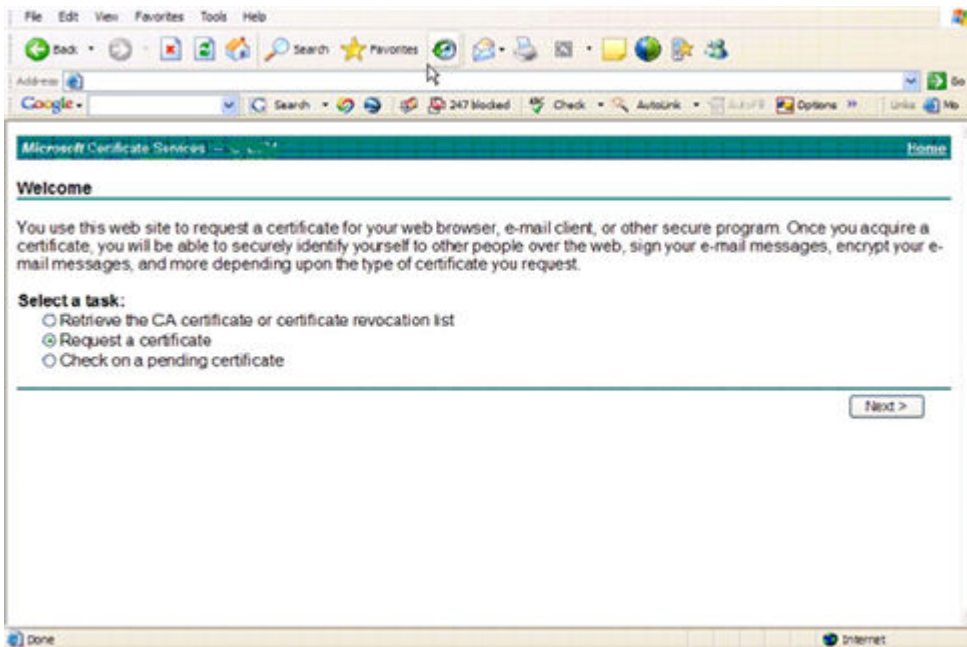
For example, `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

Example Method to Request a Certificate

An example method to request a certificate is to use a web browser to access the Microsoft CA Server, which will be set up internally by your organization.

- 1 Navigate to the Microsoft CA Server. The IP address will be supplied by your organization.
- 2 Select **Request a certificate** and click **Next**.

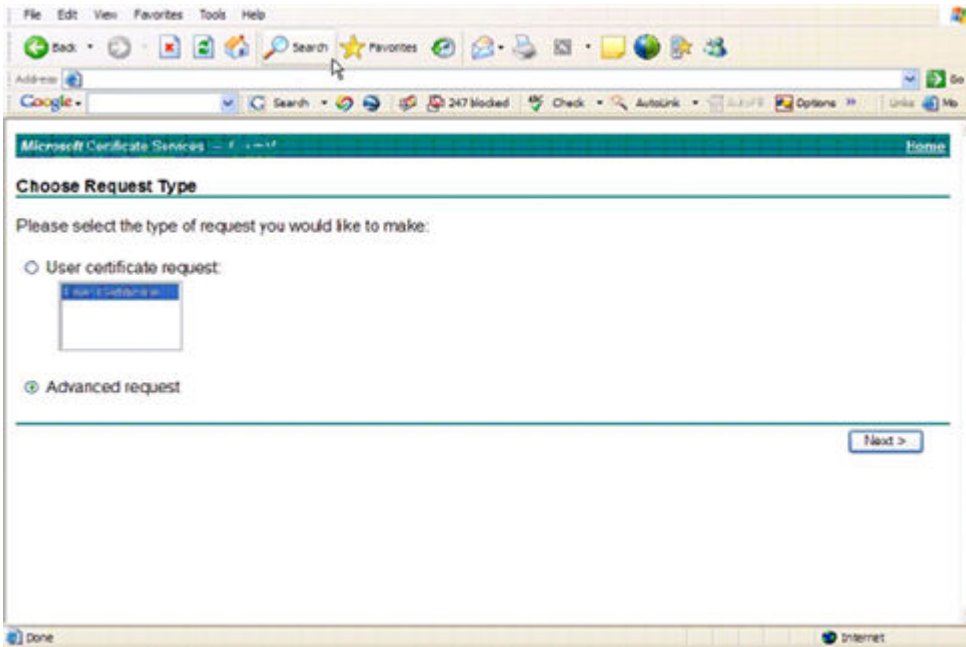
Microsoft Certificate Services



- 3 Select **Advanced Request** and click **Next**.

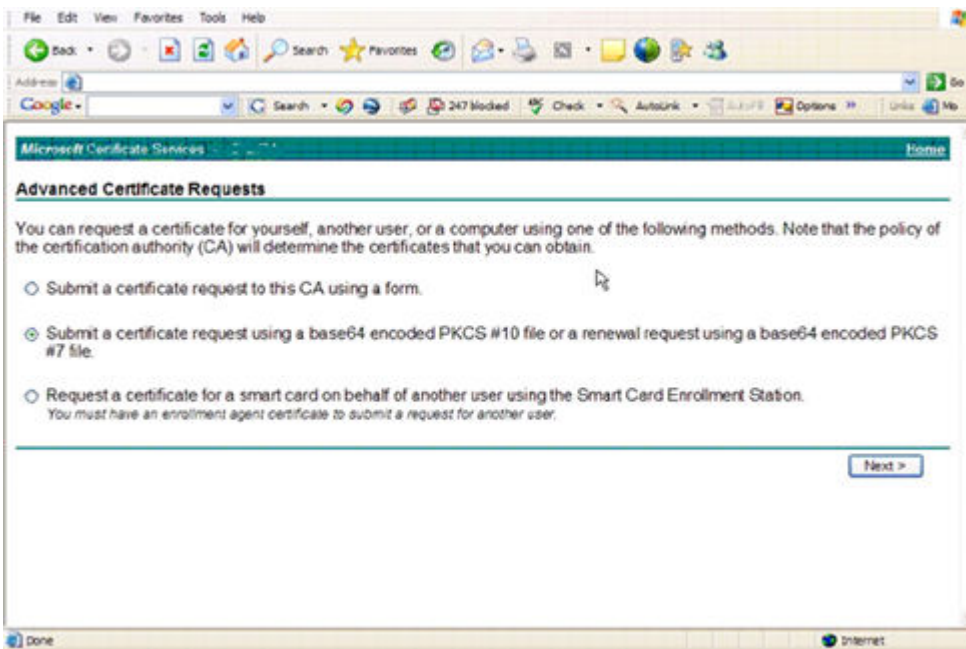
Choose Request Type





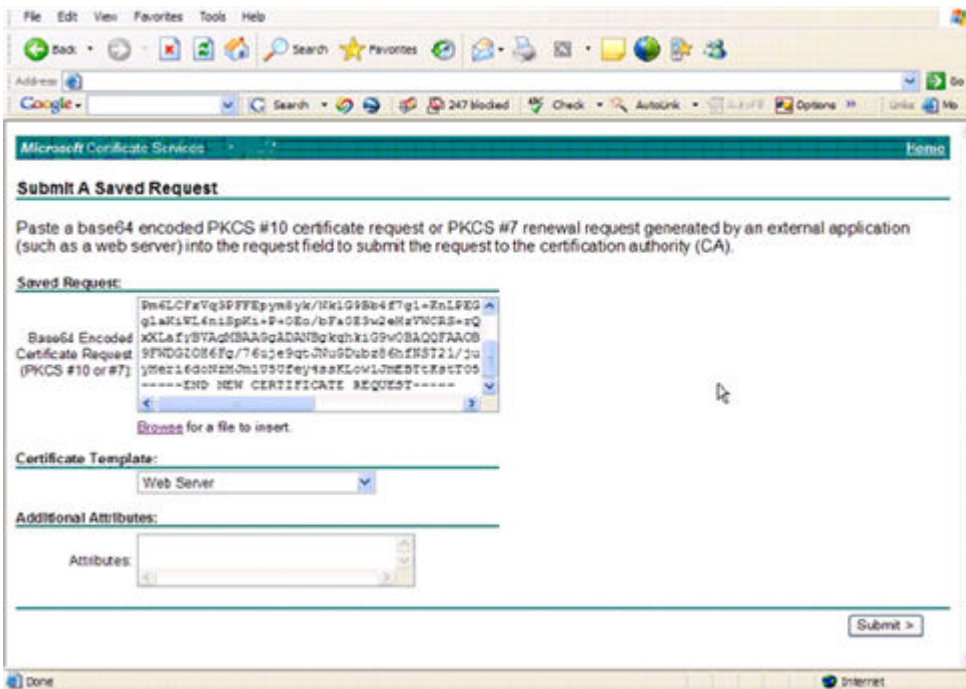
- 4 Select the option to **Submit a certificate request using a base64 encode PKCS #10 file** and click **Next**.

Advanced Certificate Request



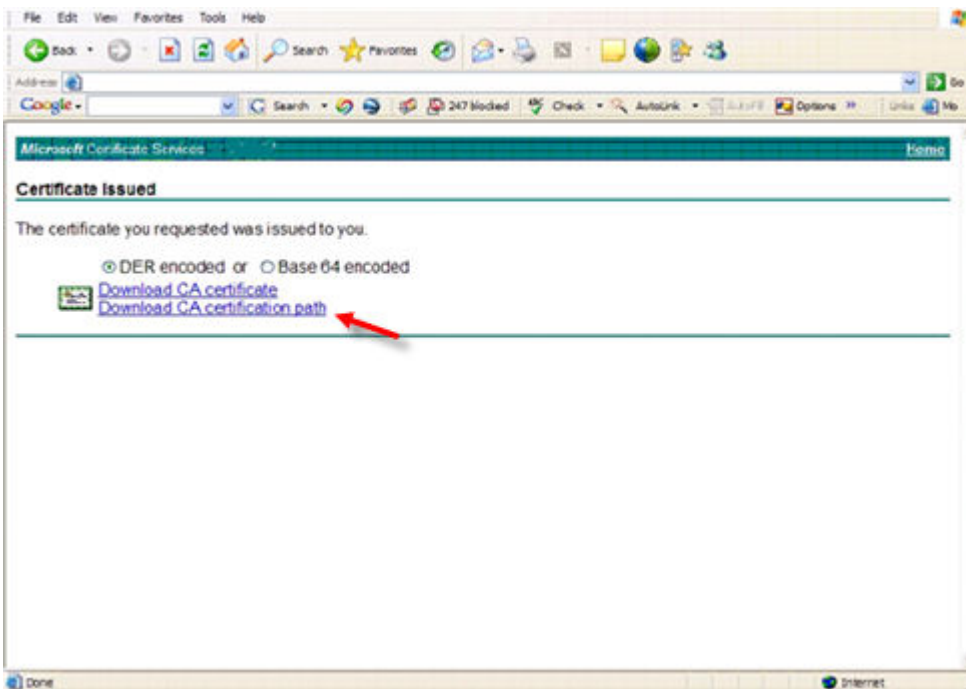
- 5 Paste in the contents of the CSR request in the text box. Select a certificate template of **Web Server** and click **Submit**.

Submit a Saved Request



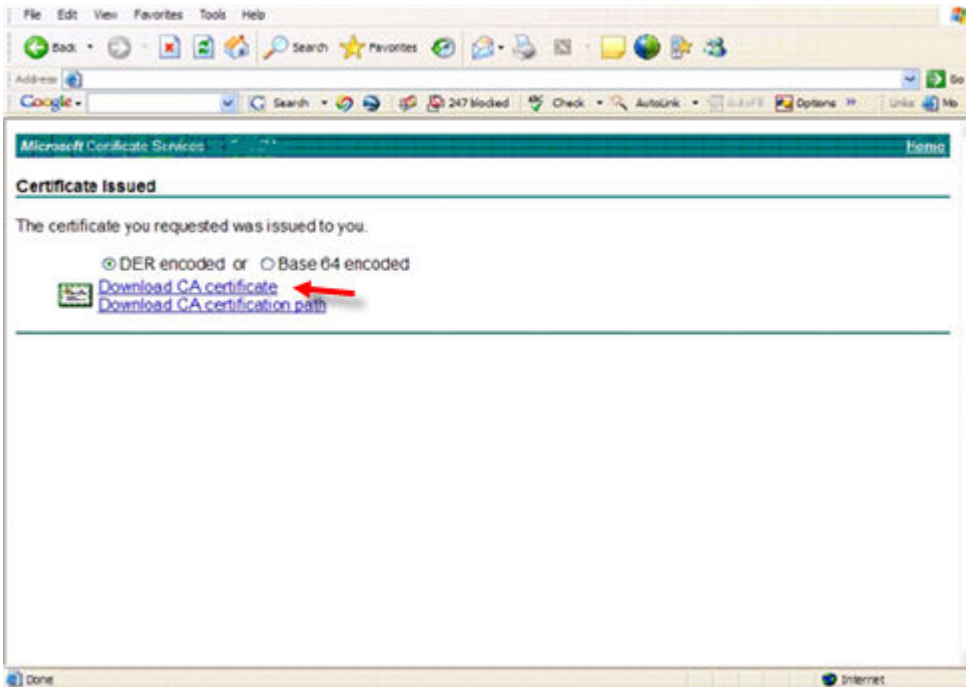
- 6 Save the certificate. Select **DER encoded** and click **Download CA certificate**.

Download CA Certificate



- 7 Save the certificate. Select **DER encoded** and click **Download CA certification path**.

Download CA Certification Path



8 Import the converted signing authority certificate. Return to the DOS window. Type:

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

9 Now that the signing authority certificate has been imported, the server certificate can be imported (the chain of trust can be established). Type:

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

Use the alias of the self-signed certificate to pair the CSR request with the server certificate.

10 A listing of the cacerts file will show that the server certificate has a **certificate chain length** of **2**, which indicates that the certificate is not self-signed. Type:

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

The certificate fingerprint of the second certificate in the chain is the imported signing authority certificate (which is also listed below the server certificate in the listing).

Export a Certificate to .PFX Using the Certificate Management Console

Once you have a certificate in the form of a .crt file in the MMC, it must be converted to a .pfx file for use with Keytool when the Dell Security Server is used in DMZ Mode *and* when importing a Dell Manager certificate into the Dell Server Configuration Tool.

- 1 Open the Microsoft Management Console.
- 2 Click **File > Add/Remove Snap-in**.
- 3 Click **Add**.
- 4 At the *Add Standalone Snap-in* window, select **Certificates** and click **Add**.
- 5 Select **Computer Account** and click **Next**.
- 6 At the *Select Computer* window, select **Local computer (the computer this console is running on)** and click **Finish**.
- 7 Click **Close**.
- 8 Click **OK**.
- 9 In the *Console Root* folder, expand *Certificates (Local Computer)*.
- 10 Go to the *Personal* folder and locate the desired certificate.

- 11 Highlight the desired certificate, right-click **All Tasks > Export**.
- 12 When the Certificate Export wizard opens, click **Next**.
- 13 Select **Yes, export the private key** and click **Next**.
- 14 Select **Personal Information Exchange - PKCS #12 (.PFX)** and then select the sub-options **Include all certificates in the certification path if possible** and **Export all extended properties**. Click **Next**.
- 15 Enter and confirm a password. This can be any password of your choosing. Choose a password that is easy for you to remember, but no one else. Click **Next**.
- 16 Click **Browse** to browse to the location of where you would like to save the file.
- 17 In the *File Name* field, enter a name to save the file as. Click **Save**.
- 18 Click **Next**.
- 19 Click **Finish**.

A message stating that the export was successful displays. Close the MMC.

Add a Trusted Signing Cert to the Security Server when an Untrusted Certificate was used for SSL

- 1 Stop the Security Server Service, if running.
- 2 Back up the cacerts file in <Security Server install dir>\conf\
Use Keytool to complete the following:
- 3 Export the trusted PFX into a text file and document the Alias:
`keytool -list -v -keystore "`
- 4 Import the PFX into the cacerts file in <Security Server install dir>\conf\
`keytool -importkeystore -v -srckeystore "`
- 5 Modify the keystore.alias.signing value in <Security Server install dir>\conf\application.properties.
`keystore.alias.signing=AliasNamePreviouslyDocumented`

Start the Security Server Service.

