Dell Security Management Server

Installation and Migration Guide v11.10

July 2024
Rev. A01

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

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

Contents

1

Introduction

About Security Management Server

The Security Management Server has the following features:

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

Contact Dell ProSupport for Software

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

Additionally, online support for Dell 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 Tag or Express Service Code available when you call.

For phone numbers outside of the United States, see Dell ProSupport for Software international phone numbers.

2

Requirements and Architecture

This section details hardware and software requirements and architecture design recommendations for Dell Security Management Server implementation.

Security Management Server Architecture Design

Encryption Enterprise and Endpoint Security Suite Enterprise solutions are highly scalable products, based on the number of endpoints that are targeted for encryption in your organization.

Architecture Components

Below are suggested hardware configurations that suit most environments.

Security Management Server

- Operating System: Windows Server 2012 R2 (Standard, Datacenter 64-bit), Windows Server 2016 (Standard, Datacenter 64-bit), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard or Datacenter)
- Virtual or Physical Machine
- CPU: 4 Core(s)
- RAM: 16.00 GB
- Drive C: 30 GB available disk space for logs and application databases

NOTE: Up to 10 GB may be consumed for a local event database that is stored within PostgreSQL.

Proxy Server

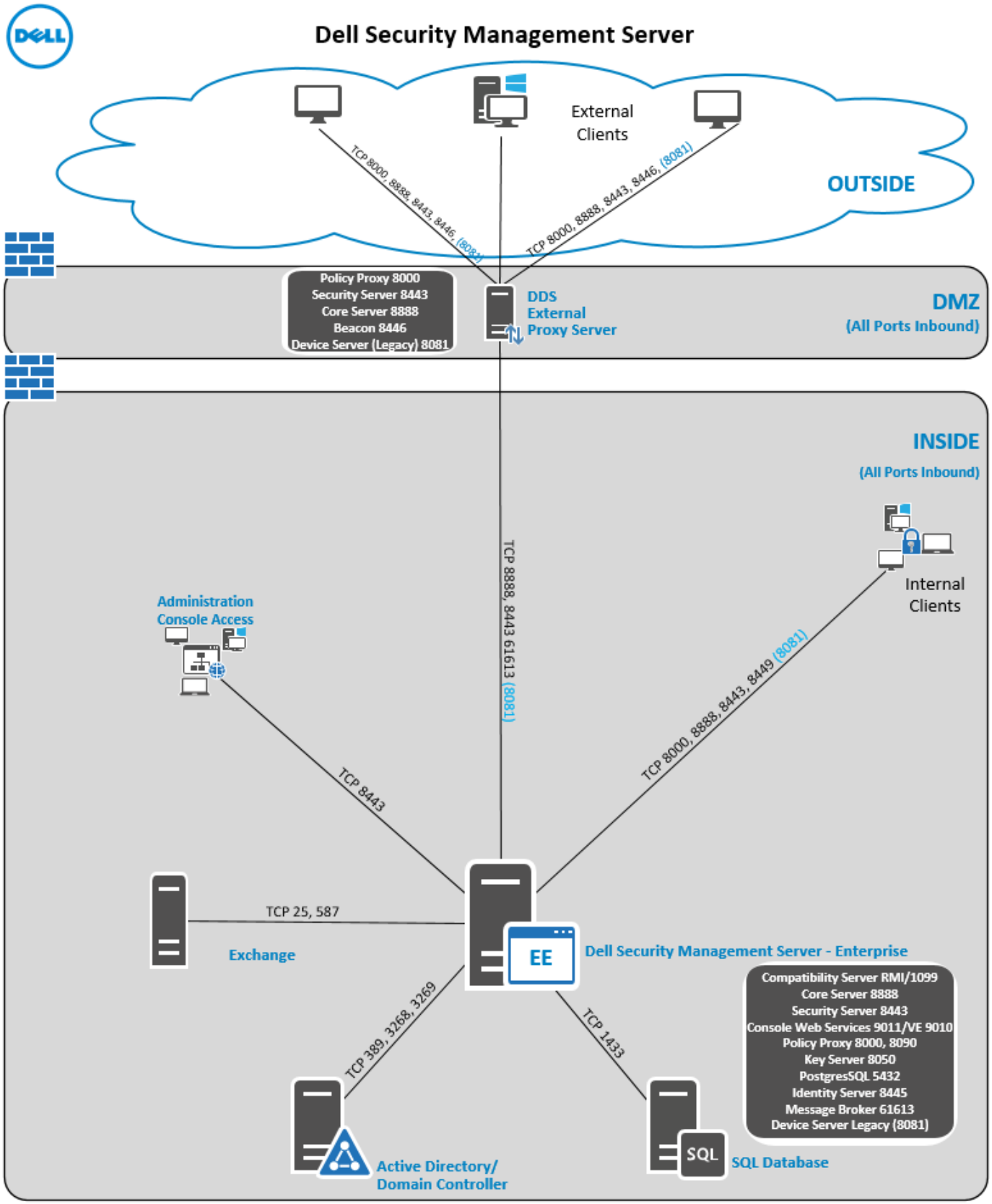
- Operating System: Windows Server 2012 R2 (Standard, Datacenter 64-bit), Windows Server 2016 (Standard, Datacenter 64-bit), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard or Datacenter)
- Virtual/ or Machine
- CPU: 2 Core(s)
- RAM: 8.00 GB
- Drive C: 20 GB available disk space for logs

SQL Server Hardware Specs

- CPU: 4 Core(s)
- RAM: 24.00 GB
- Data Drive: 100 -150 GB of available disk space (This amount may vary based on environment.)
- Log Drive: 50 GB of available disk space (This amount may vary based on environment.).

NOTE: Dell Technologies recommends following SQL Server Best Practices, though the above information should cover most environments.

Below is a basic deployment for the Dell Security Management Server.



NOTE: If the organization has more than 20,000 endpoints, contact Dell ProSupport for assistance.

Requirements

The hardware and software prerequisites for installing the Security Management Server software are included below.

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

Hardware

The following table details the *minimum* hardware requirements for Security Management Server see Security Management Server Architecture Design for additional information about scaling based on the size of your deployment.

Hardware Requirements
Processor Modern Quad-Core CPU (1.5 GHz+)
RAM 16GB
Free Disk Space 20GB of free disk space **NOTE:** Up to 10GB may be consumed for a local event database that is stored within PostgreSQL.
Network Card 10/100/1000 or better
Miscellaneous IPv4 or IPv6 or Hybrid IPv4/IPv6 environment required

The following table details the *minimum* hardware requirements for a Security Management Server Front - End / Proxy Server.

Hardware Requirements
Processor Modern Dual-Core CPU
RAM 8GB
Free Disk Space 20GB of free disk space for log files
Network Card 10/100/1000 or better
Miscellaneous IPv4 or IPv6 or Hybrid IPv4/IPv6 environment required

Virtualization

The Security Management Server can be installed in a virtual environment. Only the following environments are recommended. Security Management Server v11.7 has been validated on the following platforms.

Hyper-V Server that is installed as a Full or Core installation or as a role in Windows Server 2012, Windows Server 2016, Windows Server 2019, or Windows Server 2022.

- Hyper-V Server
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - Hardware must conform to minimum Hyper-V requirements.
  - 4 GB minimum RAM for dedicated image resource
  - Must be run as a Generation 1 Virtual Machine.
  - See https://technet.microsoft.com/en-us/library/hh923062.aspx for more information.

Security Management Server v11.7 has been validated with VMware ESXi 6.0, VMware ESXi 6.5, and VMware ESXi 6.5.

NOTE: When running VMware ESXi and Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022, Dell Technologies recommends VMXNET3 Ethernet Adapters.

- VMware ESXi 6.0
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems.
  - Hardware must conform to minimum VMware requirements.
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-60/index.jsp for more information.
- VMware ESXi 6.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems.
  - Hardware must conform to minimum VMware requirements.
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-65/index.jsp for more information.
- VMware ESXi 6.7
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems.
  - Hardware must conform to minimum VMware requirements.
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-65/index.jsp for more information.

NOTE: The SQL Server database hosting the Security Management Server must be run on a separate computer for performance reasons.

SQL Server

In larger environments, it is highly recommended that the SQL Database server run 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 that is enabled to ensure that any newly generated keys through user/device activation are recoverable.

Database maintenance tasks should include rebuilding database indexes and collecting statistics.

Software

The following table details the software requirements for the Security Management Server and proxy server.

NOTE: Due to the sensitive nature of the data that the Security Management Server holds, and to align with the rule of least privilege, it is recommended that you install the Security Management Server on its own dedicated operating system. Alternately, it can be a part of an application server that has limited roles and rights that are enabled to help ensure a secure environment. This recommendation includes not installing the Security Management Server on privileged infrastructure servers. See https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models for more information about implementing the least privilege rule.

NOTE: Universal Account Control (UAC) must be disabled when installing in a protected directory. After disabling UAC, you must reboot the server for this change to take effect.

NOTE: Registry locations for Policy Proxy (if installed): HKLM\SOFTWARE\Wow6432Node\Dell

NOTE: Registry location for Windows servers: HKLM\SOFTWARE\Dell

Prerequisites
• **Visual C++ 2010 Redistributable Package** If not installed, the installer installs it for you. • **Visual C++ 2013 Redistributable Package** If not installed, the installer installs it for you. • **Visual C++ 2015 Redistributable Package** If not installed, the installer installs it for you. • **.NET Framework Version 4.6.1** • **.NET Framework Version 4.5** Microsoft has published security updates for .NET Framework Version 4.6.1 and 4.5. • **.NET Framework Version 3.5 SP1** • **SQL Native Client 2012** If using SQL Server 2012 or SQL Server 2016. If not installed, the installer installs it for you.

Security Management Server - Back-End Server and Dell Front-End Server
• **Windows Server 2012 R2** - Standard Edition - Datacenter Edition • **Windows Server 2016** - Standard Edition - Datacenter Edition • **Windows Server 2019** - Standard Edition - Datacenter Edition • **Windows Server 2022** - Standard Edition - Datacenter Edition **NOTE:** The Dell Security Management Server that is installed in either a back-end configuration or a front-end configuration does not currently support operating system upgrades of the Windows Server operating system.

LDAP Repository

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

NOTE: The Security Management Server is compatible with the Microsoft requirement for LDAP channel binding and LDAP signing when Active Directory is in use.

Management Console

- Mozilla Firefox 41.x or later
- Google Chrome 46.x or later
- Microsoft Edge (Chromium)
- Microsoft Edge

NOTE: **Your browser must accept cookies.**

Recommended Virtual Environments for Security Management Server Components

The Security Management Server can be installed in a virtual environment.

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

Other infrastructure requirements, such as Active Directory and SQL Server, are still required for proper functionality.

NOTE: The SQL Server database hosting the Security Management Server must be run on a separate computer.

Database

- **SQL Server 2012 -** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2014 -** Standard Edition / Business Intelligence / Enterprise Edition
- **SQL Server 2016 -** Standard Edition / Enterprise Edition
- **SQL Server 2017 -** Standard Edition / Enterprise Edition
- **SQL Server 2019 -** Standard Edition / Enterprise Edition

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

Based on your SQL Server version, the Security Management Server **requires** one of the following is enabled:

- Full Text Indexing
- Full-text Filter
- Full-Test and Semantic Extractions for Search

For more information about errors that are encountered when the above features are not enabled for the SQL Server in use, see KB article 125164.

For more information about configuring Microsoft SQL Server permissions and features for the Security Management Server, see this KB 124909.

NOTE: Below are the requirements for SQL permissions. The user who performs the installation and the services must have local administrator rights. Also, Local administrator rights are required for the service account managing the Dell Security Management Server services.

Type	Action	Scenario	SQL Privilege Required
Back end	Upgrade	By definition, upgrades already have DB and Login/ User established.	db_owner

Type	Action	Scenario	SQL Privilege Required
Back end	Restore Install	Restore involves an existing DB and login.	db_owner
Back end	New Install	Use existing DB	db_owner
Back end	New Install	Create DB	dbcreator, db_owner
Back end	New Install	Use existing login.	db_owner
Back end	New Install	Create login.	securityadmin
Back end	Uninstall	Not applicable	Not applicable
Proxy Front end	Any	Not applicable	Not applicable

NOTE: If User Account Control (UAC) is enabled, you must disable it before installation on Windows Server 2012 R2 when installing in `C:\Program Files`. 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. Regardless of which type of credentials are used, the account must have the appropriate privileges for the action being performed. The previous table details the privileges that are required for each type of installation. Also, the account that is used to *create and set up the database* must have its default schema set to dbo.

These privileges are only required during installation to set up the database. Once the Security Management Server is installed the account that is used to manage SQL access can be restricted to the db_owner and public roles.

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

Language Support for Management Console

The Management Console is Multilingual User Interface (MUI) compliant and supporst 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	

3

Pre-Installation Configuration

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

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

Configuration

Access the Management Console

Since Internet Explorer is no longer supported, you must install a third-party browser to properly access the Management Console.

If Internet Explorer is required to validate the Management Console, you must disable Internet Explorer Enhanced Security Configuration for the account type that corresponds to the logged-in administrator.

Port and Firewall Configuration

Client and Server Communication to the Public (Outbound)

The below services and ports are required for the Dell Server to communicate with managed endpoints. These ports and services must be capable of outbound communication. If SSL inspection and proxy services are in use, the URLs require exclusions from them.

- On-the-Box Entitlement Validation
  - Destination URL
    - cloud.dell.com
  - Port
    - 443
  - Outbound Device
    - Security Management Server or Security Management Server Virtual in Back-End configuration
  - Originating Service
    - Dell Security Server
  - Originating Port
    - 8443
- Advanced Threat Prevention client communication
  - Destination URLs
    - North America
      - login.cylance.com
      - protect.cylance.com
      - data.cylance.com
      - update.cylance.com
      - api.cylance.com
      - protect-api.cylance.com
      - download.cylance.com
    - South America
      - login-sae1.cylance.com
      - protect-sae1.cylance.com
      - data-sae1.cylance.com
      - update-sae1.cylance.com
      - api-sae1.cylance.com
      - protect-api-sae1.cylance.com
      - download-sae1.cylance.com
    - Europe

        - login-euc1.cylance.com
        - protect-euc1.cylance.com
        - data-euc1.cylance.com
        - update-euc1.cylance.com
        - api-euc1.cylance.com
        - protect-api-euc1.cylance.com
        - download-euc1.cylance.com
    - Middle East and Asia
        - login-au.cylance.com
        - protect-au.cylance.com
        - data-au.cylance.com
        - update-au.cylance.com
        - api-au.cylance.com
        - protect-api-au.cylance.com
        - download-au.cylance.com
    - Japan, Australia, and New Zealand
        - login-apne1.cylance.com
        - protect-apne1.cylance.com
        - data-apne1.cylance.com
        - update-apne1.cylance.com
        - api-apne1.cylance.com
        - protect-api-apne1.cylance.com
        - download-apne1.cylance.com
- Port
    - 443
- Outbound Device
    - All managed endpoints
- Outbound Service
    - CylanceSVC
- Originating Port
    - 443

Public Communication to Front-End Server (if needed)

This sees information traveling from the Internet to the Front-End server. Firewall or routing configuration must have ports set as inbound from a public or Internet connection to one or more Front-End servers or a load balancer.

- Dell Core Server Proxy: HTTPS/8888
- Dell Device Server: HTTPS/8081
- Dell Policy Proxy: TCP/8000
- Dell Security Server: HTTPS/8443

DMZ or Front-End Communication to Back-End Server (if needed)

The below services and ports communicate from any Security Management Server that is configured in Front-End mode to the Security Management Server configured in Back-End mode. Firewall or routing configuration must have ports set as inbound from one or more Front-End servers or load balancers to the Back-End server.

- Front-End Dell Policy Proxy and Dell Beacon Server to Back-End Dell Message Broker: STOMP/61613
- Front-End Dell Security Server Proxy to Back-End Dell Security Server: HTTPS/8443
- Front-End Dell Core Server Proxy to Back-End Dell Core Server: HTTPS/8888
- Front-End Dell Device Server to Back-End Dell Security Server: HTTPS/8443

Back-End Server to Internal Network

The below services and ports are used for communication to the respective services internally by clients on the domain or connected through VPN. Dell Technologies recommends that several of these services should not be forwarded outside of the network, or the service is filtered in the Front-End Server's configuration by default. Firewall or routing configuration must have these ports set as inbound from the internal network to the Back-End Security Management Server.

- Management Console hosted on the Dell Security Server: HTTPS/8443
- Dell Core Server: HTTPS/8888
- Dell Device Server: HTTP(S)/8081

NOTE: This legacy service is only required for Dell Encryption clients pre-8.x. This service can be safely disabled if all clients within the environment are 8.0 or later.

- Key Server: TCP/8050
- Dell Policy Proxy: TCP/8000
- Dell Security Server: HTTPS/8443
- Certificate-based Authentication, hosted through the Dell Security Server: HTTPS/8449

NOTE: Dell Encryption clients that are installed on Windows Server Operating Systems or clients that are installed in Server mode use this function. For additional information about installing clients in this Server mode, see Encryption Enterprise Advanced Installation Guide.

Infrastructure Communication

- Active Directory, leveraged for User Authentication with Dell Encryption TCP/389/636 (local domain controller), TCP/3268/3269 (global catalog), TCP/135/49125+ (RPC)
- Email communication (optional): 25/587
- Microsoft SQL Server: 1433 (default port)

Microsoft SQL Database Creation and Management

Create the Dell Server Database:

These instructions are optional. If a database does not exist, the installer creates it by default. If you prefer to set up a database before installing the Security Management Server, follow the instructions below to create the SQL database and SQL user in SQL Management Studio. Ensure that appropriate permissions are set for SQL databases that are not automatically created during installation of the Security Management Server. To see a list of required permissions, see Software Requirements.

When precreating the database, follow the instructions in Install Back-End Server with Existing Database.

The Security Management Server is configured for both SQL and Windows authentication.

NOTE: The expected nondefault coalition that is supported for your SQL database or SQL instance is "SQL_Latin1_General_CP1_CI_AS" collation. Collation must be case insensitive and accent sensitive.

Installation Prerequisites

Prerequisites are installed by default during the Security Management Server's installation on Windows Server operating systems. The below prerequisites can optionally be installed before the Security Management Server installation to bypass reboot requirements.

Install Visual C++ Redistributable Packages

If not already installed, install Visual C++ 2010, 2013, and 2015 (or later) Redistributable packages. Optionally, you can allow the Security Management Server installer to install these components.

NOTE: Installing the Microsoft Visual C++ Redistributable packages may require a reboot.

Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022 - https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads

Install .NET Framework 4.5

.NET Framework 4.5 is preinstalled on Windows Server 2012 R2 and later as a feature of Server Manager.

Install SQL Native Client 2012

If using SQL Server 2012 or SQL Server 2016, install SQL Native Client 2012. Optionally, you can allow the Security Management Server installer to install the component.

Import the Server Installation License

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 Security Management Server installer.

NOTE: The EnterpriseServerInstallKey.ini is present in the Security Management Server's download package, available here.

The preinstallation configuration of the server is complete. Continue to Install or Upgrade/Migrate.

4

Install or Upgrade/Migrate

The chapter provides instructions for the following:

- New Installation - To install a new Security Management Server.
- Upgrade/Migration - To upgrade from an existing, functional Enterprise Server v9.2 or later. Dell Server v11.0 or higher requires Windows Server 2019 or higher.
- Uninstall Security Management 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 *Security Management Server Technical Advisories* for any current workarounds or known issues related to Security Management Server installation.

Antivirus and anti-malware should be disabled while installing or upgrading the Security Management Server to avoid impacting Microsoft C++ runtime installers, Java activities (certificate creation and manipulation), and PostgreSQL creation and modification. All these items are triggered by executables or scripts.

As a work-around, exclude:

- [INSTALLATION PATH]:\Dell\Enterprise Edition
- C:\Windows\Installer
- The file path from which the installer is run

Dell recommends that database best practices are used for the Dell Server 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:\Users\<LoggedOnUser>\AppData\Local\Temp`

New Installation

Choose one of two options for back end server installation:

- Install Back End Server and New Database - To install a new Security Management Server and a new database.
- Install Back End Server with Existing Database - To install a new Security Management 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 Security Management Server version to be installed. A v9.2 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-v9.2 database, contact Dell ProSupport for assistance.

NOTE:

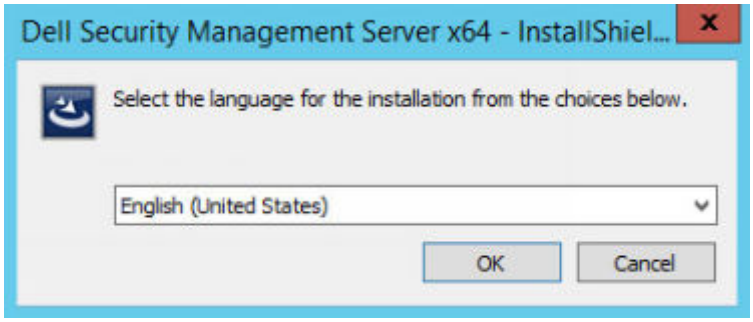
If you have a functional Enterprise Server v9.2 or later, refer to instructions in **Upgrade/Migrate Back End Server(s)**.

If you install a front end server, perform this installation after back end server installation:

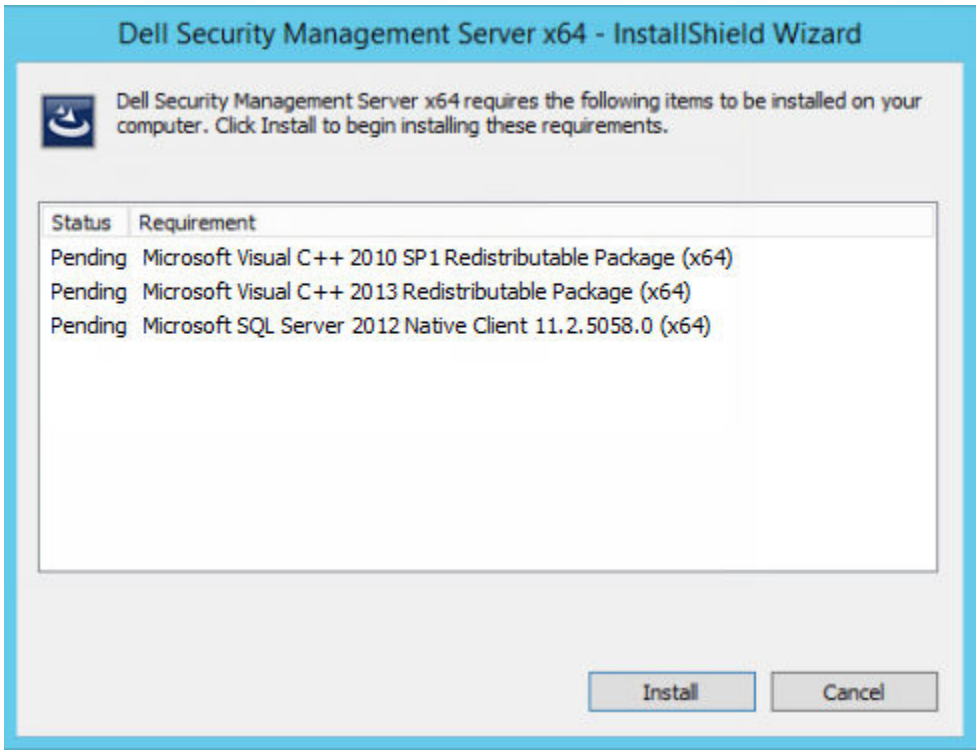
- Install Front End Server - To install a front end server to communicate with a back end server.

Install Back-End Server and New Database

1. In the Dell installation media, go to the Security Management Server directory. **Extract** (DO NOT copy and paste or drag and drop) Security Management Server-x64 to the root directory of the server where you are installing Security Management Server. ***Copying and pasting or dragging and dropping produces errors and an unsuccessful installation.***
2. Double-click **setup.exe**.
3. Select the language for installation, and then click **OK**.

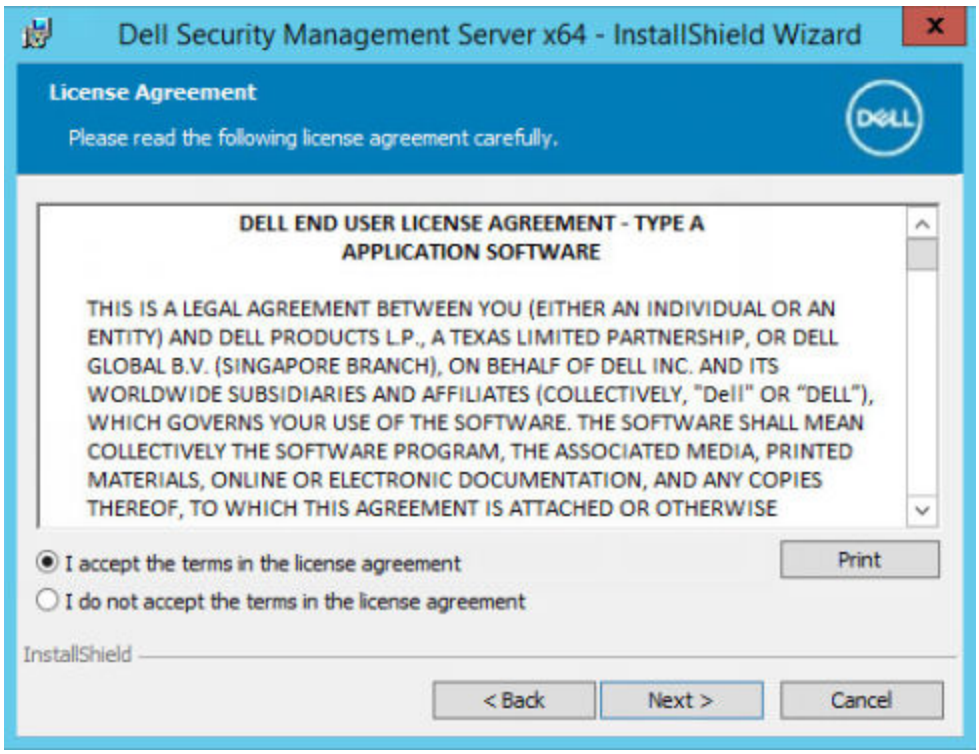


4. If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.

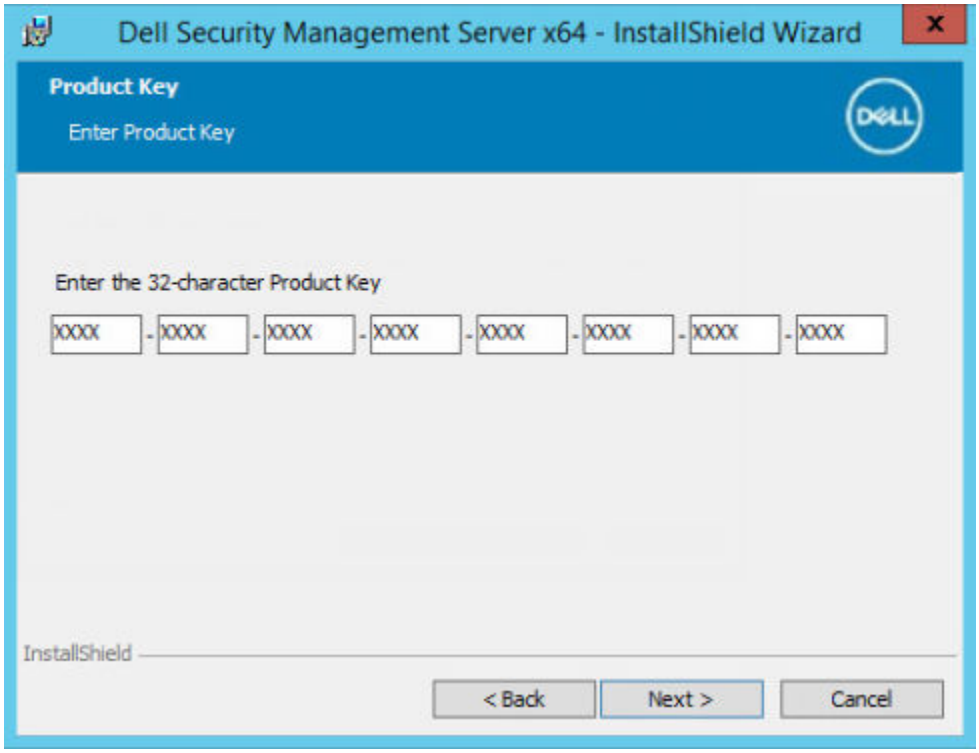


5. In the *Welcome* dialog, click **Next**.

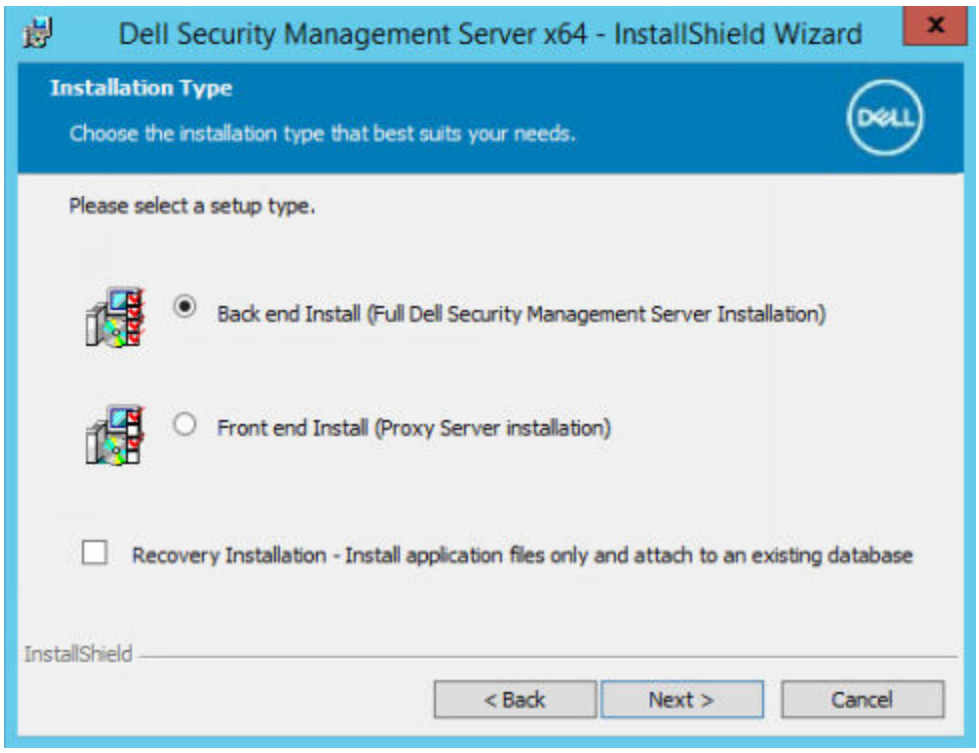
6. Read the license agreement, accept the terms, and then click **Next**.



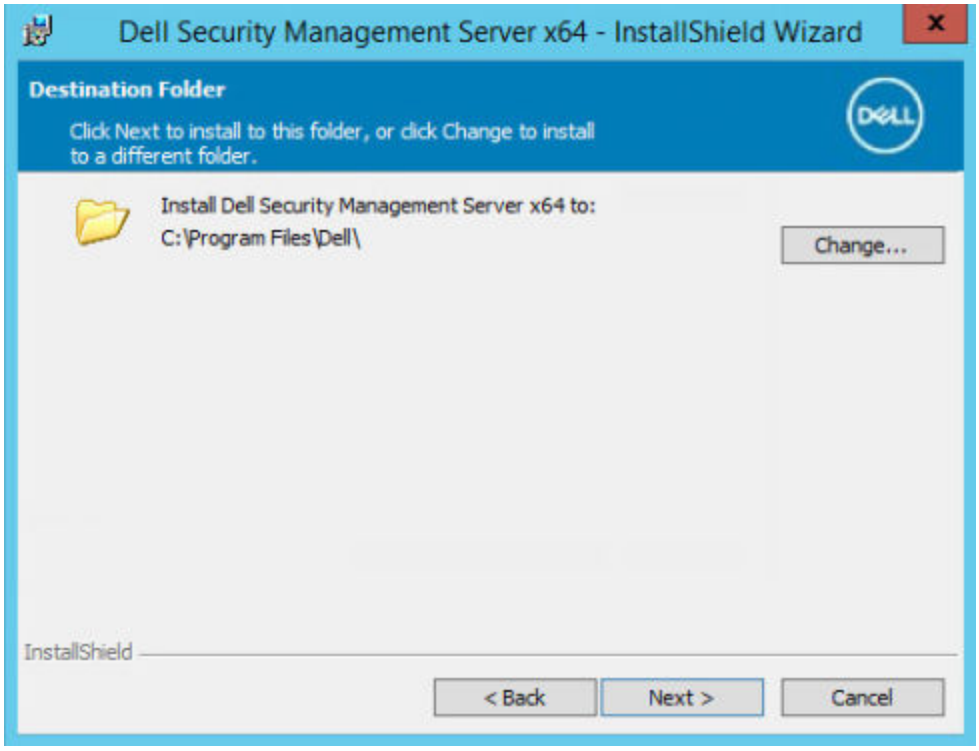
7. If you optionally copied your `EnterpriseServerInstallKey.ini` file to `C:\Windows` as explained in Pre-Installation Configuration, click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is in the `EnterpriseServerInstallKey.ini` file.



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

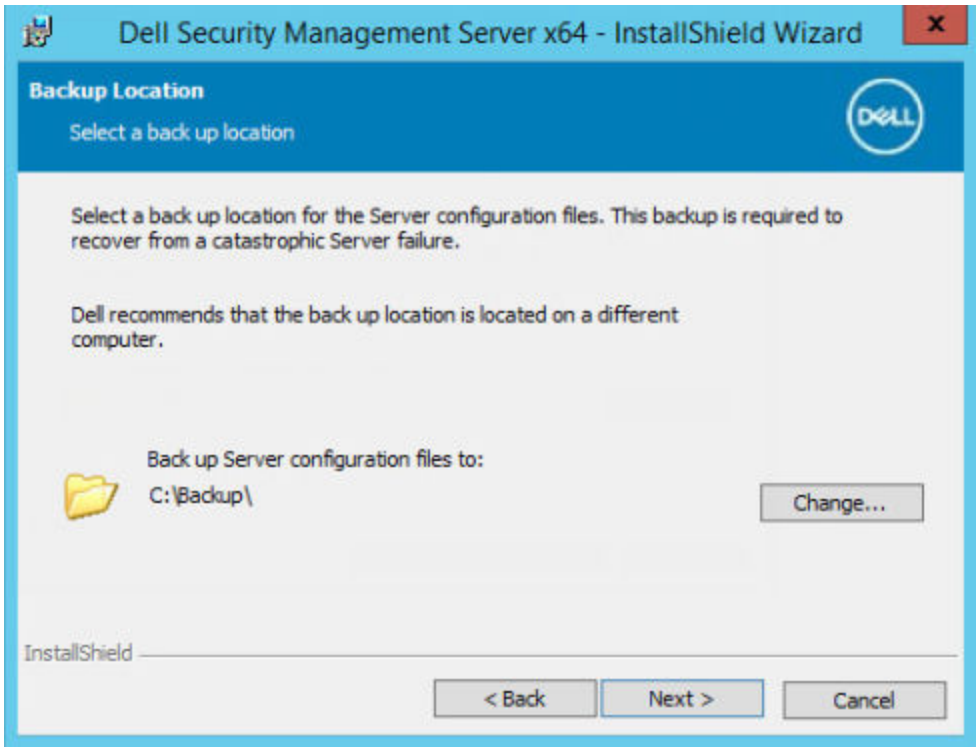


9. To install the Security Management Server to the default location of `C:\Program Files\Dell`, click **Next**. Otherwise, click **Change** to select another location, and then click **Next**.



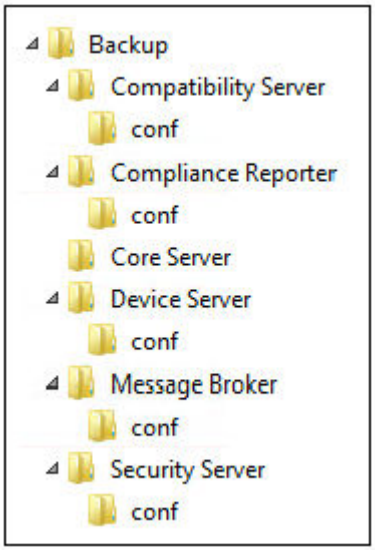
10. To select a location for backup configuration files to be stored, click **Change**, go to the folder, and then click **Next**.

    Dell Technologies recommends that you select a remote network location or external drive for backup.



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

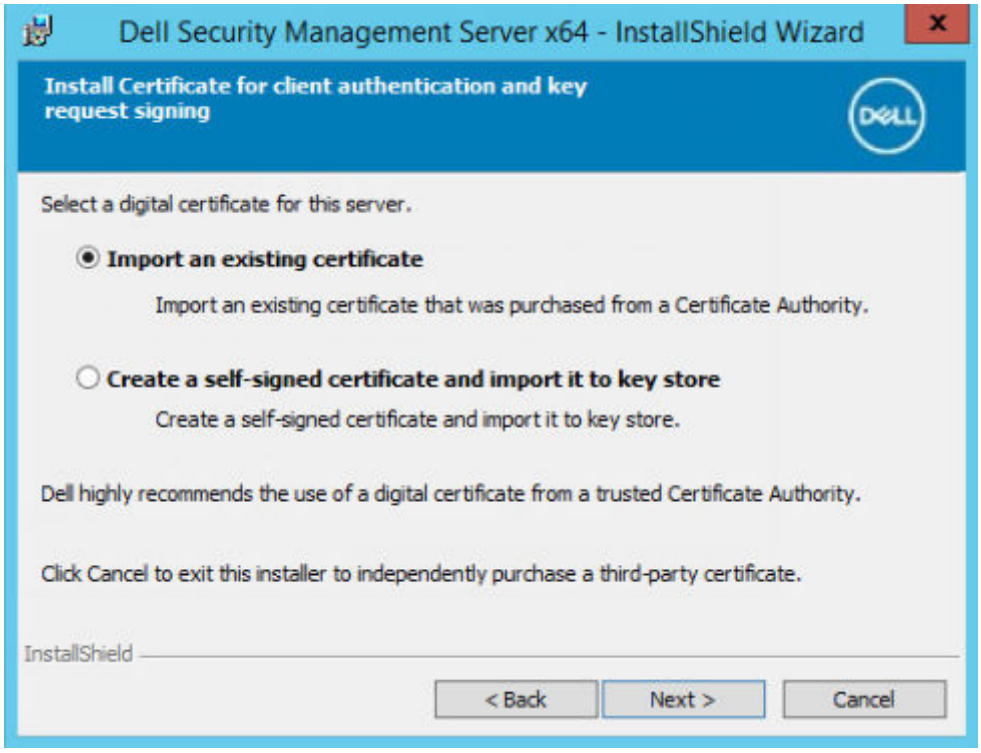
NOTE: The folder structure created by the installer during this installation step (example shown below) must remain unchanged.



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.

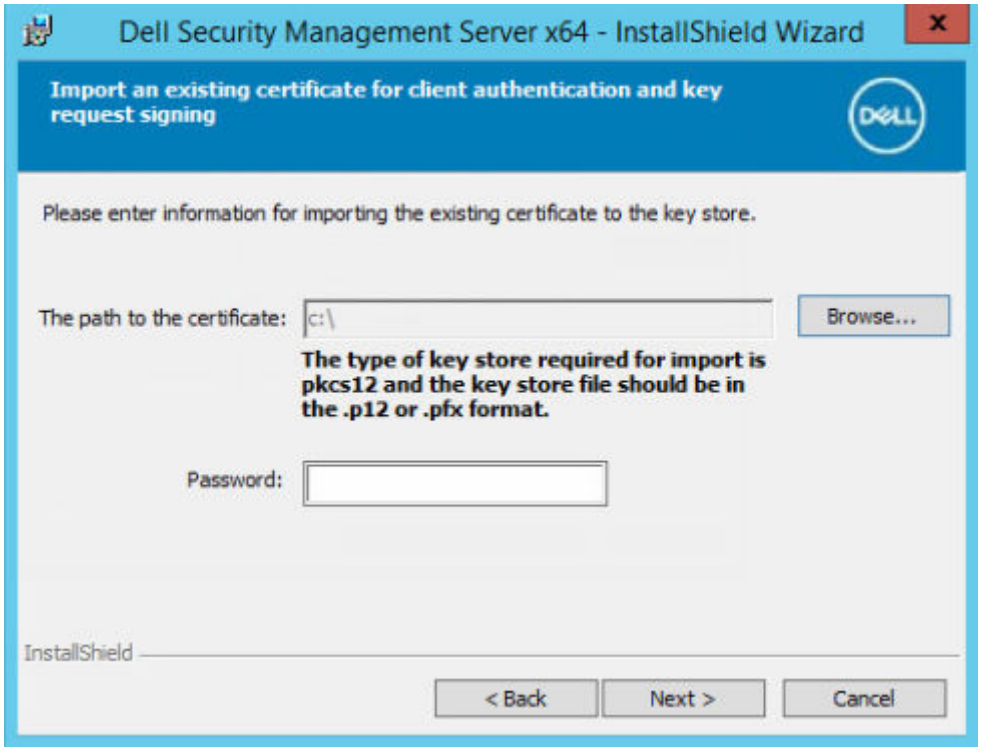
    Click **Next**.

    NOTE:

    To use this setting, confirm that the exported CA certificate being imported must have the full trust chain. If unsure, reexport 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)

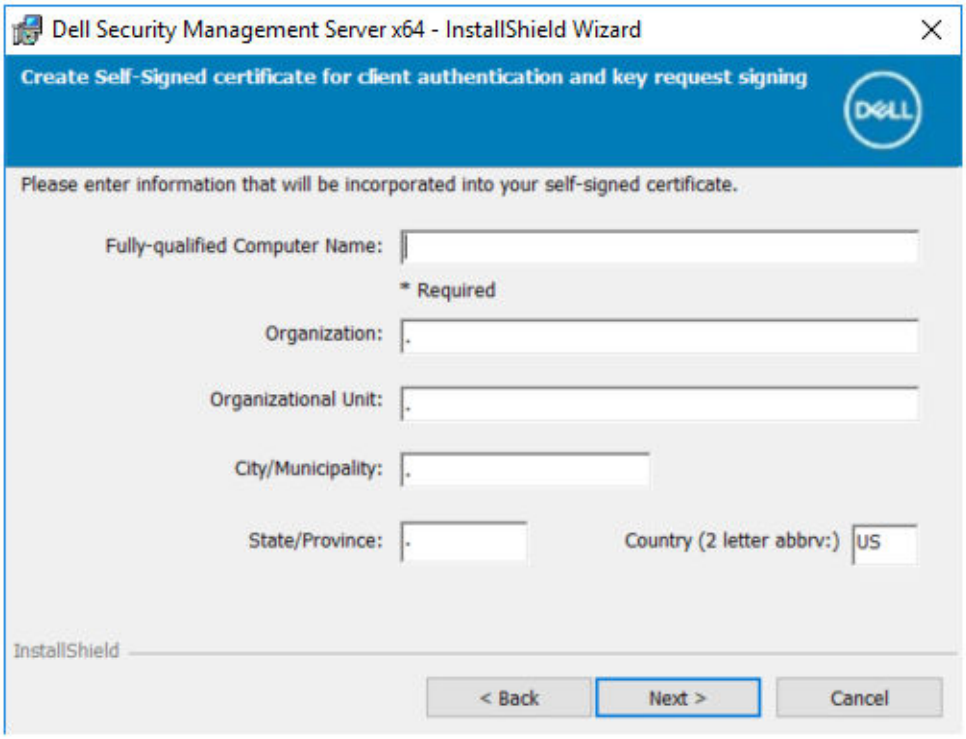
City

State (full name)

Country: Two-letter country or region abbreviation

Click **Next**.

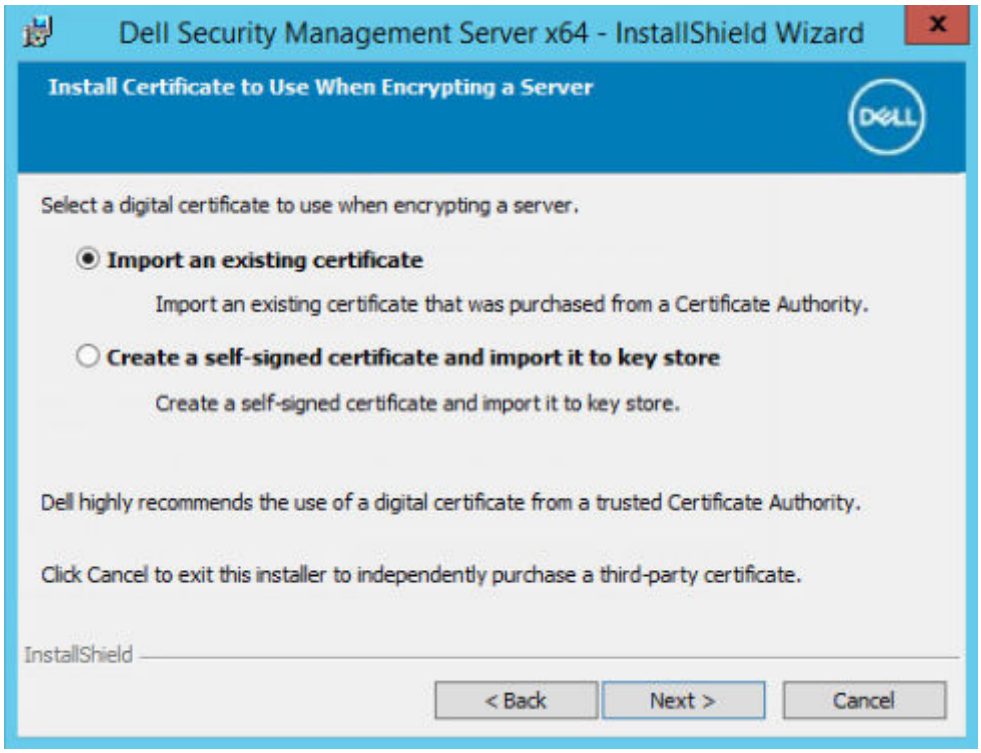
NOTE: The certificate expires in 10 years, by default.



12. For Server Encryption, 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.

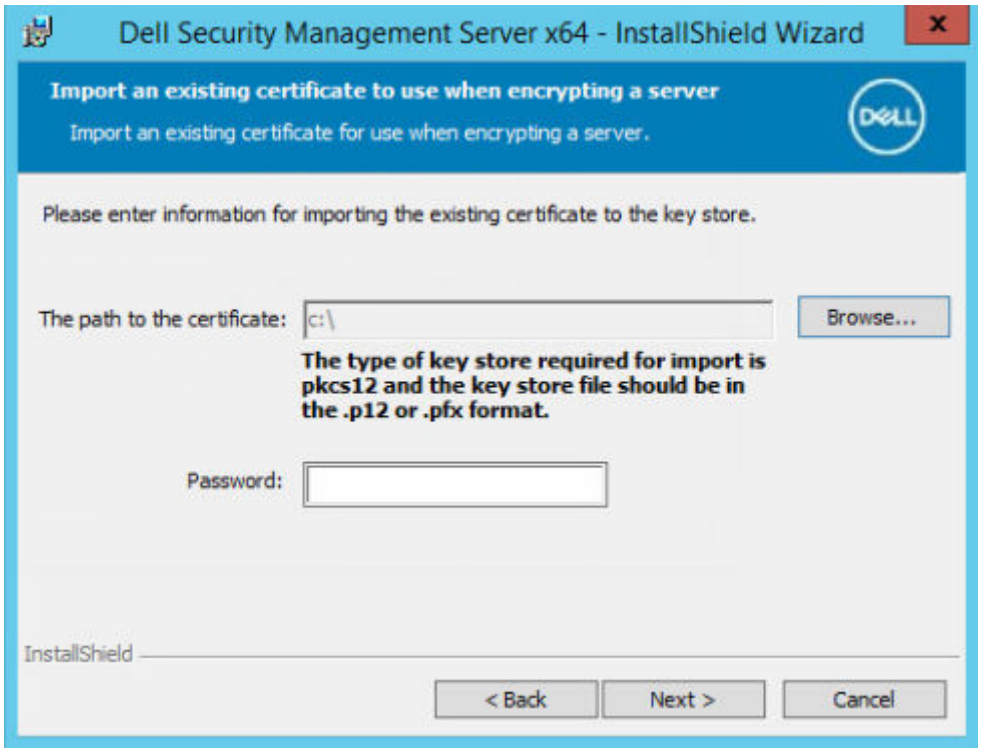
    Enter the password associated with this certificate. The key store file must be .p12 or pfx. See Exporting a Certificate to .PFX Using the Certificate Management Console for instructions.

Click **Next**.

NOTE:

To use this setting, confirm that the exported CA certificate being imported has the full trust chain. If unsure, reexport 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)

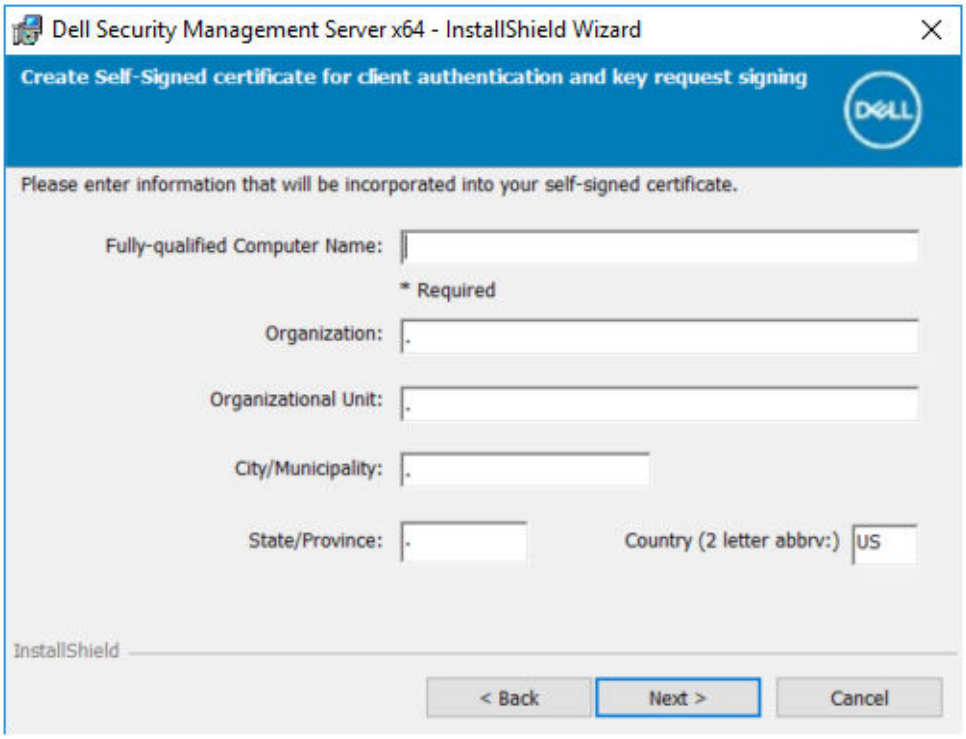
City

State (full name)

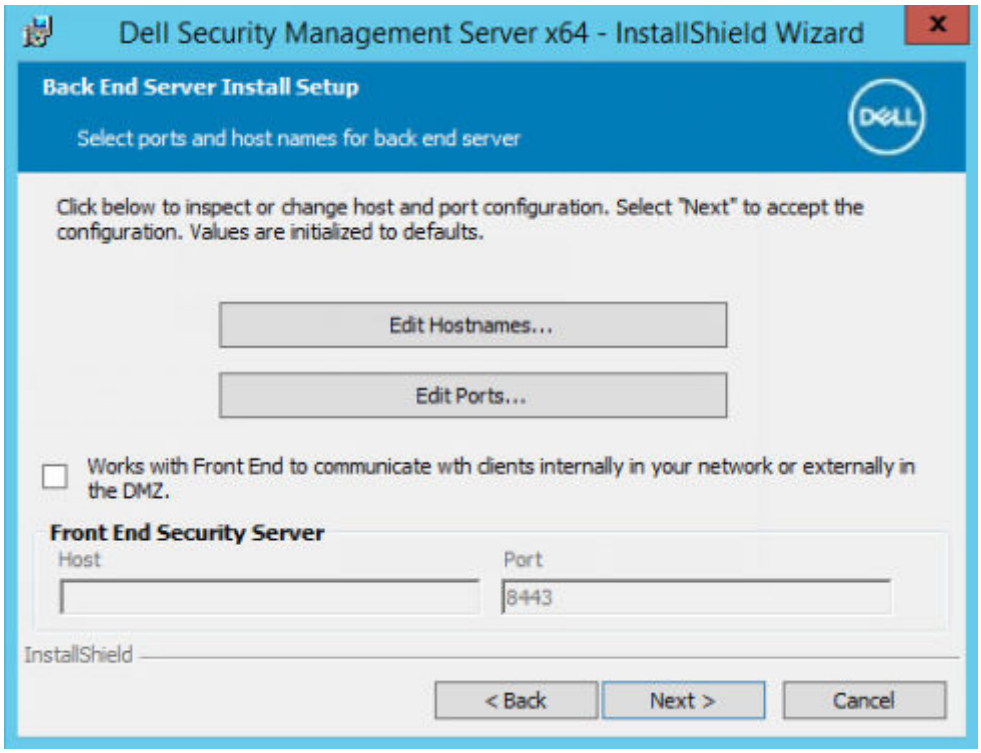
Country: Two-letter country or region abbreviation

Click **Next**.

NOTE: The certificate expires in 10 years, by default.



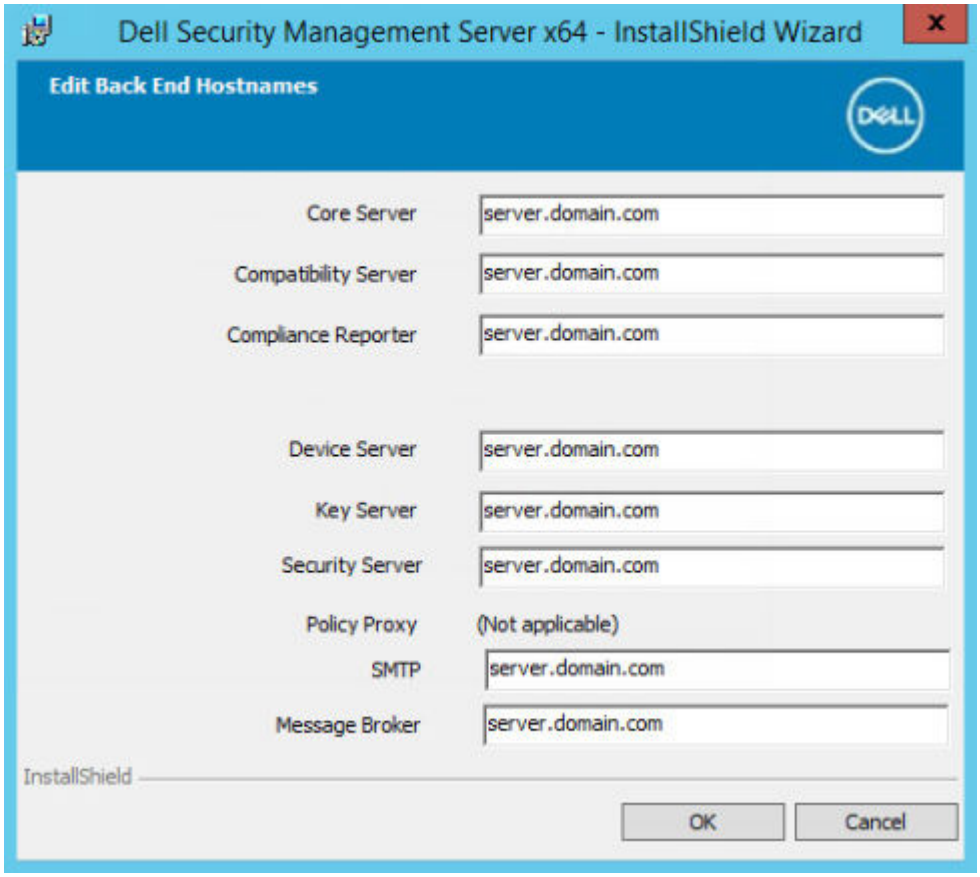
13. From the *Back-End Server Install Setup* dialog, you can view or edit hostnames and ports.
    - To accept the default hostnames and ports, in the *Back-End Server Install Setup* dialog, click **Next**.
    - If you are using a front-end server, select **Works with Front End to communicate with clients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



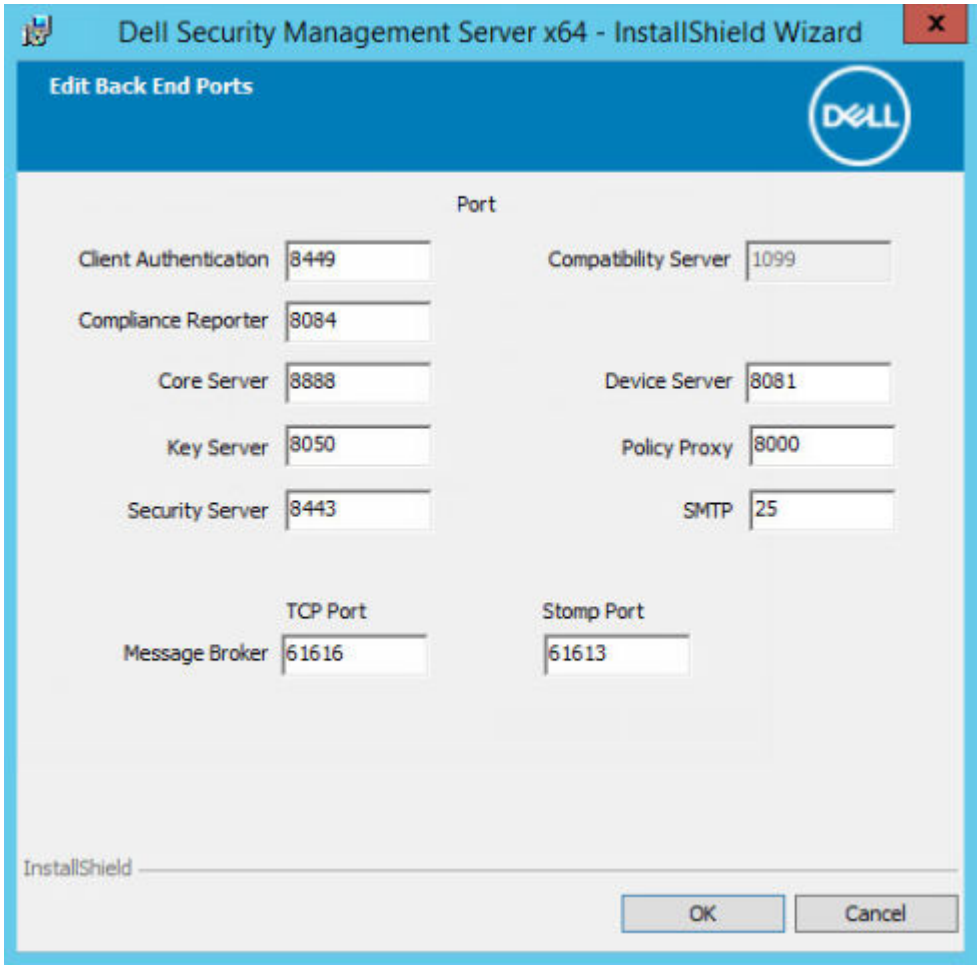
    - To view or edit hostnames, click **Edit Hostnames**. Edit hostnames only if necessary. Dell Technologies recommends using the defaults.

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

When finished, click **OK**.

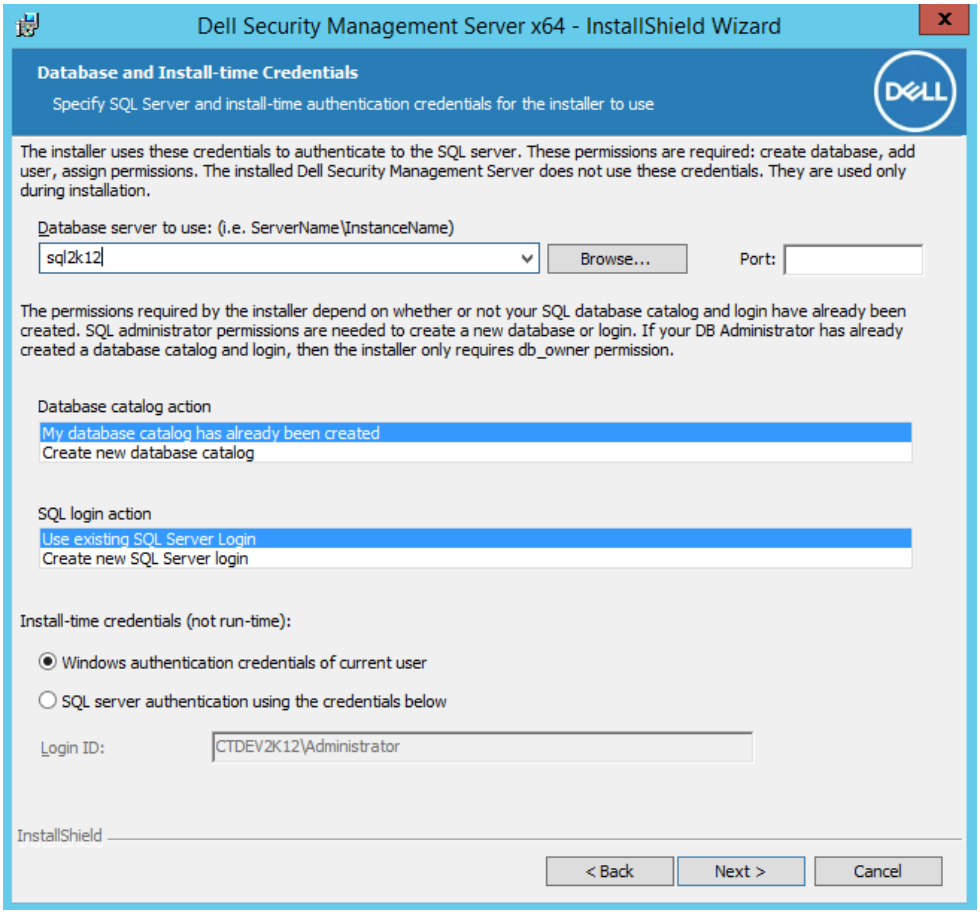


- To view or edit ports, click **Edit Ports**. Edit ports only if necessary. Dell Technologies recommends using the defaults. When finished, click **OK**.



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 Server database. After installation, the installed product does not use the credentials that are specified here.
        - **Windows authentication credentials of current user**

          If you choose Windows Authentication, the same credentials that were used to log in to Windows are used for authentication. (*User Name* and *Password* are not 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 that is used must have system administrator rights on the SQL Server.

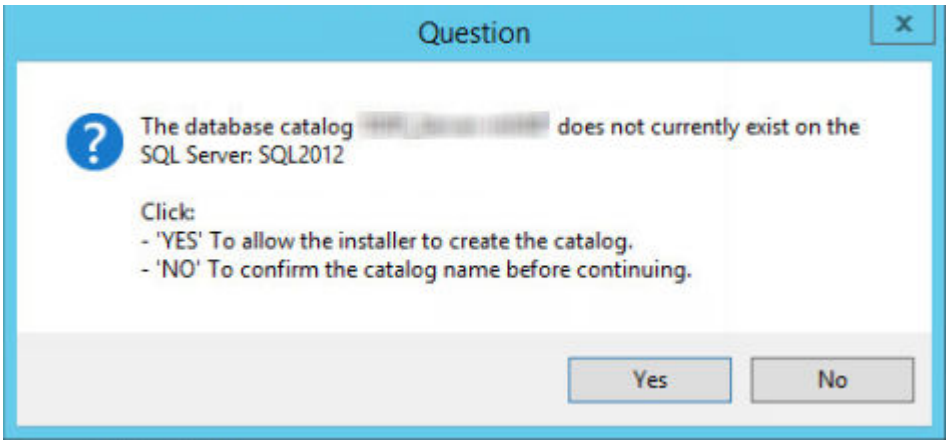
  The installer must authenticate to the SQL Server with these permissions: create database, add user, assign permissions.

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**.



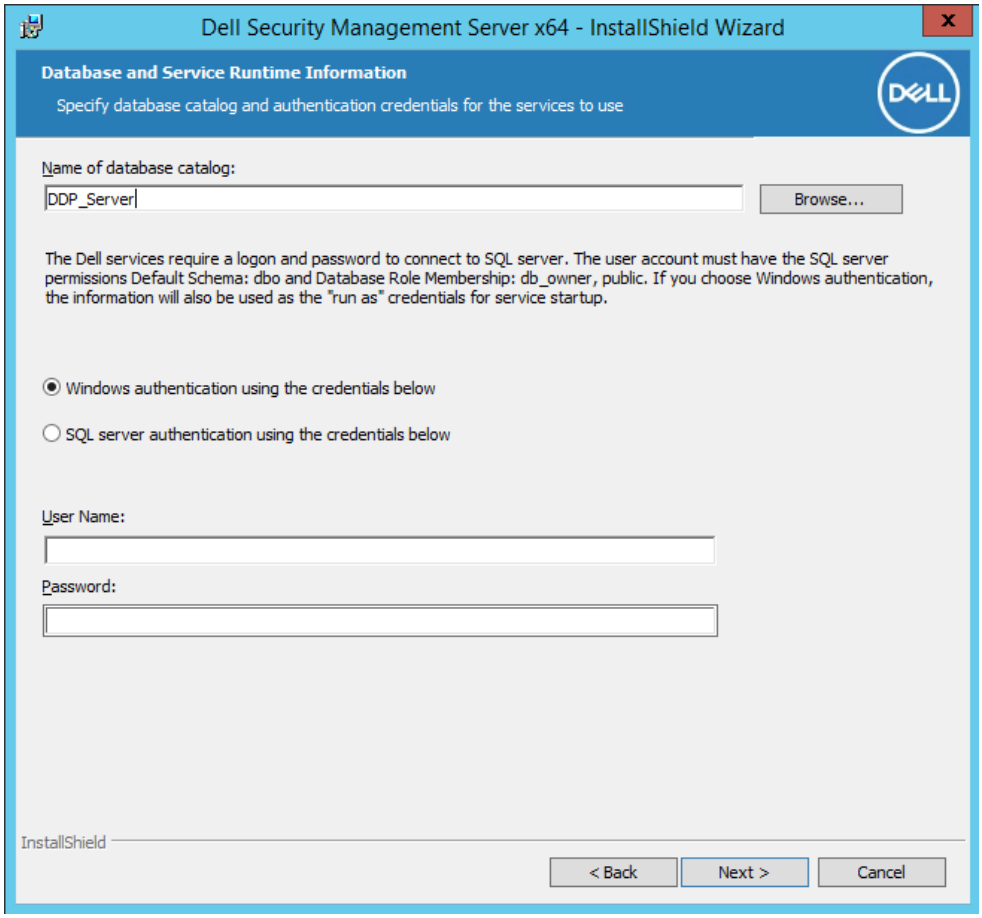
15. Select the authentication method for the product to use. This step connects an account to the product.

- **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.

  Dell services also use these credentials as they work with the Security Management Server.

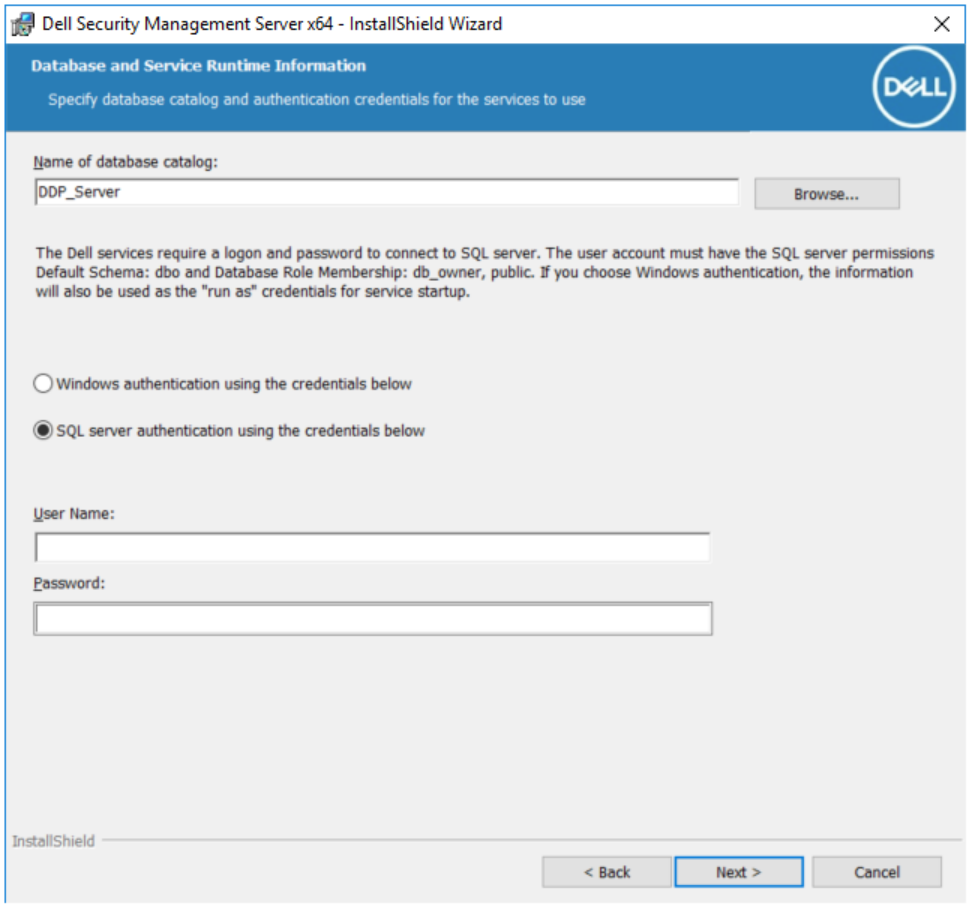


  OR

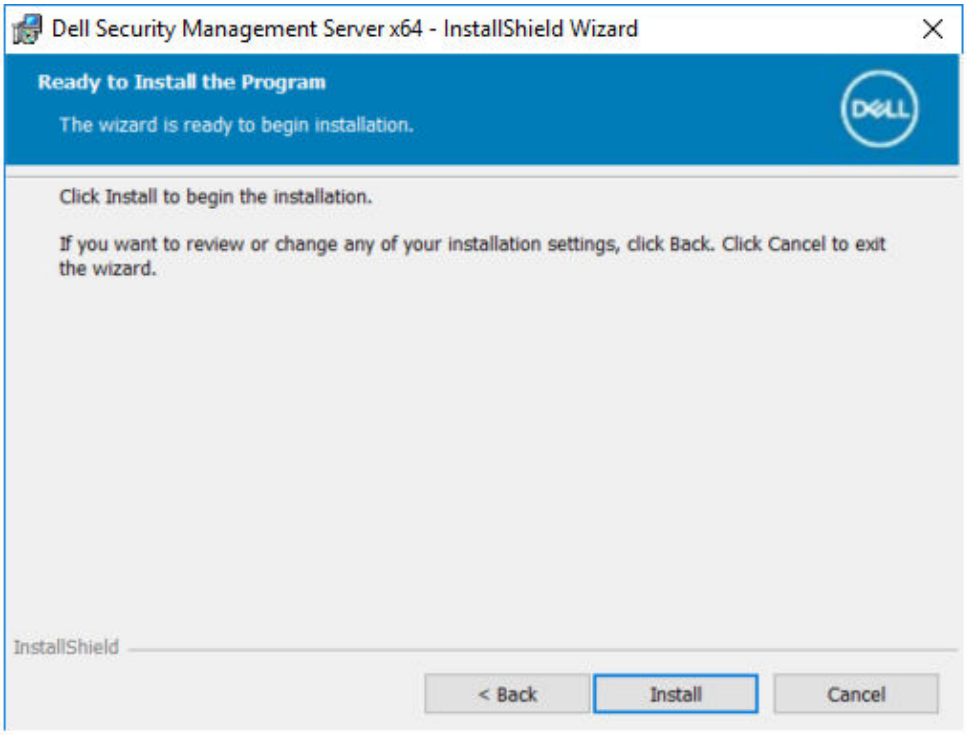
- **SQL Server authentication**

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

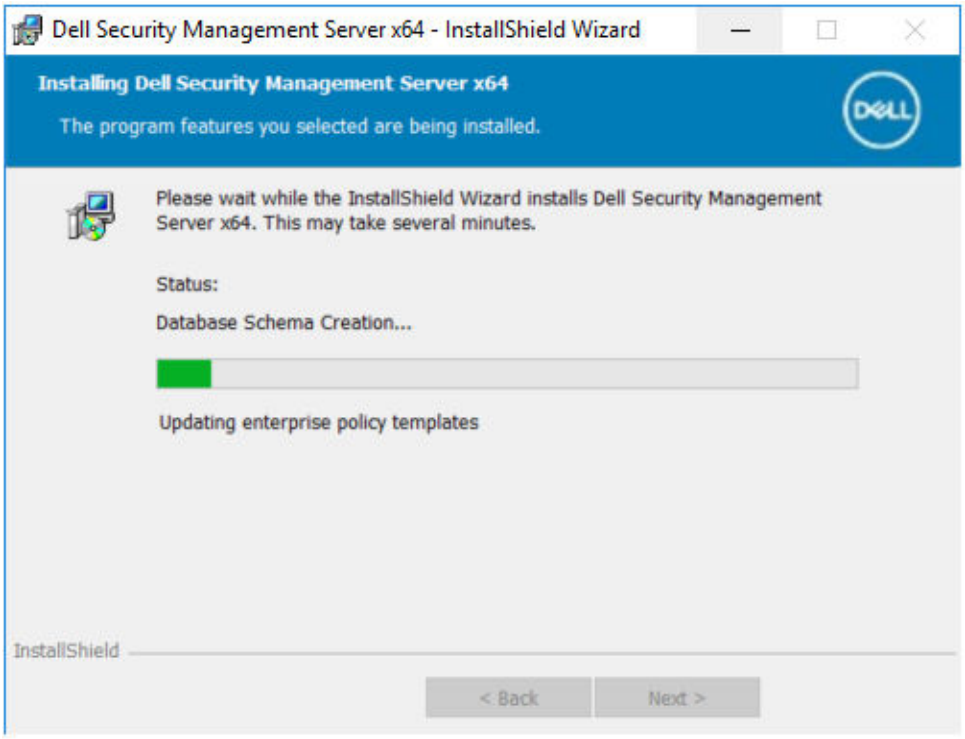
  The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.



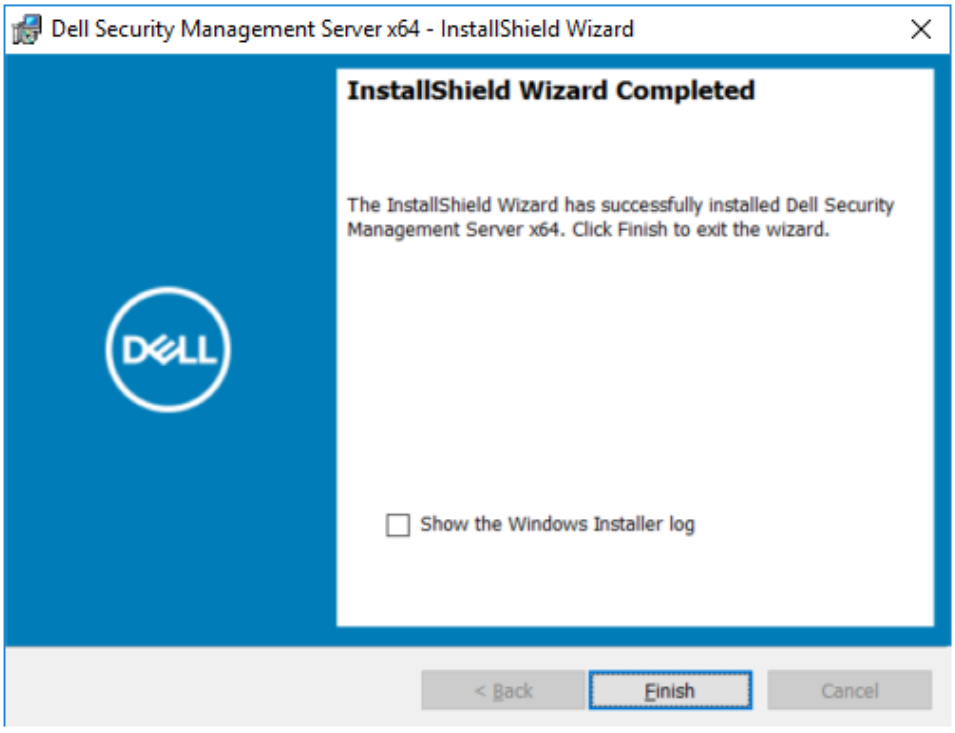
16. In the *Ready to Install the Program* dialog, click **Install**.



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 Dell Server.

Install Back-End Server with Existing Database

NOTE:

If you have a functional Dell Server v9.2 or later, see instructions in Upgrade/Migrate Back End Server(s).

You can install a new Security Management Server and connect to a SQL database in one of these ways:

- Connect to a SQL database created during Pre-Installation Configuration.

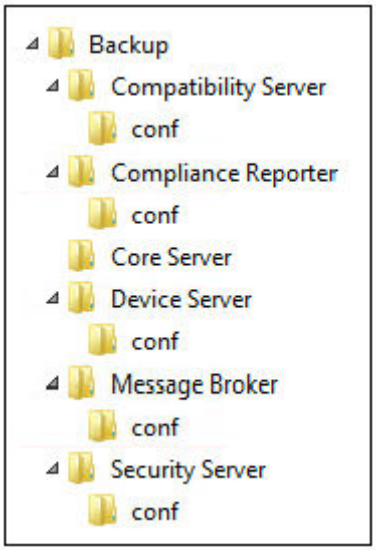
  Or

- Connect to an existing SQL database that is v9.x or later, when the schema version matches the Security Management Server version to be installed.

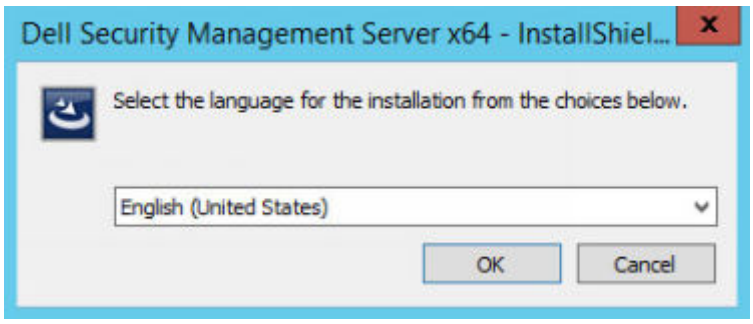
OR

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 options before you begin installation.

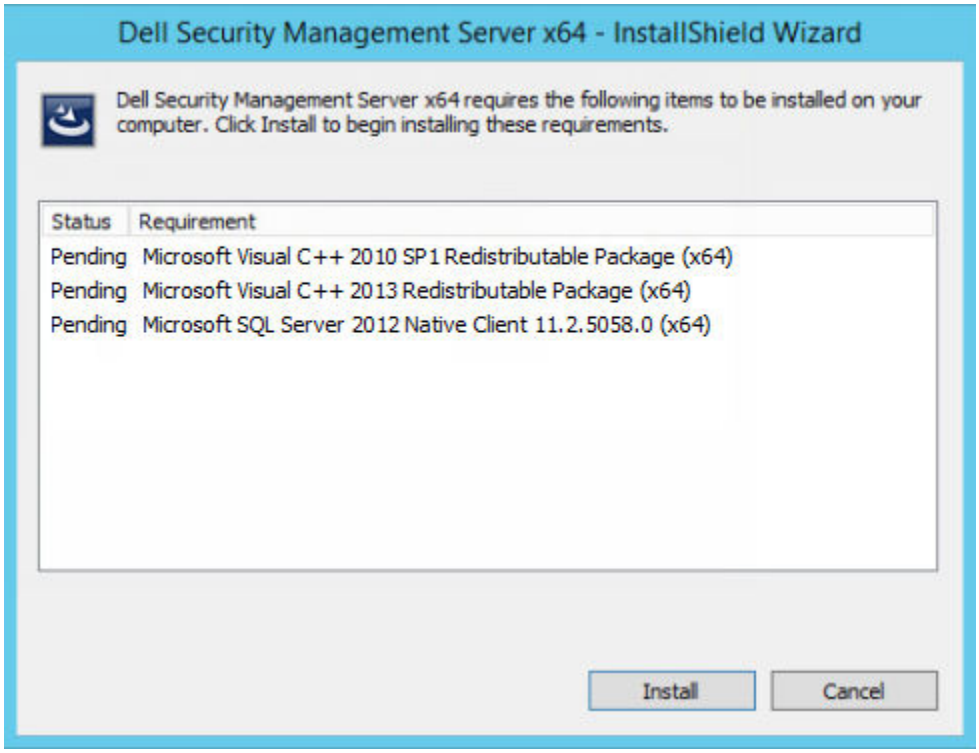
If the existing database has previously been installed with Security Management Server, before you begin installation, ensure that the database, configuration files, and the secretKeyStore are backed up and accessible from the server on which you are installing Security Management Server. Access to these files is necessary to configure Security Management 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, go to the Security Management Server directory. **Extract** (DO NOT copy and paste or drag and drop) Security Management Server-x64 to the root directory of the server where you are installing the Security Management Server. ***Copying and pasting or dragging and dropping produces errors and an unsuccessful installation.***
2. Double-click **setup.exe**.
3. Select the language for installation, and then click **OK**.



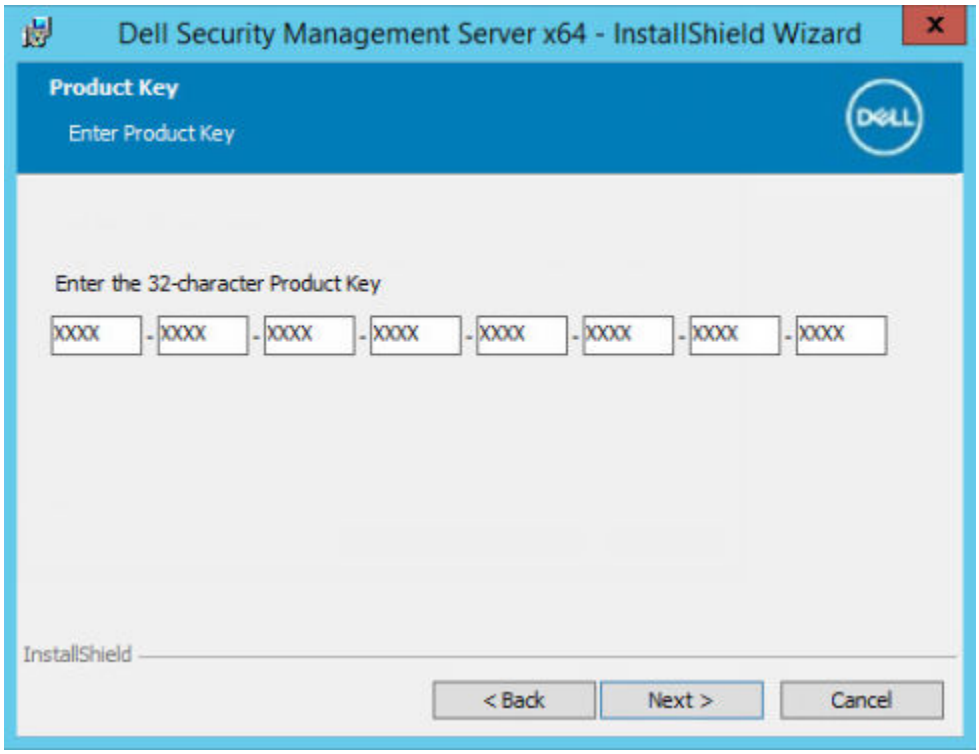
4. If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.



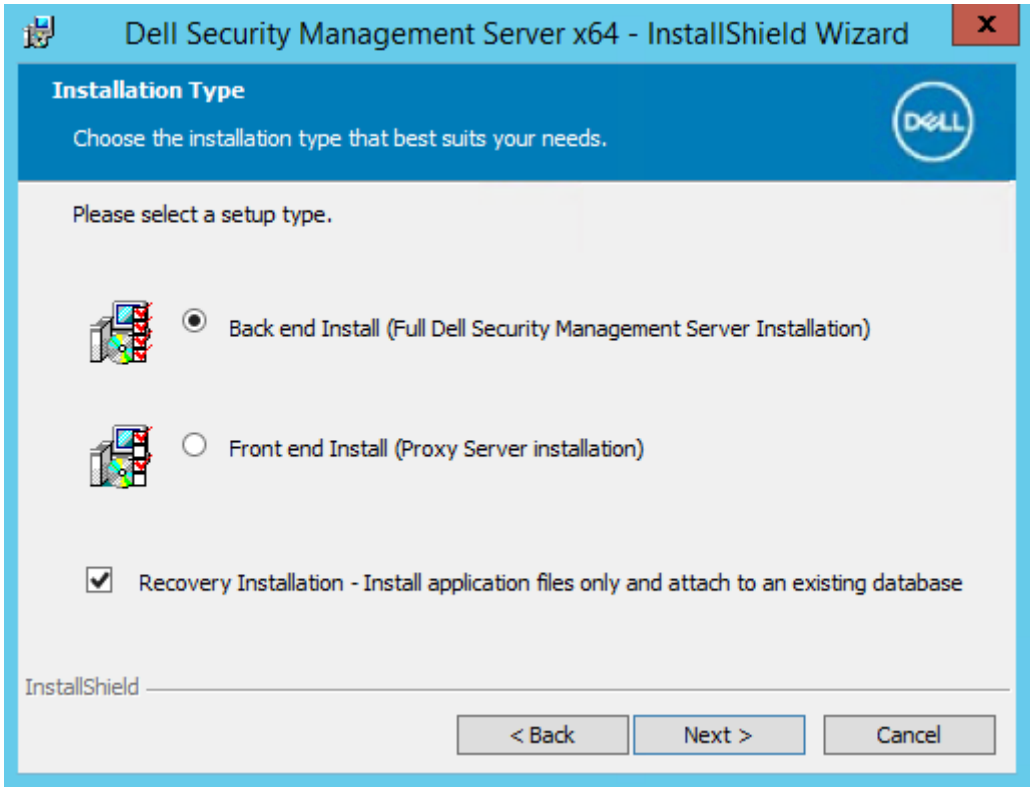
5. In the *Welcome* dialog, click **Next**.

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

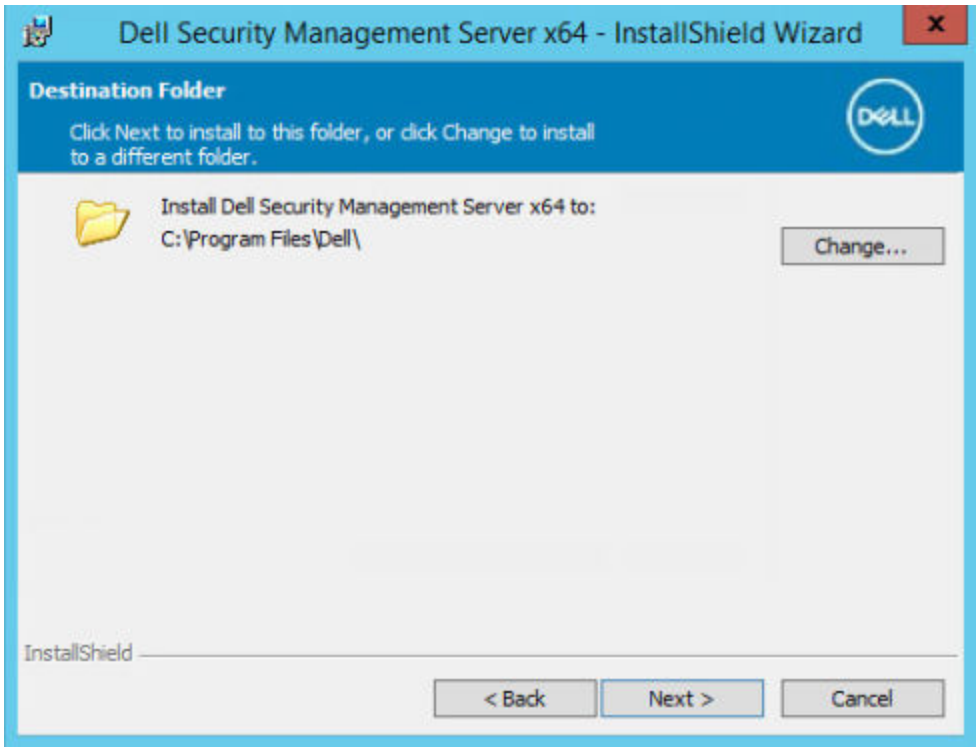
7. If you optionally copied your `EnterpriseServerInstallKey.ini` file to `C:\Windows` as explained in Pre-Installation Configuration, click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is in the `EnterpriseServerInstallKey.ini` file.



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

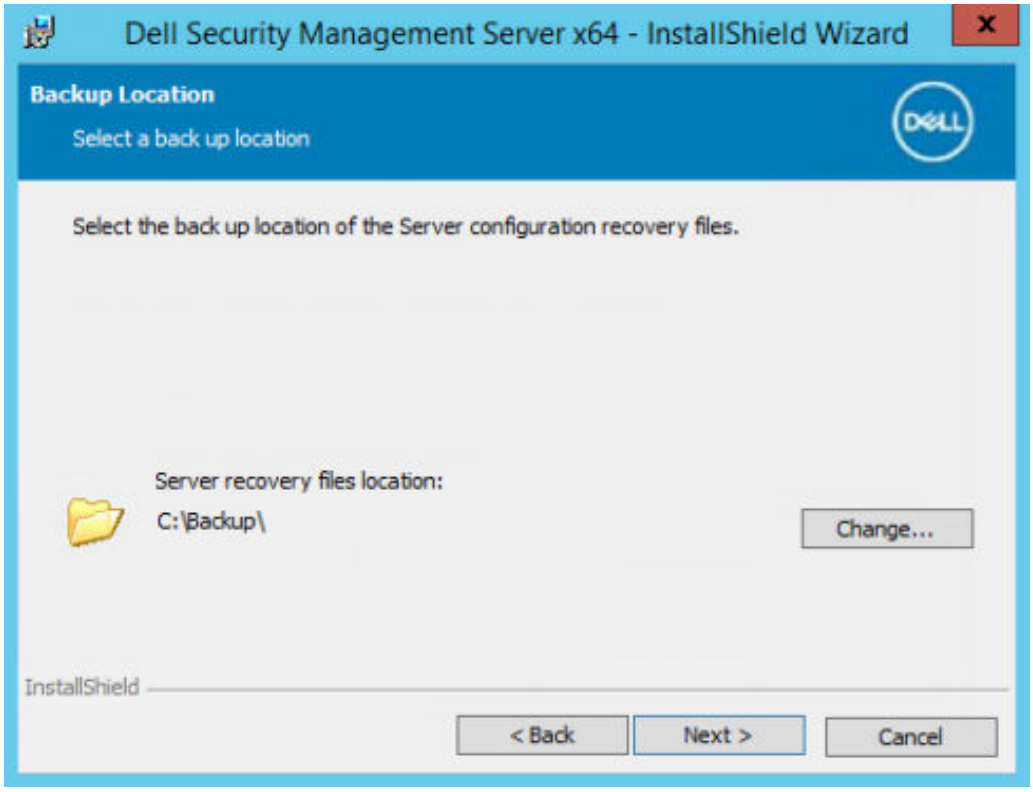


9. To install the Security Management Server to the default location of `C:\Program Files\Dell`, click **Next**. Otherwise, click **Change** to select a different location, and then click **Next**.



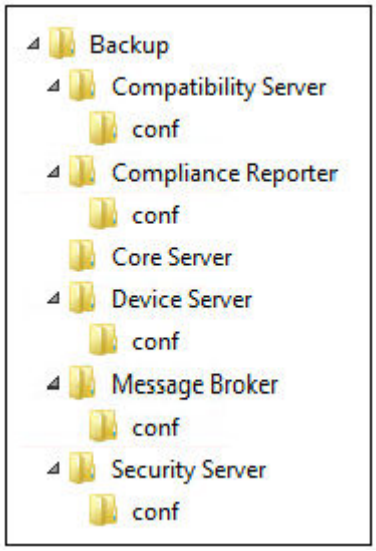
10. To select a location for backup configuration recovery files to be stored, click **Change**, go to your choice of folder, and then click **Next**.

    Dell Technologies recommends that you select a remote network location or external drive for backup.



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

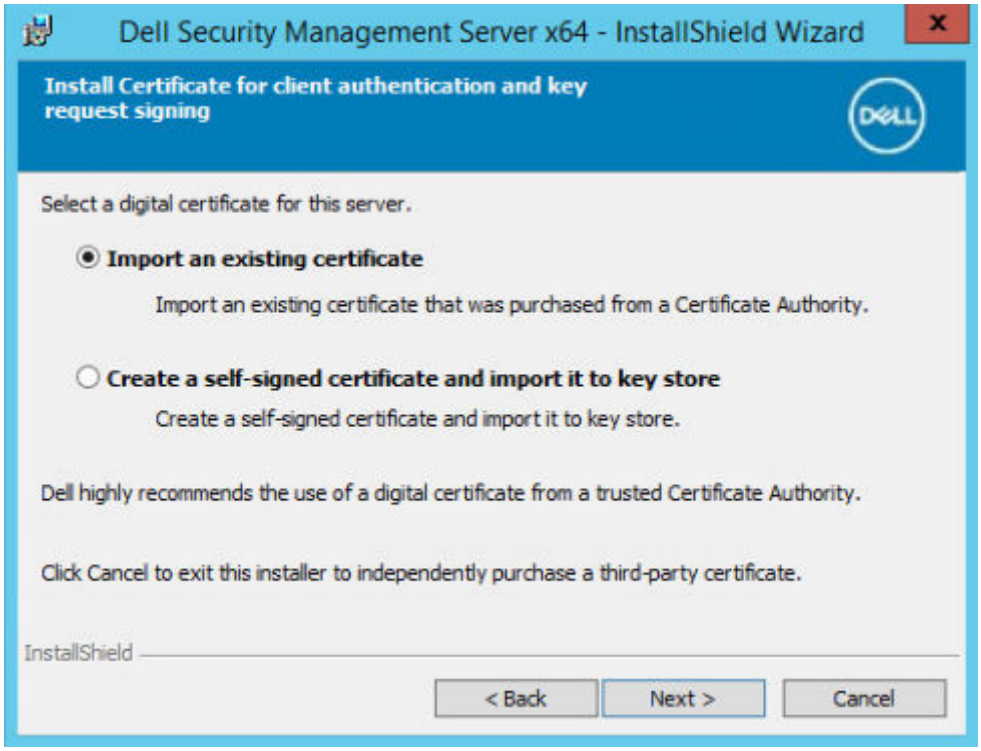
NOTE: The folder structure created by the installer during installation (example shown below) must remain unchanged.



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.

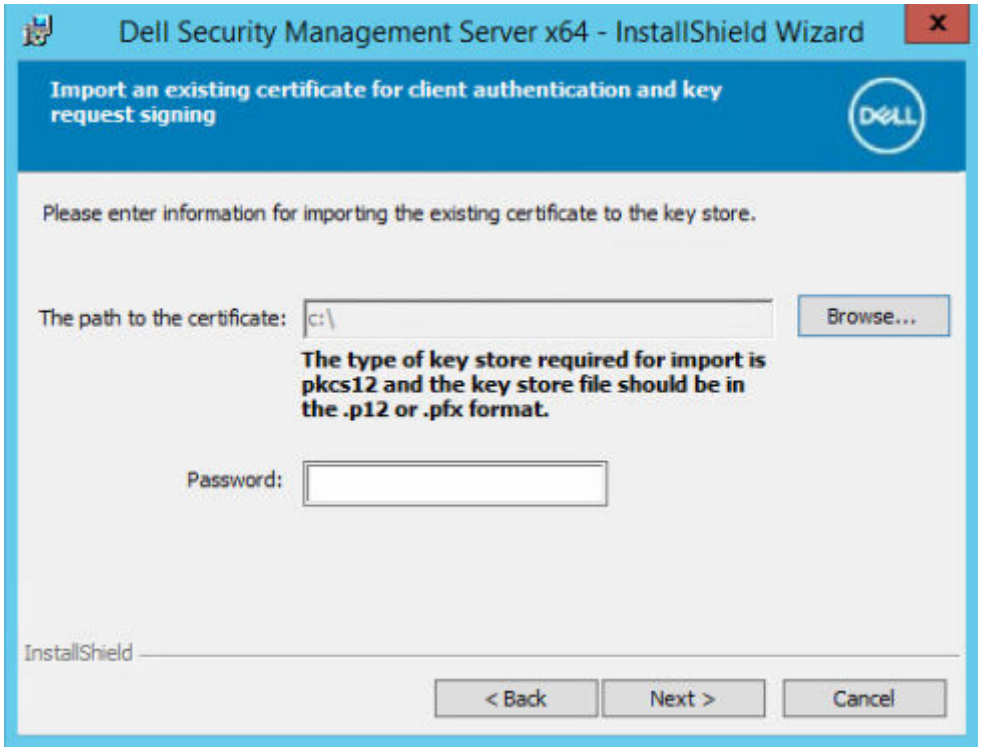
Enter the password associated with this certificate. The key store file must be .p12 or pfx. See Exporting a Certificate to .PFX Using the Certificate Management Console for instructions.

Click **Next**.

NOTE:

To use this setting, confirm that the exported CA certificate being imported has the full trust chain. If unsure, reexport 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)

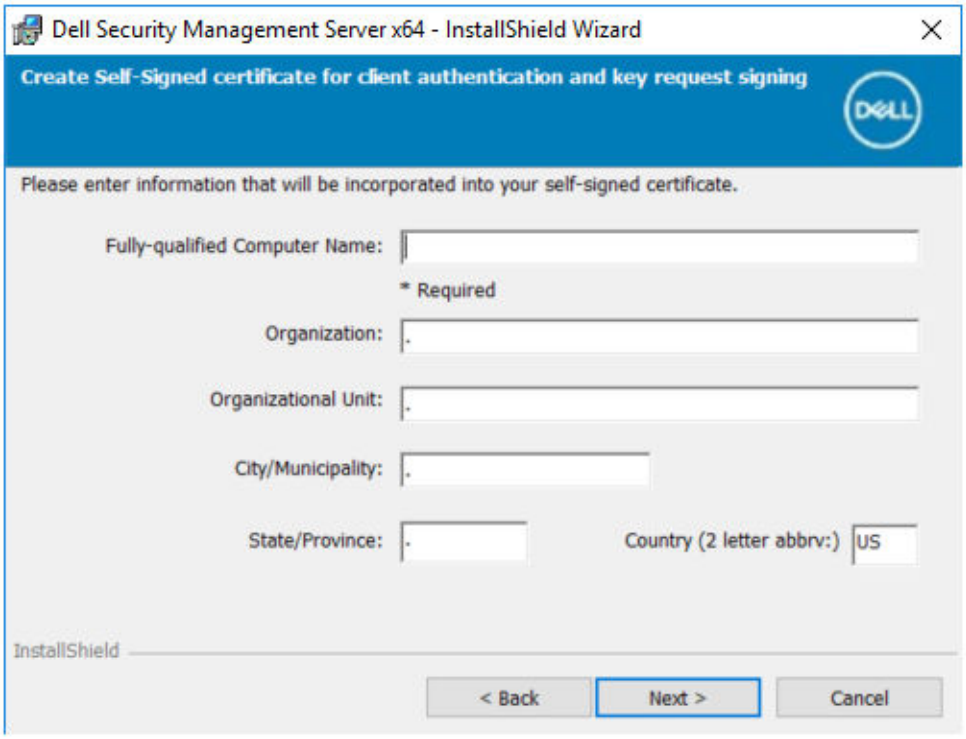
   City

   State (full name)

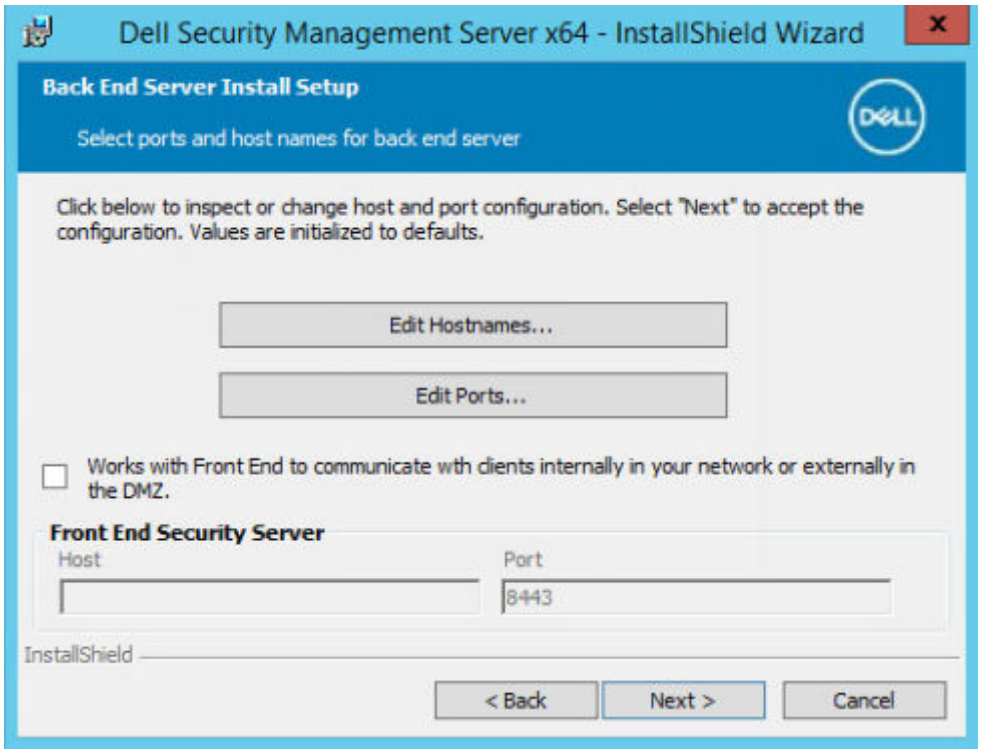
   Country: Two-letter country or region abbreviation

   Click **Next**.

   NOTE: The certificate expires in 10 years, by default.



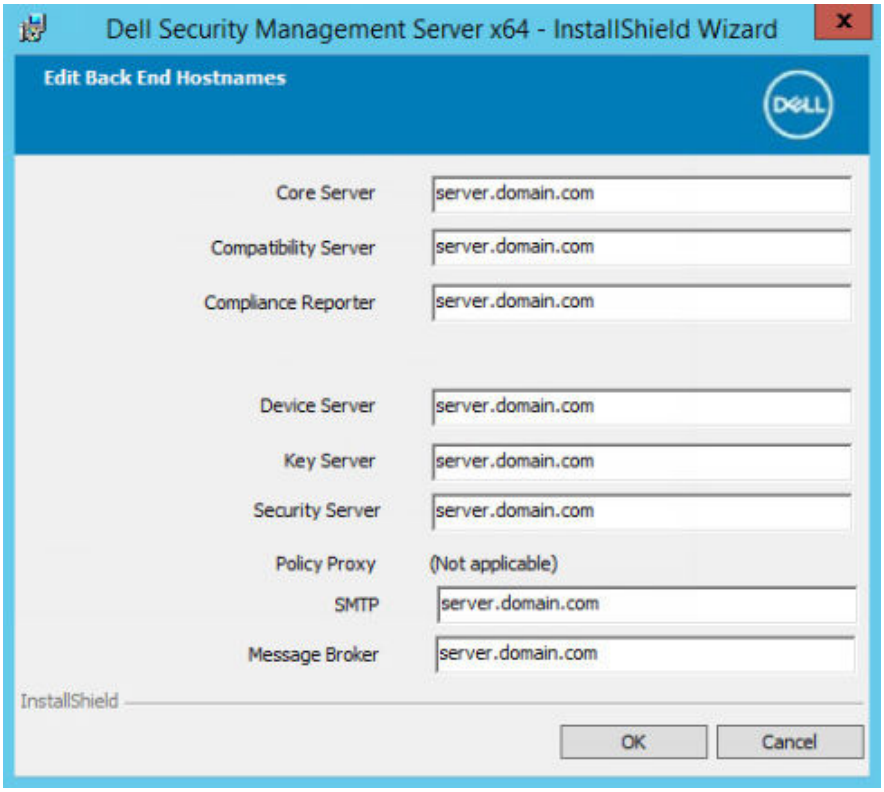
12. From the *Back-End Server Install Setup* dialog, you can view or edit hostnames and ports.
    - To accept the default hostnames and ports, in the *Back-End Server Install Setup* dialog, click **Next**.
    - If you are using a front-end server, select **Works with Front End to communicate with clients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



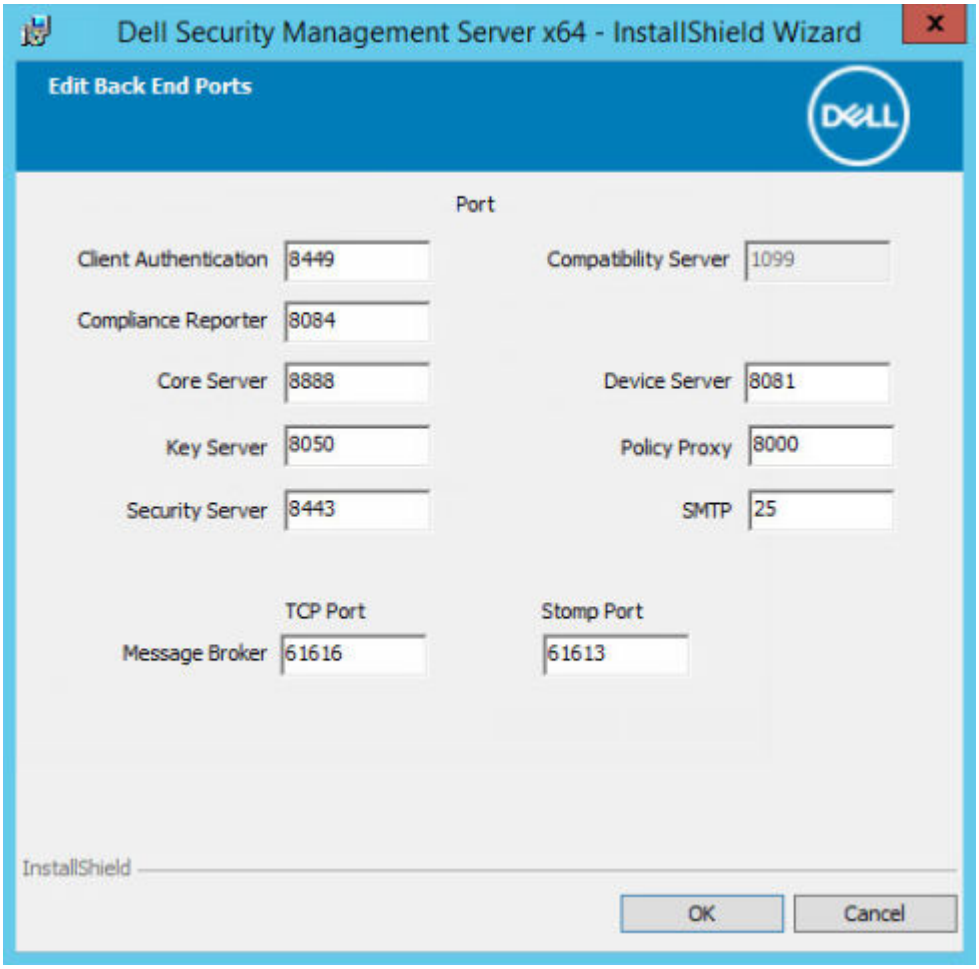
    - To view or edit hostnames, click **Edit Hostnames**. Edit hostnames only if necessary. Dell Technologies recommends using the defaults.

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

When finished, click **OK**.

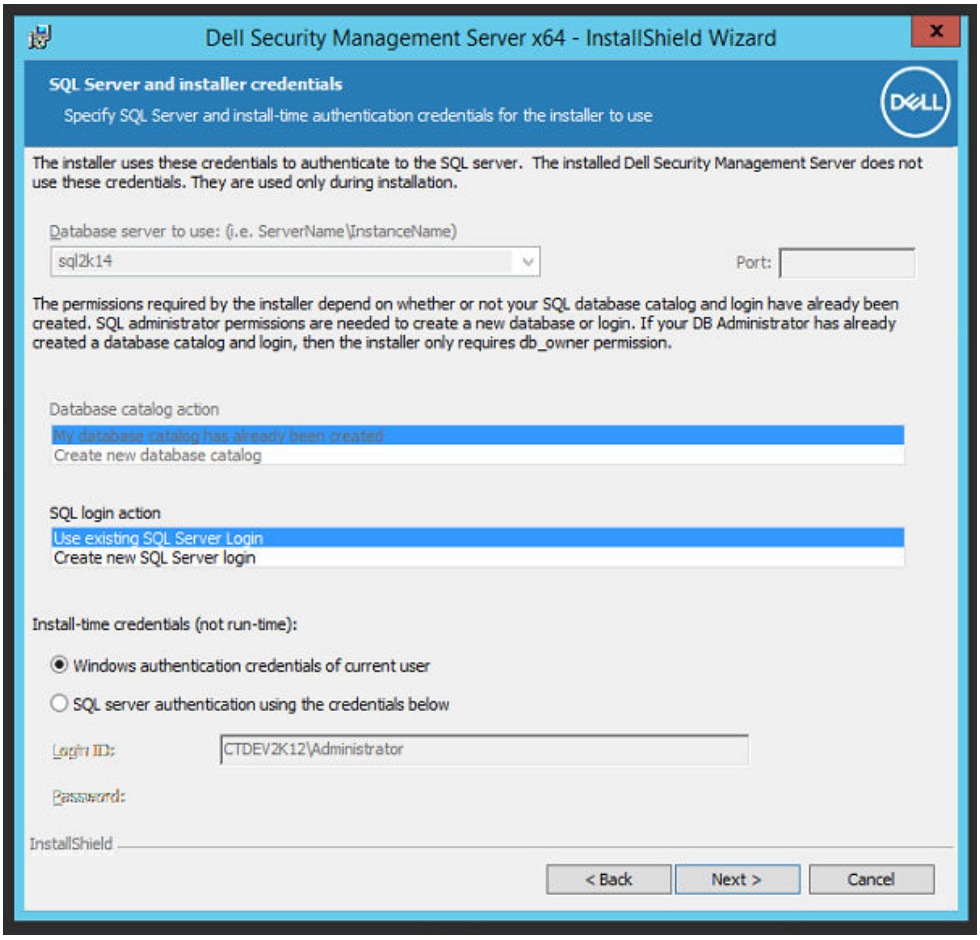


- To view or edit ports, click **Edit Ports**. Edit ports only if necessary. Dell Technologies recommends using the defaults. When finished, click **OK**.



13. 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 are used for authentication. (*User Name* and *Password* are not 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 that is 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**.

14. If the Existing Database Error dialog displays, select the appropriate option.

    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. (See step a.)
    - The database already has a database schema that matches the version currently being installed. (See 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.

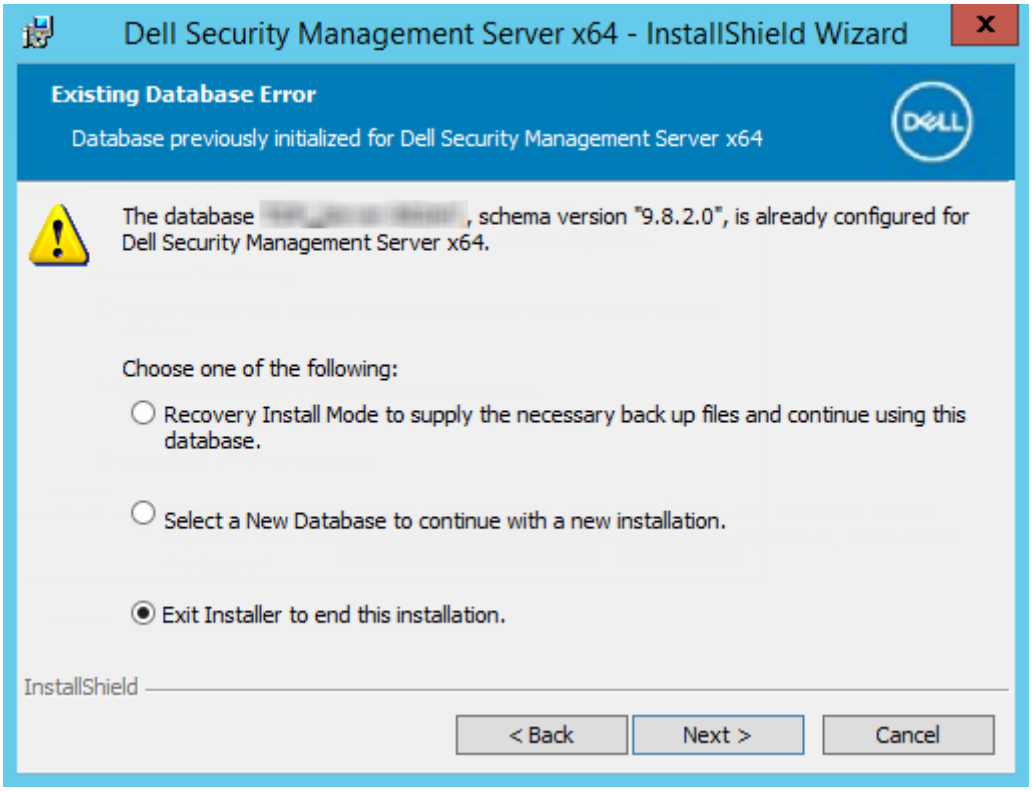
The following options MUST be used only with the help of Dell ProSupport:

- 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 reinstall the correct version of Security Management Server, and then running the latest installer to upgrade.
- The **Proceed without migrating the database** option installs the Security Management 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 schema of the current version, but is not connected to a Security Management Server backend, it is considered a *Recovery*. If **Recovery Installation** was not selected in this step, 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**.



15. Select the authentication method for the product to use. This authentication is the account that the product uses to engage 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, and then click **Next.**

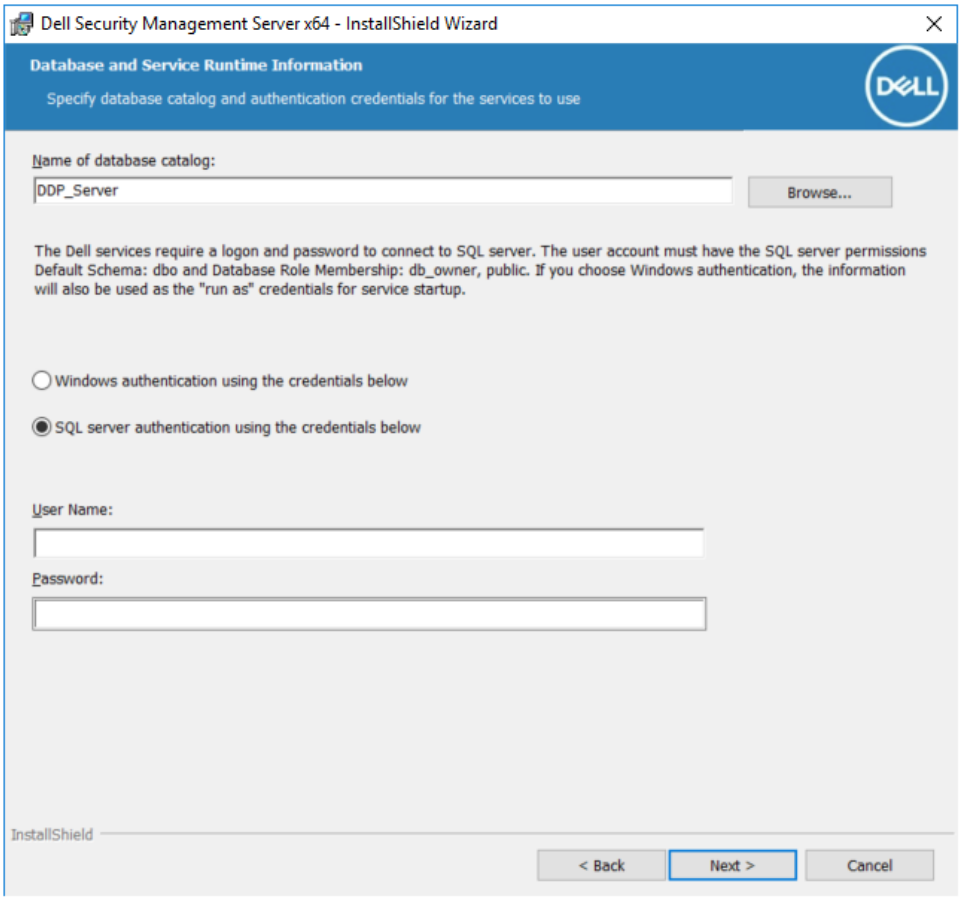
      Ensure that the account has system administrator rights and the ability to manage the SQL Server. The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.

      OR

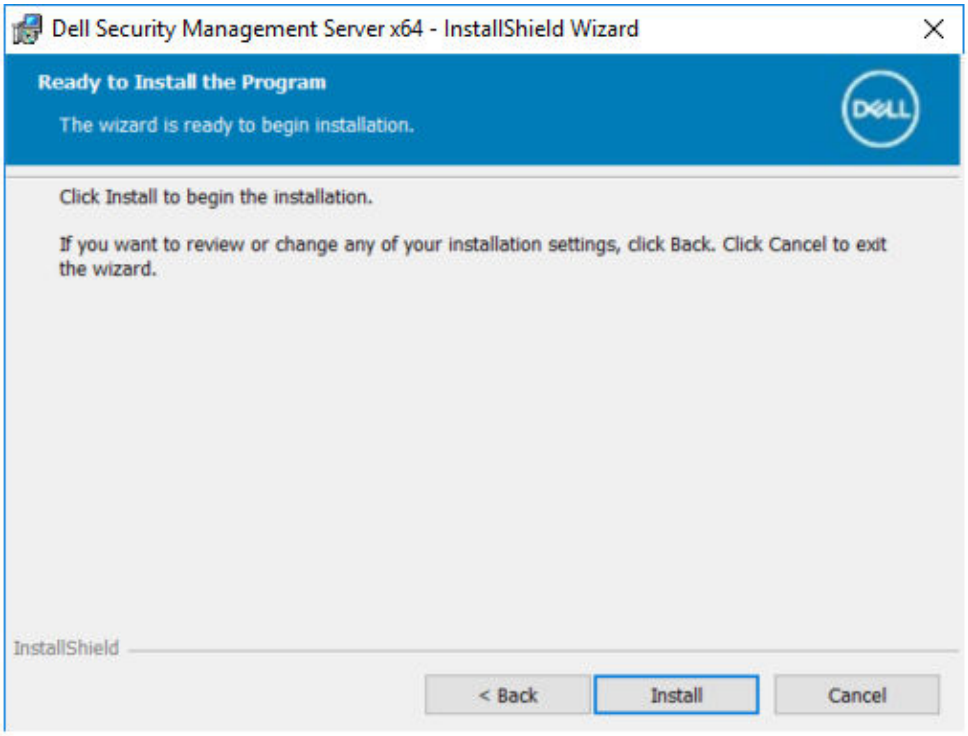
    - **To use SQL Server authentication**:

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

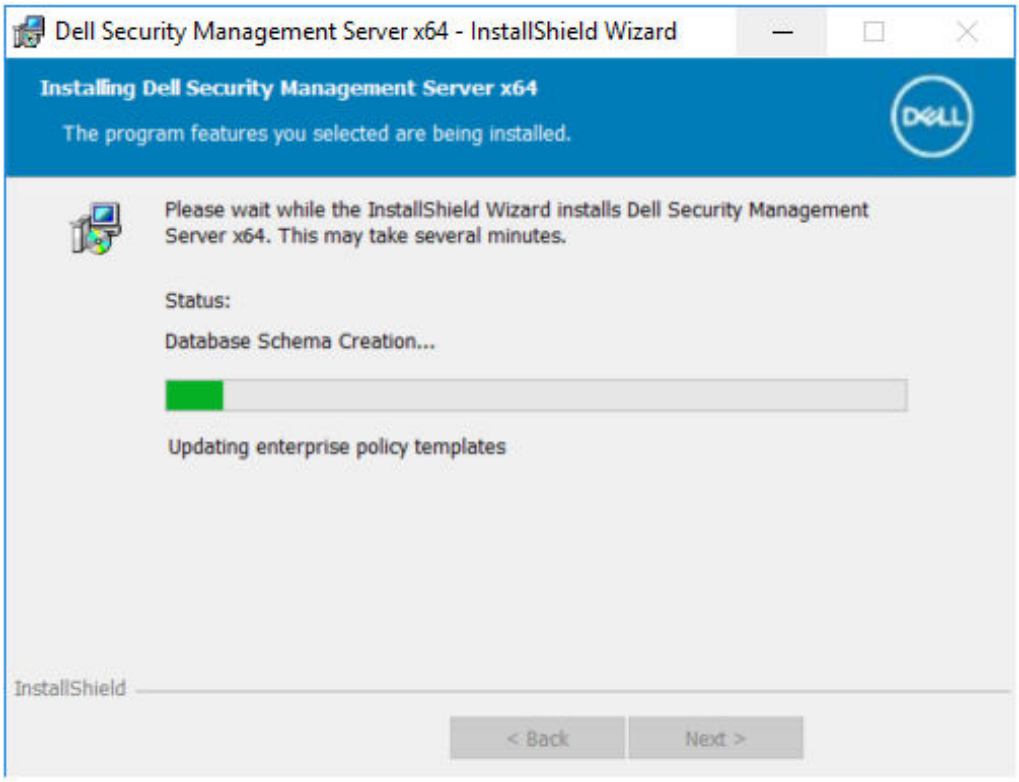
      The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.



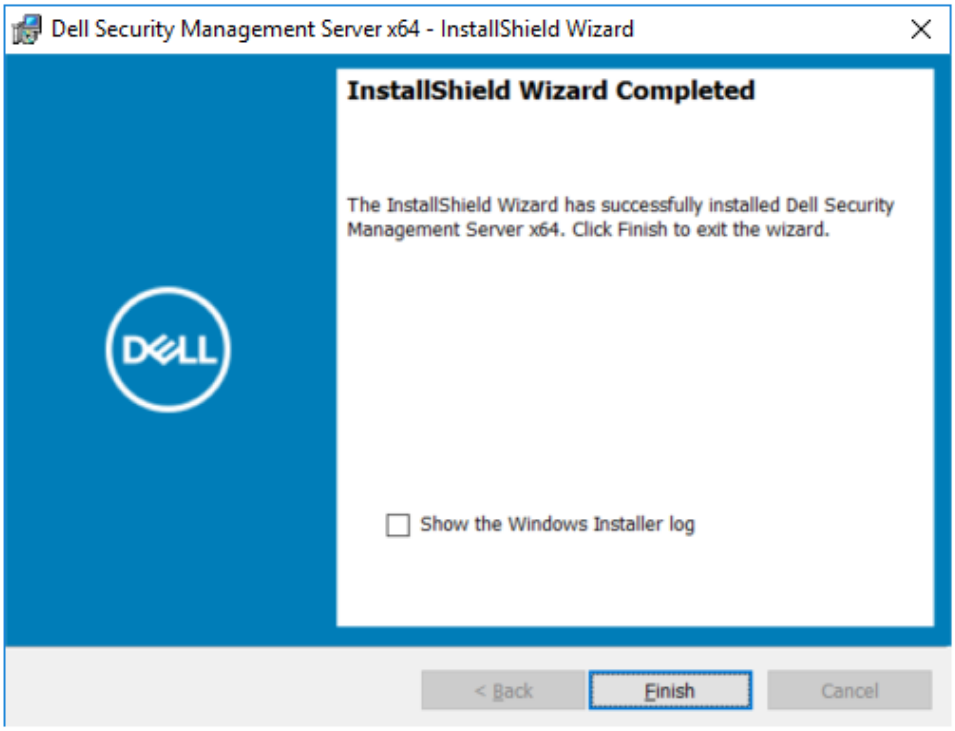
16. In the *Ready to Install the Program* dialog, click **Install**.



A progress dialog displays status throughout the installation process.



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



Back-end server installation tasks are complete.

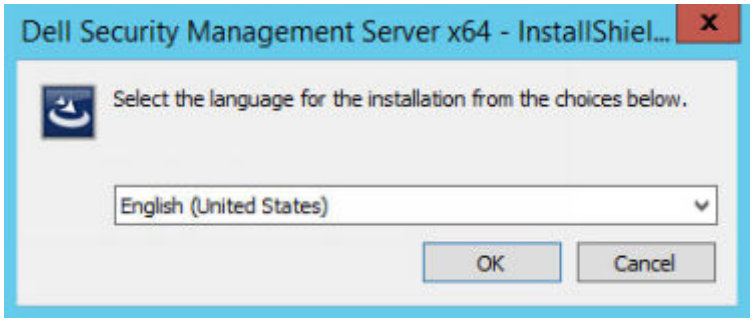
Dell Services are restarted at the end of installation. It is not necessary to reboot the server.

Install Front End Server

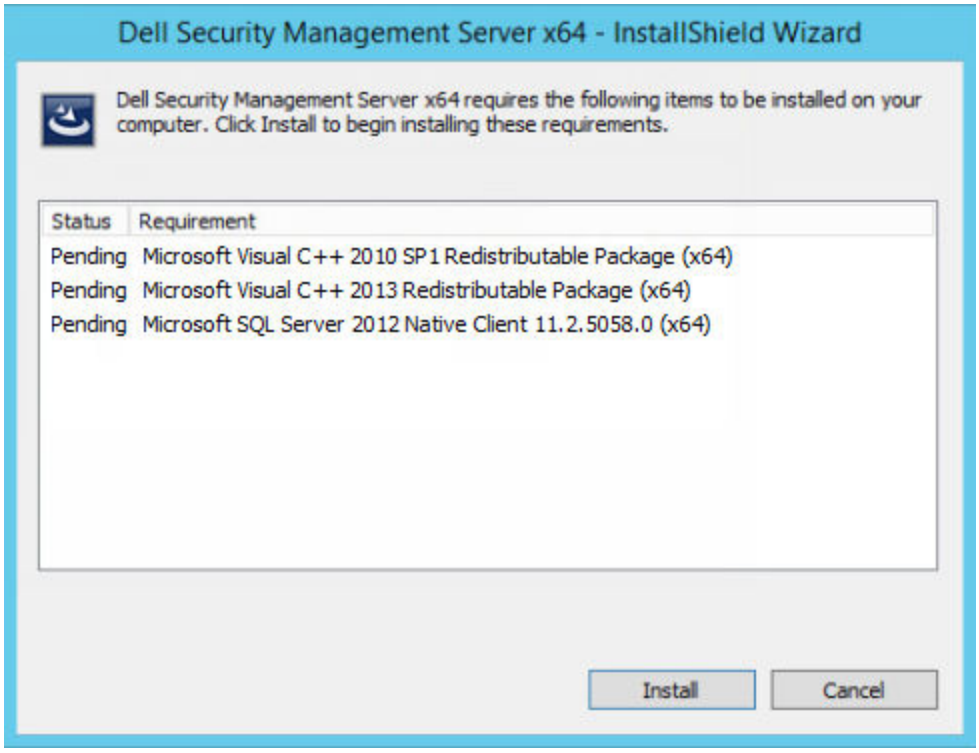
Front end server installation provides a front end (DMZ mode) option for use with Security Management Server. If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

To install, you need the fully qualified hostname of the DMZ server.

1. In the Dell installation media, go to the Security Management Server directory. **Extract** (DO NOT copy and paste or drag and drop) Security Management Server-x64 to the root directory of the server where you are installing Security Management Server. ***Copying and pasting or dragging and dropping produces errors and an unsuccessful installation.***
2. Double-click **setup.exe**.
3. Select the language for installation, and then click **OK**.

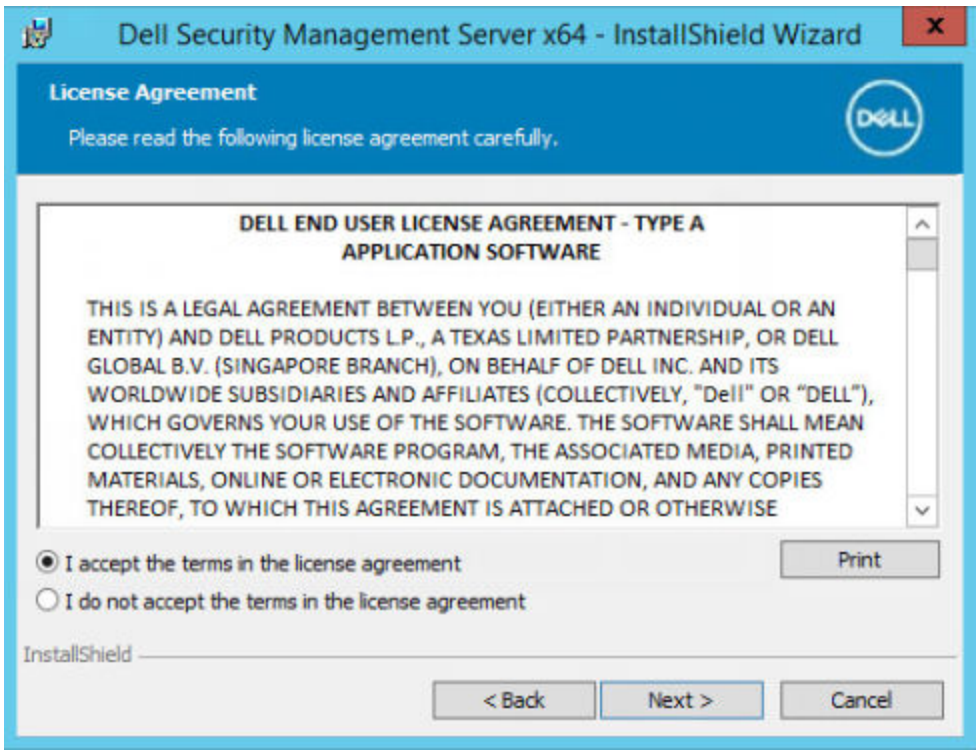


4. If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.

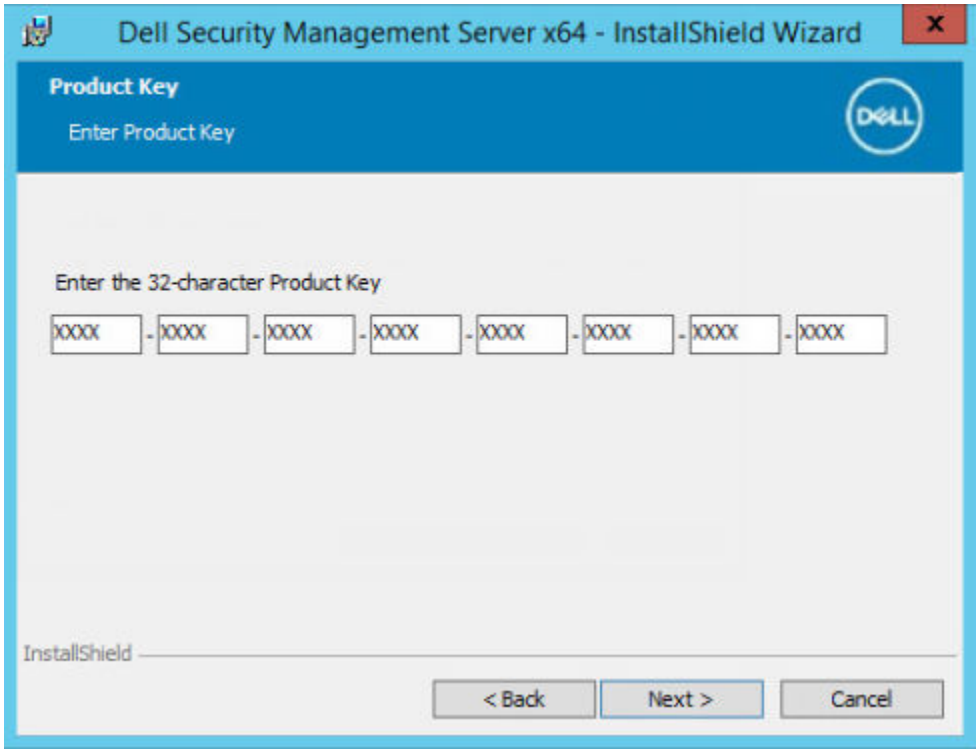


5. Click **Next** in the Welcome dialog.

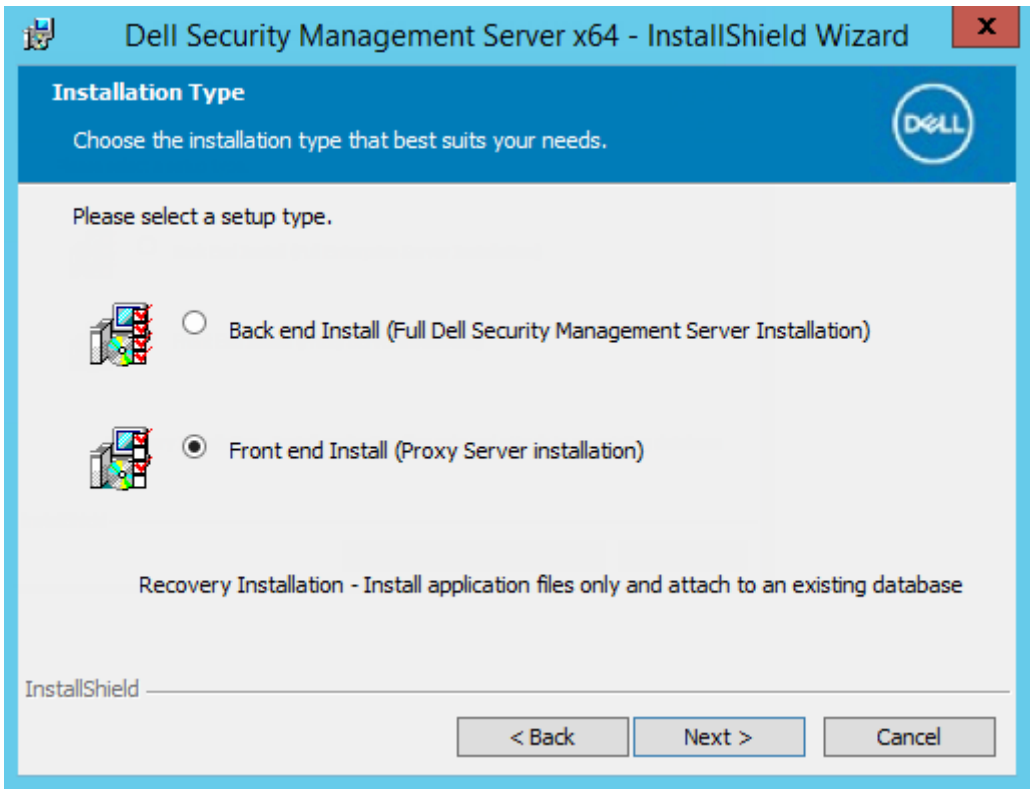
6. Read the license agreement, accept the terms, and then click **Next**.



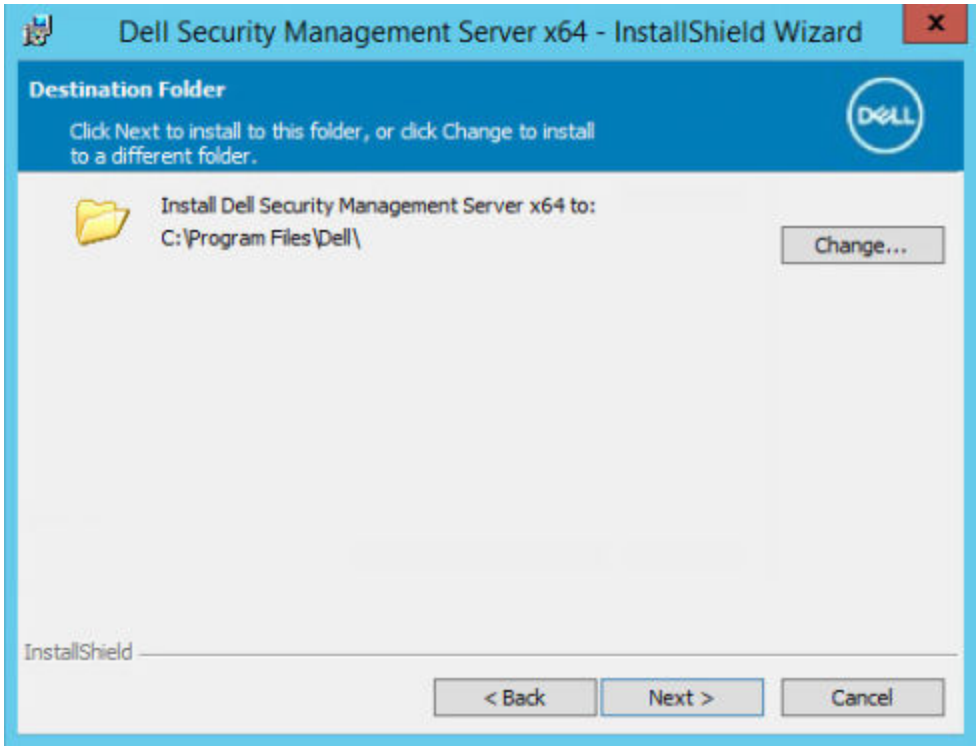
7. If you optionally copied your `EnterpriseServerInstallKey.ini` file to `C:\Windows` as explained in Pre-Installation Configuration, click **Next**. If not, enter the 32-character Product Key and then click **Next**. The Product Key is located in the `EnterpriseServerInstallKey.ini` file.



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 another location, and then click **Next**.

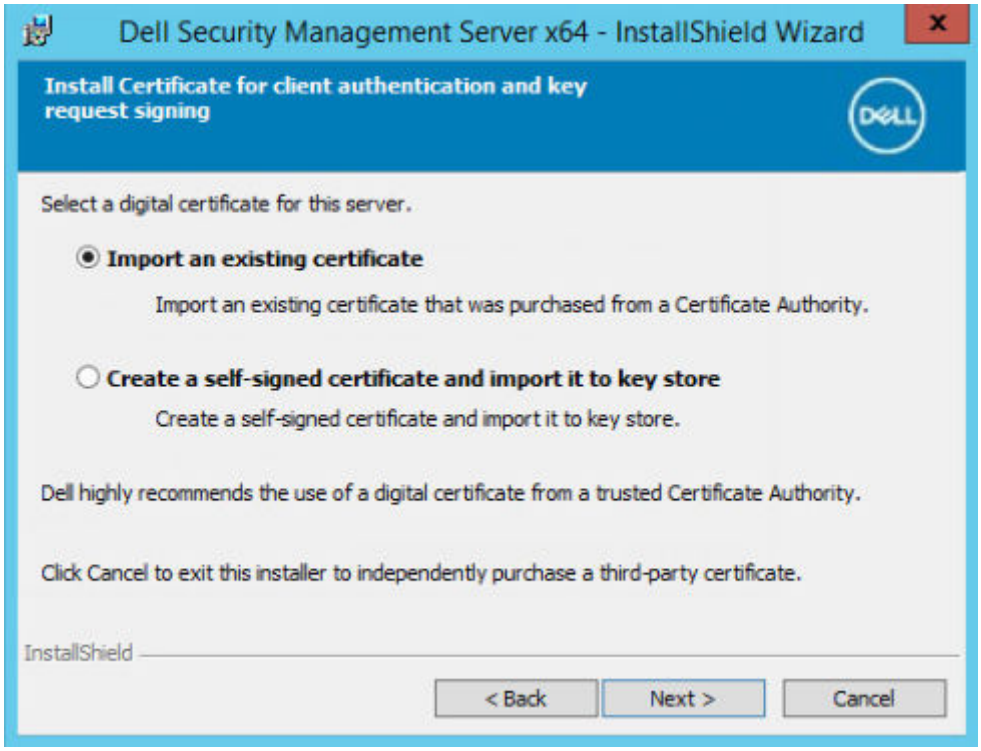


10. You have a choice of digital certificate types to use.

    NOTE: 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.

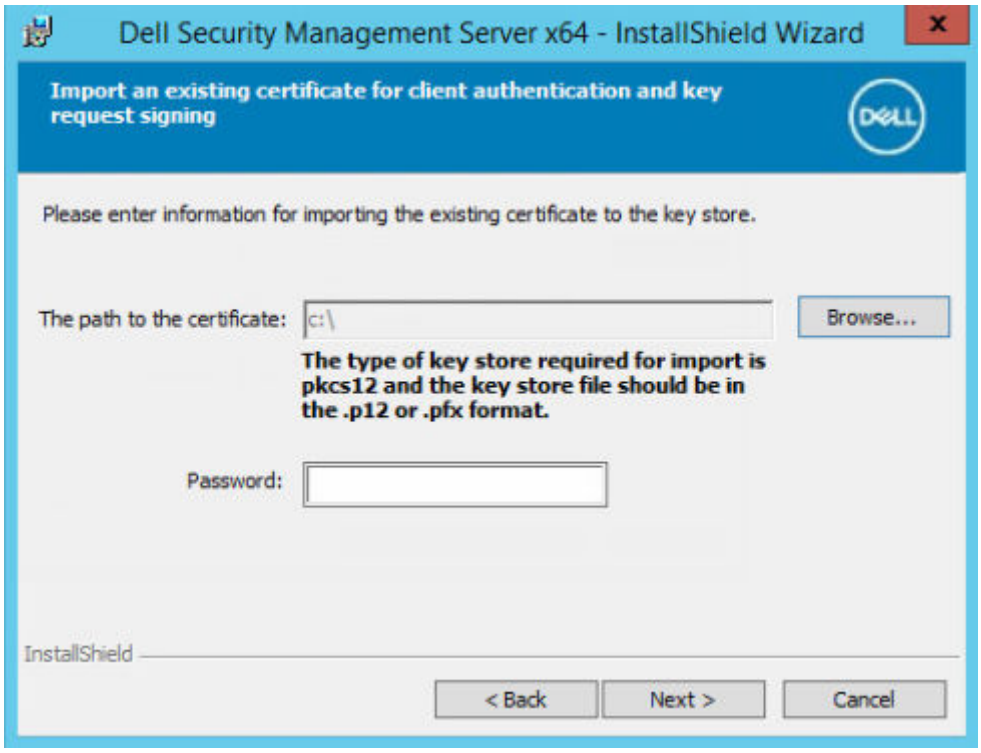
    Enter the password associated with this certificate. The key store file must be .p12 or pfx. SeeExporting a Certificate to .PFX Using the Certificate Management Console for instructions.

Click **Next**.

NOTE:

To use this setting, confirm that the exported CA certificate being imported has the full trust chain. If unsure, reexport 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)

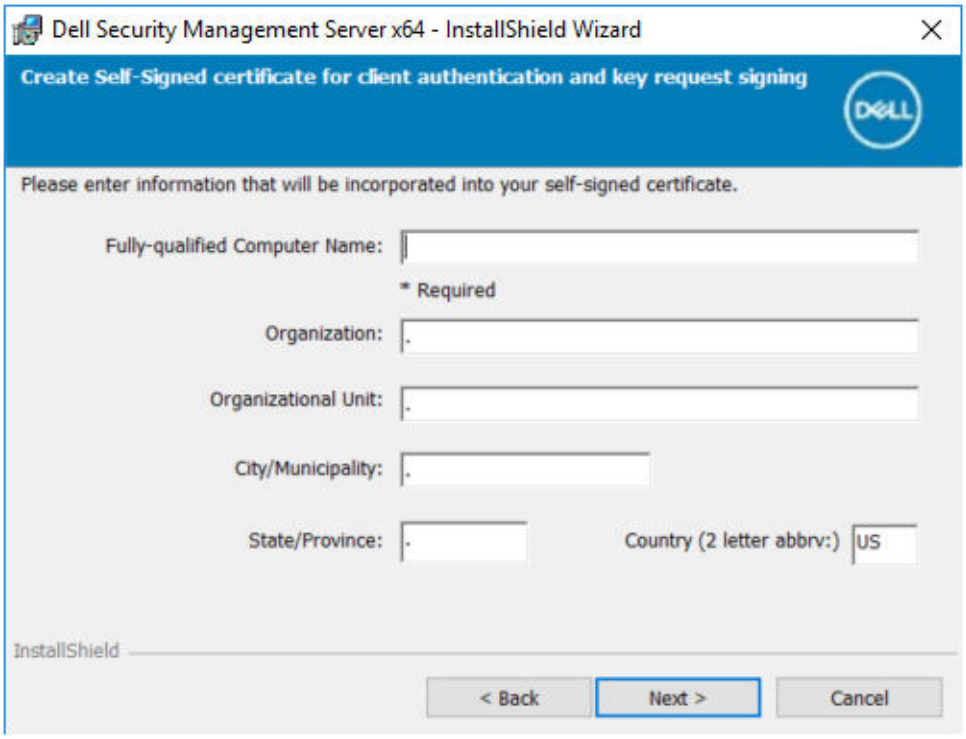
City

State (full name)

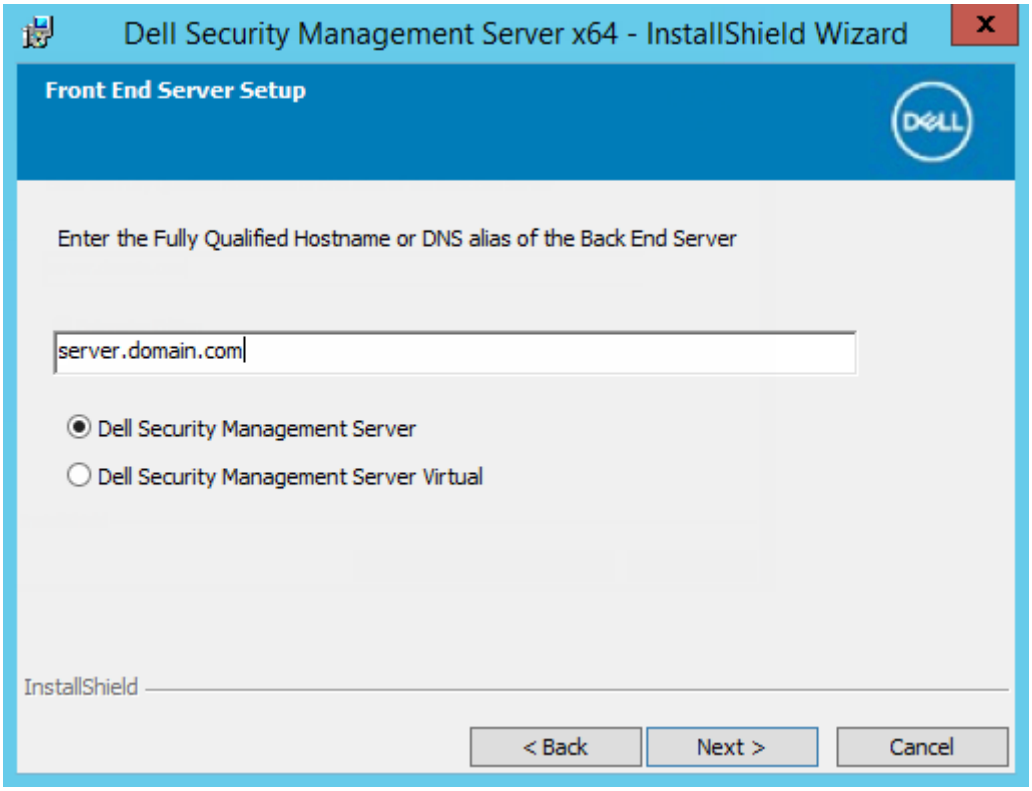
Country: Two-letter country or region abbreviation

Click **Next**.

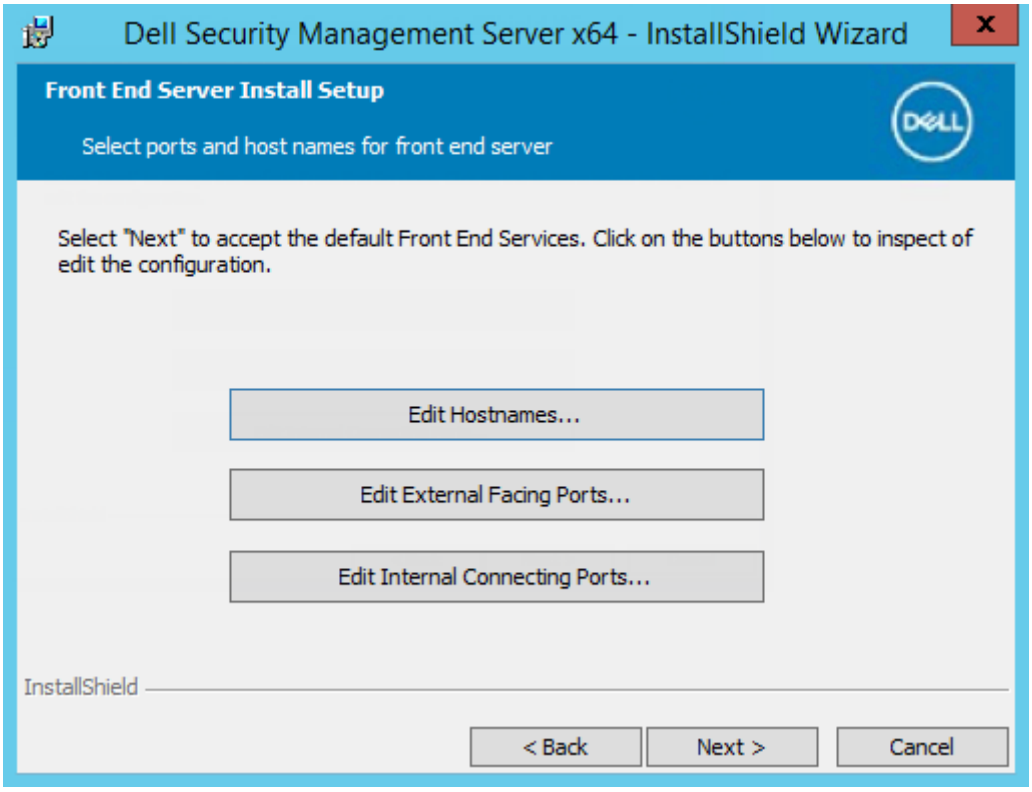
NOTE: The certificate expires in 10 years, by default.



11. In the *Front-End Server Setup* dialog, enter the fully qualified hostname or DNS alias of the back-end server, select **Dell Security Management Server**, 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**.



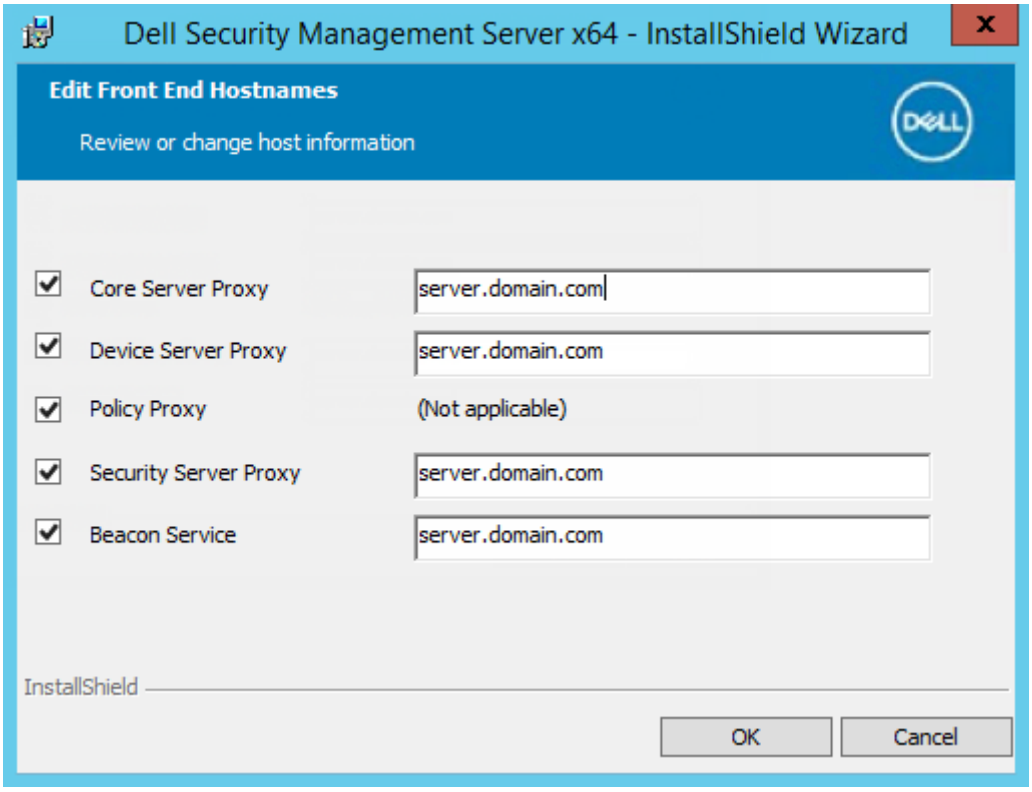
- To view or edit hostnames, in the *Front-End Server Setup* dialog, click **Edit Hostnames**. Edit hostnames only if necessary. Dell Technologies recommends using the defaults.

  NOTE:

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

  Clear a proxy only if certain that you do not want to configure it for installation. If you clear a proxy in this dialog, it is not installed.

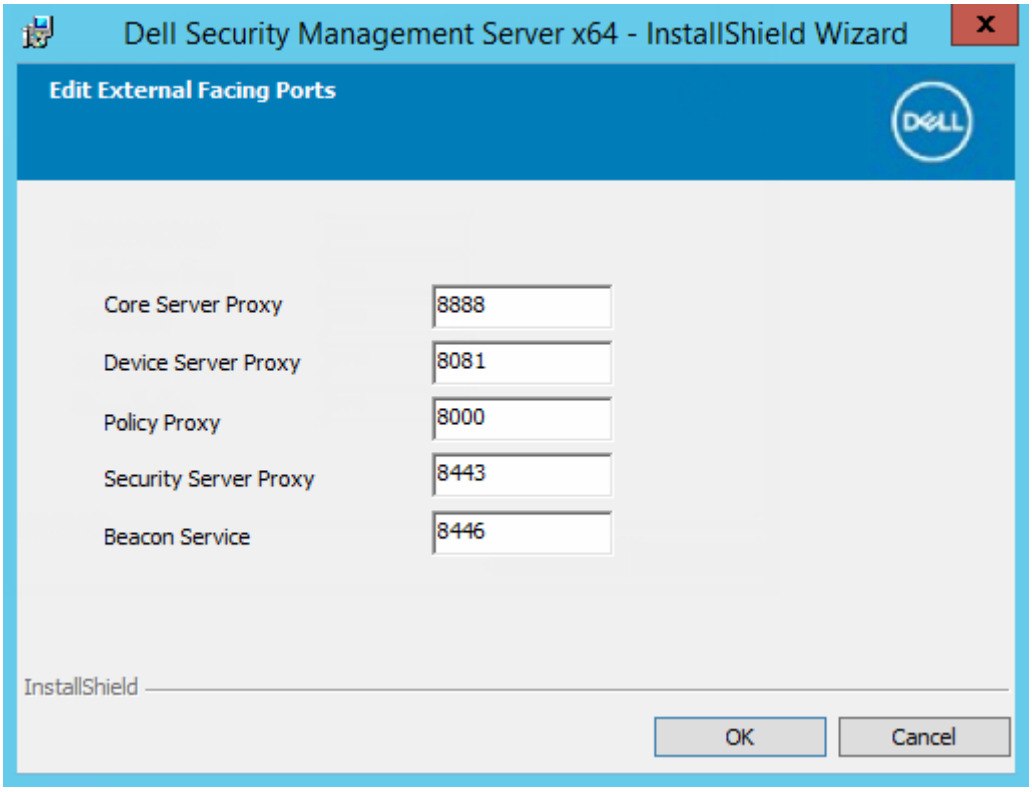
  When finished, click **OK**.

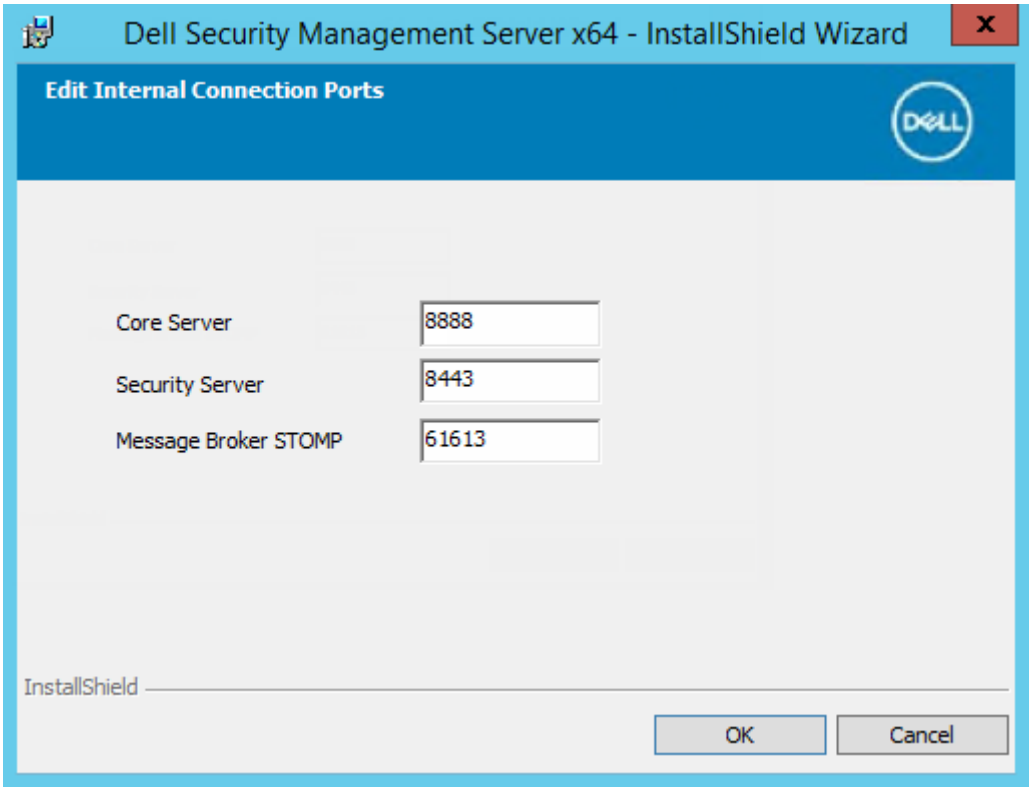


- To view or edit ports, in the *Front-End Server Setup* dialog, click either **Edit External Facing Ports** or **Edit Internal Connecting Ports**. Edit ports only if necessary. Dell Technologies recommends using the defaults.

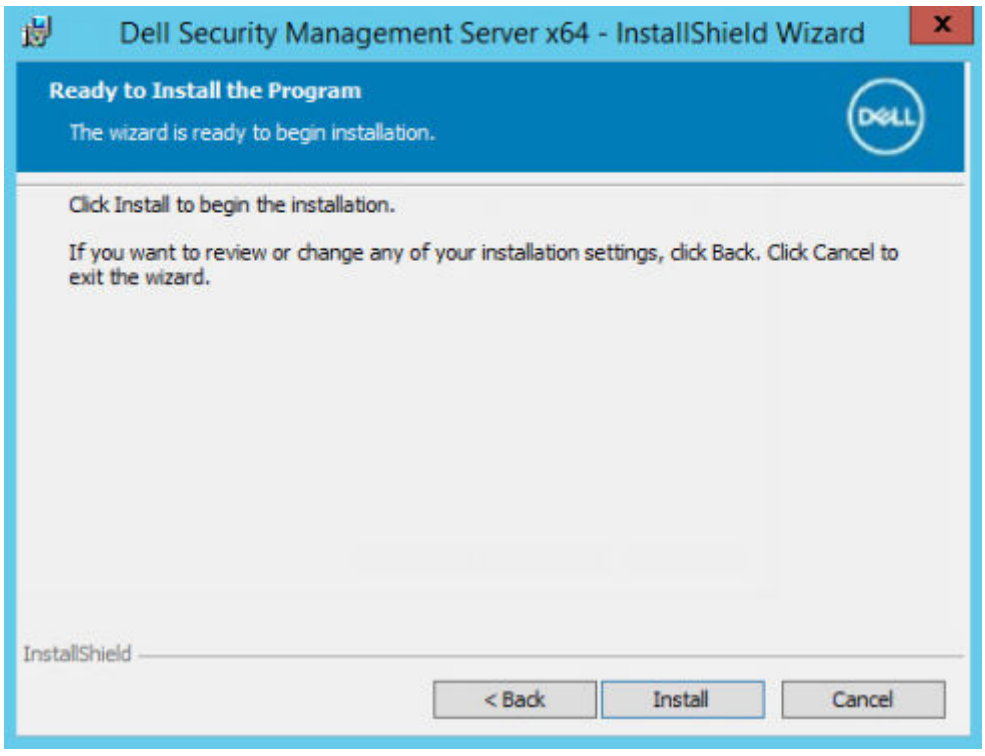
  If you clear a proxy in the *Edit Front-End Host Names* dialog, its port does not display in the External Ports or Internal Ports dialogs.

  When finished, click **OK**.

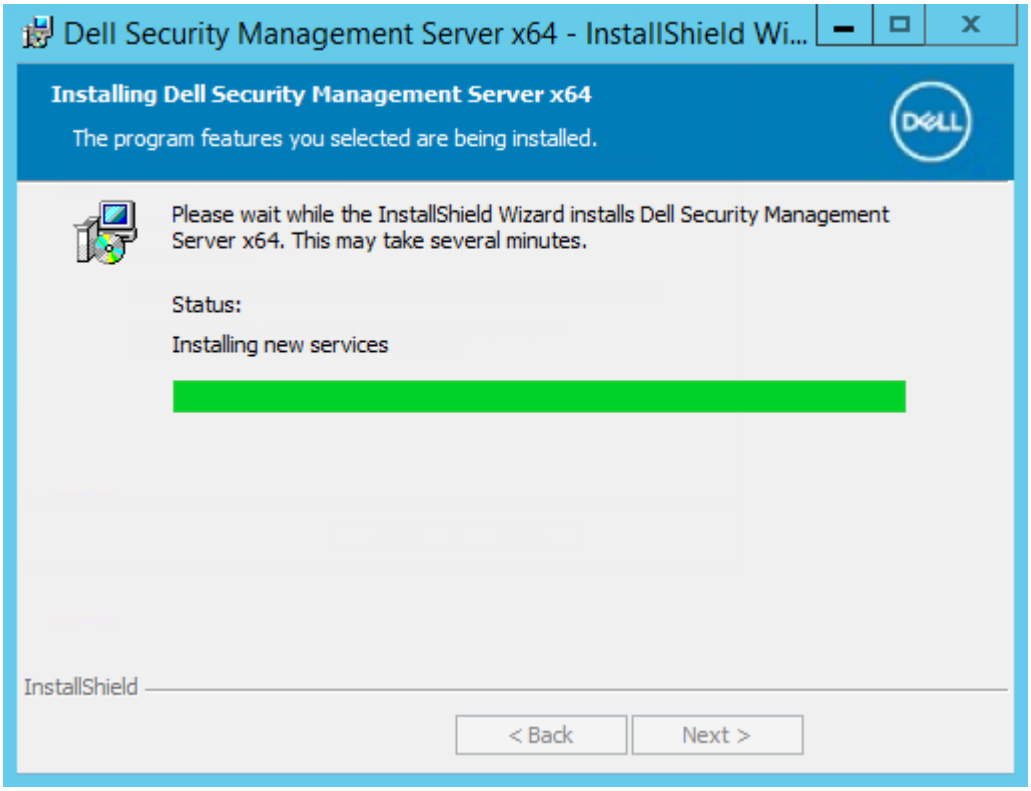




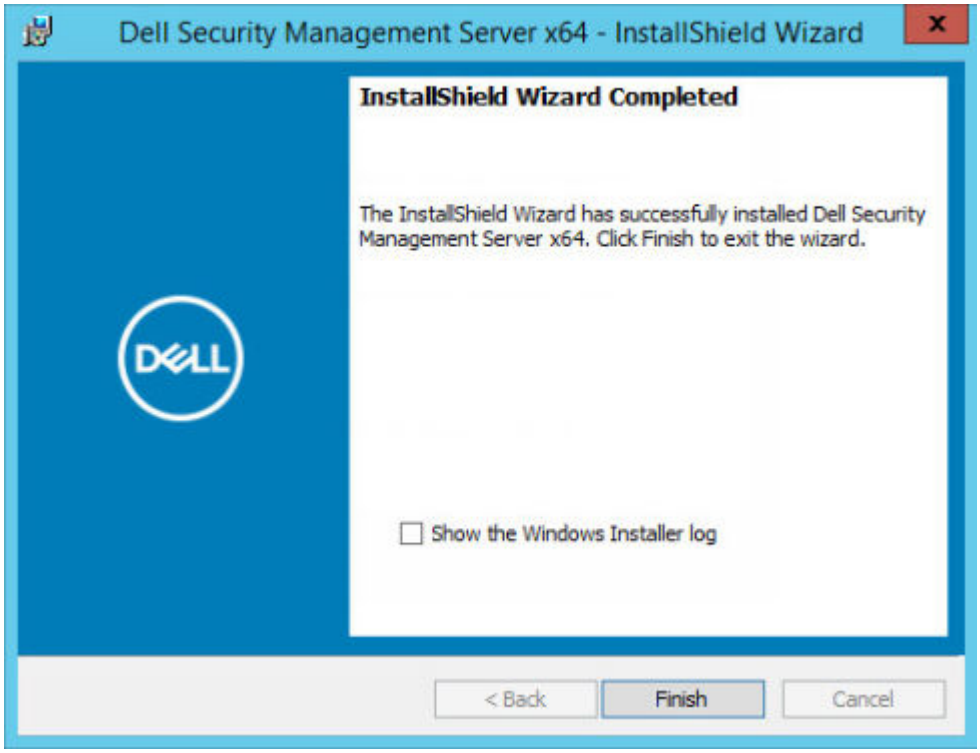
13. In the *Ready to Install the Program* dialog, click **Install**.



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 Enterprise Server v9.2 and later to Security Management Server v10.x. If your Dell Server version is older than v9.2, you must first upgrade to v9.2 then upgrade to later versions.

Before You Begin Upgrade/Migration

Before you begin, ensure that all Pre-Installation Configuration is complete.

Read the *Security Management Server Technical Advisories* for any current workarounds or known issues that are related to Security Management 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 privileges before you begin installation.

Dell Technologies recommends that database best practices are used for the Dell Server 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 Technologies recommends installing the SQL Server on a dedicated server.

To leverage full capabilities of policies, Dell Technologies recommends updating to the most current versions of both the Security Management Server and clients.

Security Management Server v11.x supports:

- Encryption Enterprise:
  - Windows clients v8.x/v10.x/v11.x
  - Mac clients v8.x/v10.x/v11.x
  - SED Management v8.x/v10.x/v11.x
  - BitLocker Manager v8.x/10.x/v11.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprisev1.x/v2.x/v3.x
- Upgrade/Migration from Security Management Server v9.2 or later. (When migrating from pre-v9.2 Security Management Server, contact Dell ProSupport for assistance.)

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

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

Apply Policy Changes

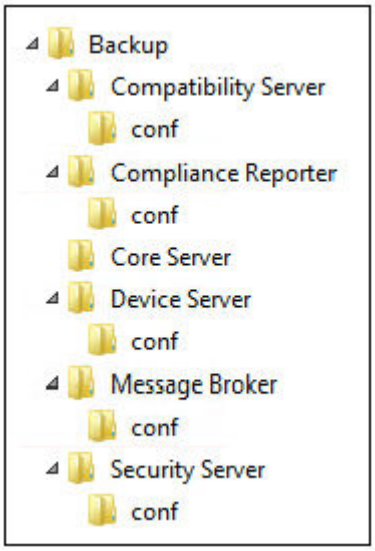
1. As a Dell administrator, log in to the Management Console.
2. In the left menu, click **Management** > **Commit**.
3. In *Comment* enter a description of the change.
4. Click **Commit Policies**.
5. When the commit is complete, log off from the Management Console.

   Ensure that Dell Services are running.
6. From the Windows *Start* menu, click **Start** > **Run**. Type *services.msc* and click **OK**. When *Services* opens, go 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 are needed after the upgrade/migration process is complete.

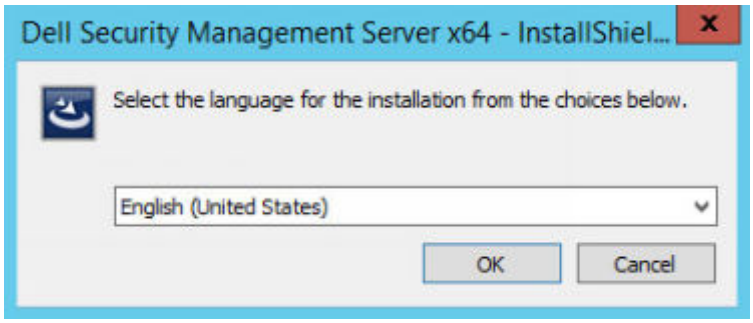
   NOTE:

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



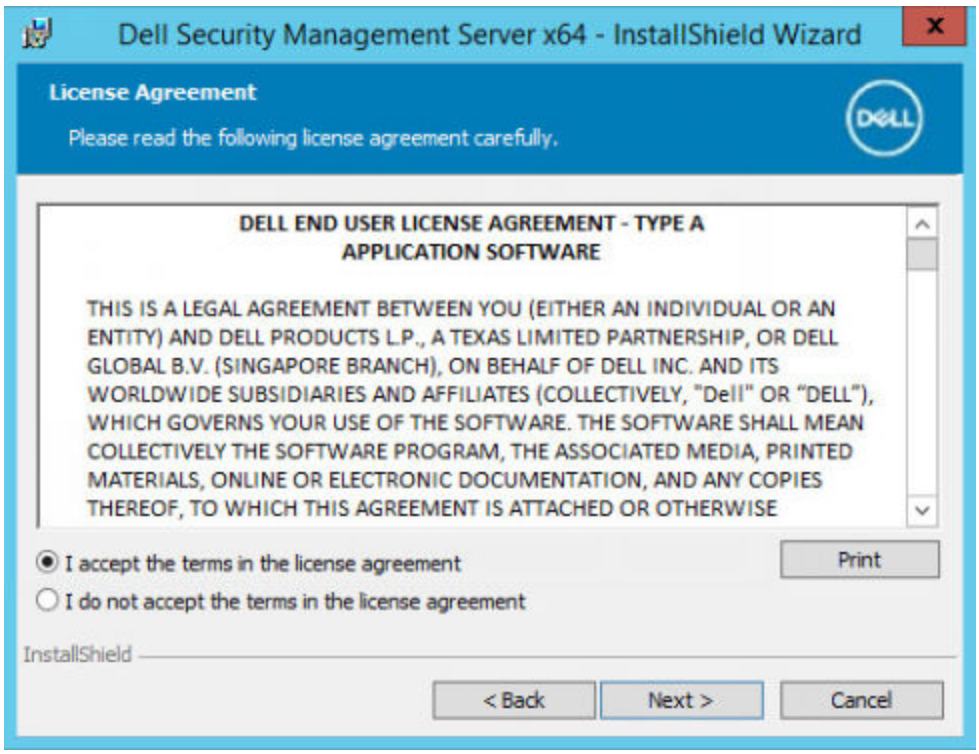
Upgrade/Migrate Back End Server(s)

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

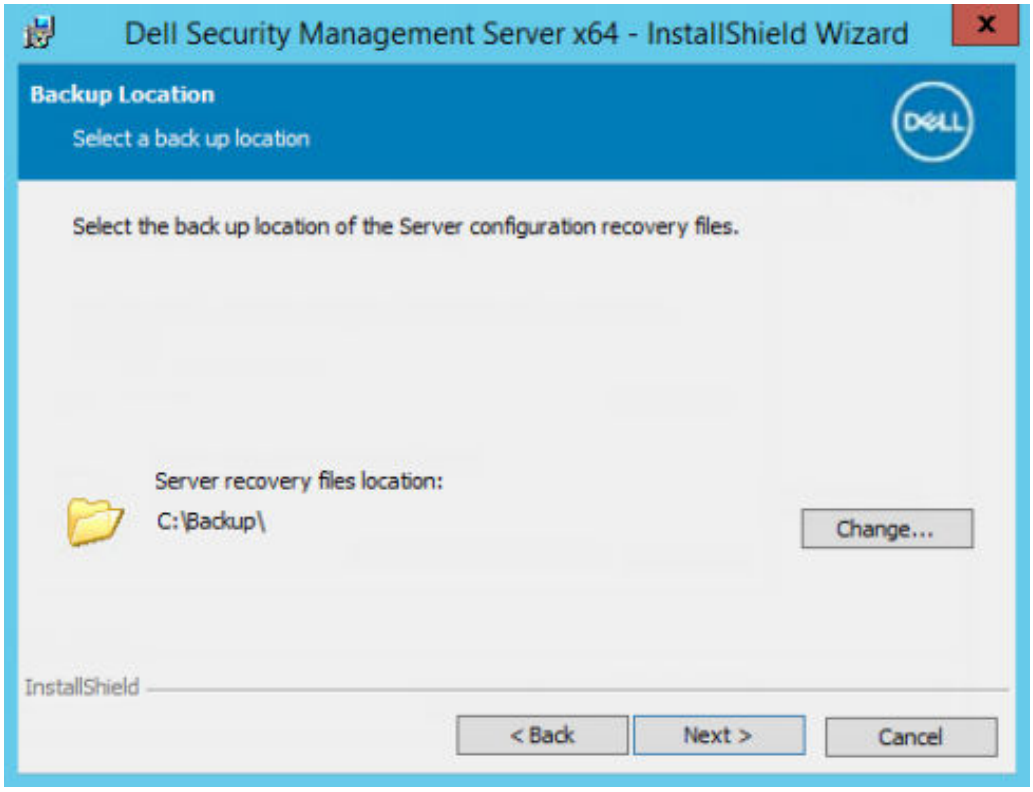


4. In the *Welcome* dialog, click **Next**.

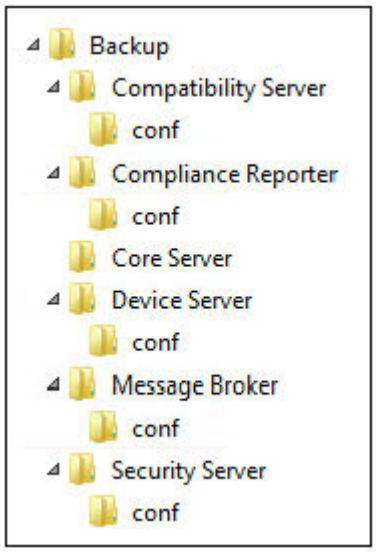
5. Read the license agreement, accept the terms, then click **Next**.



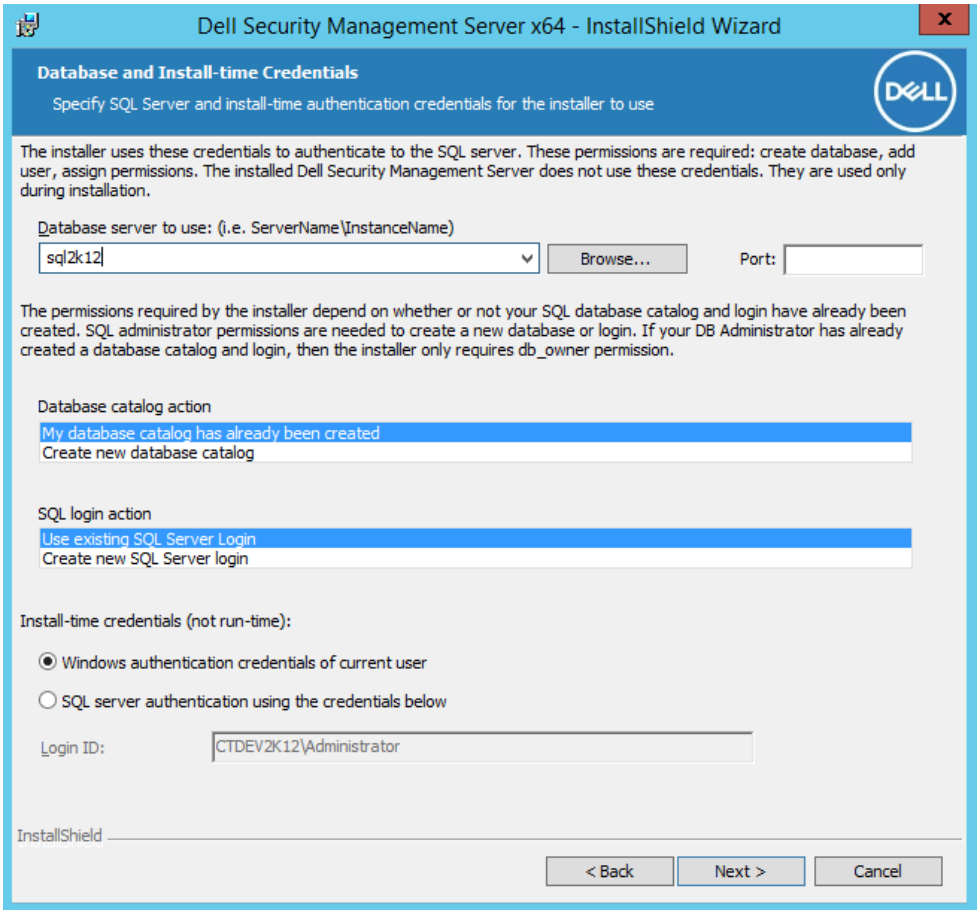
6. To select a location for backup configuration files to be stored, click **Change**, navigate to the desired folder, and click **Next**. Dell recommends that you select a remote network location or external drive for backup.



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 are used for authentication (*User Name* and *Password* are not 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**

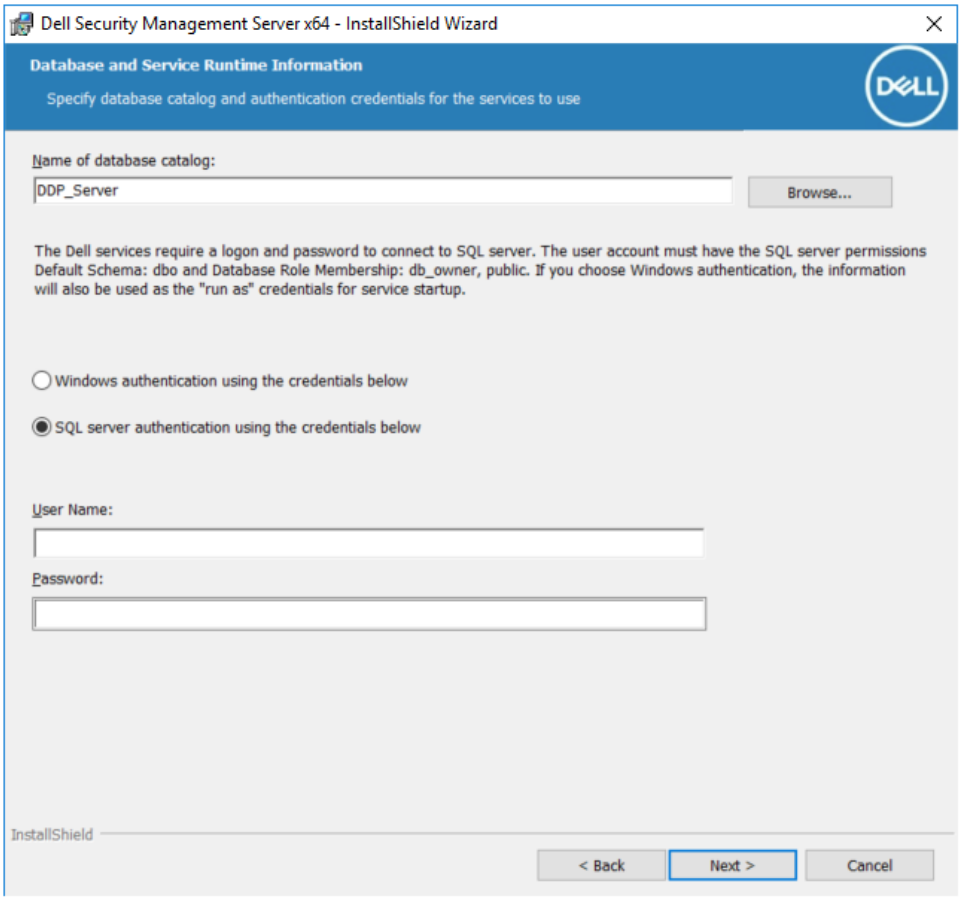
     If you use SQL authentication, the SQL account used must have system administrator rights on the SQL Server.

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

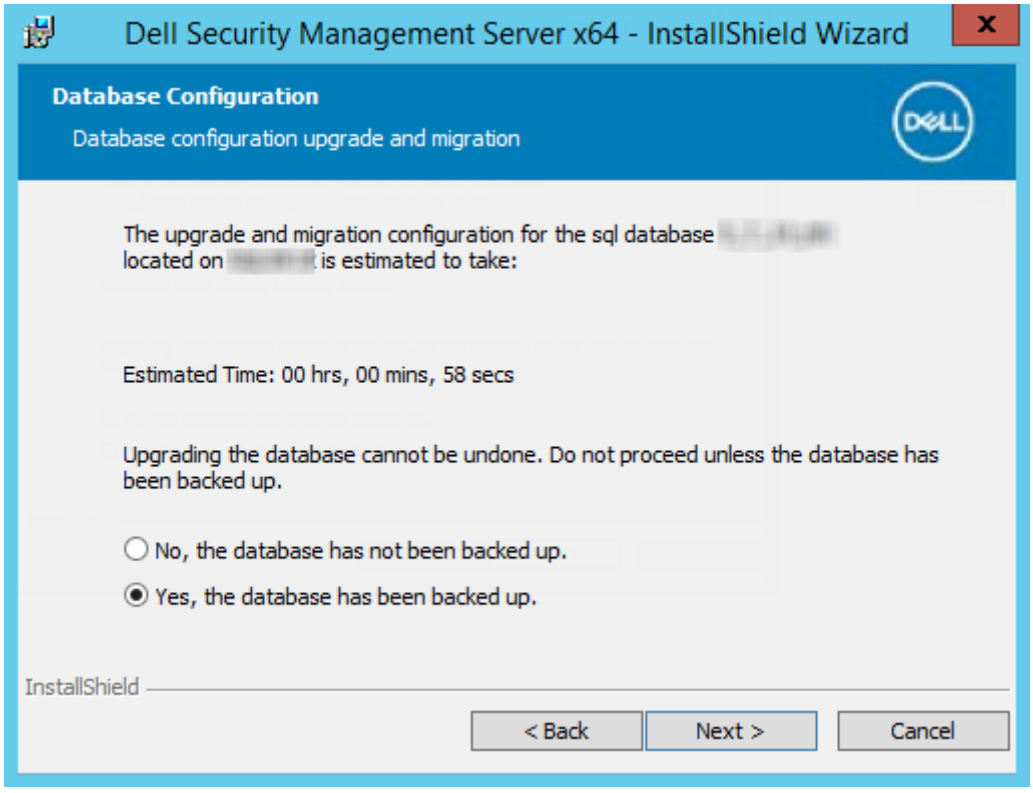
b. Click **Next**.

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**.

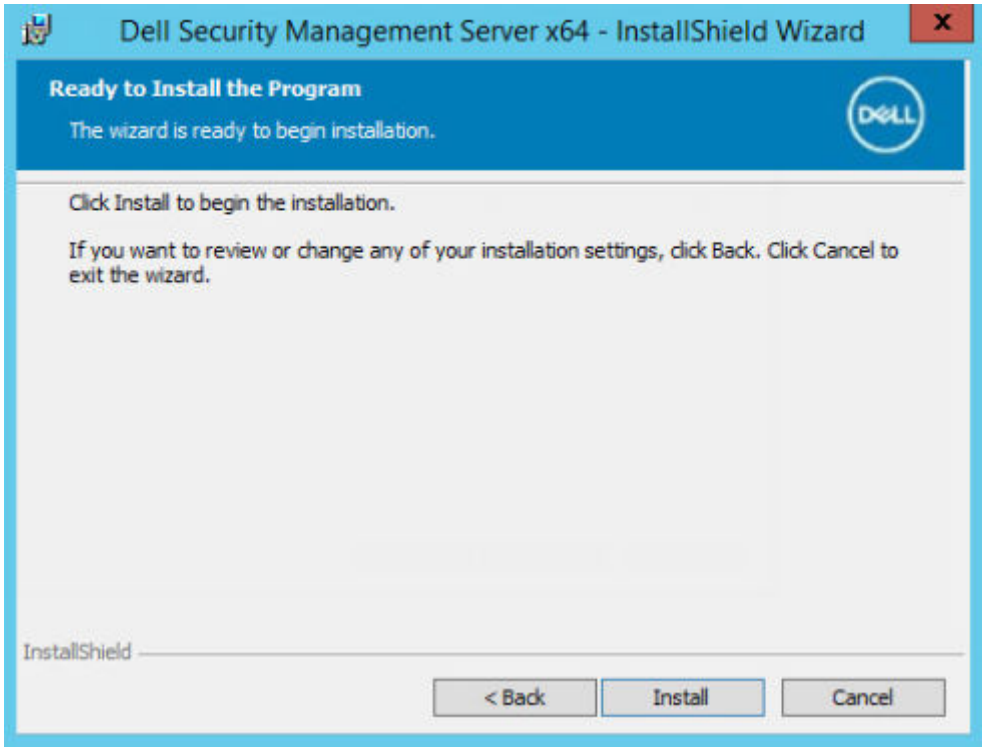
      The user account must be in the format DOMAIN\Username and have the SQL Server permissions Default Schema: dbo and Database Role Membership: dbo_owner, public.



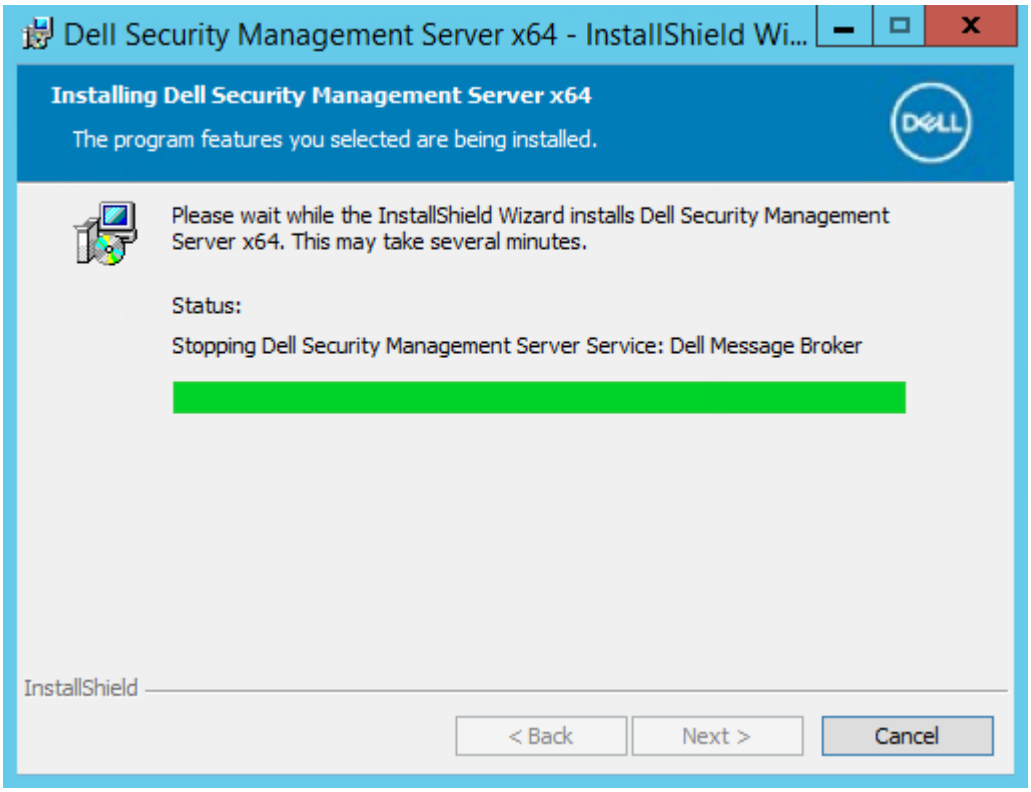
9. If the database is not backed up, you ***must*** back it up before continuing the installation. ***Database upgrade cannot be rolled back.*** Only after the database is backed up, select **Yes**, **the database has been backed up**, and click **Next**.



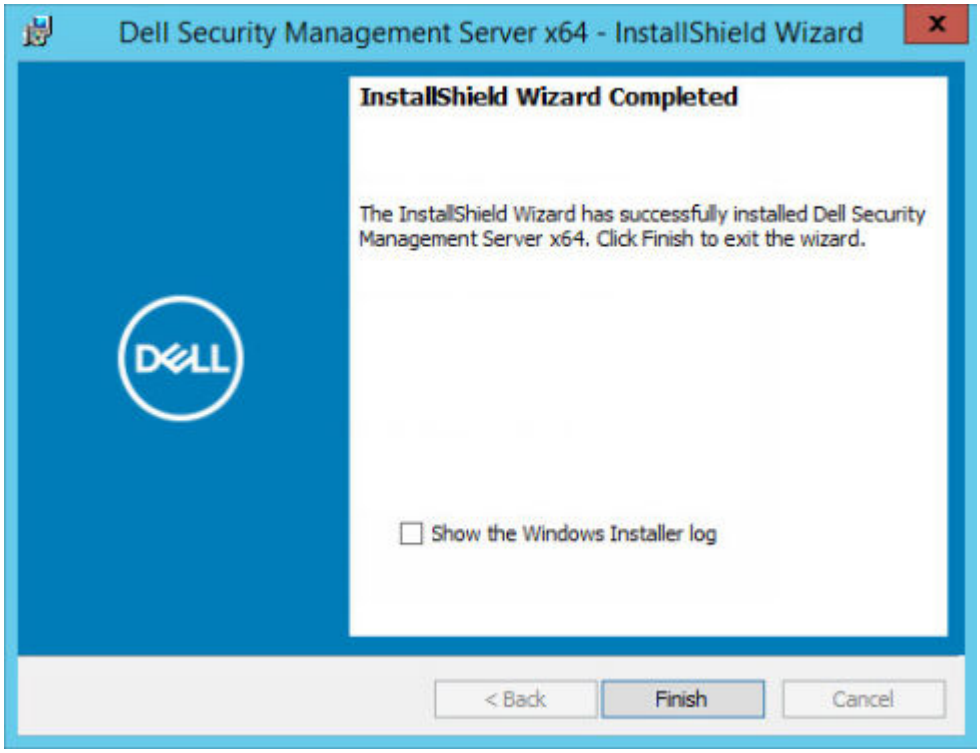
10. Click **Install** to begin the installation.



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 Dell 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

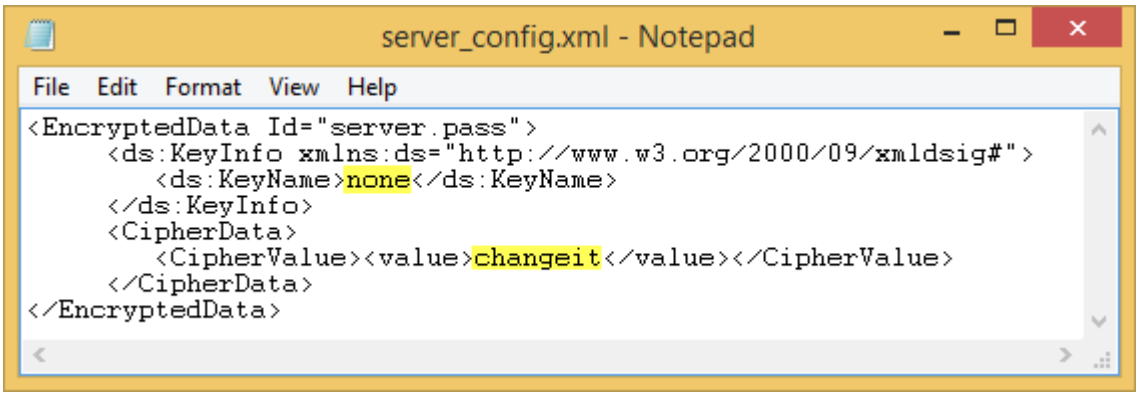
13. In the new installation, open <Compatibility Server install dir>\conf\server_config.xml and replace the **server.pass** value with the value from the backed up <Compatibility Server install dir>\conf\server_config.xml, as follows:

    Instructions for server.pass:

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

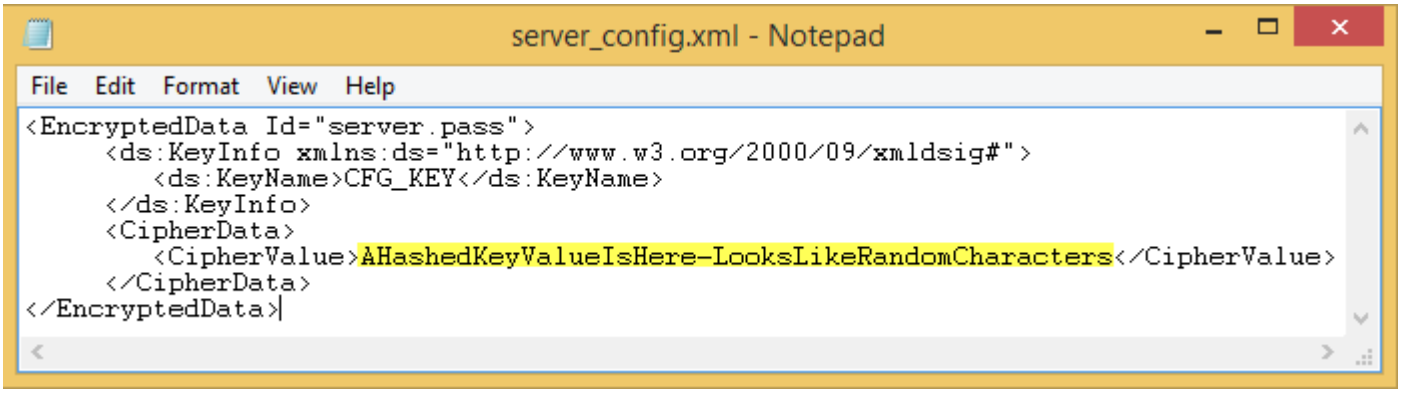
    - Edit the *KeyName* from **CFG_KEY** value to **none**.
    - Enter the plain text password and enclose it between *<value>* *</value>*, which in this example is **<value>changeit</value>**
    - When the Security Management Server starts, the plain text password is hashed, and the hashed value replaces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



Save and close the file.

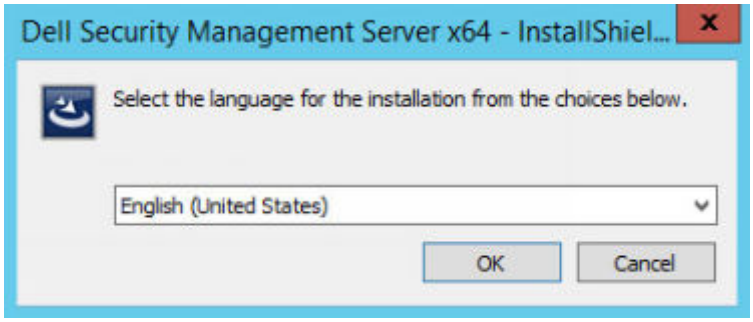
NOTE:

Do not attempt to change the Security Management 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.

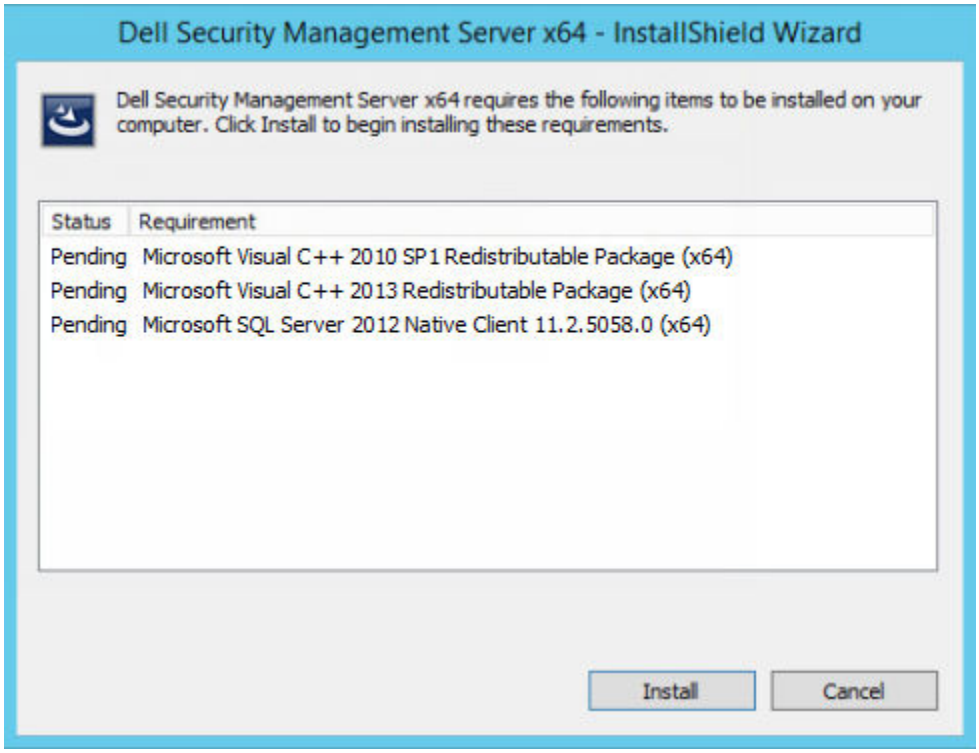
Back end server migration tasks are complete.

Upgrade/Migrate Front End Server(s)

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



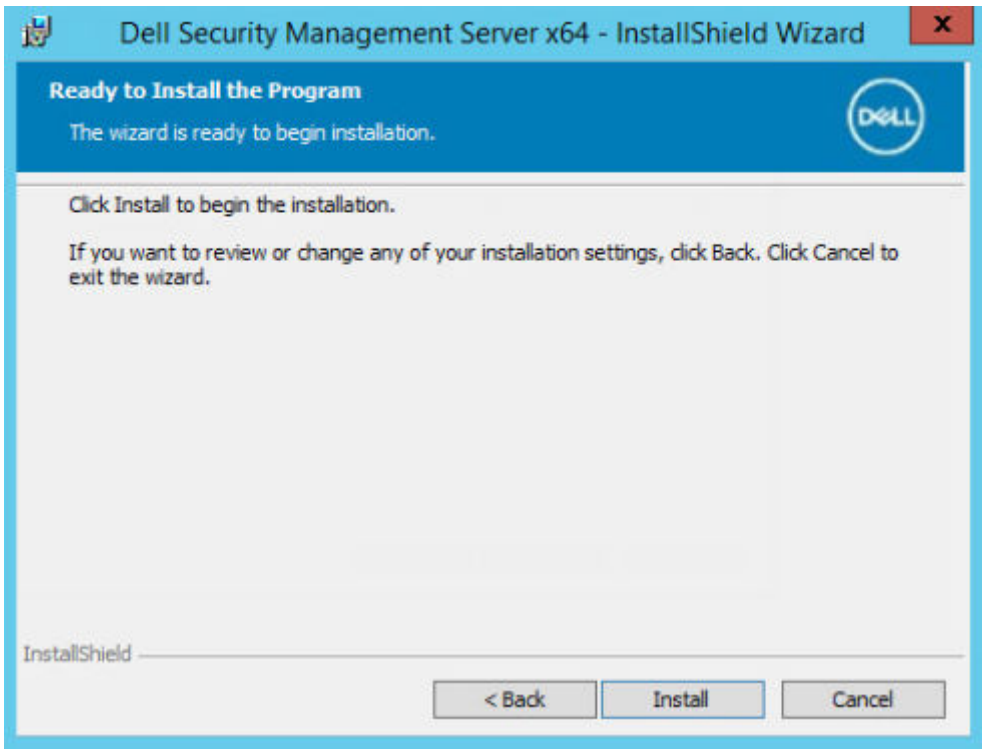
4. If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.



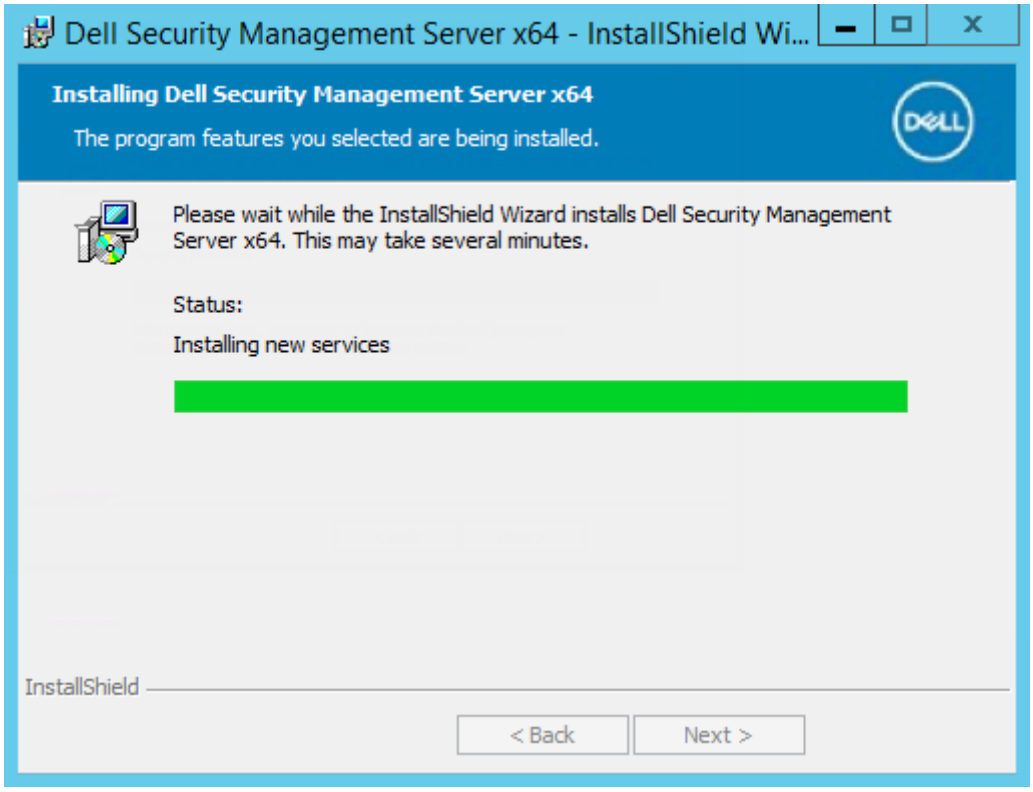
5. In the *Welcome* dialog, click **Next**.

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

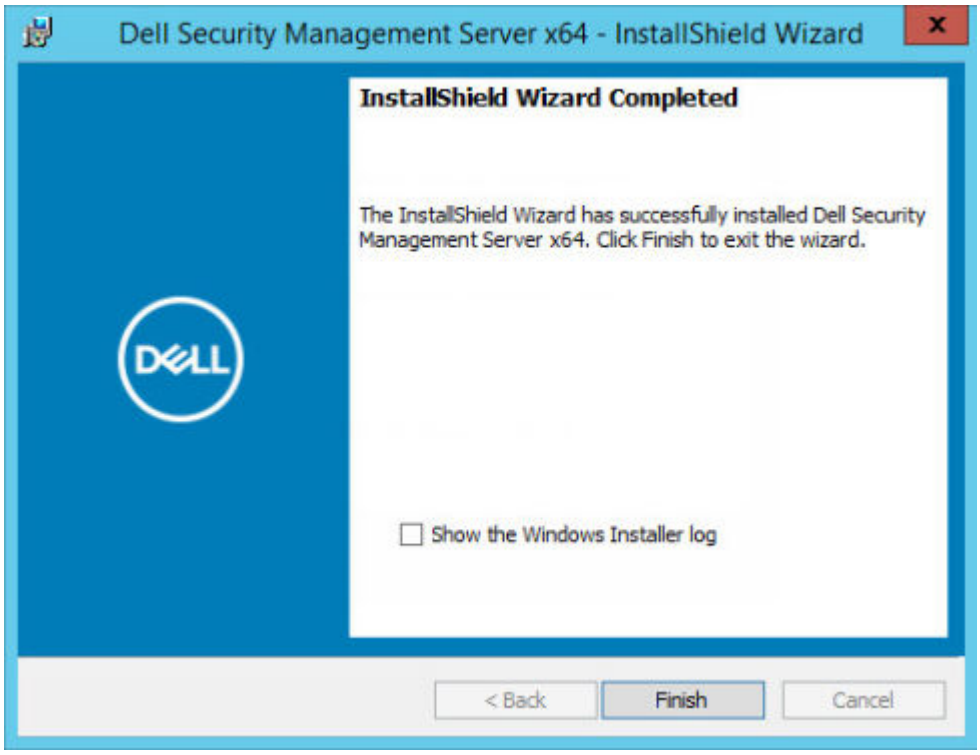
7. In the *Ready to Install the Program* dialog, click **Install**.



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.
   a. On the back end server, go to <Security Server install dir>\conf\ and open the application.properties file.
   b. Locate publicdns.server.host and set the name to an externally resolvable hostname.
   c. 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 Dell Server until Post-Installation Configuration tasks are complete.

Disconnected Mode Installation

Disconnected mode isolates Security Management Server from the Internet and an unsecured LAN or other network. After Security Management Server is installed in Disconnected mode, it remains in Disconnected mode and cannot be changed back to Connected mode.

Security Management 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 are 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 Security Management 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"

Parameters
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. 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 is parsed to get SQL 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 engage with the Security Management 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 user name 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.
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 attempts to add the user's SQL authentication credentials and set privileges to allow the credentials to be used by the product.

Parameters
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.
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 Security Management Server in Disconnected Mode

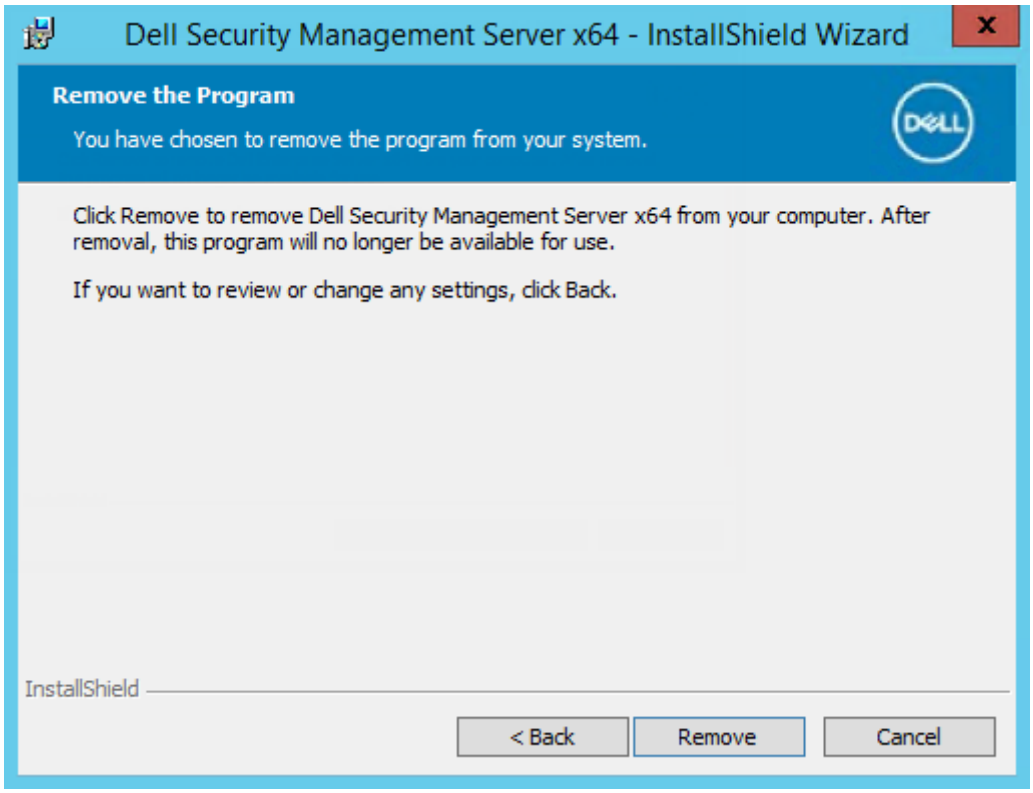
The following example installs Security Management Server in silent mode with a progress dialog, using installation parameters listed in the file, `C:\mysetups\eeoptions.txt\" "`

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

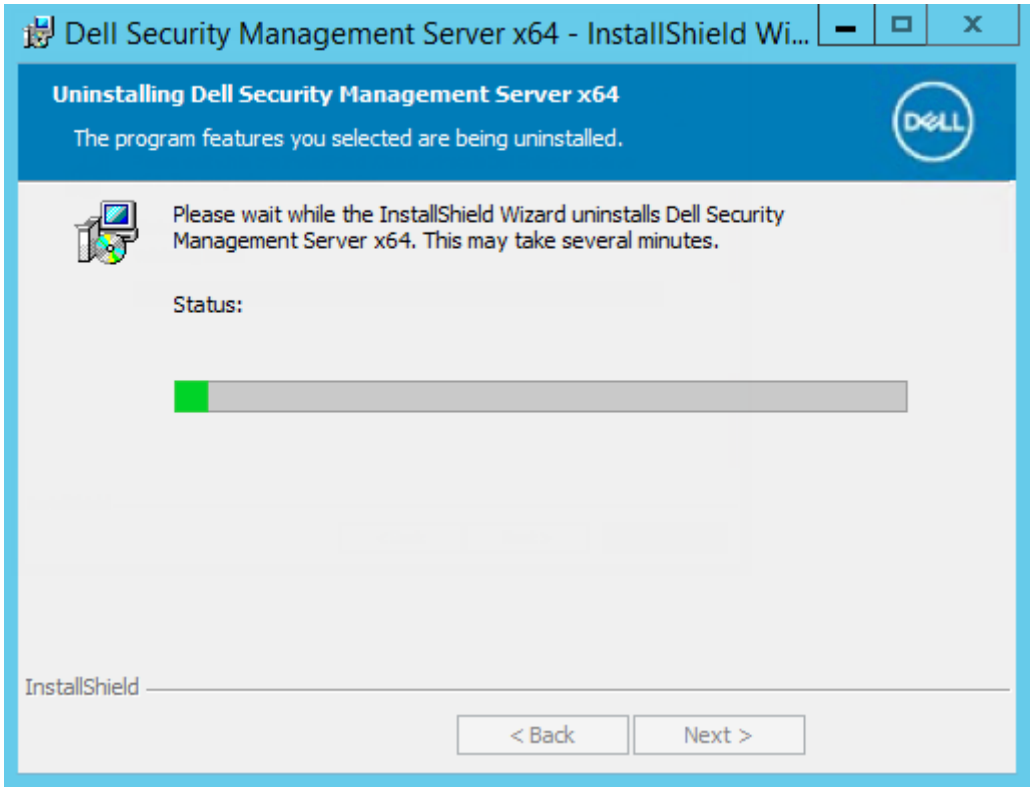
Uninstall Security Management Server

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

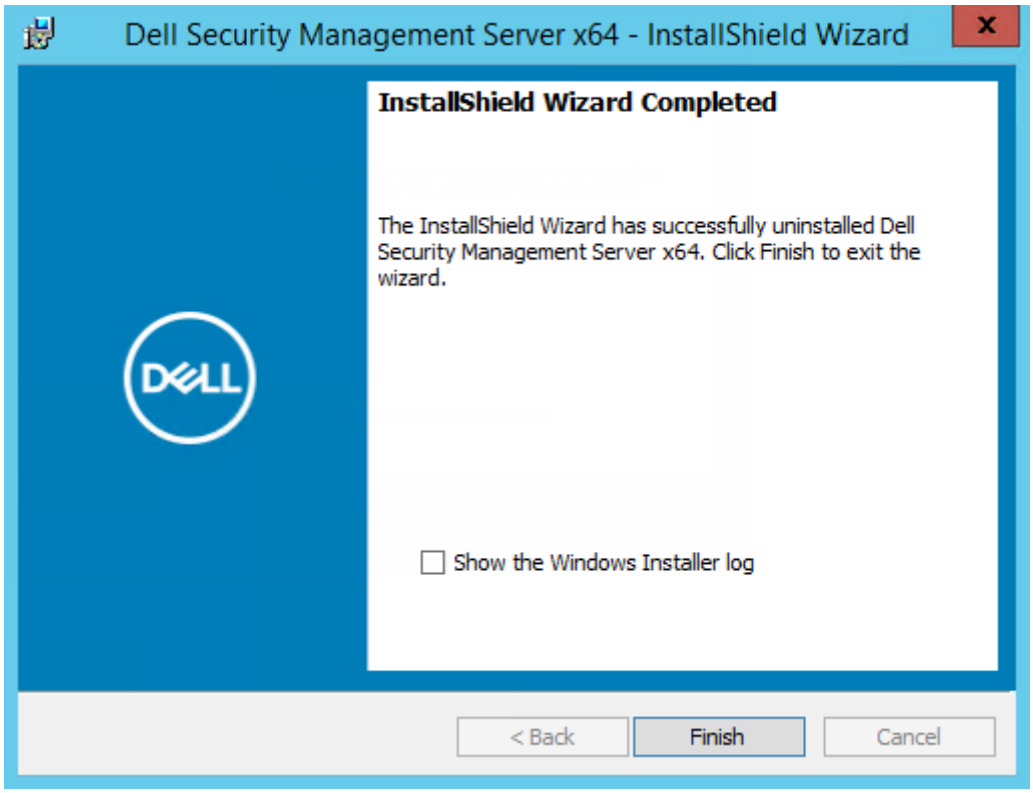
4. In the *Remove the Program* dialog, click **Remove**.



A progress dialog displays status throughout the uninstallation process.



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



5

Post-Installation Configuration

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

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

After installing the Security Management Server, the following defaults should be modified:

- Change the back end server password at the following location:

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

- Change password for every front end server in your environment at the following location:

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

The password displays as follows: `proxy-server.password=ENC(<texthere>)`

To change the password:

1. Select: `ENC(<texthere>)`
2. Change the selected text to: `CLR(<newpasswordhere>)`

   After service restart, the modified line changes to `ENC` from `CLR` and the password is encrypted.

NOTE: The proxy-server.username may also be modified, but this must match within the Message Broker's application.properties file and all active front end servers.

DMZ Mode Configuration

If the 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 Security Server.

If a trusted certificate is being used, disregard this section.

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

For information about updating the certificate for Dell Encryption with an existing certificate in the Microsoft keystore, see http://www.dell.com/support/article/us/en/19/sln297240/.

Timeout properties for Management Console

To modify the timeout property for the Management Console, go to the application.properties file, and modify the default values:

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

Server Configuration Tool

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

The Server Configuration Tool allows you to:

- Add New or Updated Certificates

- Import Dell Manager Certificate
- Import Identity Certificate
- Configure settings for Server SSL Certificate
- Configure SMTP settings for Email Services
- Change Database Name, Location, or Credentials
- Migrate the Database

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

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

  The Server Configuration Tool logs to `C:\Program Files\Dell\Enterprise Edition\Server 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, so on. 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. For 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 is 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, Device Server and so on)
- .NET Applications (Core Server)
- Validation of smart cards used for Preboot Authentication (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 managed Encryption clients with self-encrypting drives, or BitLocker Manager.
- Client Workstations:
  - Workstations running BitLocker Manager
  - Workstations running Encryption Enterprise (Windows)
  - Workstations running Endpoint Security Suite Enterprise

Information regarding which type of certificates to use:

Preboot Authentication using smart cards requires SSL validation with the Security Server. Dell Manager performs SSL validation when connecting to the Dell Core Server. For these types of connections, the signing CA must 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 Security Server Java keystore. 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.

  The Security Management Server is compatible with the Microsoft requirement for LDAP channel binding and LDAP signing when Active Directory is in use.

  To enable this on the Security Management Server, it must have the root issuing certificate for the domain controller certificates that are imported into the "Trusted Root" store within the Microsoft Certificate Key Store.
- Modify the behavior of Server-side SSL validation. To turn off Server-side SSL trust validation, select **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, and so on 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 Security Management Server is used, if available.
3. From the top menu, select **Configuration** > **Save**. If prompted, confirm the save.

Certificate setup 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 Security Management Server is used, if available.
4. From the top menu, select **Configuration** > **Save**. If prompted, confirm the save.

Certificate setup 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 Security Management Serveris 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 that is 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 Security Management Server is 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 that is 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 Security Management 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 that is 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 Security Management Server is used, if available.

    Click **Next**.

    Click **Finish** when complete.

Certificate setup is complete.

When changes are complete:

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

Import Dell Manager Certificate

If your deployment includes Security Management Server remotely-managed clients with Encryption Management Agents, 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 Security Management Server remotely-managed clients and Encryption Management Agent. 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 *File Name*, 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 DM 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 SSL/TLS Certificate BETA

If your deployment includes Server Encryption, you must import your newly created (or existing) certificate. The SSL/TLS Certificate BETA protects the private key which is used to sign the policy bundles being sent to client servers.

1. From the top menu, select **Actions** > **Import SSL/TLS Certificate BETA**.
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

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

Dell Manager:

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

SCEP:

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

NOTE: As of v9.8, Mobile Edition is no longer supported.

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

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

This tab configures SMTP settings for Product Bulletins, notifications, and Advanced Threat Prevention Threat Relay messages.

When configuration changes are complete, restart the Security Server service. The Security Server service must be restarted in order for the settings to be updated.

Enter the following information:

1. In *Host Name*, enter the FQDN of your SMTP server, such as smtpservername.domain.com.
2. In *User Name*, enter the user name to log in to the mail server. The format can be DOMAIN\jdoe, jdoe, or whatever form your organization requires.
3. In *Password*, enter the Password associated with this user name.
4. In *From Address*, 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 *Port*, enter the Port number (typically 25).
6. In the *Authentication* menu, select either *True* or *False*.

NOTE: The username and password should be left blank if authentication is set to 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 *Server Name*, 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*Server Portt*, enter the port number.

   When using a non-default SQL Server instance, you must specify the dynamic port of the instance in *Port:*. 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.
3. In *Database*, enter the name of the database.
4. In *Authentication:*, select either **Windows Authentication** or **SQL Server Authentication**. If you choose Windows Authentication, the same credentials that were used to log in to Windows is used for authentication (*User Name* and *Password* are not editable).
5. In *User Name:*, enter the appropriate user name associated with this database.
6. In *Password:*, enter the password for the user name listed in *User Name*.
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 used to run the Security Management 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.

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 v9.2 or later database to the latest schema with the latest upgrade of the server.

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

1. If you have not yet backed up your existing Dell Server 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**.

6

Administrative Tasks

Assign Dell Administrator Role

1. As a Security Management Server administrator, log in to the Management Console: https://server.domain.com:8443/webui/ . The default credentials are **superadmin/changeit**.
2. In the left pane, click **Populations** > **Domains**.
3. Click a domain 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 display 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 Management Console.
2. Log in to the Management Console and log in 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. In *Comment*, enter a description of the change.
3. Click **Commit Policies**.

Perform Back ups

For the purposes of disaster recovery, ensure that the following locations are backed up weekly, with nightly differentials. For more information about planning for disaster recovery, seehttp://www.dell.com/support/article/us/en/04/sln292355/plan-for-disaster-recovery-and-high-availability-with-dell-security-management-server-dell-data-protection-server?lang=en.

Security Management 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\gkconfig.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, Dell recommends database best practices are used for the Dell Server database and that Dell software is included in your organization's disaster recovery plan.

For additional information on SQL Server best practices, see the following list, which should be implemented when Dell Security is installed if not already implemented.

PostgreSQL Server Backups

Audit events are stored in the PostgreSQL Server at C:\ProgramData\Dell\PostgreSQL\10.7\data, which should be routinely backed up. For backup instructions, refer to /C:/ProgramData/Dell/PostgreSQL/10.7/data.

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.

7

Ports

The following table describes each component and its function.

Name	Default Port	Description
ACL Service	TCP/ 8006	Manages various permissions and group access for various Dell Security products. **NOTE:** Port 8006 is not secured. Ensure that this port is properly filtered through a firewall. This port is internal only.
Management Console	HTTP(S)/ 8443	Administration console and control center for the entire enterprise deployment.
Core Server	HTTPS/ 8888	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Prevention. Processes inventory data for use by the Management Console. Collects and stores authentication data. Controls role-based access.
Device Server	HTTPS/ 8081	Supports activations and password recovery. A component of the Security Management Server. Required for Encryption Enterprise (Windows and Mac)
Security Server	HTTPS/ 8443	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, SED-PBA and Full Disk Encryption-PBA communication, and Active Directory for authentication or reconciliation. This includes identity validation for authentication into the Management Console. Requires SQL database access.
Compatibility Server	TCP/ 1099	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. **NOTE:** Port 1099 should be filtered through a firewall. Dell

Name	Default Port	Description
		Technologies recommends this port be internal only.
Message Broker Service	TCP/ 61616 and STOMP/ 61613	Handles communication between services of the Dell Server. Stages policy information that the Compatibility Server creates for Policy Proxy queuing. Requires SQL database access. **NOTE:** Port 61616 should be filtered through a firewall. Dell Technologies recommends this port be internal only. **NOTE:** Only open port 61613 to Security Management Servers configured in Front-End mode.
Key Server	TCP/ 8050	Negotiates, authenticates, and encrypts a client connection using Kerberos APIs. Requires SQL database access to pull the key data.
Policy Proxy	TCP/ 8000	Provides a network-based communication path to deliver security policy updates and inventory updates.
PostGres	TCP/ 5432	Local database used for eventing data. **NOTE:** Port 5432 should be filtered through a firewall. Dell Technologies recommends this port be internal only.
LDAP	TCP/ 389/636 (local domain controller), 3268/3269 (global catalog) TCP/ 135/ 49125+ (RPC)	Port 389 - This port is used for requesting information from the local domain controller. LDAP requests sent to port 389 can be used to search for objects only within the home domain of the global catalog. However, the requesting application can obtain all the attributes for those objects. For example, a request to port 389 could be used to obtain a user's department. Port 3268 - This port is used for queries that are specifically targeted for the global catalog. LDAP requests sent to port 3268 can be used to search for objects in the entire forest. However, only the attributes marked for replication to the global catalog can be returned. For example, a user's department could not be returned using port 3268 since this attribute is not replicated to the global catalog.

Name	Default Port	Description
Microsoft SQL Database	TCP/ 1433	The default SQL Server port is 1433, and client ports are assigned a random value 1024–5000.
Client Authentication	HTTPS/ 8449	Allows client servers to authenticate with Dell Server. Required for Server Encryption.

8

SQL Server Best Practices

The following list explains SQL Server best practices, which should be implemented when Dell security 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."

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 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3. 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 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

4. Ensure that all Indexes are covered by a weekly maintenance job to rebuild the indexes.

5. Validate that permissions and features are appropriate for the database leveraged by the Security Management Server. For more information, see KB article 124909.

9

Certificates

This chapter explains how to obtain certificates for use with Security Management Server.

For information on how to configure to configure SmartCard Authentication, see http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en.

For information about the minimum requirements to request SSL/TLS certificates for use by the Dell Data Security server, see http://www.dell.com/support/article/us/en/19/sln307037/dell-data-protection-enterprise-edition-and-virtual-edition-dell-security-management-sever-and-virtual-server-ssl-tls-certificate-minimum-requirements?lang=en.

For information about updating the certificate for Dell Encryption with an existing certificate in the Microsoft keystore, see http://www.dell.com/support/article/us/en/19/sln297240/.

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.

Dell recommends 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 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. Go to the **conf** directory of Security Server or 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 Security Management Server.

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

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

<Security Server install dir>\conf\application.properties. Set the value 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 hostname 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 or region code.
- The utility prompts for confirmation that the information is correct. If information is correct, type **yes**.

  If information is not correct, type **no**. The Keytool displays each value that was 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.

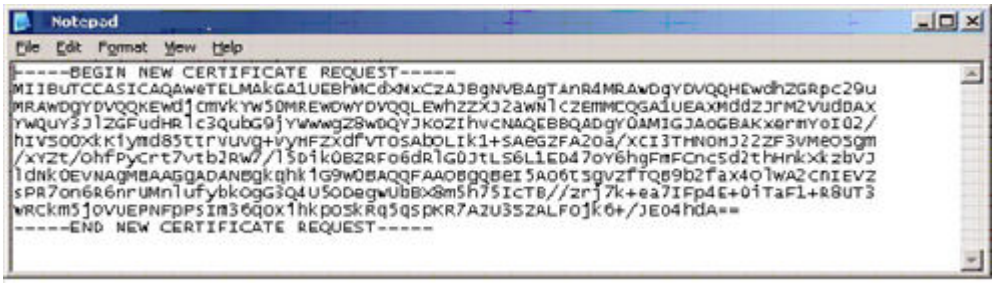
1. Substitute the same value used previously for <**certificatealias**>:

   ```
   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 contains a BEGIN/END pair to use 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 prevents having to start the process over.

Import a Root Certificate

If the root certificate Certificate Authority is Verisign (but not Verisign Test), go 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 Security Server or Device Server, change to the component **conf** directory.
   - If you are enabling SSL between the Security Management 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>
   ```

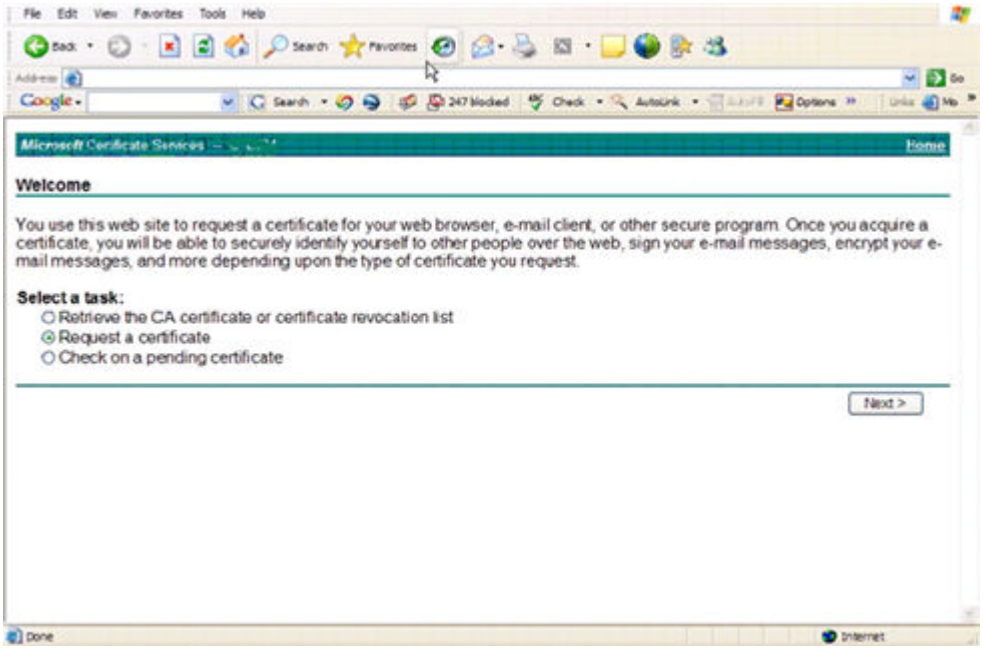
   For example, **keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer**

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 is set up internally by your organization.

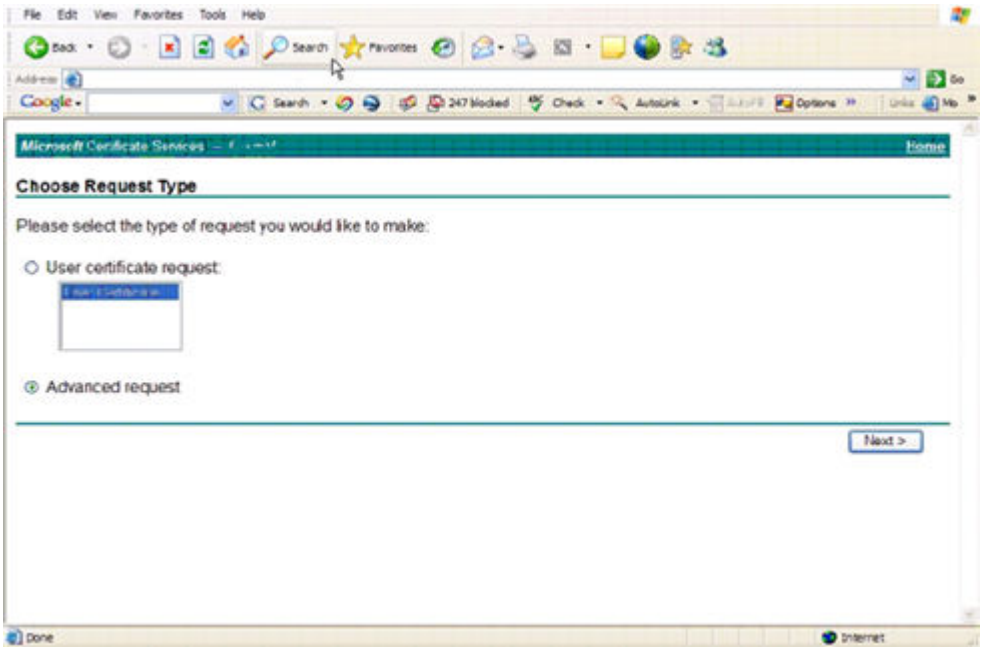
1. Navigate to the Microsoft CA Server. The IP address is supplied by your organization.
2. Select **Request a certificate** and click **Next**.

   Microsoft Certificate Services



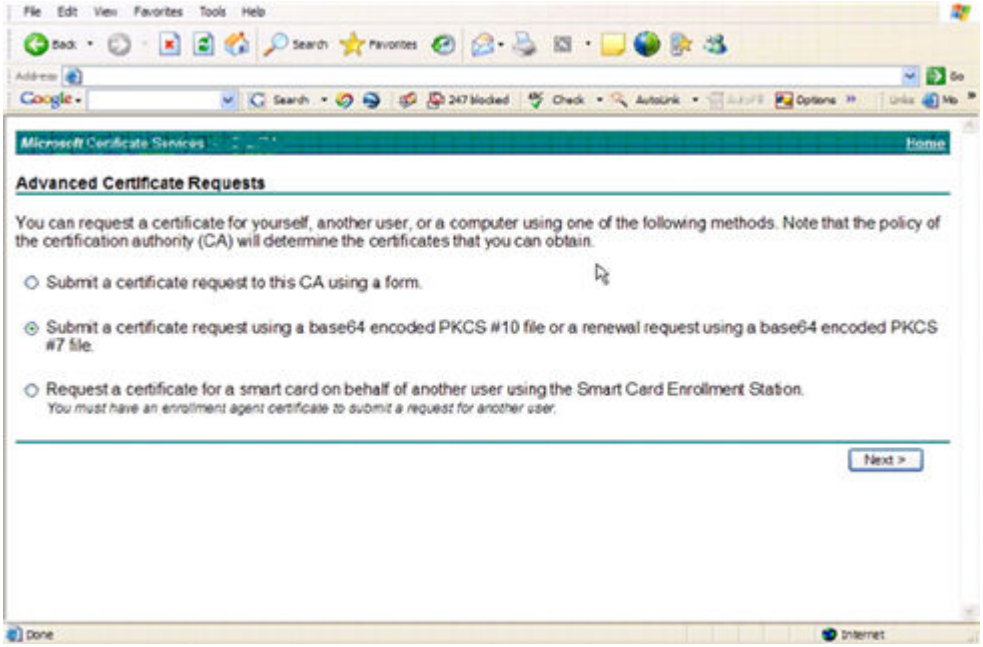
3. Select **Advanced Request** and click **Next**.

   Choose Request Type



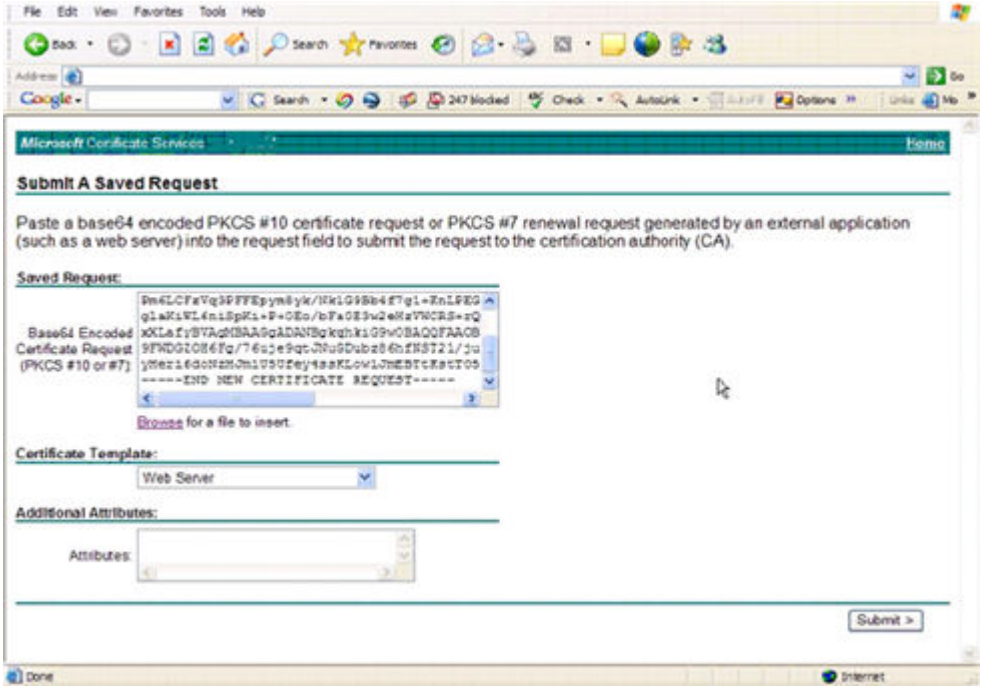
4. Select the option to **Submit a certificate request using a base64 encode PKCS #10 file** and click **Next**.

Advanced Certificate Request



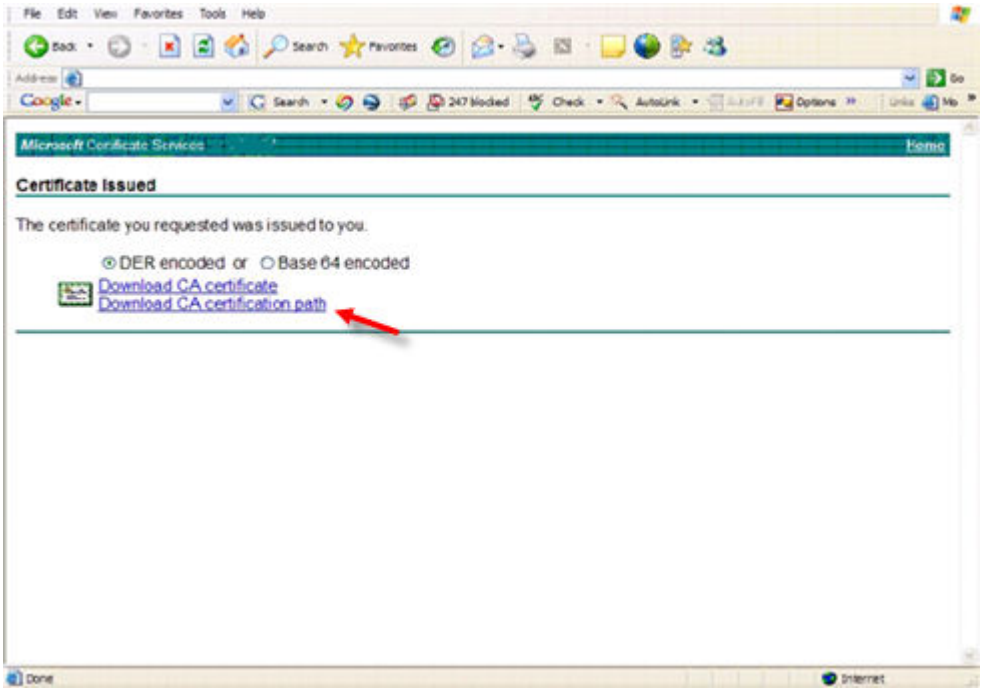
5. Paste in the contents of the CSR request in the text box. Select a certificate template of **Web Server** and click **Submit**.

Submit a Saved Request



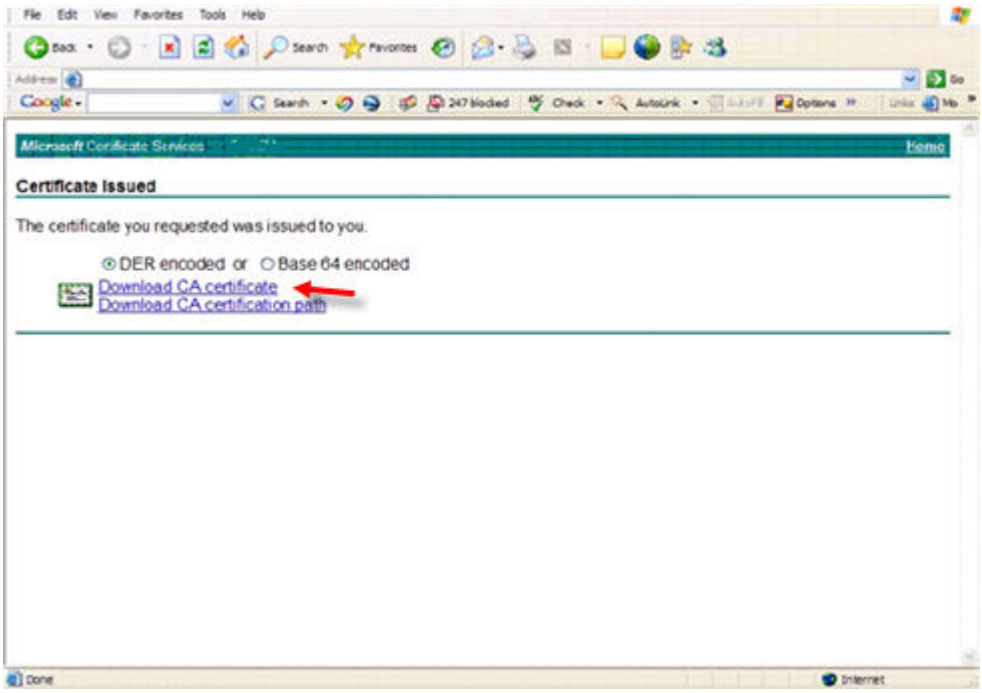
6. Save the certificate. Select **DER encoded** and click **Download CA certificate**.

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 command prompt. 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 shows 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 Security Server is used in DMZ mode *and* when importing a Dell Manager certificate into the 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 *File Name*, 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.