Dell Security Management Server

Installations- und Migrationshandbuch v10.2.12

August 2020
Rev. A01

Hinweise, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS warnt vor möglichen Beschädigungen der Hardware oder vor Datenverlust und zeigt, wie diese vermieden werden können.

WARNUNG: Mit WARNUNG wird auf eine potenziell gefährliche Situation hingewiesen, die zu Sachschäden, Verletzungen oder zum Tod führen kann.

Inhaltsverzeichnis

1

Einleitung

Informationen zu Security Management Server

Der Security Management Server bietet die folgenden Funktionen:

- Zentrale Verwaltung von Geräten, Benutzern und Sicherheitsrichtlinie
- Zentrale Compliance-Prüfverfahren und -Berichterstellung
- Aufteilung administrativer Aufgaben
- Erstellung und Verwaltung rollenbasierter Sicherheitsrichtlinien
- Verteilung von Sicherheitsrichtlinien bei Herstellung einer Client-Verbindung
- Gerätewiederherstellung durch einen Administrator
- Vertrauenswürdige Kommunikation zwischen Komponenten
- Generierung eindeutiger Verschlüsselungsschlüssel und automatische, sichere Schlüsselhinterlegung

Kontaktieren des Dell ProSupports

Telefonischen Support rund um die Uhr für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport – Internationale Telefonnummern.

2

Anforderungen und Architektur

In diesem Abschnitt werden die Hardware- und Softwareanforderungen und Architektur-Design-Empfehlungen für die Implementierung von Dell Security Management Server erläutert.

Architektur-Design von Security Management Server

Encryption Enterprise- und Endpoint Security Suite Enterprise-Lösungen sind basierend auf der Anzahl an Endpunkten zur Verschlüsselung in Ihrer Organisation hochgradig skalierbare Produkte.

Architekturkomponenten

Nachstehend finden Sie empfohlene Hardware-Konfigurationen, die sich für die meisten Umgebungen eignen.

Security Management Server

- Betriebssystem: Microsoft Windows Server 2012 R2 (Standard, Datacenter 64-Bit), Windows Server 2016 (Standard, Datacenter 64-Bit), Windows Server 2019 (Standard und Datacenter)
- Virtuelle/physische Maschine
- CPU: 4 Kern(e)
- RAM: 16,00 GB
- Laufwerk C: 30 GB freier Festplattenspeicher für Protokolle und Anwendungsdatenbanken

  ANMERKUNG: Bis zu 10 GB können für eine lokale Ereignisdatenbank mit PostgreSQL verbraucht werden.

Proxy-Server

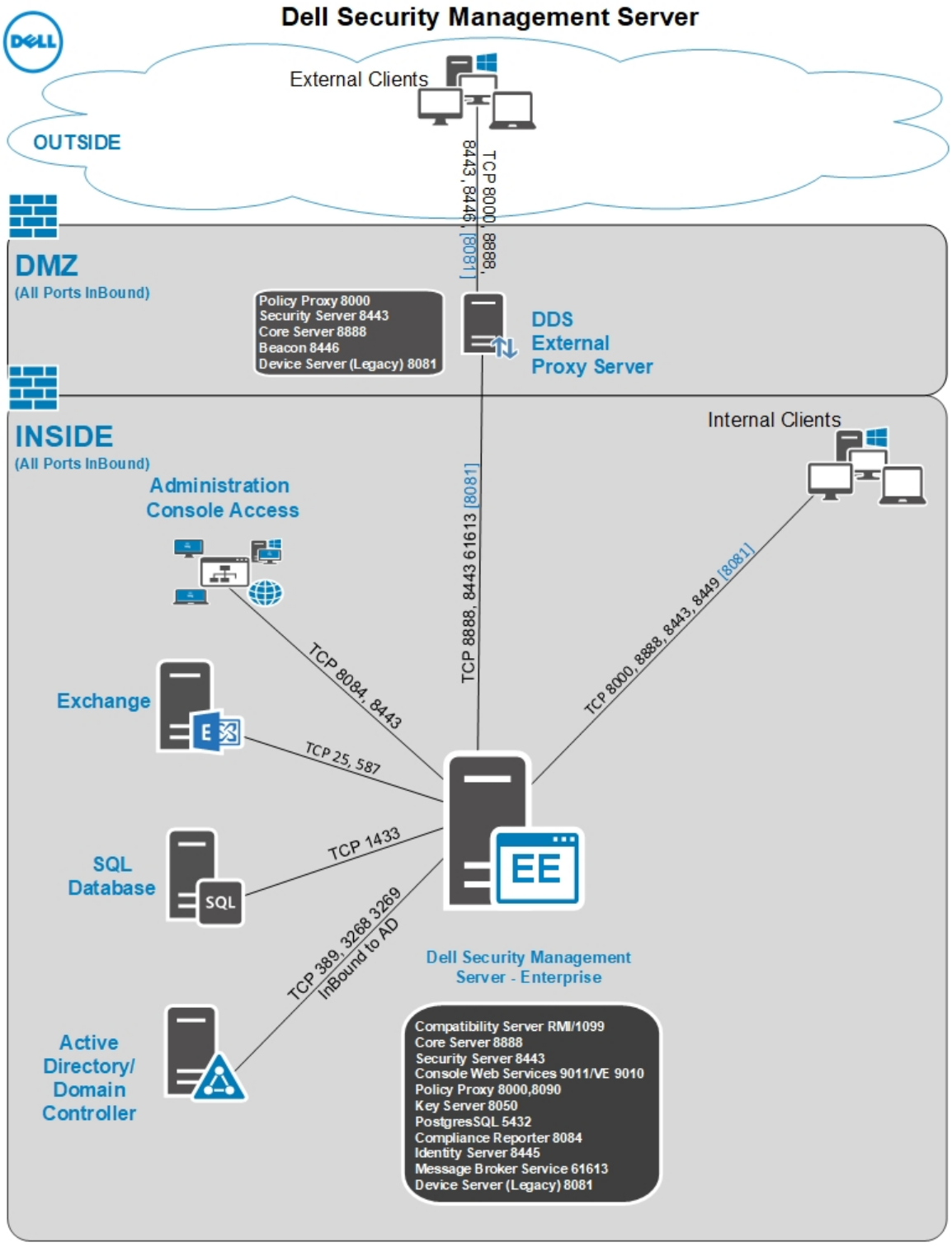
- Betriebssystem: Microsoft Windows Server 2012 R2 (Standard, Datacenter 64-Bit), Windows Server 2016 (Standard, Datacenter 64-Bit), Windows Server 2019 (Standard und Datacenter)
- Virtuelle/physische Maschine
- CPU: 2 Kern(e)
- RAM: 8,00 GB
- Laufwerk C: 20 GB freier Festplattenspeicher für Protokolle

SQL Server - Hardwarespezifikationen

- CPU: 4 Kern(e)
- RAM: 24,00 GB
- Datenlaufwerk: 100 bis 150 GB verfügbaren Speicherplatz (dies kann variieren je nach Umgebung)
- Protokolllaufwerk: 50 GB freier Speicherplatz (dies kann variieren je nach Umgebung)

  ANMERKUNG: Dell empfiehlt, dass Sie die SQL Server Best Practices befolgen, obwohl die oben genannten Informationen den Großteil von Umgebungen abdecken sollten.

Im Folgenden ist eine einfache Bereitstellung für Dell Security Management Server beschrieben.



ANMERKUNG: Falls die Organisation mehr als 20.000 Endpunkte hat, bitten Sie den ProSupport von Dell um Hilfe.

Requirements

Die Hardware- und Softwarevoraussetzungen für die Installation der Software Security Management Server sind unten aufgeführt.

Bevor Sie die Installation beginnen, stellen Sie sicher, dass alle Patches und Aktualisierungen auf den Servern, die zur Installation verwendet werden, angewendet wurden.

Hardware

In der folgenden Tabelle sind die Details der *Hardware-Mindestanforderungen* für Security Management Server aufgeführt. Siehe Architektur-Design von Security Management Server für zusätzliche Informationen zur Skalierung basierend auf der Größe Ihrer Bereitstellung.

Hardwareanforderungen
Prozessor Moderne Quad-Core-CPU (1,5 GHz+)
RAM 16 GB
Freier Speicherplatz 20 GB freier Speicherplatz **ANMERKUNG:** Bis zu 10 GB können für eine lokale Ereignisdatenbank mit PostgreSQL verbraucht werden
Netzwerkkarte 10/100/1000 oder besser
Sonstiges IPv4 oder IPv6 oder IPv4/IPv6-Hybridumgebung erforderlich

In der folgenden Tabelle sind die Details der *minimalen* Hardwareanforderungen für Front-End/Proxy Server eines Security Management Server aufgeführt.

Hardwareanforderungen
Prozessor Moderne Dual-Core CPU
RAM 8 GB
Freier Speicherplatz 20 GB freier Speicherplatz für Protokolldateien
Netzwerkkarte 10/100/1000 oder besser
Sonstiges IPv4 oder IPv6 oder IPv4/IPv6-Hybridumgebung erforderlich

Virtualisierung

Der Security Management Server kann in einer virtuellen Umgebung installiert werden. Nur die folgenden Umgebungen werden empfohlen.

Security Management Server v10.2.11 wurde auf den folgenden Plattformen validiert.

Hyper-V Server wird als Voll- oder Core-Installation oder als Rolle in Windows Server 2012, Windows Server 2016 oder Windows Server 2019 installiert.

- Hyper-V Server
  - 64-Bit x86 CPU erforderlich

- Hostcomputer mindestens mit Doppelkern
- Mindestens 8 GB RAM empfohlen
- Die Hardware muss die Mindestanforderungen für Hyper-V erfüllen.
- Mindestens 4 GB RAM für dedizierte Bildressource
- Muss als virtuelle Maschine der 1. Generation ausgeführt werden.
- Weitere Informationen finden Sie unter https://technet.microsoft.com/en-us/library/hh923062.aspx

Security Management Server v10.2.11 wurde mit VMware ESXi 6.0, VMware ESXi 6.5 und VMware ESXi 6.5 validiert.

ANMERKUNG: Beim Ausführen von VMware ESXi und Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019 werden VMXNET3 Ethernet-Adapter empfohlen.

- VMware ESXi 6.0
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-60/index.jsp
- VMware ESXi 6.5
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-65/index.jsp
- VMware ESXi 6.7
  - 64-Bit x86 CPU erforderlich
  - Hostcomputer mindestens mit Doppelkern
  - Mindestens 8 GB RAM empfohlen
  - Unter http://www.vmware.com/resources/compatibility/search.php finden Sie eine vollständige Liste der unterstützten Host-Betriebssysteme
  - Die Hardware muss die Mindestanforderungen für VMware erfüllen
  - Mindestens 4 GB RAM für dedizierte Bildressource
  - Weitere Informationen finden Sie unter http://pubs.vmware.com/vsphere-65/index.jsp

ANMERKUNG: Die SQL Server-Datenbank, auf der Security Management Server gehostet wird, muss aus Leistungsgründen auf einem anderen Computer ausgeführt werden.

SQL-Server

In größeren Umgebungen wird empfohlen, dass der SQL-Datenbankserver auf einem redundanten System ausgeführt wird, wie z. B. einem SQL-Cluster, um die Verfügbarkeit und Datenkontinuität sicherzustellen. Es wird auch empfohlen, täglich eine vollständige Sicherung mit aktivierter Transaktionsprotokollierung auszuführen, um sicherzustellen, dass neu durch Benutzer-/Geräteaktivierung generierte Schlüssel wiederherstellbar sind.

Aufgaben zur Datenbankwartung sollten den Neuaufbau von Datenbankindizes und das Sammeln von Statistik einschließen.

Software

In der folgenden Tabelle sind die Software-Anforderungen für den Security Management Server und den Proxy-Server enthalten.

ANMERKUNG: Aufgrund der sensiblen Daten, die der Security Management Server enthält, und zur Einhaltung der Regel der geringsten Rechte wird eine Installation des Security Management Servers auf einem eigenen Betriebssystem oder als Teil eines Anwendungsservers empfohlen, auf dem eingeschränkte Rollen und Berechtigungen aktiviert sind, um eine sichere Umgebung

sicherzustellen. Zur Empfehlung gehört auch, den Security Management Server auf privilegierten Infrastrukturservern nicht zu installieren. Weitere Informationen zur Implementierung der Regel der geringsten Rechte finden Sie unter https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models.

ANMERKUNG: Die universelle Kontensteuerung (UAC) muss bei der Installation in einem geschützten Verzeichnis deaktiviert sein. Nach der Deaktivierung des UAC, müssen Sie den Server neu starten, damit diese Änderungen in Kraft treten.

ANMERKUNG: Registrierungspfade für Policy Proxy (sofern installiert): HKLM\SOFTWARE\Wow6432Node\Dell

ANMERKUNG: Registrierungspfad für Windows Server: HKLM\SOFTWARE\Dell

Voraussetzungen
• **Visual C++ 2010 Redistributable-Paket** Wenn sie nicht installiert ist, installiert der Installer sie für Sie. • **Visual C++ 2013 Redistributable-Paket** Wenn sie nicht installiert ist, installiert der Installer sie für Sie. • **Visual C++ 2015 Redistributable-Paket** Wenn sie nicht installiert ist, installiert der Installer sie für Sie. • **.NET Framework Version 4.6.1** • **.NET Framework Version 4.5** Für .NET Framework Version 4.6.1 und 4.5 hat Microsoft Sicherheitsupdates veröffentlicht. • **.NET Framework Version 3.5 SP1** • **SQL Native Client 2012** Wenn Sie SQL Server 2012 oder SQL Server 2016 verwenden. Wenn sie nicht installiert ist, installiert der Installer sie für Sie.

Security Management Server – Back-End-Server und 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 **ANMERKUNG:** Dell Security Management Server, der in einer Back-End-Konfiguration oder einer Front-End-Konfiguration installiert ist, unterstützt derzeit keine Betriebssystemupgrades des Windows-Server-Betriebssystems.
LDAP-Repository
• Active Directory 2008 R2 • Active Directory 2012 R2 • Active Directory 2016

ANMERKUNG: Der Security Management Server ist kompatibel mit der Microsoft Anforderung für die LDAP-Kanalbindung und LDAP-Signierung, wenn Active Directory verwendet wird.

Verwaltungskonsole and Compliance Reporter

- Internet Explorer 41.x oder höher
- Google Chrome 46.x oder höher
- Microsoft Edge (Chromium)
- Microsoft Edge

ANMERKUNG: Ihr Browser muss Cookies akzeptieren.

Empfohlene virtuelle Umgebungen für Security Management Server-Komponenten

Der Security Management Server kann in einer virtuellen Umgebung installiert werden.

Dell unterstützt derzeit das Hosten von Dell Security Management Server oder Dell Security Management Server Virtual innerhalb einer in der Cloud gehosteten Infrastructure-as-a-Service (IaaS)-Umgebung, wie z. B. Amazon Web Services, Azure und mehrere andere Anbieter. Die Unterstützung dieser Umgebungen ist auf die Funktionalität von Security Management Server beschränkt. Die Verwaltung und Sicherheit dieser Virtual Machines obliegen dem Administrator der IaaS-Lösung.

Zusätzliche Infrastruktur-Anforderungen Zusätzliche Infrastruktur-Anforderungen, wie z. B. Active Directory und SQL Server, sind für ordnungsgemäße Funktionalität weiterhin erforderlich.

ANMERKUNG: Die SQL Server-Datenbank, auf der Security Management Server gehostet wird, muss auf einem anderen Computer ausgeführt werden.

Datenbank

- **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

ANMERKUNG: Der Einsatz von Express Editionen in Produktionsumgebungen wird nicht unterstützt. Express Editionen werden möglicherweise nur für Machbarkeitsnachweise und Bewertungen verwendet.

Basierend auf Ihrer SQL Server-Version **muss** für den Security Management Server eine der folgenden Optionen aktiviert sein:

- Volltextindexierung
- Volltextfilter
- Vollständiger Test und semantische Extraktionen für die Suche

Weitere Informationen zu den Fehlern, die auftreten, wenn die oben genannten Funktionen für den verwendeten SQL Server nicht aktiviert sind, finden Sie im KB-Artikel SLN308557.

Weitere Informationen zum Konfigurieren von Microsoft SQL Server-Berechtigungen und -Funktionen für den Security Management Server finden Sie in diesem KB-Artikel SLN307771.

ANMERKUNG: Nachstehend finden Sie die Anforderungen für SQL-Berechtigungen. Der Benutzer, der die Installation und Dienste durchführt, muss über lokale Administratorrechte verfügen. Darüber hinaus sind lokale Administratorrechte erforderlich für die Dienstkontoverwaltung der Dienste des Dell Security Management Servers.

Geben Sie	Aktion	Szenario	SQL-Berechtigung erforderlich
Back-End	Upgrade	Per Definition ist bei Upgrades bereits DB und Anmeldung/ Benutzer eingerichtet	db_owner

Geben Sie	Aktion	Szenario	SQL-Berechtigung erforderlich
Back-End	Installation wiederherstellen	Die Wiederherstellung umfasst eine vorhandene DB und Anmeldung.	db_owner
Back-End	Neuinstallation	Vorhandene DB verwenden	db_owner
Back-End	Neuinstallation	Neue DB erstellen	dbcreator, db_owner
Back-End	Neuinstallation	Vorhandene Anmeldung verwenden	db_owner
Back-End	Neuinstallation	Neue Anmeldung erstellen	securityadmin
Back-End	Deinstallieren von	k. A.	k. A.
Proxy-Front-End	beliebig	k. A.	k. A.

ANMERKUNG: Wenn die Benutzerkontensteuerung (UAC, User Account Control) aktiviert ist, müssen Sie diese deaktivieren, bevor Sie Windows Server 2012 R2 unter `C:\Programme` installieren. Der Server muss neu gestartet werden, damit diese Änderung in Kraft tritt.

Während der Installation benötigen Sie Ihre Windows oder SQL Anmeldeinformationen, um die Datenbank einrichten zu können. Unabhängig davon, welche Art von Anmeldeinformationen verwendet werden, muss das Konto über die entsprechenden Berechtigungen für die auszuführende Aktion verfügen. In der vorherigen Tabelle sind die für jeden Installationstyp erforderlichen Berechtigungen aufgeführt. Zusätzlich muss für das Konto, mit dem die Datenbank erstellt und eingerichtet wird, das Standardschema auf dbo gesetzt sein.

Diese Berechtigungen werden nur während der Installation benötigt, um die Datenbank einzurichten. Sobald der Security Management Server installiert ist, kann das für die Verwaltung des SQL-Zugriffs verwendete Konto auf die Rollen db_owner und public beschränkt werden.

Wenn Sie sich unsicher sind in Bezug auf die Zugriffsberechtigungen oder die Konnektivität zur Datenbank, bitten Sie Ihren Datenbankadministrator um Auskunft, bevor Sie mit der Installation beginnen.

Unterstützte Sprachen der Verwaltungskonsole

Die Verwaltungskonsole ist Multilingual User Interface (MUI)-konform und unterstützt folgende Sprachen:

Sprachunterstützung	
EN: Englisch	JA: Japanisch
ES: Spanisch	KO: Koreanisch
FR: Französisch	PT-BR: Portugiesisch, Brasilien
IT: Italienisch	PT-PT: Portugiesisch, Portugal
DE: Deutsch	

3

Vorinstallationskonfiguration

Lesen Sie vor Beginn den *Technischen Ratgeber für Security Management Server*, um sich über aktuelle Lösungen oder bekannte Probleme in Verbindung mit Security Management Server zu informieren.

Die Vorinstallationskonfiguration des/der Server(s), auf denen Sie Security Management Server installieren möchten, ist sehr wichtig. Sehen Sie sich diesen Abschnitt genau an, um sicherzustellen, dass Security Management Server fehlerfrei installiert wird.

Konfiguration

Zugriff auf die Verwaltungskonsole

Da Internet Explorer nicht mehr unterstützt wird, müssen Sie einen Drittanbieter-Browser installieren, um ordnungsgemäß auf die Verwaltungskonsole zugreifen zu können.

Wenn Internet Explorer zum Validieren der Verwaltungskonsole erforderlich ist, müssen Sie Explorer Enhanced Security Configuration für den Kontotyp deaktivieren, der dem angemeldeten Administrator entspricht.

Anschluss- und Firewall-Konfiguration

Client- und Serverkommunikation mit Dritten (ausgehend)

Die folgenden Services und Anschlüsse sind für den Dell Server für die Kommunikation mit verwalteten Endpunkten erforderlich. Diese Anschlüsse und Services müssen in der Lage sein, eine ausgehende Kommunikation zu haben. Wenn die SSL-Inspektions- und Proxy-Services verwendet werden, müssen Sie von den URLs ausgeschlossen werden.

- „On-the-Box“-Berechtigungsvalidierung
  - Ziel-URL
    - cloud.dell.com
  - Port
    - 443
  - Ausgehendes Gerät
    - Security Management Server oder Security Management Server Virtual als Back-End-Konfiguration
  - Ursprungsservice
    - Dell Security Server
  - Ursprungsport
    - 8443
- Advanced Threat Prevention Client – Kommunikation
  - Ziel-URLs
    - Nordamerika
      - login.cylance.com
      - protect.cylance.com
      - data.cylance.com
      - update.cylance.com
      - api.cylance.com
      - protect-api.cylance.com
      - download.cylance.com
    - Südamerika
      - 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
    - Europa
        - 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
    - Naher Osten und Asien
        - 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, Australien und Neuseeland
        - 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
- Ausgehendes Gerät
    - Alle verwalteten Endpunkte
- Ausgehender Service
    - CylanceSVC
- Ursprungsport
    - 443

Öffentliche Kommunikation mit Front-End-Server (falls erforderlich)

Damit sind Informationen gemeint, die vom Internet zum Front-End-Server gehen. Die Firewall- bzw. Routing-Konfiguration muss Anschlüsse Ports verfügen, die als eingehende Anschlüsse von einer öffentlichen/Internetverbindung zu den Front-End-Servern oder zum Lastenausgleich festgelegt wurden.

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

DMZ- oder Front-End-Kommunikation mit Back-End-Server (falls erforderlich)

Die folgenden Services und Anschlüsse kommunizieren von jedem Security Management Server, der im Front-End-Modus konfiguriert ist, mit dem Security Management Server, der im Back-End-Modus konfiguriert ist. Die Firewall- bzw. Routing-Konfiguration muss über Anschlüsse verfügen, die als eingehende Anschlüsse von den Front-End-Servern oder als Lastenausgleich zum Back-End-Server festgelegt sind.

- Dell Policy Proxy für das Front-End und Dell Beacon Server zum Dell Message Broker für das Back-End: STOMP/61613
- Dell Security Server-Proxy für das Front-End zum Dell Security Server für das Back-End: HTTPS/8443
- Dell Core Server-Proxy für das Front-End zum Dell Core Server für das Back-End: HTTPS/8888
- Dell Device Server für das Front-End zum Dell Security Server für das Back-End: HTTPS/8443

Back-End-Server zu internem Netzwerk

Die nachfolgenden Services und Anschlüsse werden intern für die Kommunikation mit den jeweiligen Services von Clients in der Domain oder über VPN verbundene verwendet. Dell empfiehlt, dass mehrere dieser Services nicht außerhalb des Netzwerks weitergeleitet werden oder dass der Service standardmäßig in der Konfiguration des Front-End-Servers gefiltert wird. Bei der Firewall- bzw. Routing-Konfiguration müssen diese Anschlüsse als eingehende Anschlüsse vom internen Netzwerk zum Security Management Server für das Back-End festgelegt sein.

- Auf dem Dell Security Server gehostete Verwaltungskonsole: HTTPS/8443
- Über den Dell Compliance Reporter bereitgestellte Berichte: HTTP(S)/8084

  ANMERKUNG: Dieser Service ist in der Standardeinstellung deaktiviert. Verwenden Sie stattdessen verwaltete Berichte, die in der Verwaltungskonsole verfügbar sind, die vom Dell Security Server gehostet wird. Informationen zum Aktivieren des Dell Compliance Reporter für Verlaufsberichte finden Sie im KB-Artikel SLN314792.
- Dell Core Server: HTTPS/8888
- Dell Device Server: HTTP(S)/8081

  ANMERKUNG: Dieser Legacy-Service ist nur für Dell Encryption-Clients vor Version 8.x erforderlich. Dieser Service kann sicher deaktiviert werden, wenn alle Clients in der Umgebung 8.0 oder höher sind.
- Schlüssel-Server: TCP/8050
- Dell Policy Proxy: TCP/8000
- Dell Security Server: HTTPS/8443
- Zertifikatbasierte Authentifizierung, gehostet über den Dell Security Server: HTTPS/8449

  ANMERKUNG: Diese Funktion wird von Dell Encryption-Clients verwendet, die auf Windows Server-Betriebssystemen oder auf Clients installiert sind, die im Servermodus installiert sind. Weitere Informationen zum Installieren von Clients im Servermodus finden Sie unter Encryption Enterprise – Erweitertes Installationshandbuch.

Infrastrukturkommunikation

- Active Directory, das für die Benutzerauthentifizierung mit Dell Encryption TCP/389/636 (lokaler Domänencontroller), TCP/3268/3269 (globaler Katalog), TCP/135/49125+ (RPC) genutzt wird
- E-Mail-Kommunikation (optional): 25/587
- Microsoft SQL Server: 1433 (Standardport)

Erstellen und Verwalten von Microsoft SQL-Datenbanken

Dell Server-Datenbank erstellen:

Diese Anweisungen sind optional. Wenn keine Datenbank vorhanden ist, wird sie vom Installationsprogramm standardmäßig erstellt. Falls Sie vor dem Installieren des Security Management Server eine Datenbank einrichten möchten, befolgen Sie die folgenden Anweisungen zur Erstellung der SQL-Datenbank und des SQL-Benutzers im SQL Management Studio. Stellen Sie sicher, dass die entsprechenden Berechtigungen für SQL-Datenbanken eingerichtet sind, die während der Installation des Security Management Servers nicht automatisch erstellt werden. Eine Liste der erforderlichen Berechtigungen finden Sie unter Softwareanforderungen.

Folgen Sie bei der Voraberstellung der Datenbank den Anleitungen unter Back-End-Server mit vorhandener Datenbank installieren.

Der Security Management Server ist für die SQL- und Windows-Authentifizierung konfiguriert.

ANMERKUNG: Die erwartete nicht standardmäßige Sortierung, die für Ihre SQL-Datenbank oder SQL-Instanz unterstützt wird, ist „SQL_Latin1_General_CP1_CI_AS“. Bei der Sortierung sind Groß-/Kleinschreibung und Akzente zu beachten.

Installationsvoraussetzungen

Voraussetzungen werden standardmäßig während der Installation des Security Management Servers auf Windows Server-Betriebssystemen installiert. Die folgenden Voraussetzungen können optional vor der Installation des Security Management Servers installiert werden, um Neustartvoraussetzungen zu umgehen.

Installieren der Visual C++ Redistributable-Pakete

Falls noch nicht installiert, installieren Sie die Visual C++ 2010, 2013 und 2015 (oder höher) Redistributable-Pakete. Optional können Sie festlegen, dass diese Komponenten vom Security Management Server-Installationsprogramm installiert werden.

ANMERKUNG: Die Installation der Microsoft Visual C++ Redistributable-Pakete erfordert möglicherweise einen Neustart.

Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019: https://support.microsoft.com/de-de/help/2977003/the-latest-supported-visual-c-downloads

Installieren von .NET Framework 4.5

.NET Framework 4.5 ist auf Windows Server 2012 R2 und höher als eine Funktion von Server Manager vorinstalliert.

Installieren von SQL Native Client 2012

Wenn Sie SQL Server 2012 oder SQL Server 2016 verwenden, installieren Sie SQL Native Client 2012. Optional können Sie festlegen, dass diese Komponente vom Security Management Server-Installationsprogramm installiert wird. http://www.microsoft.com/en-us/download/details.aspx?id=35580

Importieren der Serverinstallationslizenz

Bei einer neuen Installation – Kopieren Sie Ihren Produktschlüssel (der Name der Datei lautet *EnterpriseServerInstallKey.ini*) nach `C:\Windows`, um den Produktschlüssel mit 32 Zeichen automatisch in das Security Management Server-Installationsprogramm zu übertragen.

ANMERKUNG: Die EnterpriseServerInstallKey.ini ist im Download-Paket des Security Management Servers vorhanden und hier verfügbar.

Die Vorinstallationskonfiguration des Servers ist abgeschlossen. Fahren Sie fort mit Installieren, Aktualisieren und Migrieren.

4

Installation oder Upgrade/Migraton

Das Kapitel enthält Anweisungen für folgende Aufgaben:

- Neue Installation – Ermöglicht die Installation eines neuen Security Management Server.
- Aktualisierung/Migration – Ermöglicht die Aktualisierung eines vorhandenen, funktionsfähigen Enterprise Server ab Version 9.2.
- Security Management Server deinstallieren – Ermöglicht bei Bedarf das Entfernen der derzeitigen Installation.

  Falls Ihre Installation mehr als einen Hauptserver (Back-End-Server) enthalten muss, kontaktieren Sie Ihren Dell ProSupport-Mitarbeiter.

Vor der Installation, Aktualisierung oder Migration

Bevor Sie beginnen, stellen Sie sicher, dass die Schritte für die Vorinstallationskonfiguration durchgeführt wurden.

Lesen Sie die *Technischen Tipps für Security Management Server*, um sich über aktuelle Lösungen oder bekannte Probleme hinsichtlich der Installation von *Security Management Server* zu informieren.

Antivirus- und Anti-Schadsoftware sollte während der Installation oder Aktualisierung von Security Management Server deaktiviert werden, um zu verhindern, dass diese sich auf Microsoft C++ Runtime-Installationsprogramme, Java Aktivitäten (Erstellen und Bearbeiten von Zertifikaten) sowie die PostgreSQL-Erstellung und -Änderung auswirkt. Alle diese Elemente werden von ausführbaren Dateien oder Skripten ausgelöst.

Schließen Sie als Workaround Folgendes aus:

- [INSTALLATIONSPFAD]:\Dell\Enterprise Edition
- C:\Windows\Installer
- Der Dateipfad, an dem das Installationsprogramm ausgeführt wurde.

Dell empfiehlt, für die Dell Server-Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfall-Wiederherstellungsplan Ihres Unternehmens einzubeziehen.

Wenn Sie Dell-Komponenten in Ihre DMZ implementieren möchten, vergewissern Sie sich, dass sie ausreichend vor Angriffen geschützt sind.

Für Produktionsumgebungen empfiehlt Dell dringend, die Installation von SQL Server auf einem dedizierten Server vorzunehmen.

Es ist ein bewährtes Verfahren, den Back-End Server vor der Installation und Konfiguration des Front-End-Servers zu installieren.

Die Installation der Protokolldateien befindet sich in diesem Verzeichnis: `C:\Benutzer\<LoggedOnUser>\AppData\Local\Temp`

Neue Installation

Wählen Sie eine von zwei Optionen für die Back-End-Serverinstallation:

- Back-End-Server und neue Datenbank installieren – Ermöglicht die Installation eines neuen Security Management Server und einer neuen Datenbank.
- Back-End-Server mit vorhandener Datenbank installieren – Ermöglicht die Installation eines neuen Security Management Server und die Verbindung mit einer im Rahmen der Vorinstallationskonfiguration erstellten oder einer vorhandenen SQL-Datenbank ab Version 9.x, wenn die Schemaversion mit der zu installierenden Security Management Server-Version übereinstimmt. Eine Datenbank ab Version v9.2 muss mit der neuesten Version des Serverkonfigurationstools auf das neueste Schema migriert werden. Anweisungen zur Datenbankmigration mit dem Serverkonfigurationstool finden Sie unter Datenbank migrieren. Um die neueste Version des Serverkonfigurationstools zu erhalten oder eine Datenbank vor Version 9.2 zu migrieren, wenden Sie sich bitte an Dell ProSupport.

ANMERKUNG:

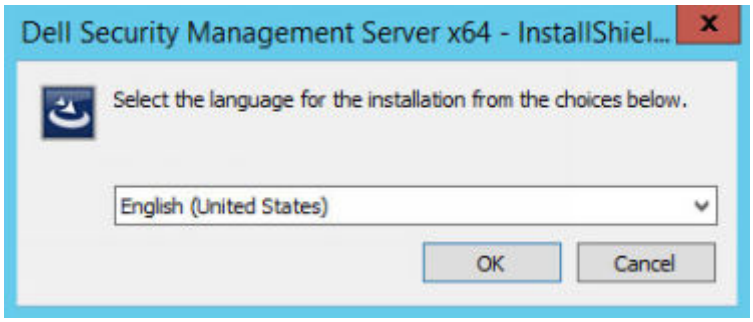
Falls Sie über einen funktionsfähigen Enterprise Server ab v9.2 verfügen, lesen Sie die Anweisungen unter Back-End-Server-Aktualisierung/Migration.

Falls Sie einen Front-End-Server installieren, führen Sie diese Installation vor der Installation des Back-End-Servers aus:

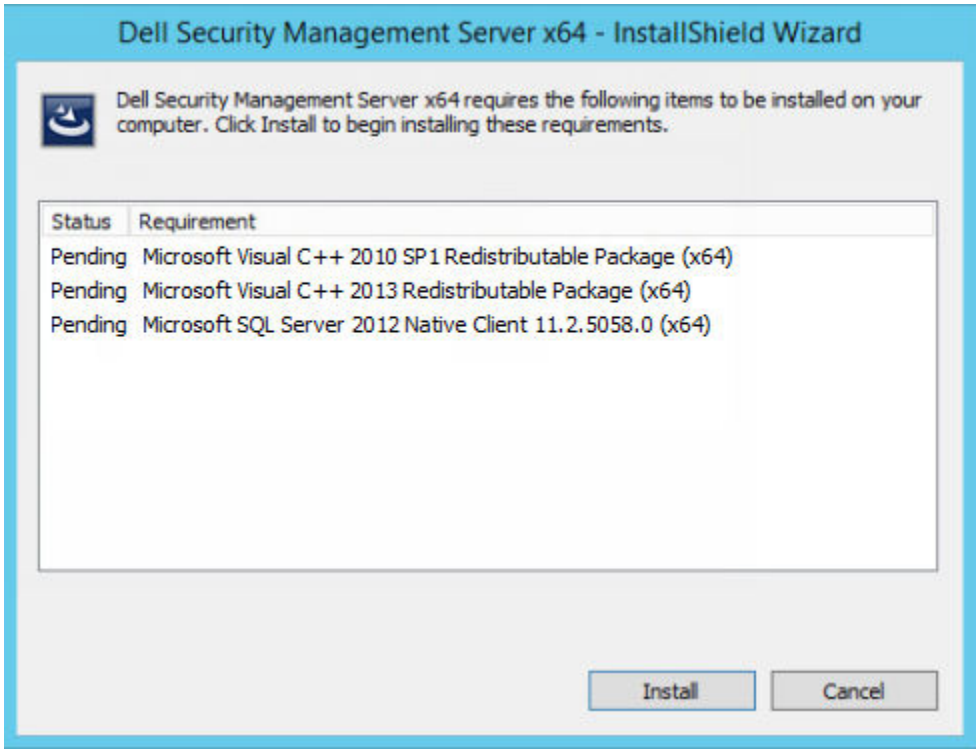
- Front-End-Server installieren – die Installation eines Front-End-Servers zur Kommunikation mit dem Back-End-Server.

Back-End-Server und neue Datenbank installieren

1. Wechseln Sie auf dem Dell Installationsmedium in das Security Management Server-Verzeichnis. **Entpacken** Sie (NICHT kopieren/einfügen oder ziehen) Security Management Server-x64 im Stammverzeichnis des Servers, auf dem Sie Security Management Server installieren möchten. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***
2. Doppelklicken Sie auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

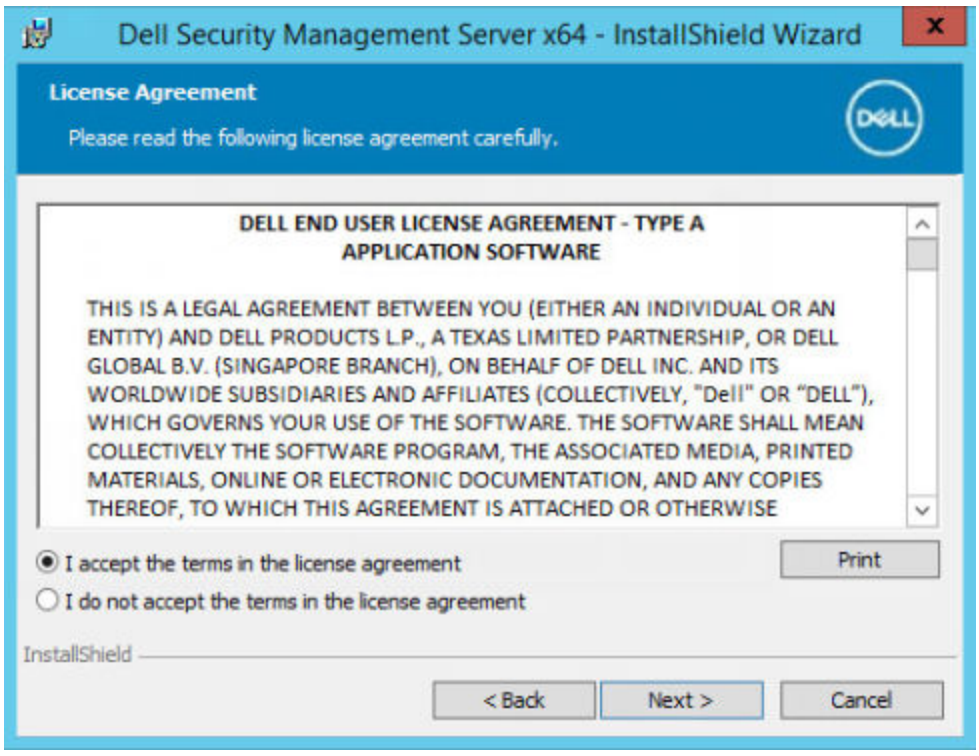


4. Wenn die Voraussetzungen noch nicht installiert wurden, wird eine Meldung angezeigt, die Sie darüber informiert, welche Voraussetzungen installiert werden Klicken Sie auf **Installieren**.

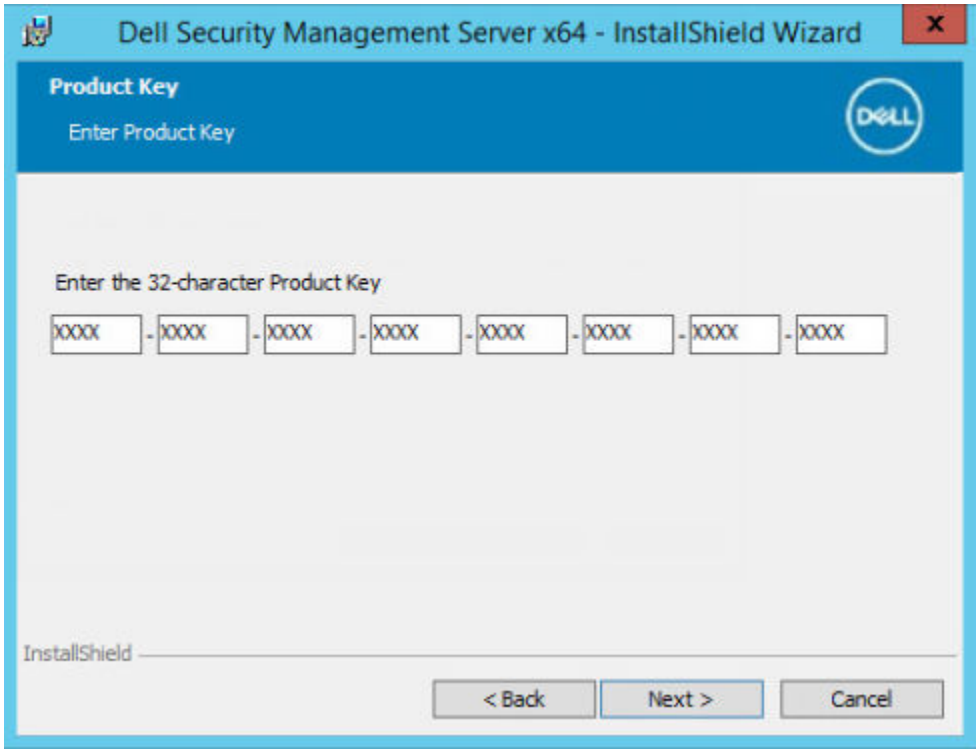


5. Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.

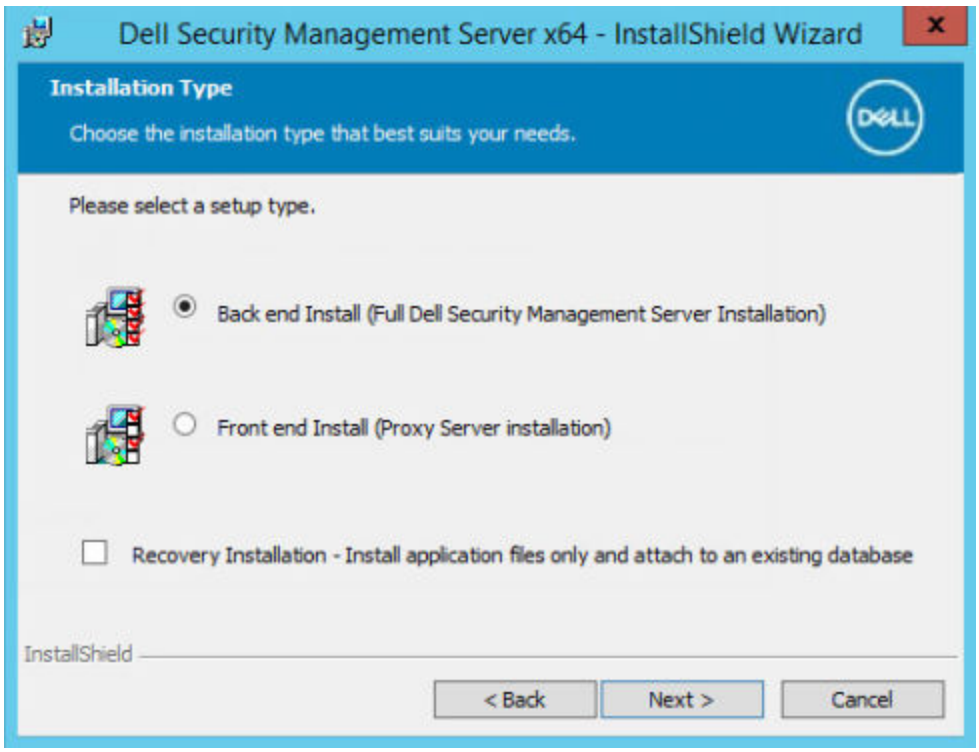
6. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen und klicken Sie auf **Weiter**.



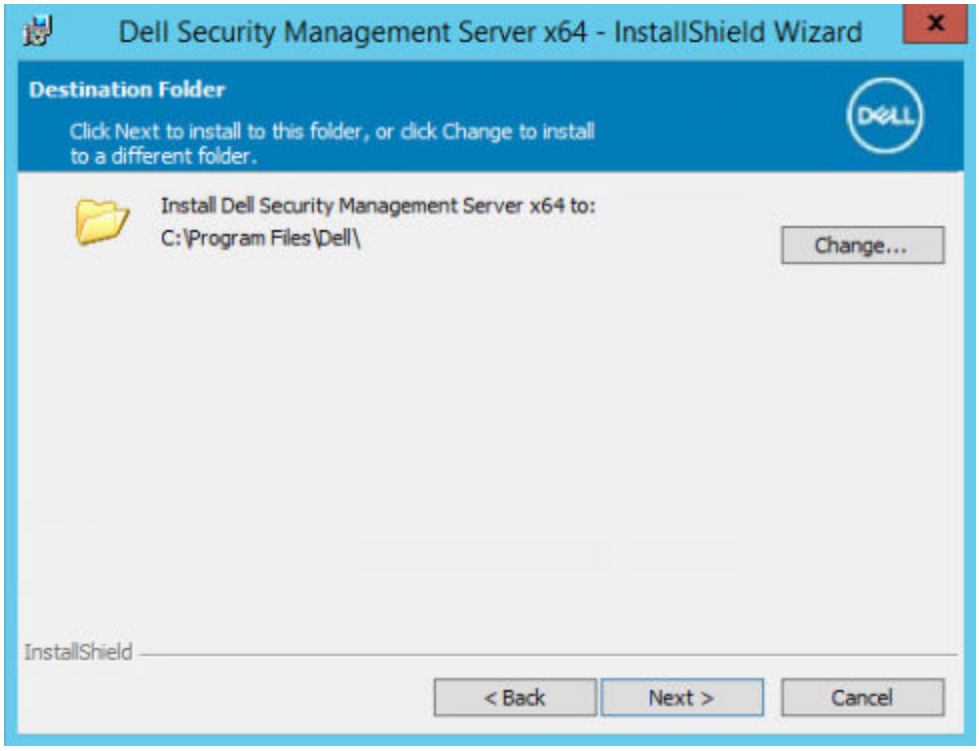
7. Wenn Sie optional Ihre `EnterpriseServerInstallKey.ini`-Datei in `C:\Windows` wie unter Vorinstallationskonfiguration erläutert kopiert haben, klicken Sie auf **Weiter**. Falls nicht, dann geben Sie den 32 Zeichen langen Produktschlüssel ein, und klicken Sie dann auf **Weiter**. Der Produktschlüssel befindet sich in der Datei `EnterpriseServerInstallKey.ini`.



8. Wählen Sie **Back-End-Installation** aus und klicken Sie auf **Weiter**.

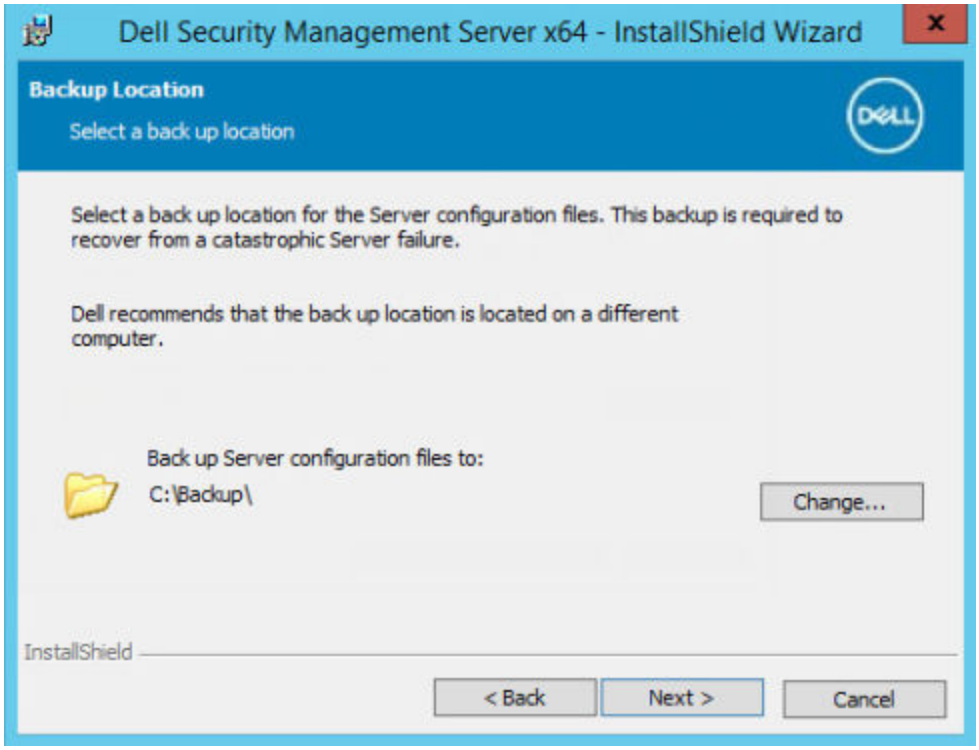


9. Klicken Sie zur Installation des Security Management Server im Standardverzeichnis `C:\Programme\Dell` auf **Weiter**. Klicken Sie anderenfalls auf **Ändern**, um einen anderen Speicherort auszuwählen; klicken Sie anschließend auf **Weiter**.



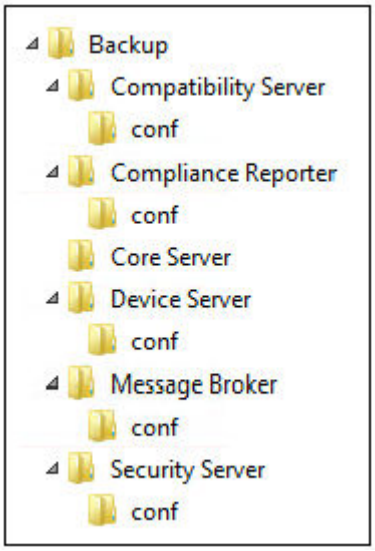
10. Klicken Sie zur Auswahl eines Speicherorts für zu speichernde Konfigurations-Sicherungsdateien auf **Ändern**, navigieren Sie zum gewünschten Ordner und klicken Sie anschließend auf **Weiter**.

Dell empfiehlt die Auswahl eines Remote-Netzwerkspeicherortes oder eines externen Sicherungslaufwerks.



Nach der Installation müssen alle Änderungen an den Konfigurationsdateien, einschließlich Änderungen, die mit dem Serverkonfigurationstool vorgenommen werden, manuell in diesen Ordnern gesichert werden. Konfigurationsdateien sind ein wichtiger Bestandteil der gesamten Informationen, die für die manuelle Wiederherstellung des Dell Servers, falls erforderlich, verwendet werden.

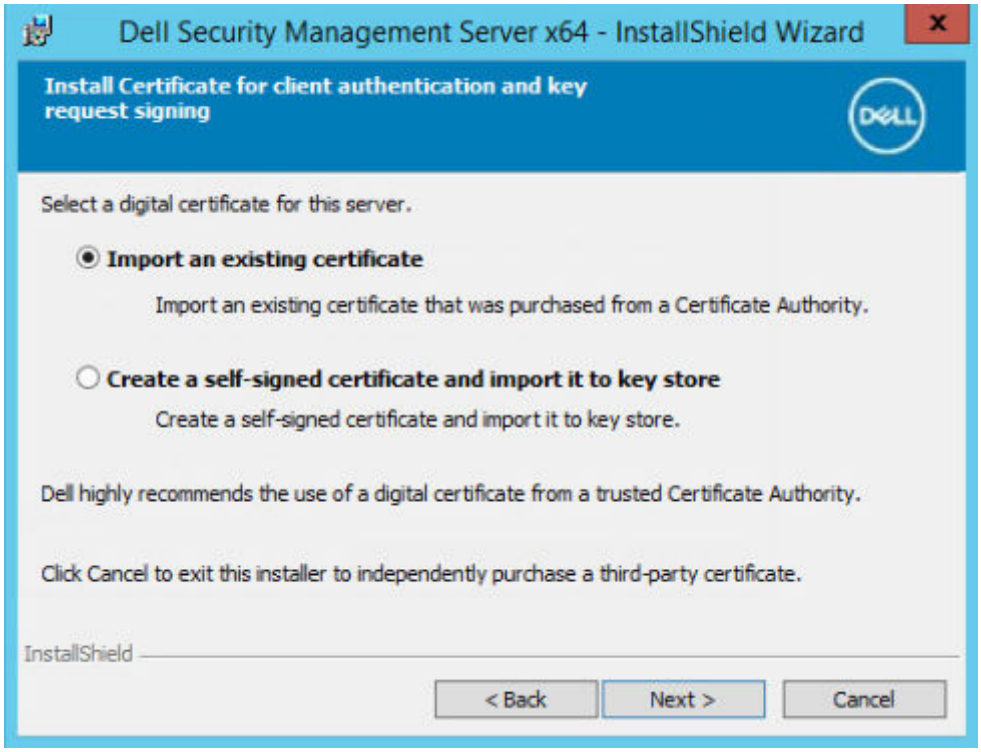
ANMERKUNG: Die durch das Installationsprogramm während des Installationsschritts erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



11. Sie können aus verschiedenen digitalen Zertifikatstypen auswählen. **Es wird dringend empfohlen, ein digitales Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zu verwenden.**

    Wählen Sie entweder Option „a“ oder „b“ unten aus:

    a. Um ein vorhandenes Zertifikat zu verwenden, das Sie bei einer Zertifizierungsstelle erworben haben, wählen Sie **Vorhandenes Zertifikat importieren** aus, und klicken Sie dann auf **Weiter**.



    Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

    Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

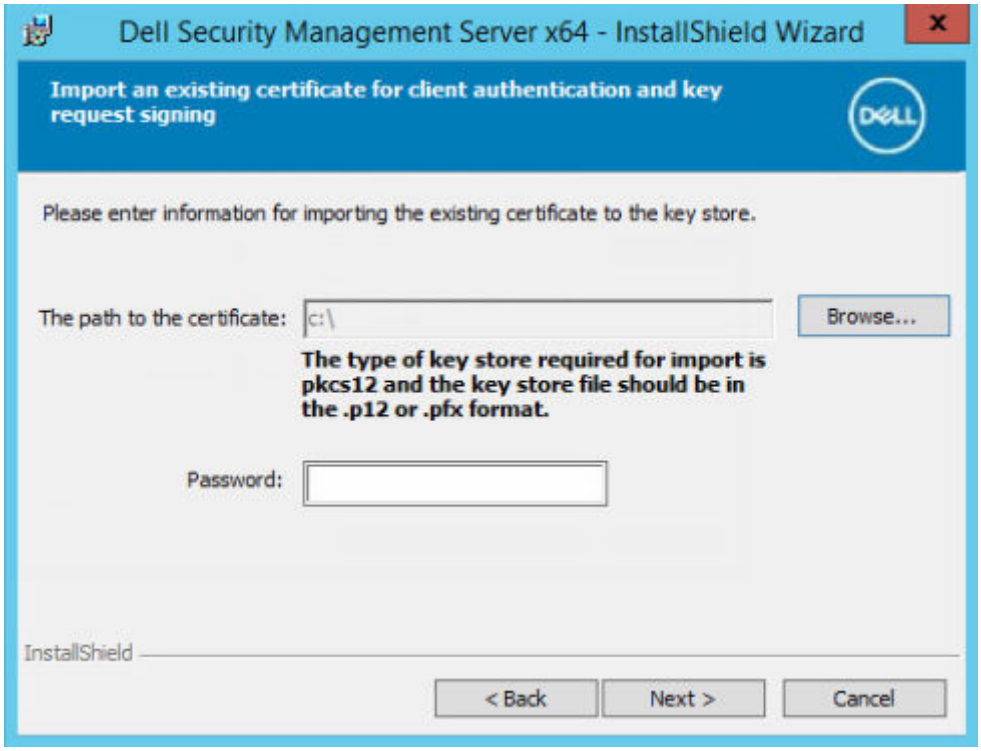
    Klicken Sie auf **Weiter**.

    ANMERKUNG:

    Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der

Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren



ODER

b. Wählen Sie zum Erstellen eines selbstsignierten Zertifikats **Ein selbstsigniertes Zertifikat erstellen und in den Schlüsselspeicher importieren** und klicken Sie auf **Weiter**.

Geben Sie im Dialogfeld *Selbstsigniertes Zertifikat erstellen* die folgenden Informationen ein:

Vollständiger Computername (Beispiel: computername.domain.com)

Organisation

Organisationseinheit (Beispiel: Sicherheit)

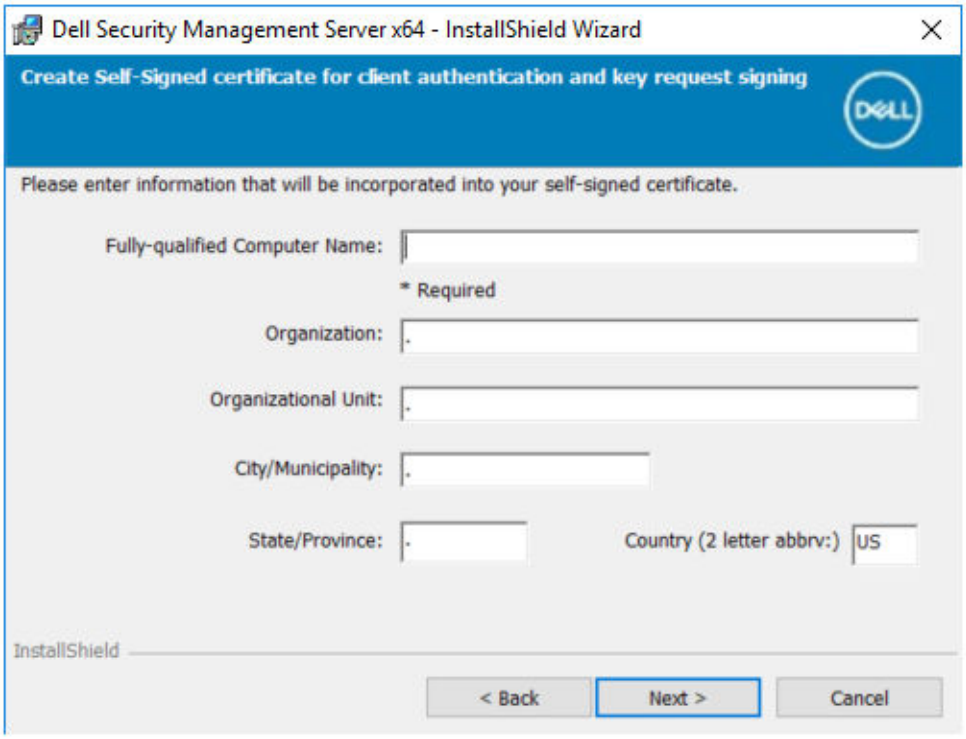
Ort

Bundesstaat (vollständiger Name)

Land: Abkürzung aus zwei Buchstaben

Klicken Sie auf **Weiter**.

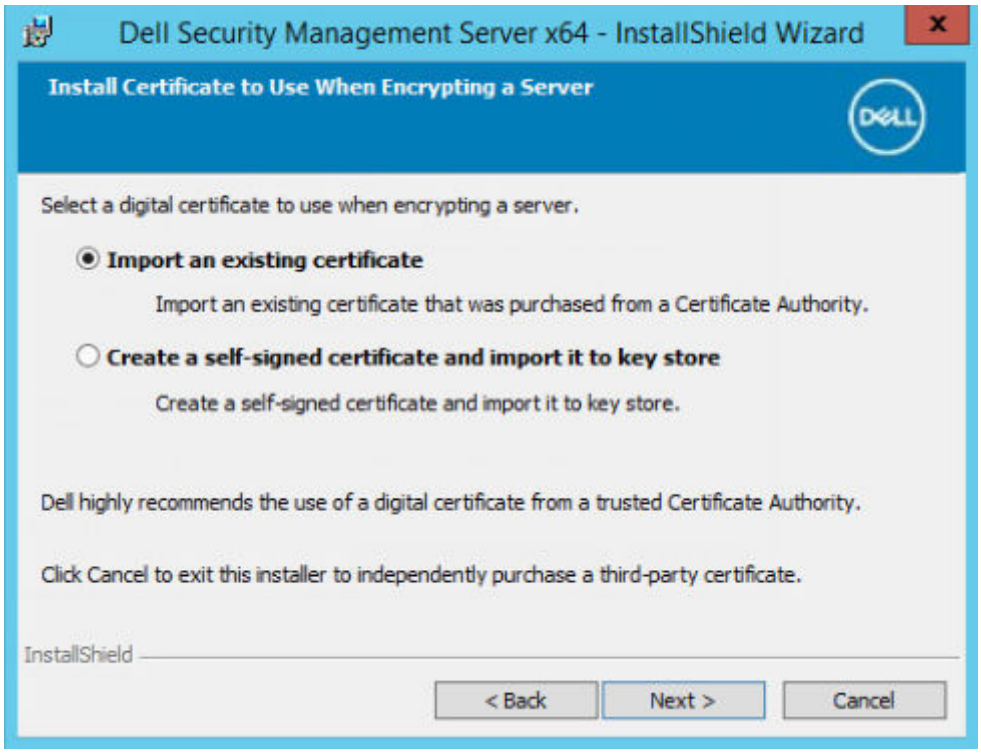
ANMERKUNG: Das Zertifikat läuft standardmäßig in zehn Jahren ab.



12. Für die Server Encryption können Sie aus verschiedenen digitalen Zertifikattypen auswählen. Es wird dringend empfohlen, ein digitales Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zu verwenden.

    Wählen Sie entweder Option „a“ oder „b“ unten aus:

    a. Um ein vorhandenes Zertifikat zu verwenden, das Sie bei einer Zertifizierungsstelle erworben haben, wählen Sie **Vorhandenes Zertifikat importieren** aus, und klicken Sie dann auf **Weiter**.



    Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

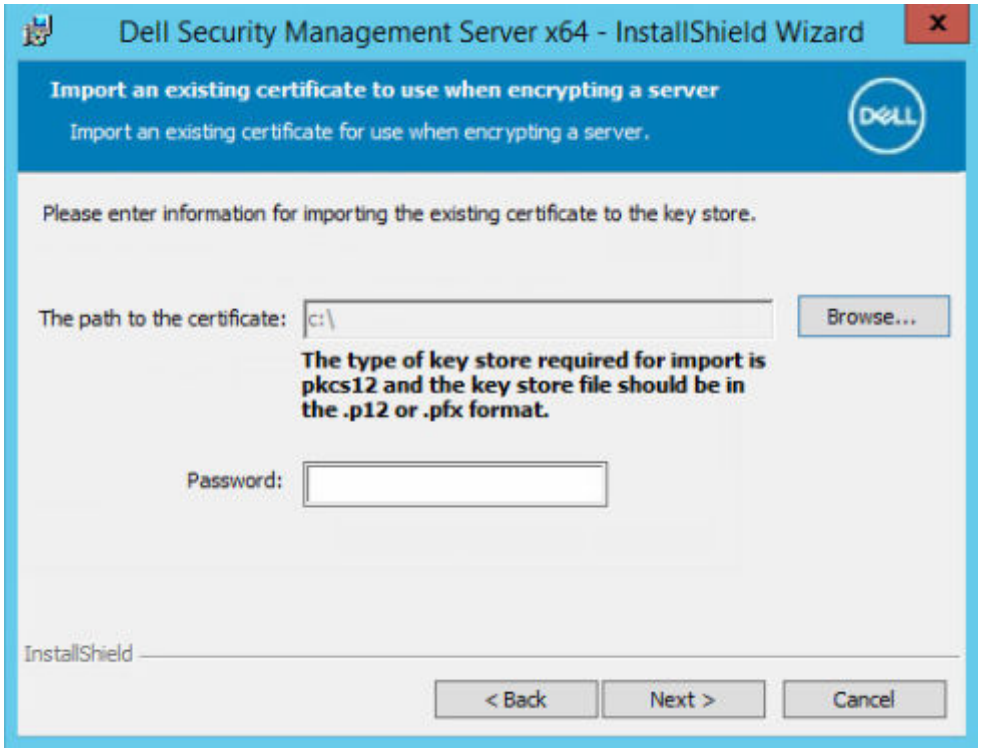
    Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

ANMERKUNG:

Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren



ODER

b. Wählen Sie zum Erstellen eines selbstsignierten Zertifikats **Ein selbstsigniertes Zertifikat erstellen und in den Schlüsselspeicher importieren und klicken Sie auf Weiter.**

Geben Sie im Dialogfeld *Selbstsigniertes Zertifikat erstellen* die folgenden Informationen ein:

Vollständiger Computername (Beispiel: computername.domain.com)

Organisation

Organisationseinheit (Beispiel: Sicherheit)

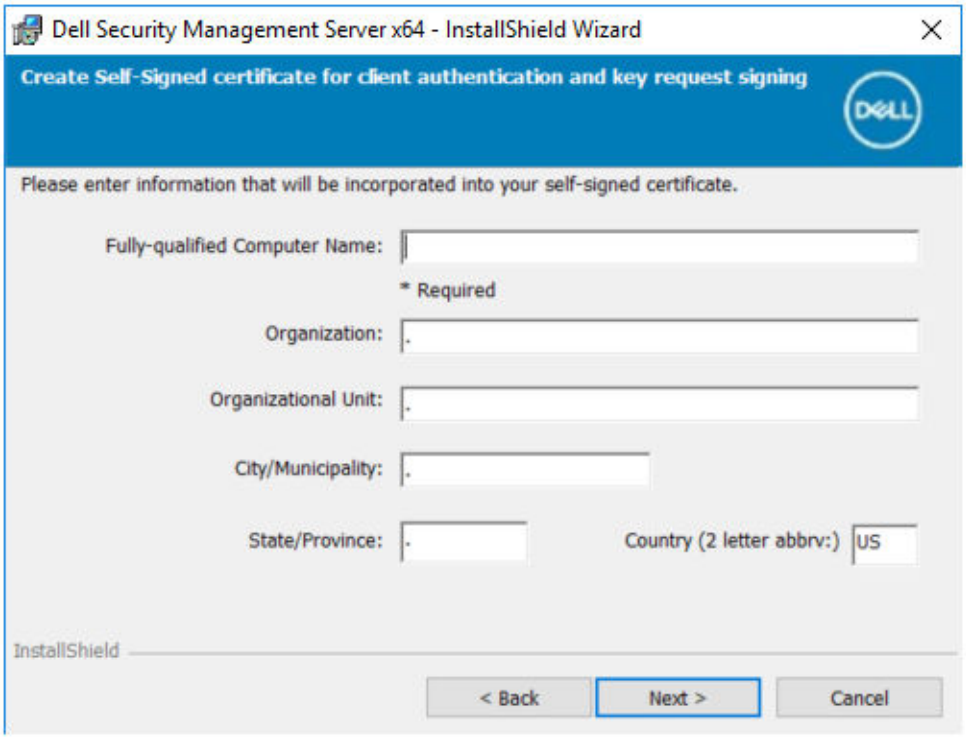
Ort

Bundesstaat (vollständiger Name)

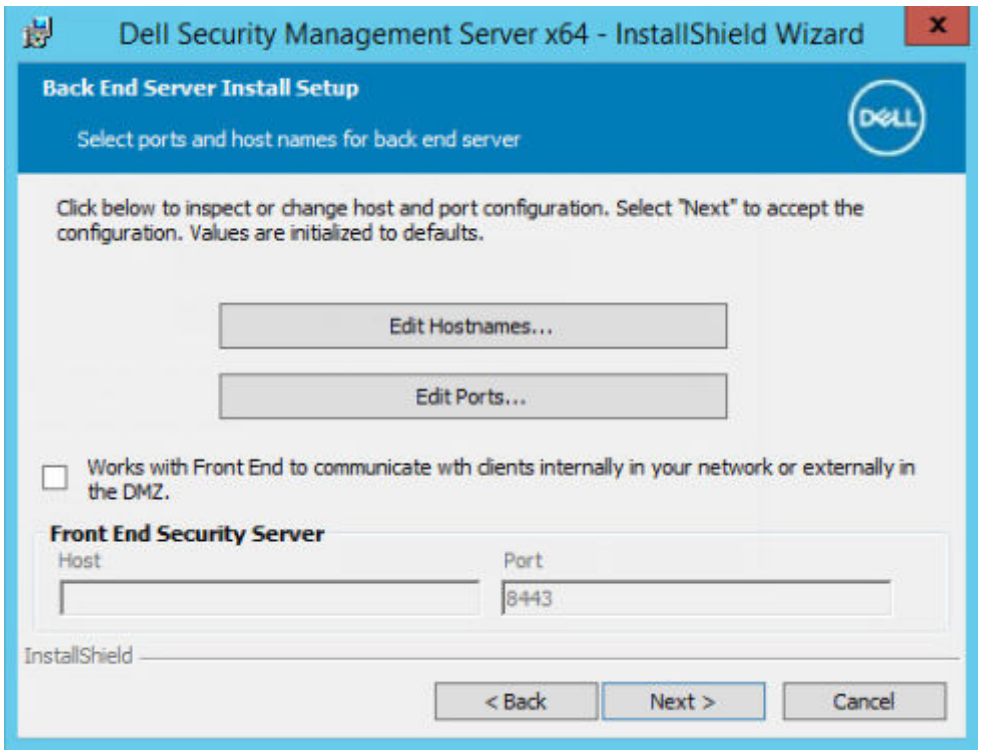
Land: Abkürzung aus zwei Buchstaben

Klicken Sie auf **Weiter**.

ANMERKUNG: Das Zertifikat läuft standardmäßig in zehn Jahren ab.



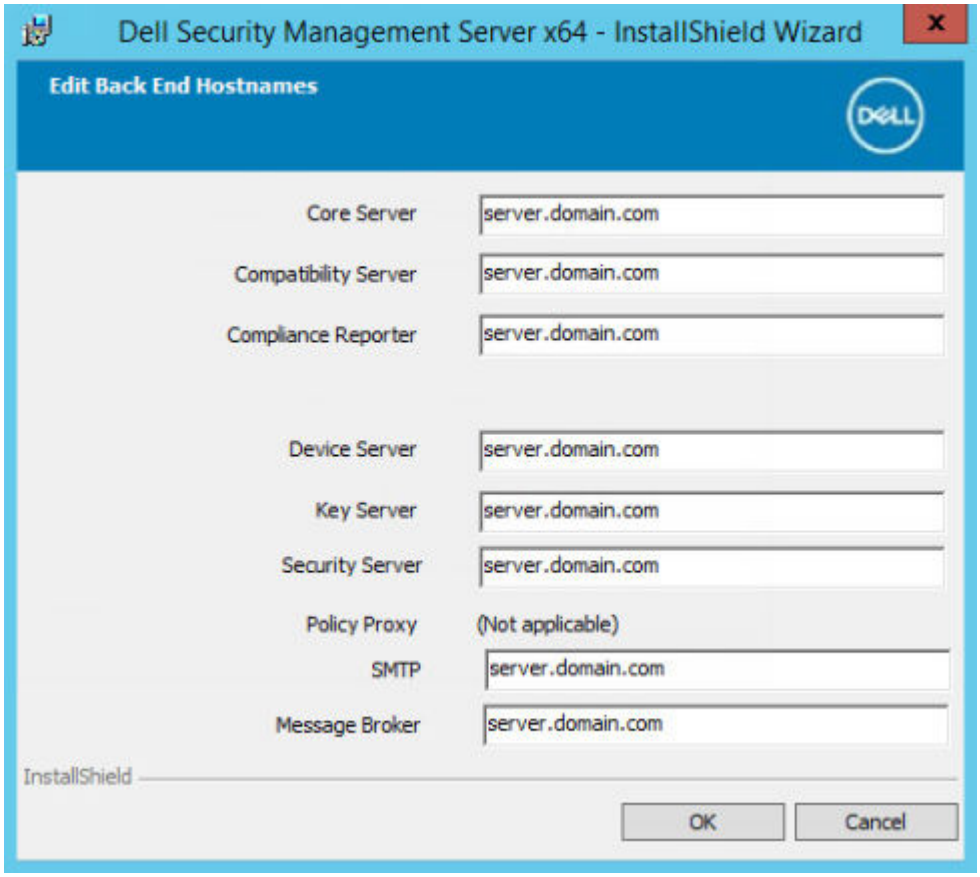
13. Über das Setup-Dialogfeld *Back-End-Server-Einrichtung* können Sie Hostnamen und Ports anzeigen oder bearbeiten.
    - Klicken Sie zum Übernehmen der Standard-Hostnamen und -Ports im Dialogfeld *Back-End-Server-Installationseinrichtung* auf **Weiter**.
    - Wenn Sie einen Front-End-Server verwenden, dann wählen Sie **Nutzt für die Kommunikation mit Clients intern in Ihrem Netzwerk oder extern in der DMZ den Front-End-Server** und geben Sie den Front-End-Sicherheitsserver-Hostnamen ein (zum Beispiel server.domain.com).



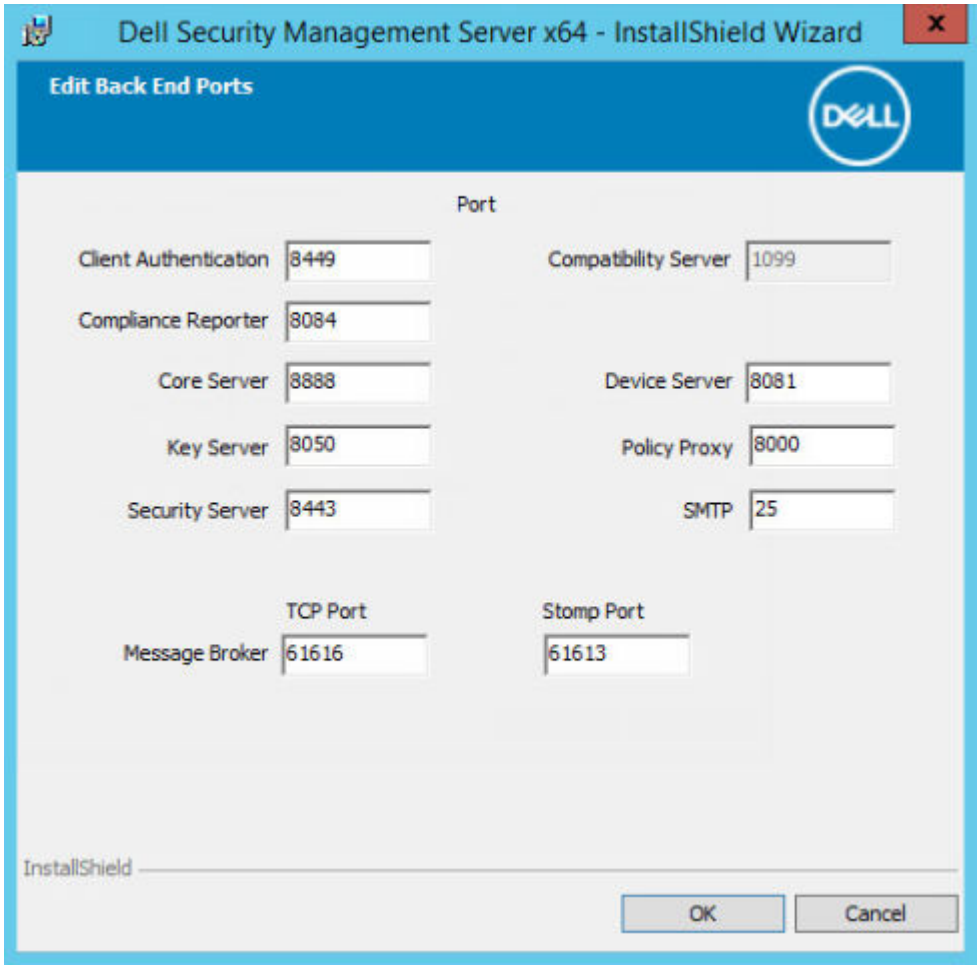
- Klicken Sie zum Anzeigen oder Bearbeiten von Hostnamen auf **Hostnamen bearbeiten**. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

  ANMERKUNG: Im Hostnamen darf kein Unterstrich (_) enthalten sein.

Klicken Sie anschließend auf **OK**.

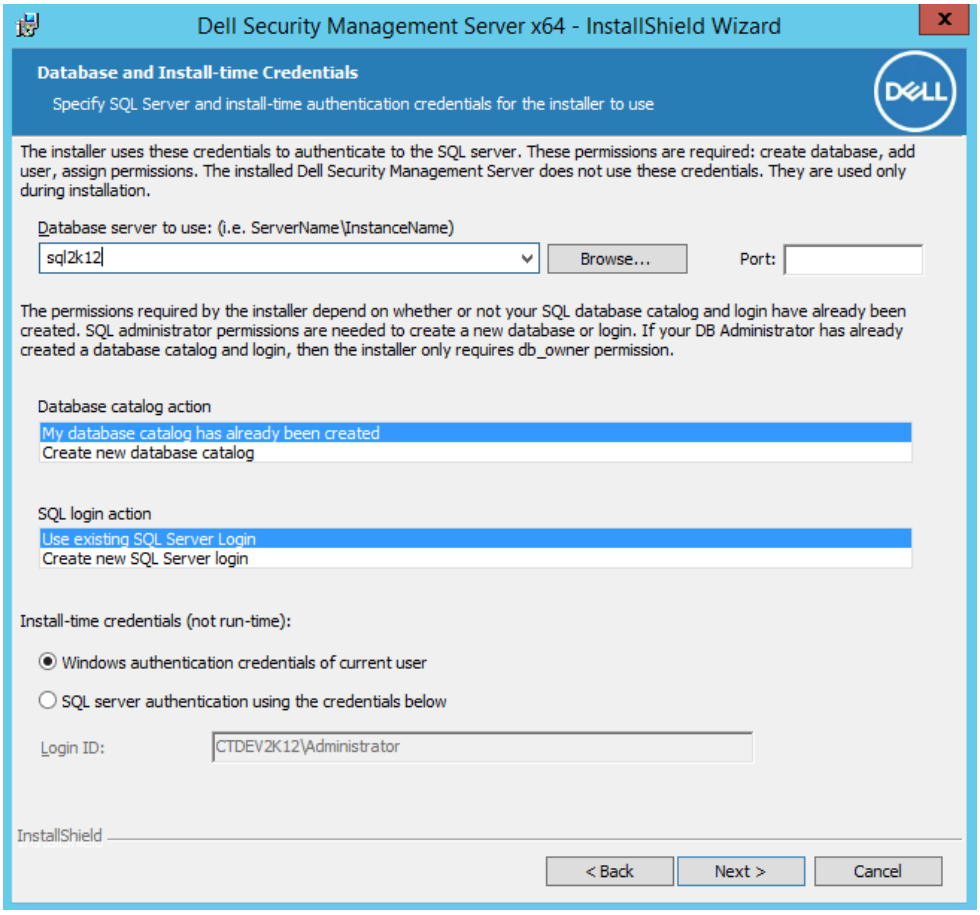


- Klicken Sie zum Anzeigen oder Bearbeiten von Ports auf **Ports bearbeiten**. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen. Klicken Sie anschließend auf **OK**.



14. Zum Erstellen einer neuen Datenbank gehen Sie wie folgt vor:
    a. Klicken Sie auf **Durchsuchen**, um den Server auszuwählen, auf dem die Datenbank installiert werden soll.
    b. Wählen Sie die Authentifizierungsmethode aus, die das Installationsprogramm zum Einrichten der Dell Server-Datenbank verwenden soll. Nach der Installation verwendet das installierte Produkt nicht die hier angegebenen Anmeldeinformationen.
        - **Anmeldeinformationen für die Windows-Authentifizierung des aktuellen Benutzers**

          Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (*Benutzername* und *Kennwort* sind nicht bearbeitbar). Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt.



ODER

- **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**

  Bei Verwendung der SQL-Authentifizierung muss das verwendete SQL-Konto auf dem SQL-Server über Systemadministratorberechtigungen verfügen.

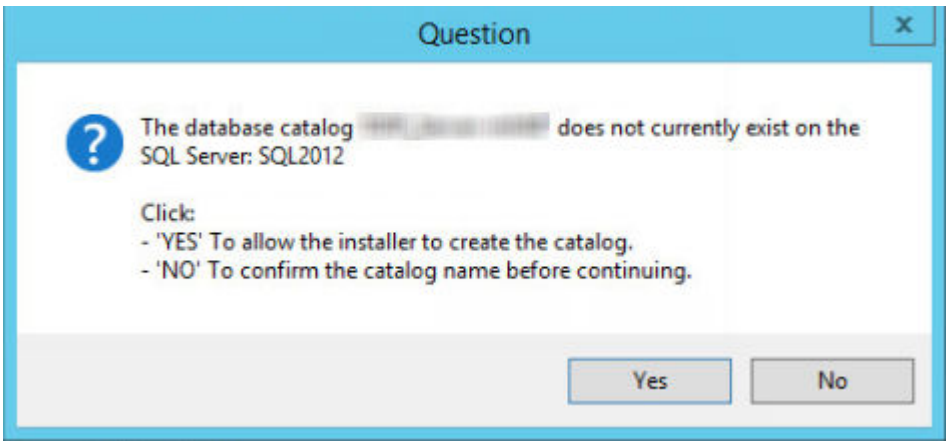
  Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen.

c. Identifizierung des Datenbank-Katalogs:

   Geben Sie den Namen für einen neuen Datenbank-Katalog ein. Sie werden im nächsten Dialogfeld zur Erstellung des neuen Katalogs aufgefordert.

d. Klicken Sie auf **Weiter**.

e. Bestätigen Sie, dass das Installationsprogramm eine Datenbank erstellen soll, indem Sie auf **Ja** klicken. Um zum vorherigen Bildschirm zurückzukehren und Änderungen vorzunehmen, klicken Sie auf **Nein**.



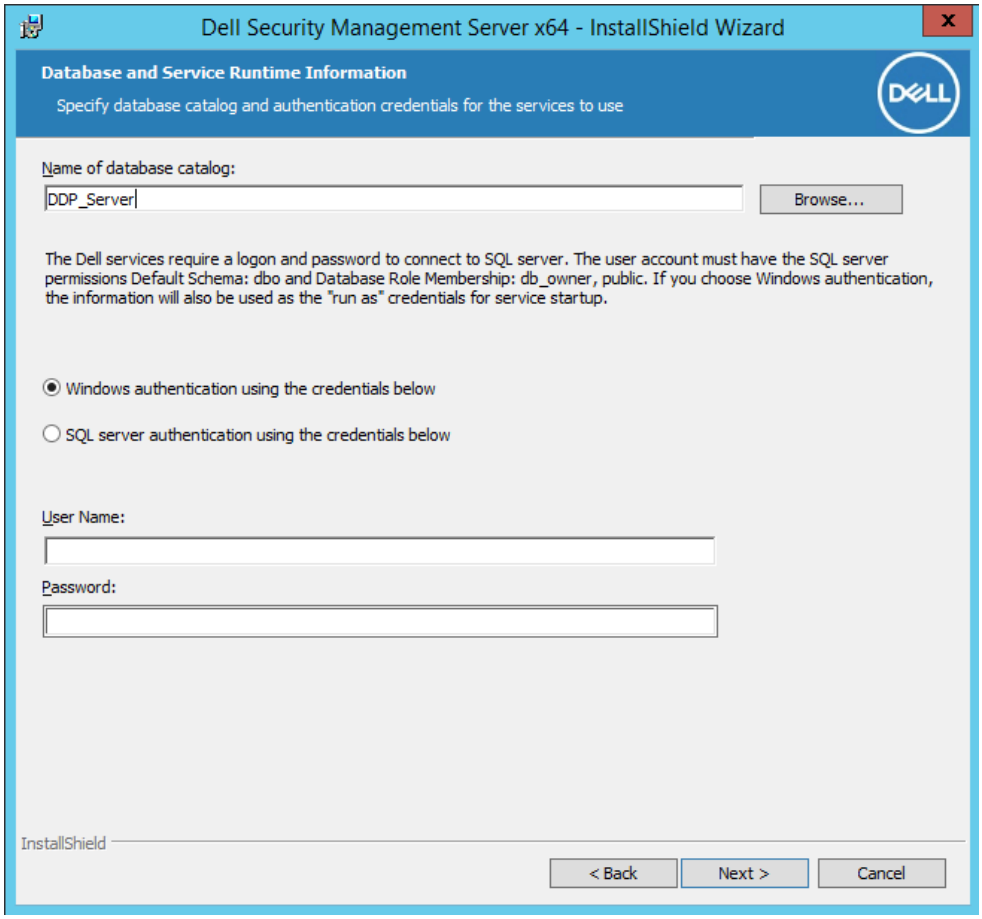
15. Wählen Sie die Authentifizierungsmethode für das zu verwendende Produkt aus. Dieser Schritt verbindet ein Konto mit dem Produkt.

- **Windows-Authentifizierung**

  Wählen Sie **Windows-Authentifizierung über die unten angegebenen Anmeldeinformationen** aus, geben Sie die Anmeldeinformationen für das zu verwendende Produkt ein, und klicken Sie auf **Weiter**.

  Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

  Diese Anmeldeinformationen werden auch von den Dell Diensten verwendet, da sie mit dem Security Management Server funktionieren.

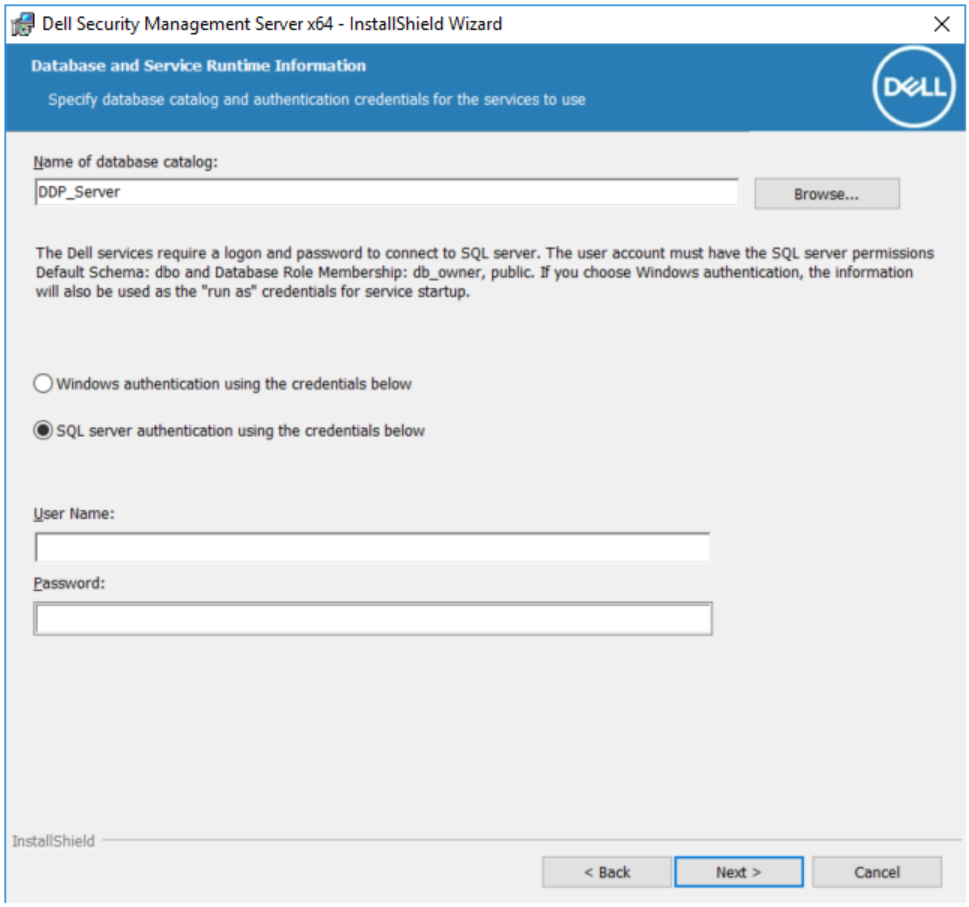


  ODER

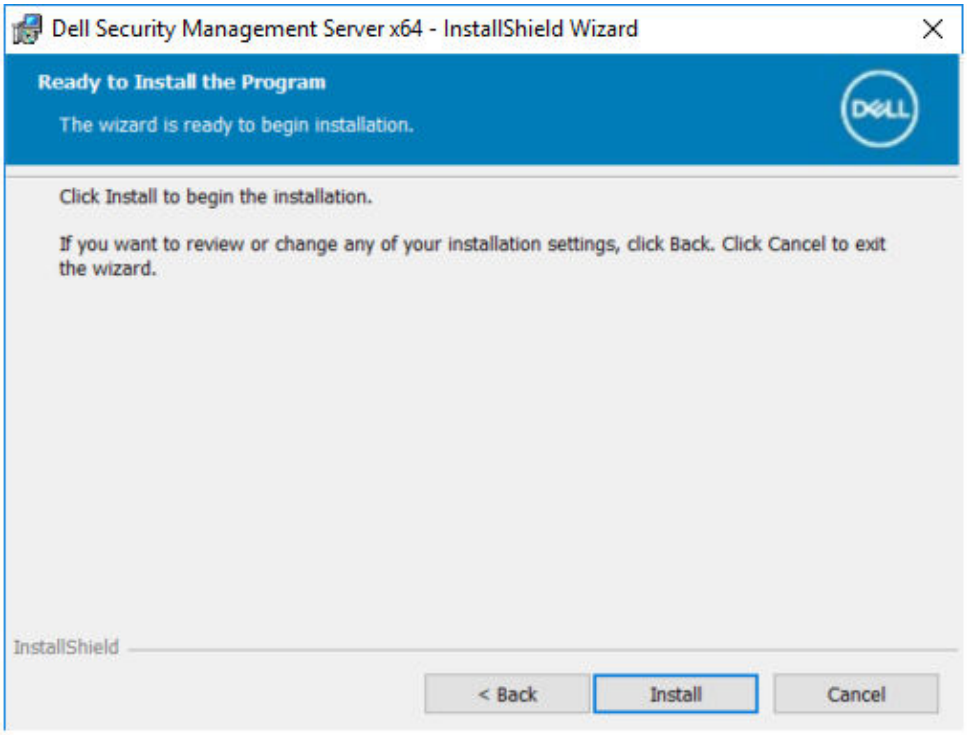
- **SQL Server-Authentifizierung**

  Wählen Sie **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen** aus, geben Sie die SQL-Server-Anmeldeinformationen für die Dell Dienste, die verwendet werden sollen, so ein, wie sie vom Security Management Server benötigt werden, und klicken Sie dann auf **Weiter.**

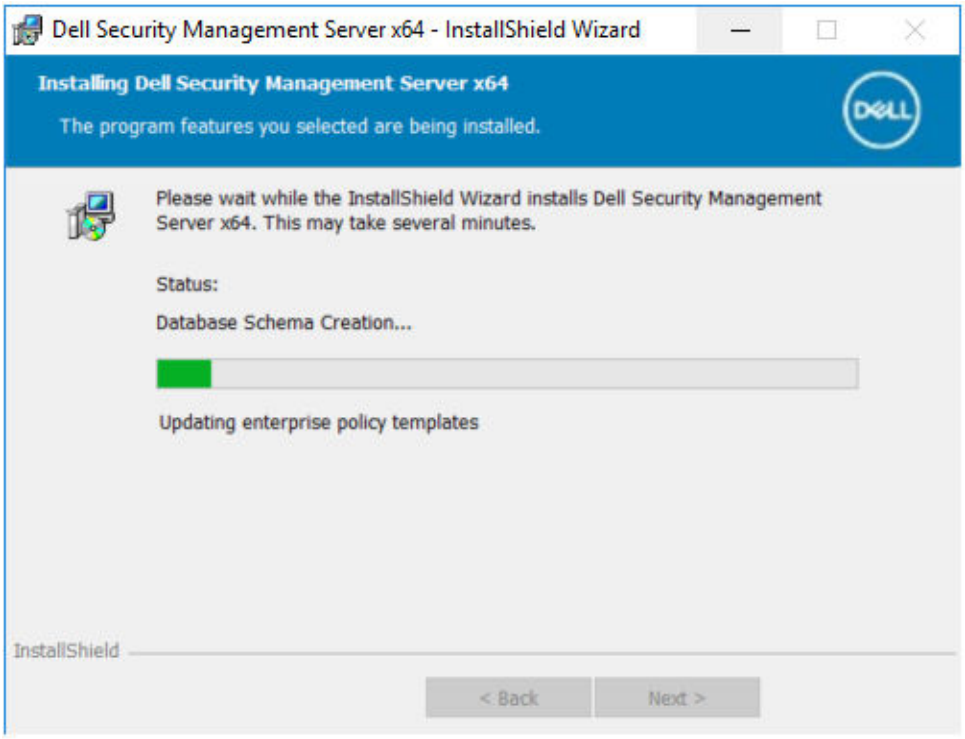
  Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.



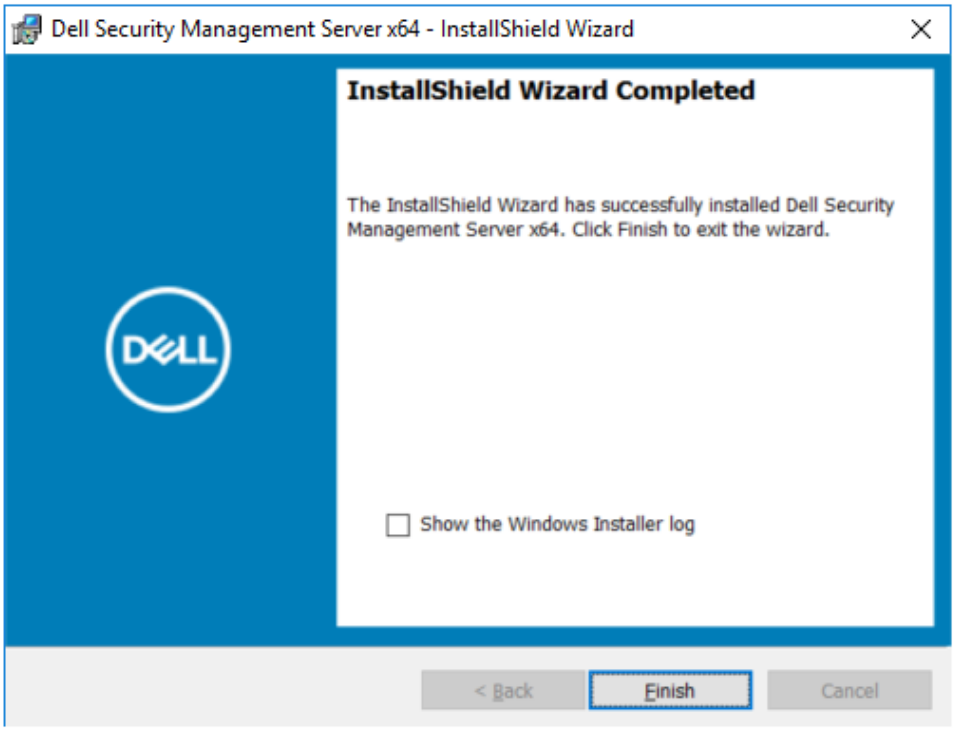
16. Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.



Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.



17. Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.



Die Back-End-Server Installationsaufgaben wurden abgeschlossen.

Die Dell Services werden am Ende der Installation neu gestartet. Es ist nicht erforderlich, den Dell Server neu zu starten.

Back-End-Server mit vorhandener Datenbank installieren

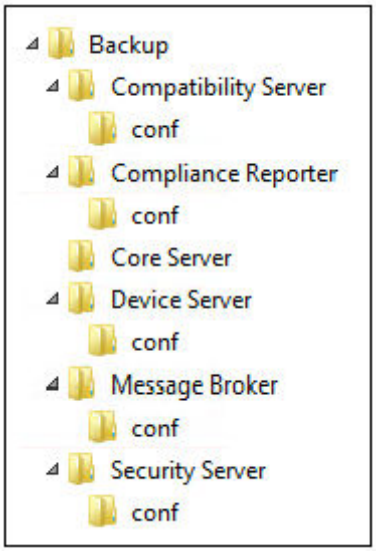
ANMERKUNG:

Falls Sie über einen funktionsfähigen Dell Server ab v9.2 verfügen, lesen Sie die Anweisungen unter Back-End-Server-Aktualisierung/Migration.

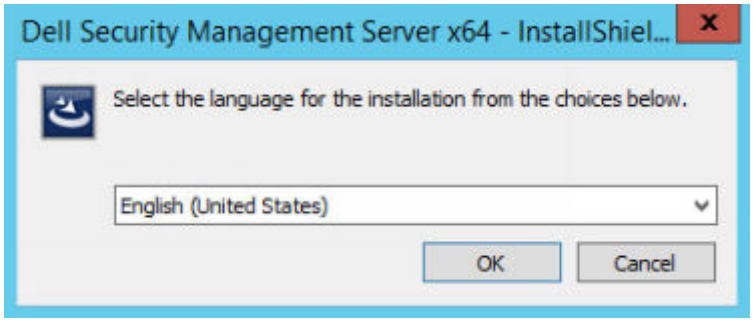
Sie können einen neuen Security Management Server installieren und diesen mit einer im Rahmen der Vorinstallationskonfiguration erstellten oder einer vorhandenen SQL-Datenbank ab Version 9.x verbinden, wenn die Schemaversion der zu installierenden Version von Security Management Server entspricht.

Das Benutzerkonto, über das die Installation durchgeführt wird, muss über Datenbankbesitzerrechte für die SQL-Datenbank verfügen. Wenn Sie sich unsicher sind in Bezug auf die Zugriffsberechtigungen oder die Konnektivität zur Datenbank, bitten Sie Ihren Datenbankadministrator um Auskunft, bevor Sie mit der Installation beginnen.

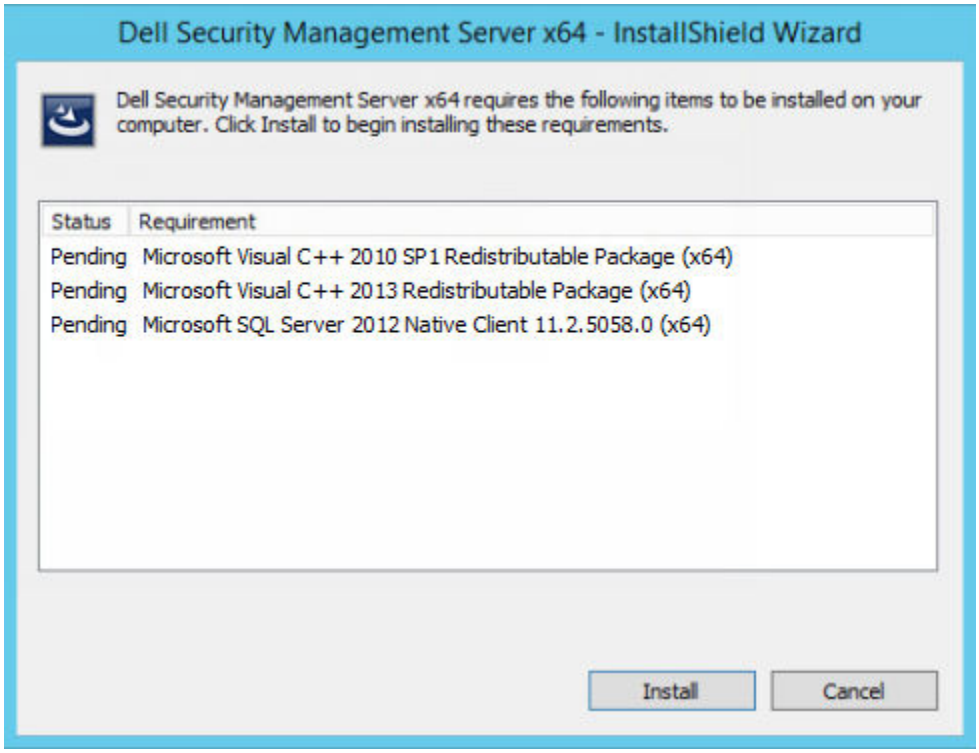
Falls die vorhandene Datenbank zuvor mit Security Management Server installiert wurde, stellen Sie vor Beginn der Installation sicher, dass die Datenbank, Konfigurationsdateien und der secretKeyStore gesichert werden, auf den Sie von dem Server aus zugreifen können, auf dem Sie Security Management Server installieren. Der Zugriff auf diese Dateien ist für die Konfiguration von Security Management Server und der vorhandenen Datenbank erforderlich. Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



1. Wechseln Sie auf dem Dell Installationsmedium in das Security Management Server-Verzeichnis. **Entpacken** Sie (NICHT kopieren/einfügen oder ziehen) Security Management Server-x64 im Stammverzeichnis des Servers, auf dem Sie Security Management Server installieren möchten. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***
2. Doppelklicken Sie auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.



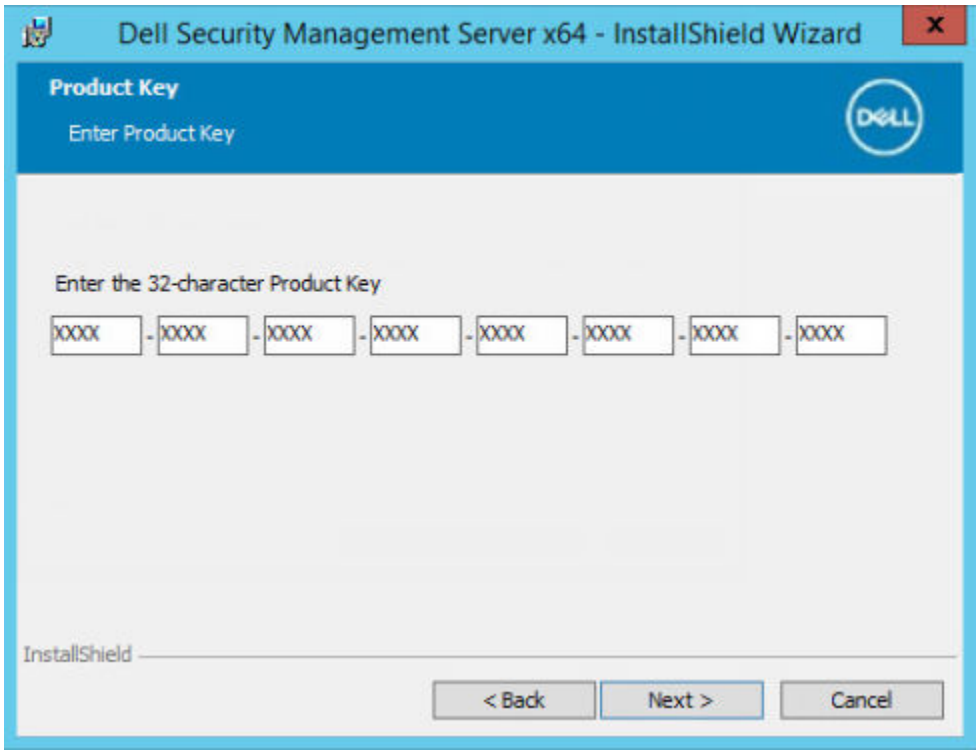
4. Wenn die Voraussetzungen noch nicht installiert wurden, wird eine Meldung angezeigt, die Sie darüber informiert, welche Voraussetzungen installiert werden Klicken Sie auf **Installieren**.



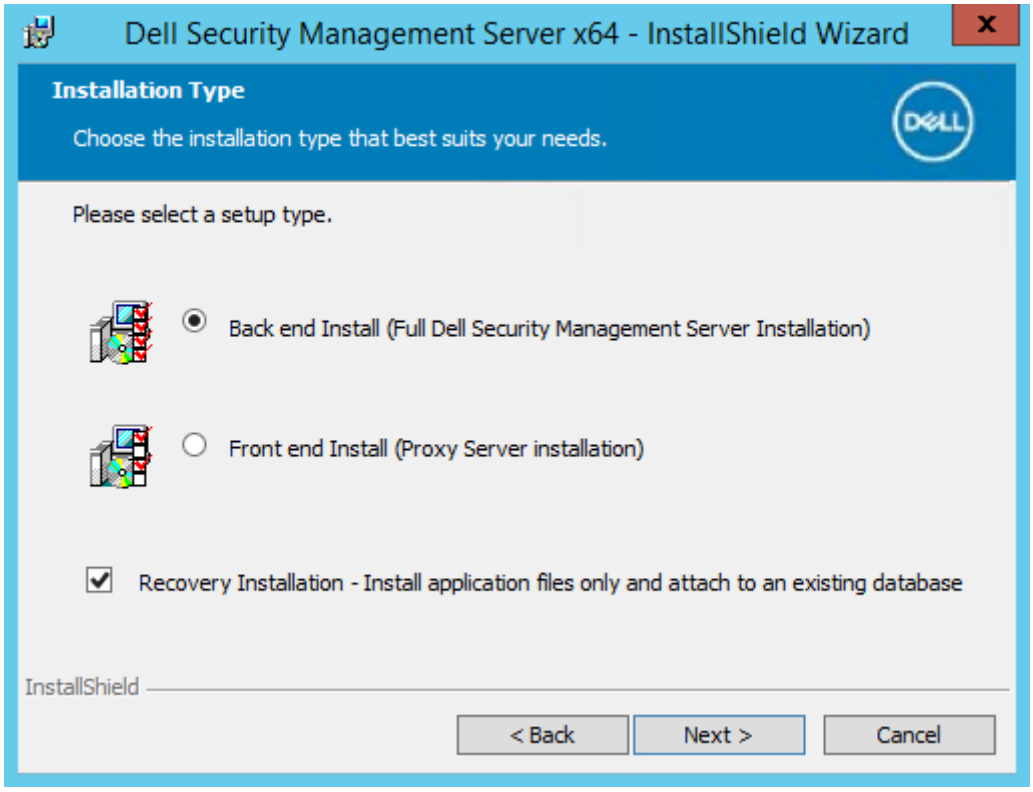
5. Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.

6. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen und klicken Sie auf **Weiter**.

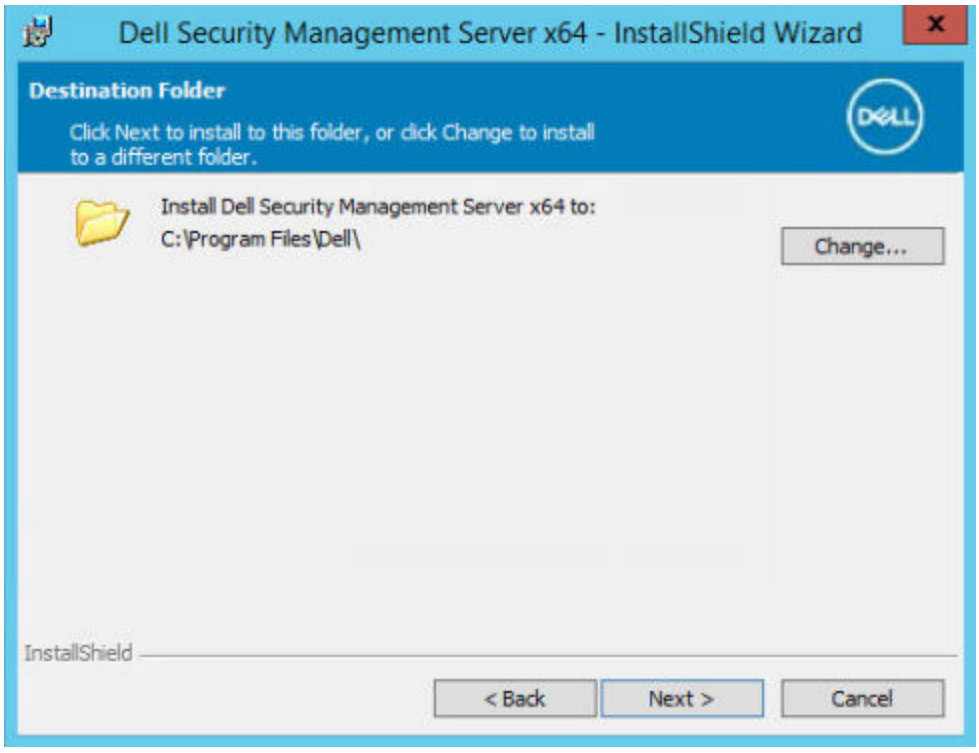
7. Wenn Sie optional Ihre `EnterpriseServerInstallKey.ini`-Datei in `C:\Windows` wie unter Vorinstallationskonfiguration erläutert kopiert haben, klicken Sie auf **Weiter**. Falls nicht, dann geben Sie den 32 Zeichen langen Produktschlüssel ein, und klicken Sie dann auf **Weiter**. Der Produktschlüssel befindet sich in der Datei `EnterpriseServerInstallKey.ini`.



8. Wählen Sie **Back-End-Installation** und **Wiederherstellungs-Installation** aus und klicken Sie auf **Weiter**.

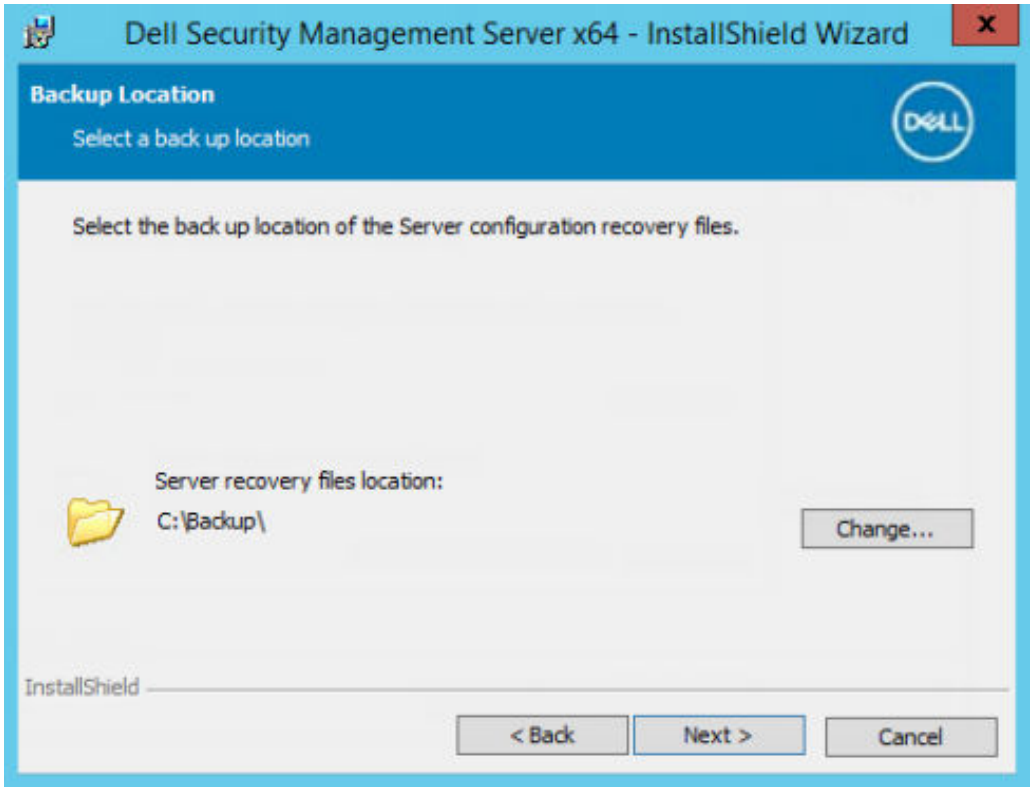


9. Klicken Sie zur Installation des Security Management Server im Standardverzeichnis `C:\Programme\Dell` auf **Weiter**. Klicken Sie anderenfalls auf **Ändern**, um einen anderen Speicherort auszuwählen; klicken Sie anschließend auf **Weiter.**



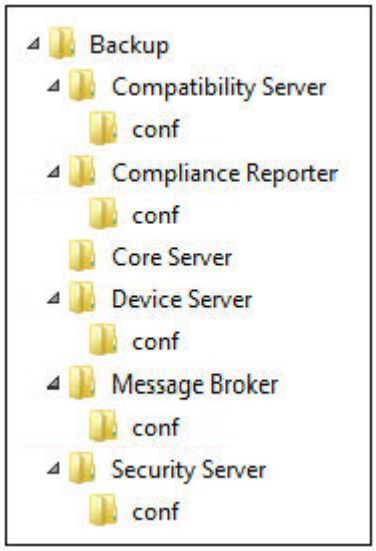
10. Klicken Sie zur Auswahl eines Speicherorts für zu speichernde Konfigurations-Wiederherstellungsdateien auf **Ändern**, navigieren Sie zum gewünschten Ordner und klicken Sie anschließend auf **Weiter**.

    Dell empfiehlt die Auswahl eines Remote-Netzwerkspeicherortes oder eines externen Sicherungslaufwerks.



Nach der Installation müssen alle Änderungen an den Konfigurationsdateien, einschließlich Änderungen, die mit dem Serverkonfigurationstool vorgenommen werden, manuell in diesen Ordnern gesichert werden. Konfigurationsdateien sind ein wichtiger Bestandteil der gesamten Informationen, die für die manuelle Wiederherstellung des Dell Servers verwendet werden.

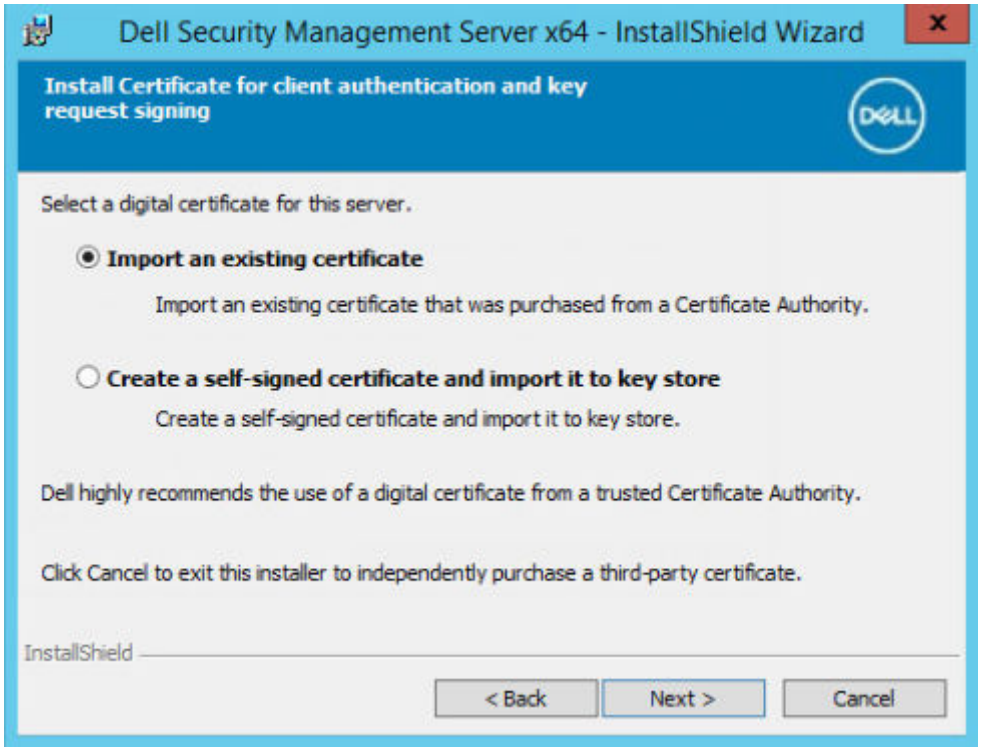
ANMERKUNG: Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



11. Sie können aus verschiedenen digitalen Zertifikatstypen auswählen. **Es wird dringend empfohlen, ein digitales Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zu verwenden.**

    Wählen Sie entweder Option „a“ oder „b“ unten aus:

    a. Um ein vorhandenes Zertifikat zu verwenden, das Sie bei einer Zertifizierungsstelle erworben haben, wählen Sie **Vorhandenes Zertifikat importieren** aus, und klicken Sie dann auf **Weiter**.



Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

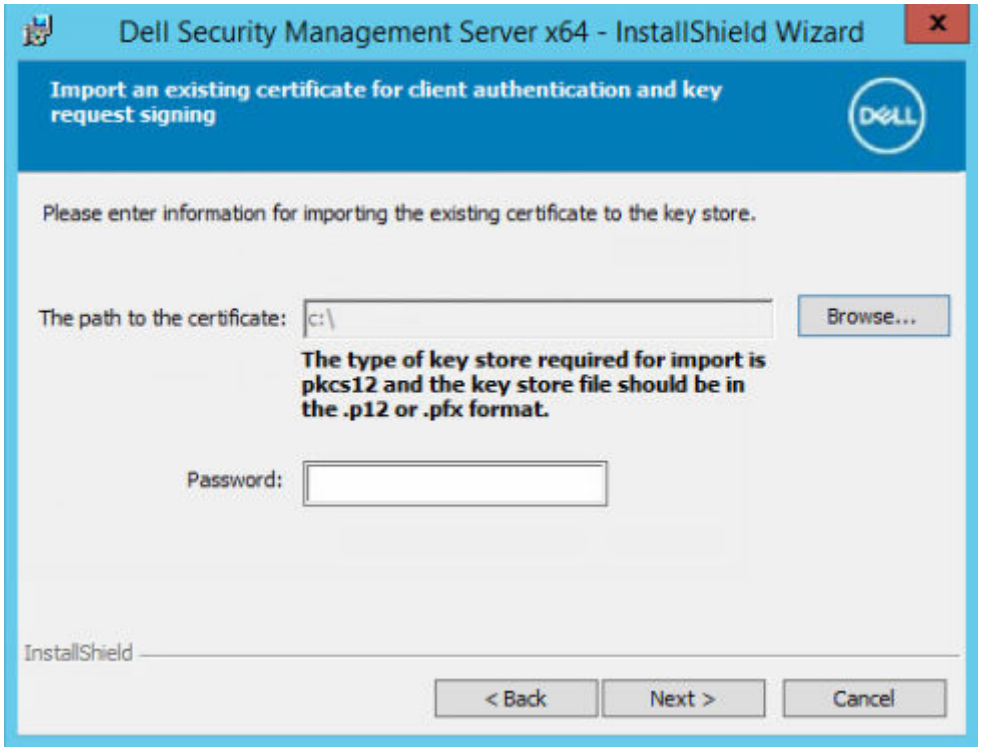
Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

ANMERKUNG:

Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren



ODER

b. Wählen Sie zum Erstellen eines selbstsignierten Zertifikats **Ein selbstsigniertes Zertifikat erstellen und in den Schlüsselspeicher importieren und klicken Sie auf Weiter.**

Geben Sie im Dialogfeld *Selbstsigniertes Zertifikat erstellen* die folgenden Informationen ein:

Vollständiger Computername (Beispiel: computername.domain.com)

Organisation

Organisationseinheit (Beispiel: Sicherheit)

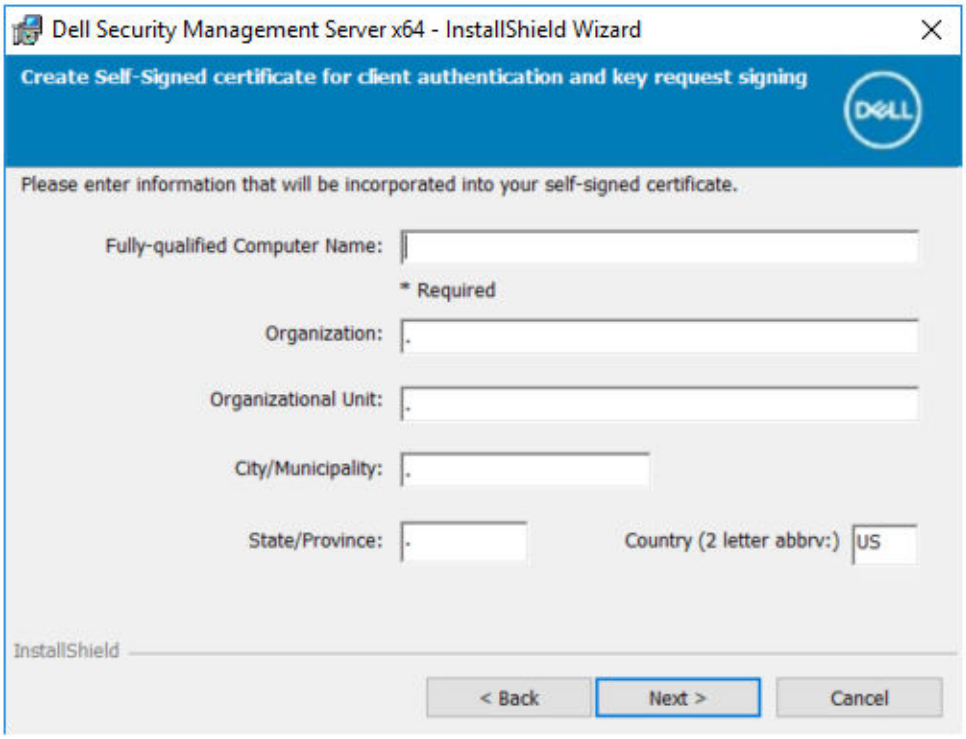
Ort

Bundesstaat (vollständiger Name)

Land: Abkürzung aus zwei Buchstaben

Klicken Sie auf **Weiter**.

ANMERKUNG: Das Zertifikat läuft standardmäßig in zehn Jahren ab.

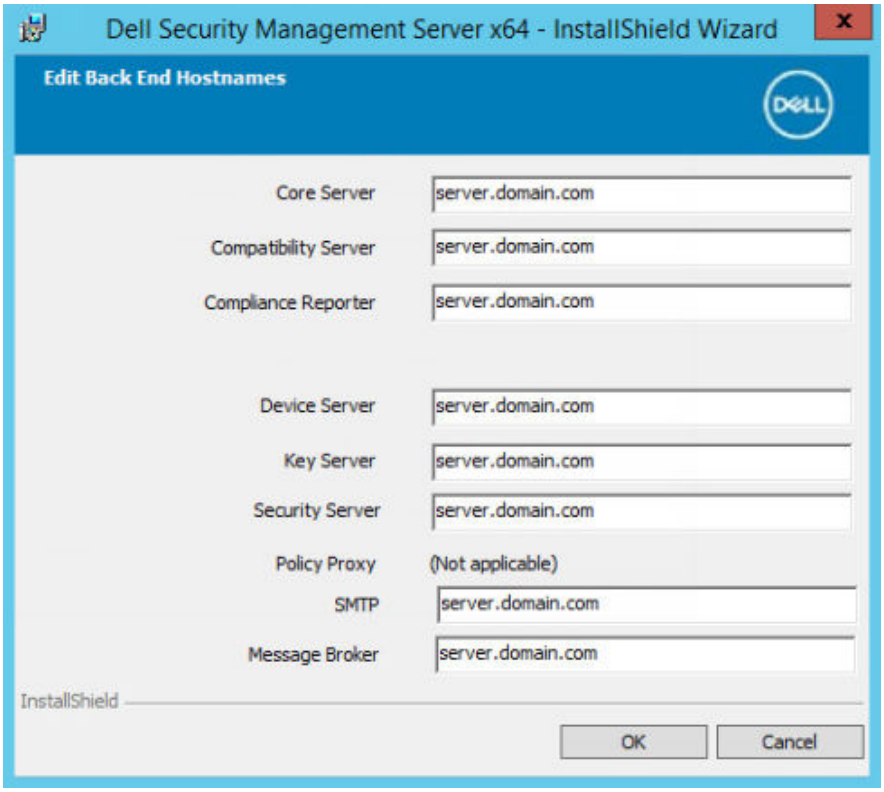


12. Über das Setup-Dialogfeld *Back-End-Server-Einrichtung* können Sie Hostnamen und Ports anzeigen oder bearbeiten.
    - Klicken Sie zum Übernehmen der Standard-Hostnamen und -Ports im Dialogfeld *Back-End-Server-Installationseinrichtung* auf **Weiter**.
    - Wenn Sie einen Front-End-Server verwenden, dann wählen Sie **Nutzt für die Kommunikation mit Clients intern in Ihrem Netzwerk oder extern in der DMZ den Front-End-Server** und geben Sie den Front-End-Sicherheitsserver-Hostnamen ein (zum Beispiel server.domain.com).

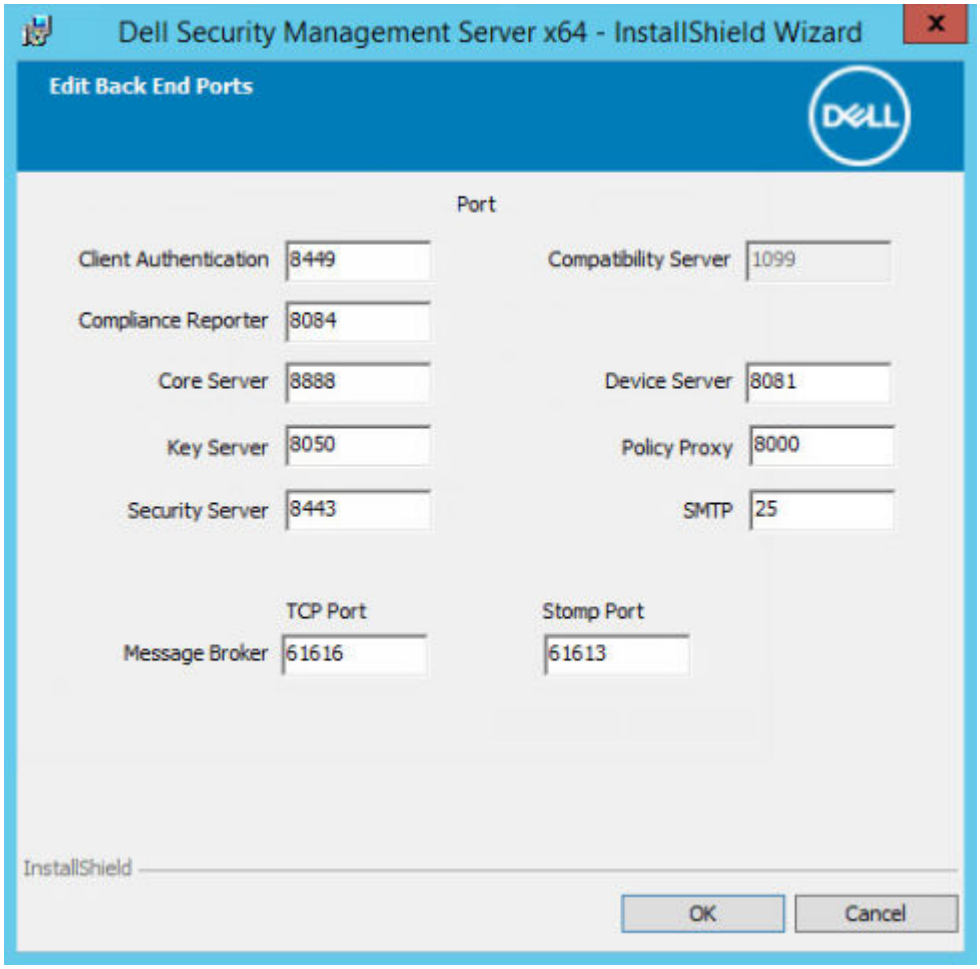
- Klicken Sie zum Anzeigen oder Bearbeiten von Hostnamen auf **Hostnamen bearbeiten**. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

  ANMERKUNG: Im Hostnamen darf kein Unterstrich (_) enthalten sein.

Klicken Sie anschließend auf **OK**.

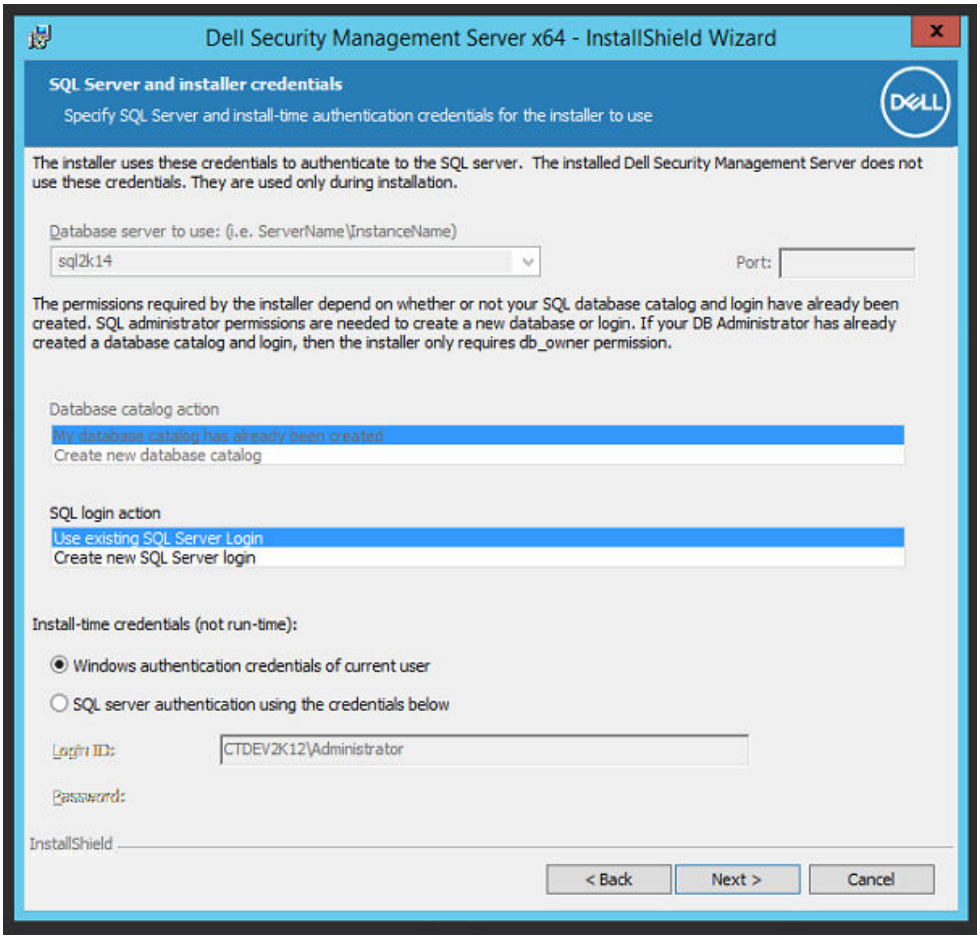


- Klicken Sie zum Anzeigen oder Bearbeiten von Ports auf **Ports bearbeiten**. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen. Klicken Sie anschließend auf **OK**.



13. Geben Sie die Authentifizierungsmethode für das zu verwendende Installationsprogramm an.
    a. Klicken Sie auf **Durchsuchen**, um den Server auszuwählen, auf dem die Datenbank sich befindet.
    b. Wählen Sie den Authentifizierungstyp aus.
        - **Anmeldeinformationen für die Windows-Authentifizierung des aktuellen Benutzers**

          Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (*Benutzername* und *Kennwort* sind nicht bearbeitbar). Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt.



ODER

- **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**

  Bei Verwendung der SQL-Authentifizierung muss das verwendete SQL-Konto auf dem SQL-Server über Systemadministratorberechtigungen verfügen.

  Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen.

c. Klicken Sie auf **Durchsuchen**, um nach dem Namen des vorhandenen Datenbank-Katalogs zu suchen.
d. Klicken Sie auf **Weiter**.

14. Wenn ein Dialogfeld mit einem bestehenden Datenbankfehler angezeigt wird, wählen Sie die entsprechende Option aus.

Wenn das Installationsprogramm ein Problem mit der Datenbank erkennt, wird das Dialogfeld *Vorhandene Datenbank – Fehler* angezeigt. Die Optionen in diesem Dialogfeld richten sich nach den jeweiligen Umständen:

- Das Datenbankschema stammt aus einer vorherigen Version. (Siehe Schritt a.)
- Die Datenbank weist bereits ein Datenbankschema auf, das mit der Version, die derzeit installiert wird, übereinstimmt. (Siehe Schritt b.)

a. Wenn das Datenbankschema aus einer vorherigen Version stammt, wählen Sie <2>Installationsprogramm beenden</2> aus, **um diese Installation zu beenden**. Im nächsten Schritt müssen Sie die Datenbank sichern.

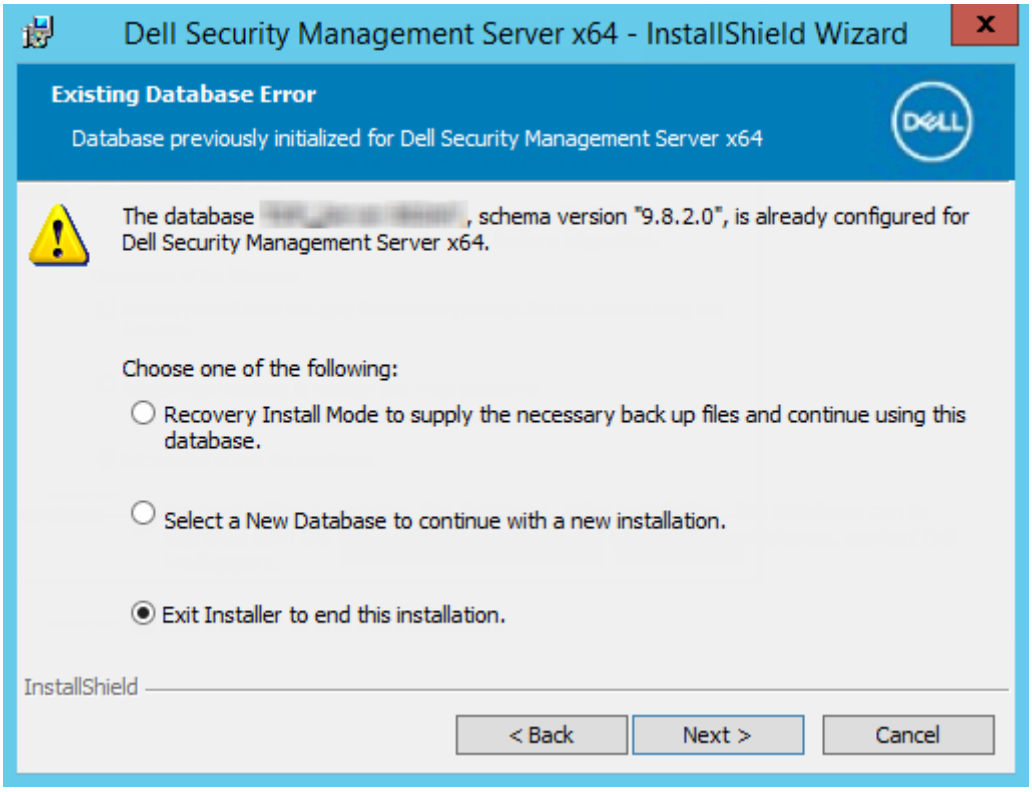
Die folgenden Optionen DÜRFEN nur mit Unterstützung durch den Dell ProSupport verwendet werden:

- Die Option **Diese Datenbank mit dem aktuellen Schema migrieren** wird verwendet, um eine gute Datenbank aus einer fehlerhaften Serverimplementierung wiederherzustellen. Diese Option verwendet die Wiederherstellungsdateien im Ordner „\Backup“, um die Verbindung zur Datenbank wiederherzustellen, und migriert anschließend die Datenbank mit dem aktuellen Schema. Diese Option sollte *erst* verwendet werden, nachdem Sie zunächst versucht haben, die korrekte Version von Security Management Server neu zu installieren und anschließend das aktuelle Installationsprogramm für die Aktualisierung ausgeführt haben.
- Mit der Option **Fortfahren, ohne die Datenbank zu migrieren** werden die Security Management Server-Dateien installiert, ohne die Datenbank zu konfigurieren. Die Datenbankkonfiguration muss später manuell über das Serverkonfigurationstool abgeschlossen werden. Außerdem sind weitere manuelle Änderungen erforderlich.

b. Wenn das Datenbankschema bereits die aktuelle Schemaversion verwendet, jedoch nicht mit einem Dell Security Management Server-Back-End verbunden ist, wird es als *Wiederherstellung* betrachtet. Wenn **Installation der Wiederherstellung** in diesen Schritt nicht ausgewählt wurde, erscheint der Dialog:

- Wählen Sie **Wiederherstellungs-Installationsmodus** aus, um die Installation mit der ausgewählten Datenbank fortzusetzen.
- Wählen Sie **Neue Datenbank auswählen** aus, um eine andere Datenbank auszuwählen.
- Wählen Sie **Installationsprogramm beenden** aus, um diese Installation zu beenden.

c. Klicken Sie auf **Weiter**.



15. Wählen Sie die Authentifizierungsmethode für das zu verwendende Produkt aus. Dies ist das Konto, das das Produkt für die Zusammenarbeit mit der Datenbank und den Dell Diensten verwendet.

- **Verwendung der Windows-Authentifizierung**

  Wählen Sie **Windows-Authentifizierung über die unten angegebenen Anmeldeinformationen** aus, geben Sie die Anmeldeinformationen für das Konto ein, auf dem das Produkt verwendet werden kann, und klicken Sie auf **Weiter**.

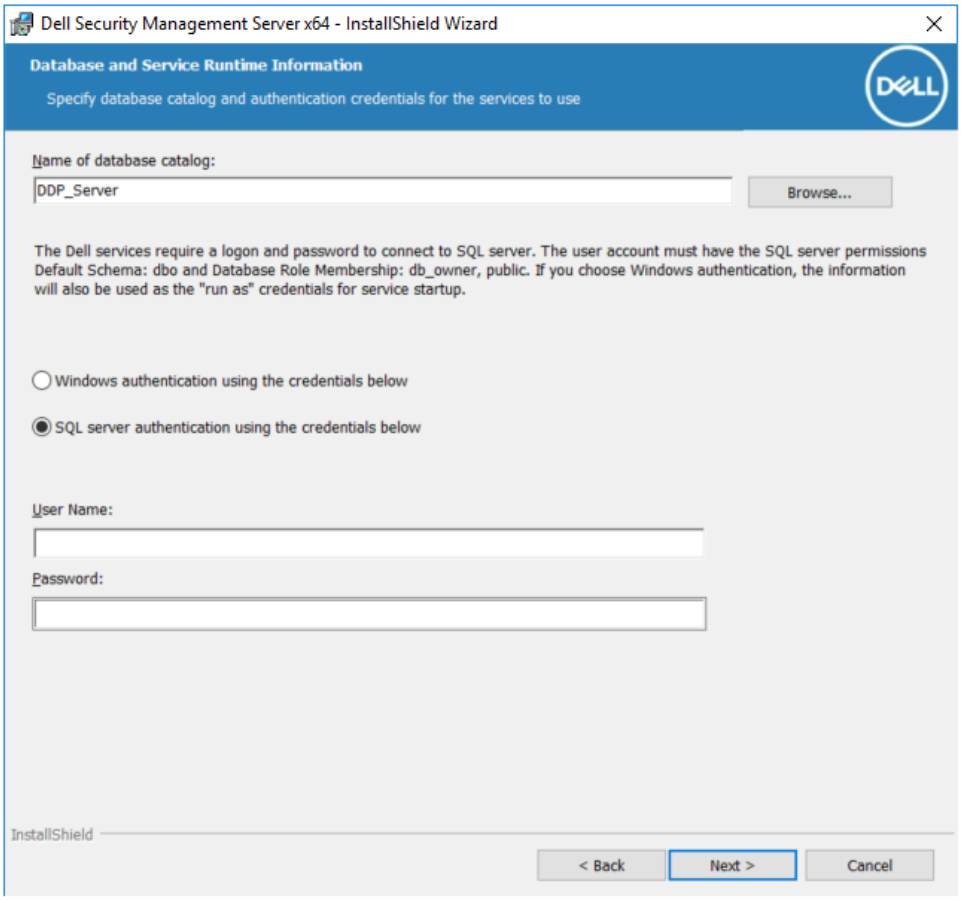
  Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

  ODER

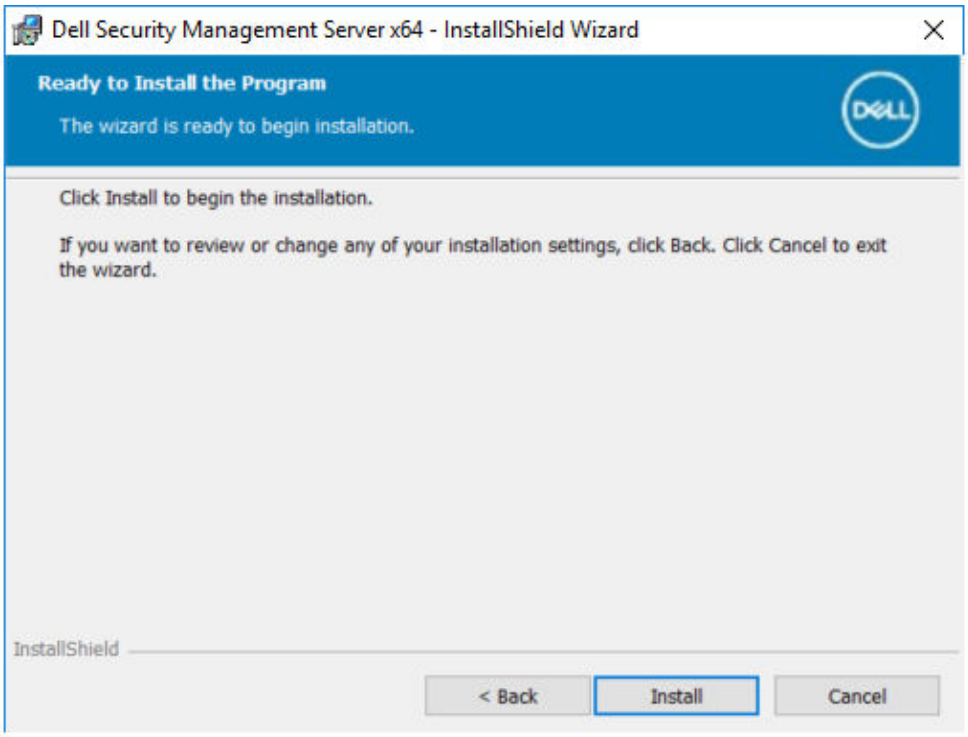
- **Verwendung der SQL Server-Authentifizierung**

  Wählen Sie **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**, geben Sie die SQL-Server-Anmeldeinformationen ein und klicken Sie auf **Weiter**.

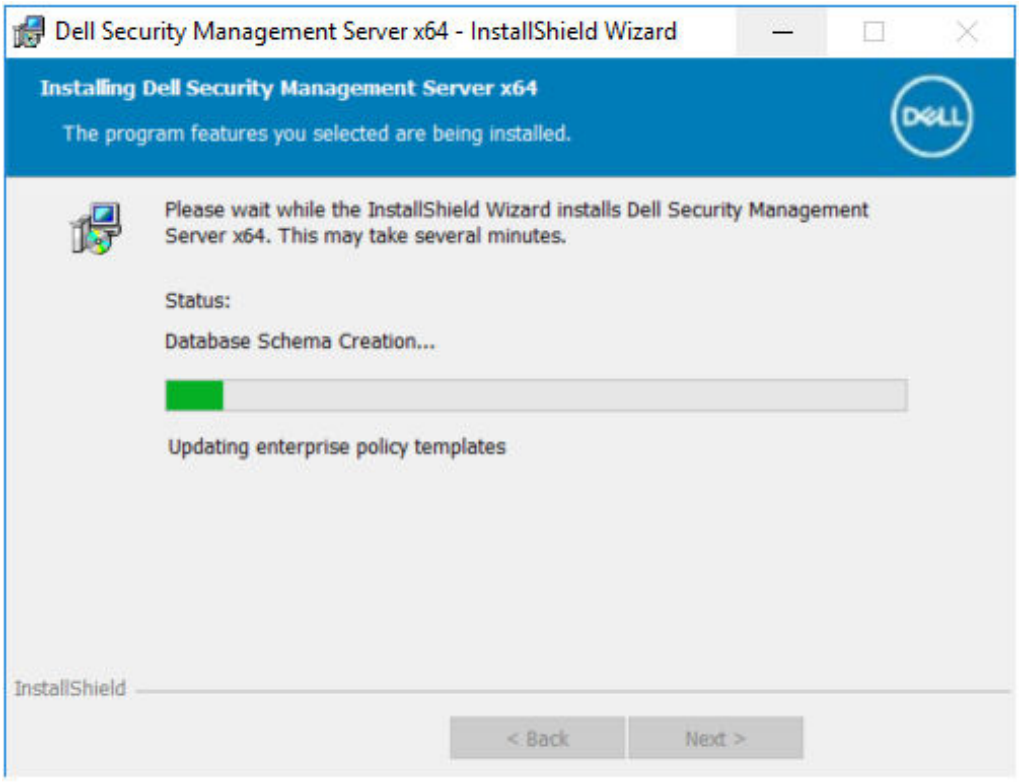
  Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.



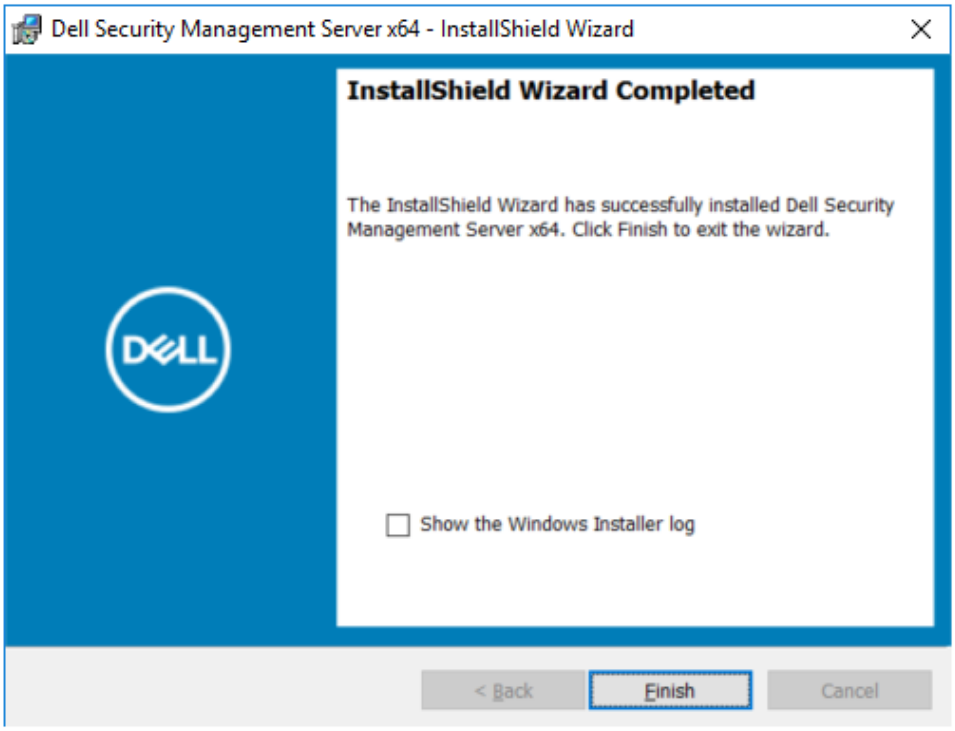
16. Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.



Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.



Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.



Die Back-End-Server Installationsaufgaben wurden abgeschlossen.

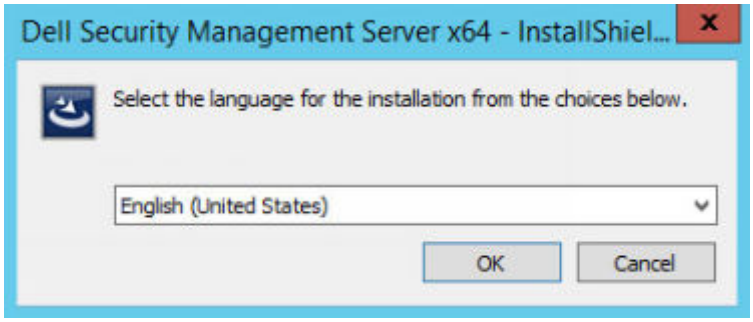
Die Dell Services werden am Ende der Installation neu gestartet. Es ist nicht erforderlich, den Server neu zu starten.

Front-End-Server installieren

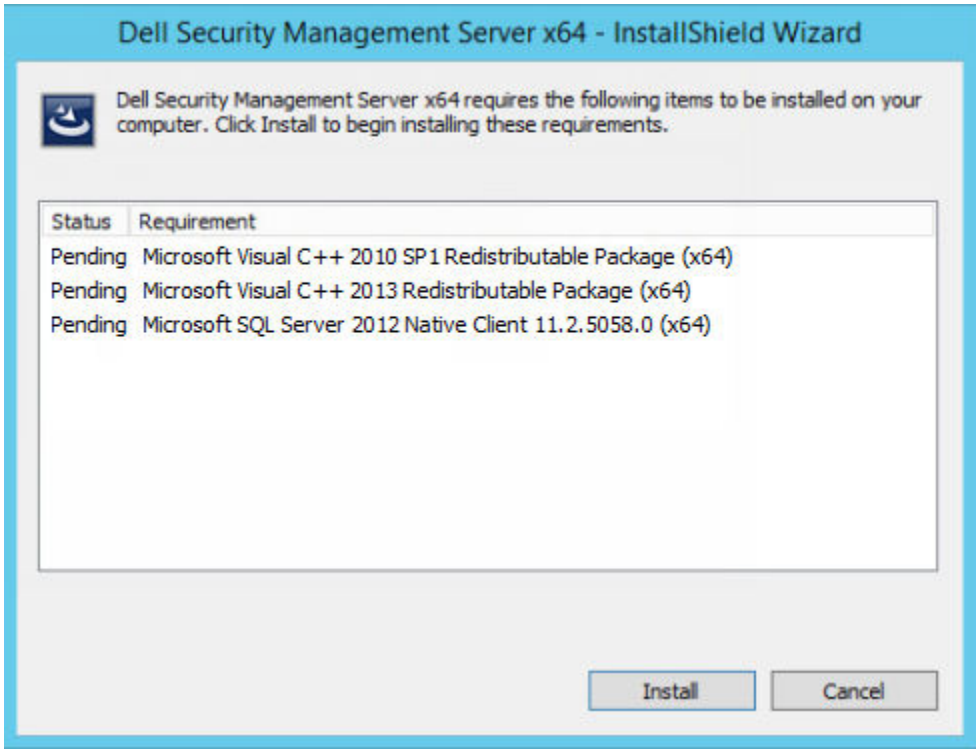
Front-End-Server-Installation bietet eine Front-End-Option (DMZ-Modus) für die Verwendung mit Security Management Server. Wenn Sie Dell-Komponenten in Ihre DMZ implementieren möchten, vergewissern Sie sich, dass sie ausreichend vor Angriffen geschützt sind.

Für diese Installation benötigen Sie den vollständig qualifizierten Hostnamen des DMZ-Servers.

1. Wechseln Sie auf dem Dell Installationsmedium in das Security Management Server-Verzeichnis. **Entpacken** Sie (NICHT kopieren/einfügen oder ziehen) Security Management Server-x64 im Stammverzeichnis des Servers, auf dem Sie Security Management Server installieren möchten. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***
2. Doppelklicken Sie auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.

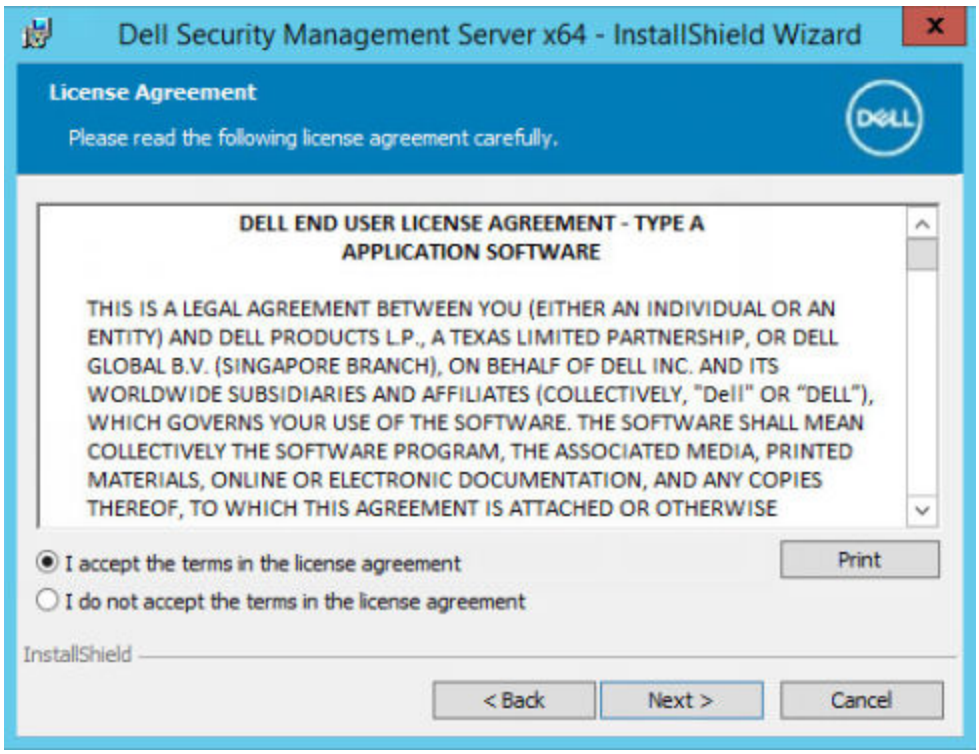


4. Wenn die Voraussetzungen noch nicht installiert wurden, wird eine Meldung angezeigt, die Sie darüber informiert, welche Voraussetzungen installiert werden Klicken Sie auf **Installieren**.

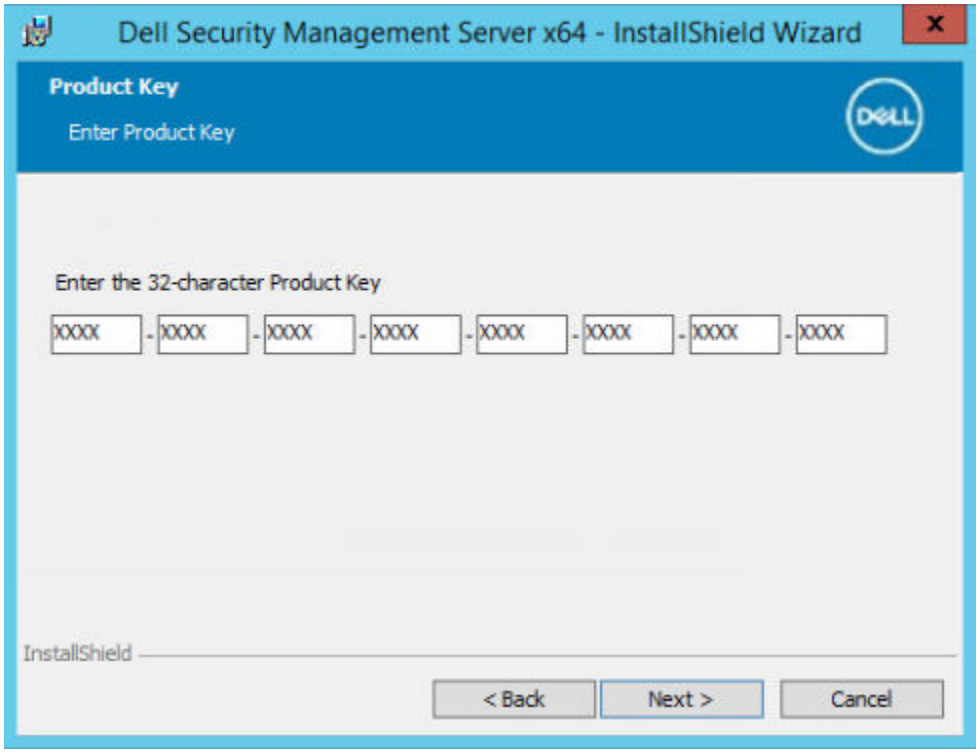


5. Klicken Sie im Dialogfeld „Willkommen“ auf **Weiter**.

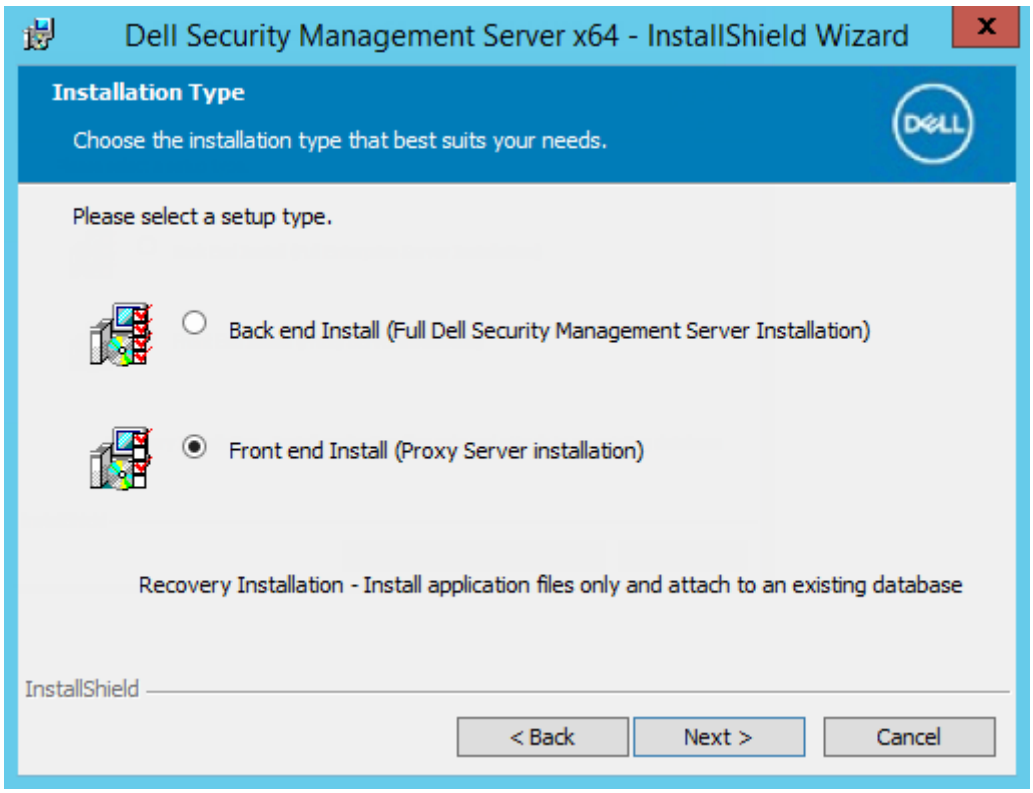
6. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen und klicken Sie auf **Weiter**.



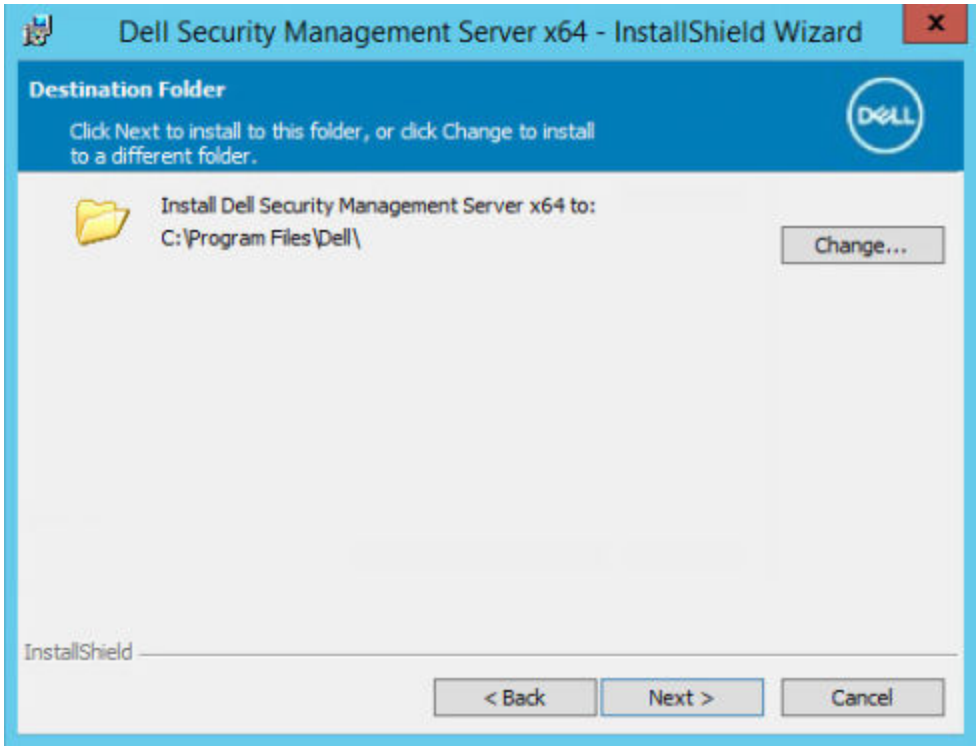
7. Wenn Sie optional Ihre `EnterpriseServerInstallKey.ini`-Datei in `C:\Windows` wie unter Vorinstallationskonfiguration erläutert kopiert haben, klicken Sie auf **Weiter**. Falls nicht, dann geben Sie den 32 Zeichen langen Produktschlüssel ein, und klicken Sie dann auf **Weiter**. Der Produktschlüssel befindet sich in der Datei `EnterpriseServerInstallKey.ini`.



8. Wählen Sie **Front-End-Installation** aus, und klicken Sie dann auf **Weiter**.



9. Klicken Sie zur Installation des Front-End-Servers im Standardverzeichnis `C:\Programme\Dell` auf **Weiter**. Klicken Sie anderenfalls auf **Ändern**, um einen anderen Speicherort auszuwählen; klicken Sie anschließend auf **Weiter**.

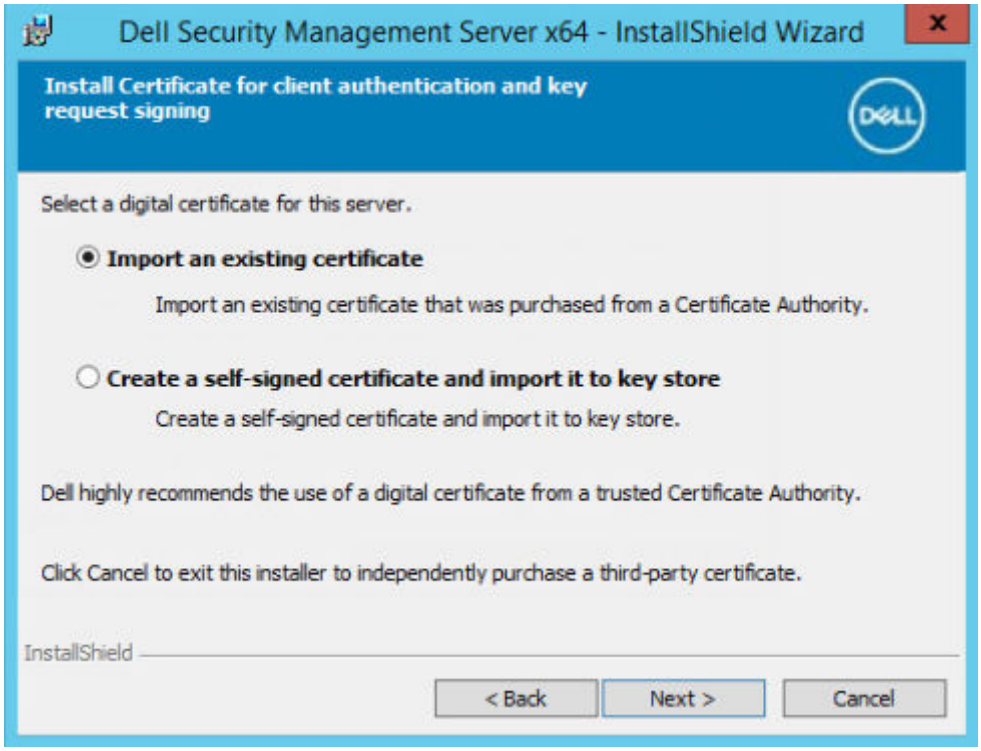


10. Sie können aus verschiedenen digitalen Zertifikatstypen auswählen.

ANMERKUNG: Es wird dringend empfohlen, ein digitales Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zu verwenden.

Wählen Sie entweder Option „a“ oder „b“ unten aus:

a. Um ein vorhandenes Zertifikat zu verwenden, das Sie bei einer Zertifizierungsstelle erworben haben, wählen Sie **Vorhandenes Zertifikat importieren** aus, und klicken Sie dann auf **Weiter**.



Klicken Sie auf **Durchsuchen**, um den Pfad zum Zertifikat einzugeben.

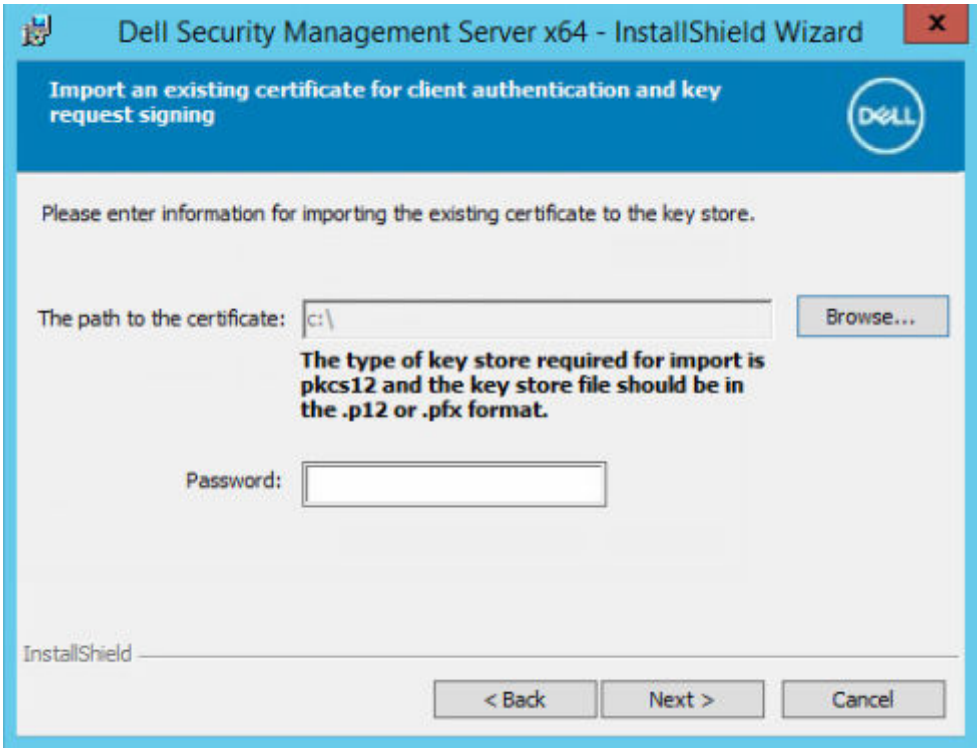
Geben Sie das Passwort ein, das mit diesem Zertifikat verknüpft ist. Die Keystore-Datei muss „.p12“ oder „pfx“ sein. Anleitungen finden Sie unter Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren.

Klicken Sie auf **Weiter**.

ANMERKUNG:

Wenn Sie diese Einstellung verwenden möchten, muss das exportierte Zertifikat der Zertifizierungsstelle für den Import eine vollständige Vertrauenskette aufweisen. Wenn Sie nicht sicher sind, führen Sie den Export des Zertifikats der Zertifizierungsstelle erneut aus, und stellen Sie sicher, dass die folgenden Optionen im Assistenten für den Zertifikatsexport ausgewählt wurden:

- Privater Informationsaustausch – PKCS#12 (.PFX)
- Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen
- Alle erweiterten Eigenschaften exportieren



b. Wählen Sie zum Erstellen eines selbstsignierten Zertifikats **Ein selbstsigniertes Zertifikat erstellen und in den Schlüsselspeicher importieren und klicken Sie auf Weiter.**

Geben Sie im Dialogfeld *Selbstsigniertes Zertifikat erstellen* die folgenden Informationen ein:

Vollständiger Computername (Beispiel: computername.domain.com)

Organisation

Organisationseinheit (Beispiel: Sicherheit)

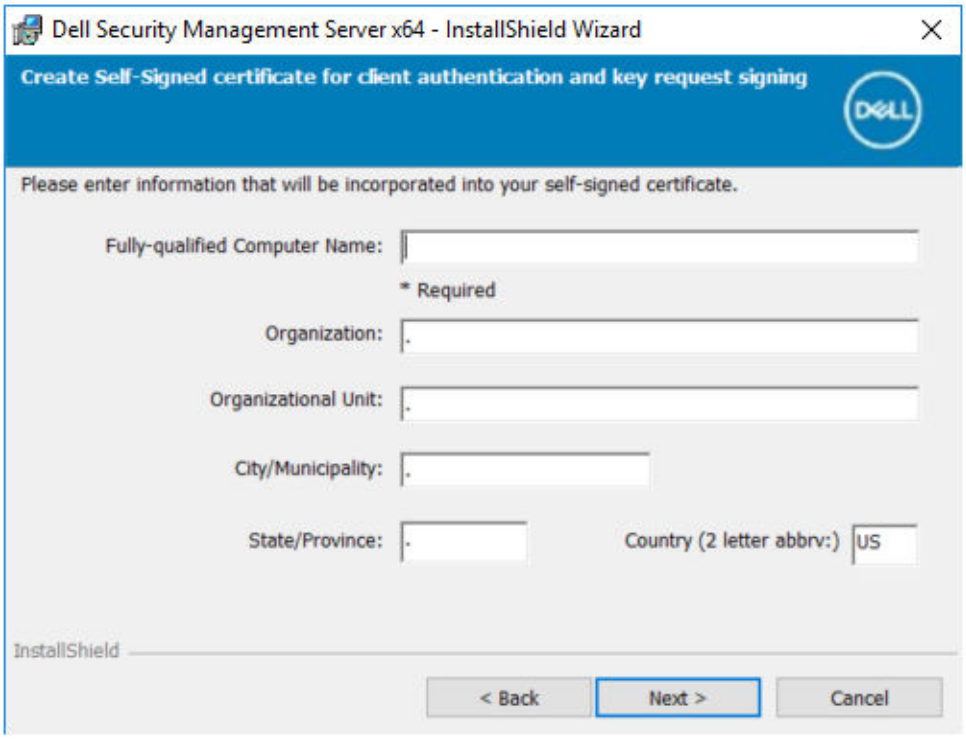
Ort

Bundesstaat (vollständiger Name)

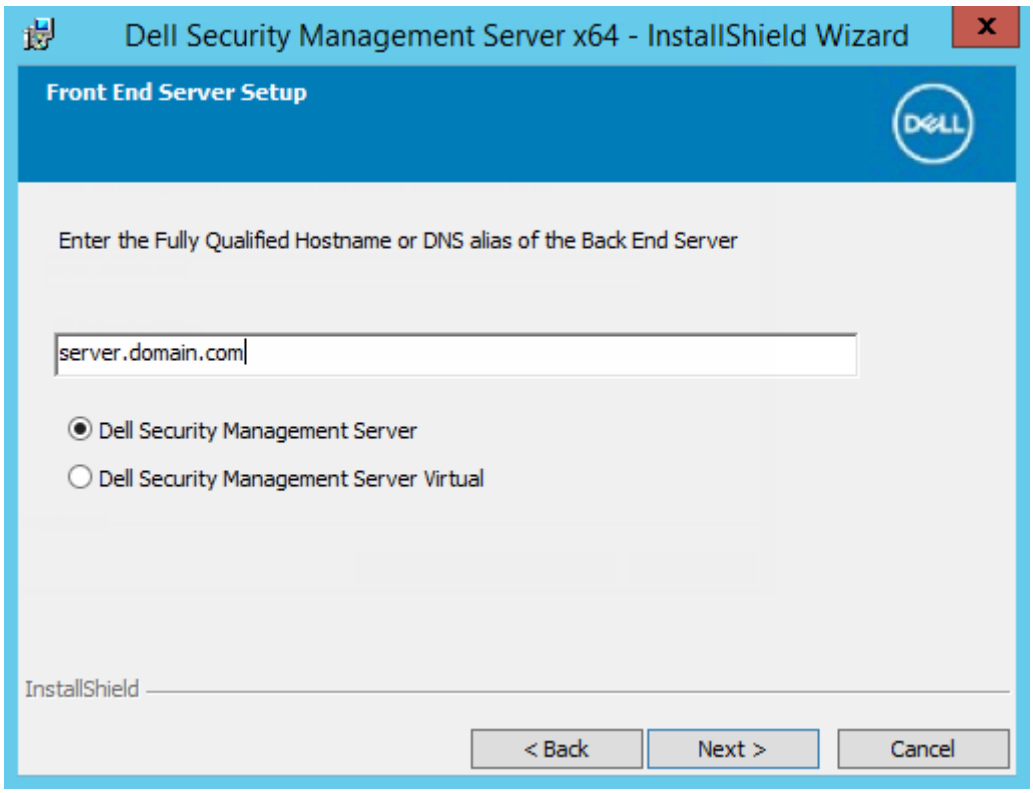
Land: Abkürzung aus zwei Buchstaben

Klicken Sie auf **Weiter**.

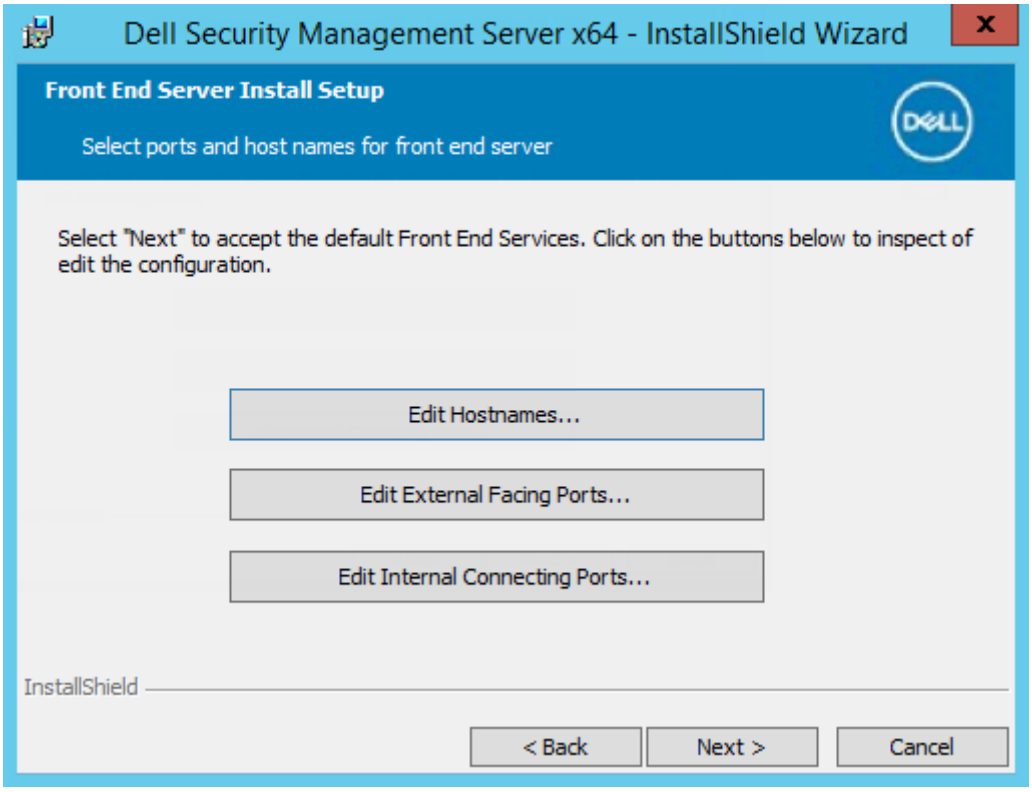
ANMERKUNG: Das Zertifikat läuft standardmäßig in zehn Jahren ab.



11. Geben Sie im Dialogfeld *Front-End-Server-Setup* den vollständigen Hostnamen oder DNS-Alias des Back-End-Servers ein, wählen Sie **Dell Security Management Server** aus und klicken Sie auf **Weiter**.



12. Über das Dialogfeld *Front-End-Server-Installationseinrichtung* können Sie Hostnamen und Ports anzeigen oder bearbeiten.
    - Klicken Sie zum Übernehmen der Standard-Hostnamen und -Ports im Dialogfeld *Front-End-Server-Installationseinrichtung* auf **Weiter**.



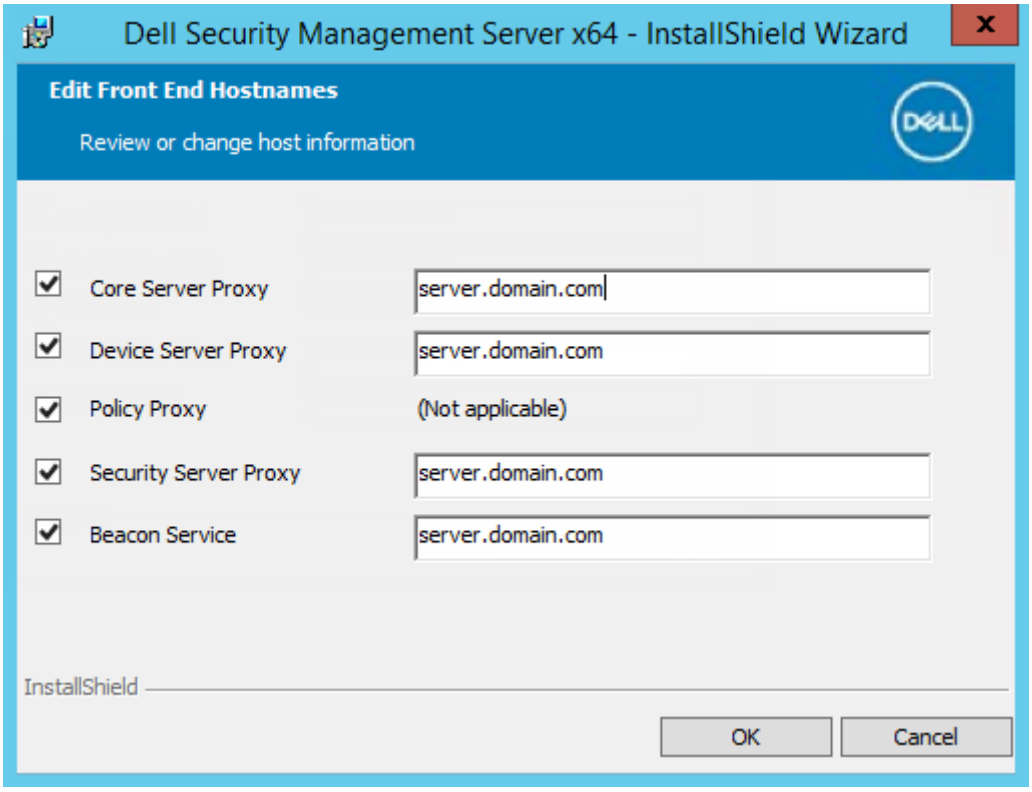
- Klicken Sie zum Anzeigen oder Bearbeiten von Hostnamen im Dialogfeld *Front-End-Server-Setup* auf **Hostnamen bearbeiten**. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

  ANMERKUNG:

  Im Hostnamen darf kein Unterstrich (_) enthalten sein.

  Heben Sie die Auswahl eines Proxys nur dann auf, wenn Sie sicher sind, dass Sie ihn nicht für die Installation konfigurieren wollen. Wenn Sie die Auswahl eines Proxys in diesem Dialogfeld aufheben, wird er nicht installiert.

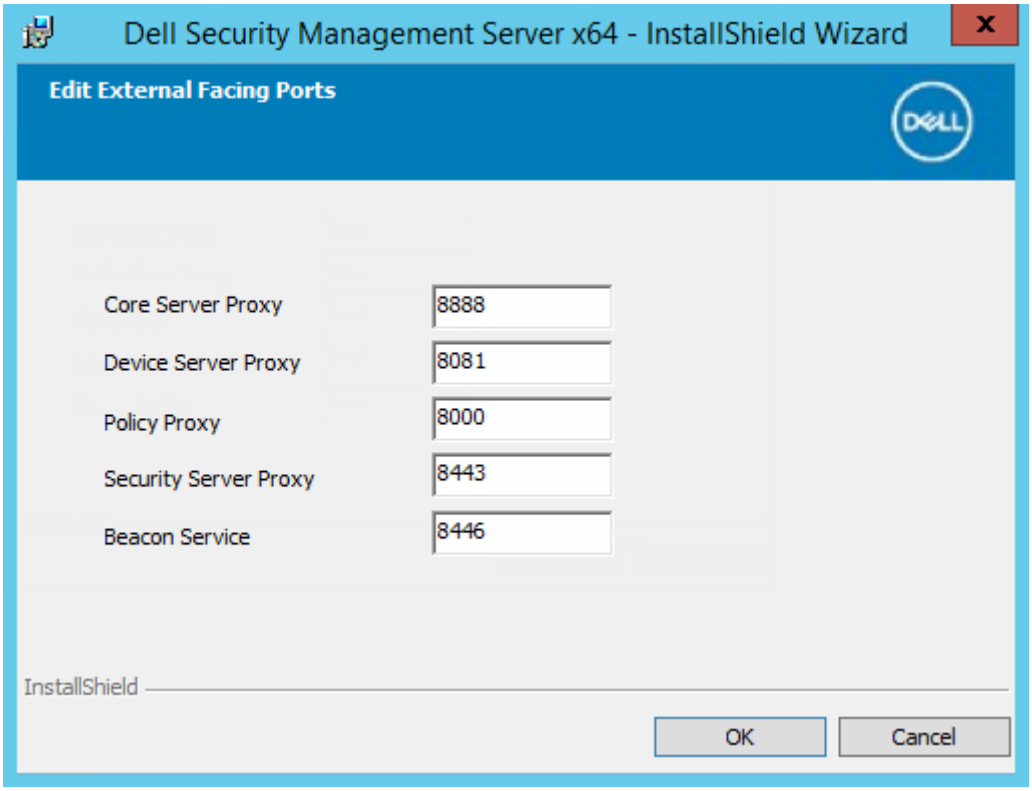
  Klicken Sie anschließend auf **OK**.

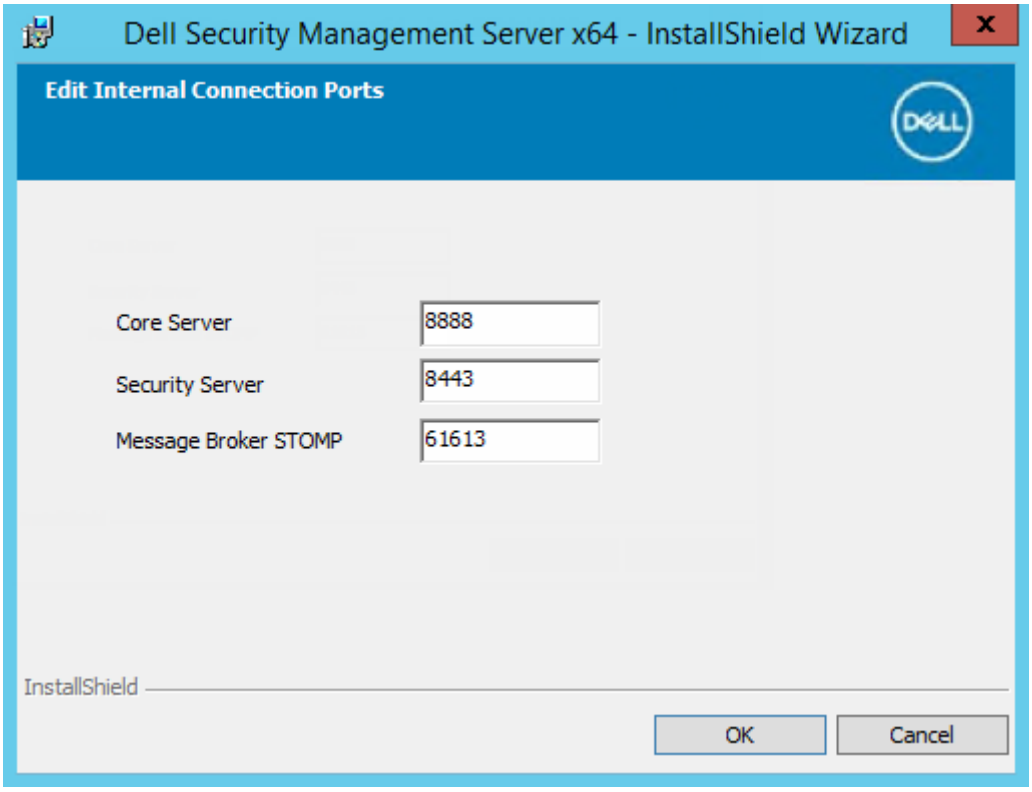


- Klicken Sie zum Anzeigen oder Bearbeiten von Ports im Dialogfeld *Front-End-Server-Setup* entweder auf **Externe Ports bearbeiten** oder **Interne Ports bearbeiten**. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen.

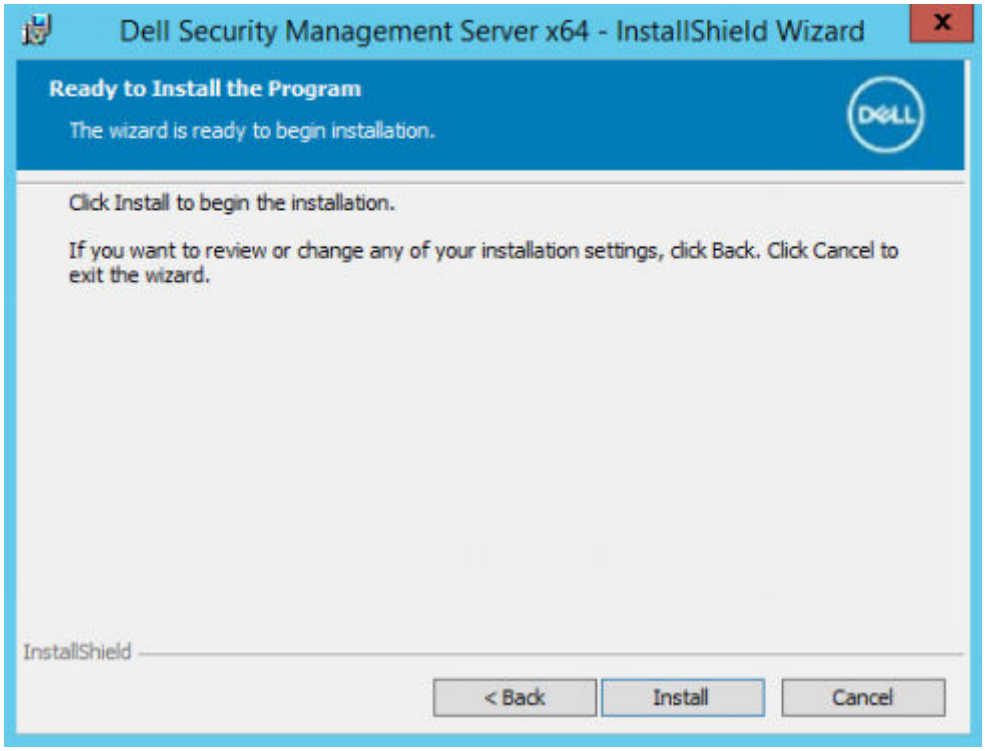
  Wenn Sie die Auswahl eines Proxys im Dialogfeld *Front-End-Hostnamen bearbeiten* aufheben, wird sein Port in den Dialogfeldern für Externe Ports und Interne Ports nicht angezeigt.

  Klicken Sie anschließend auf **OK**.

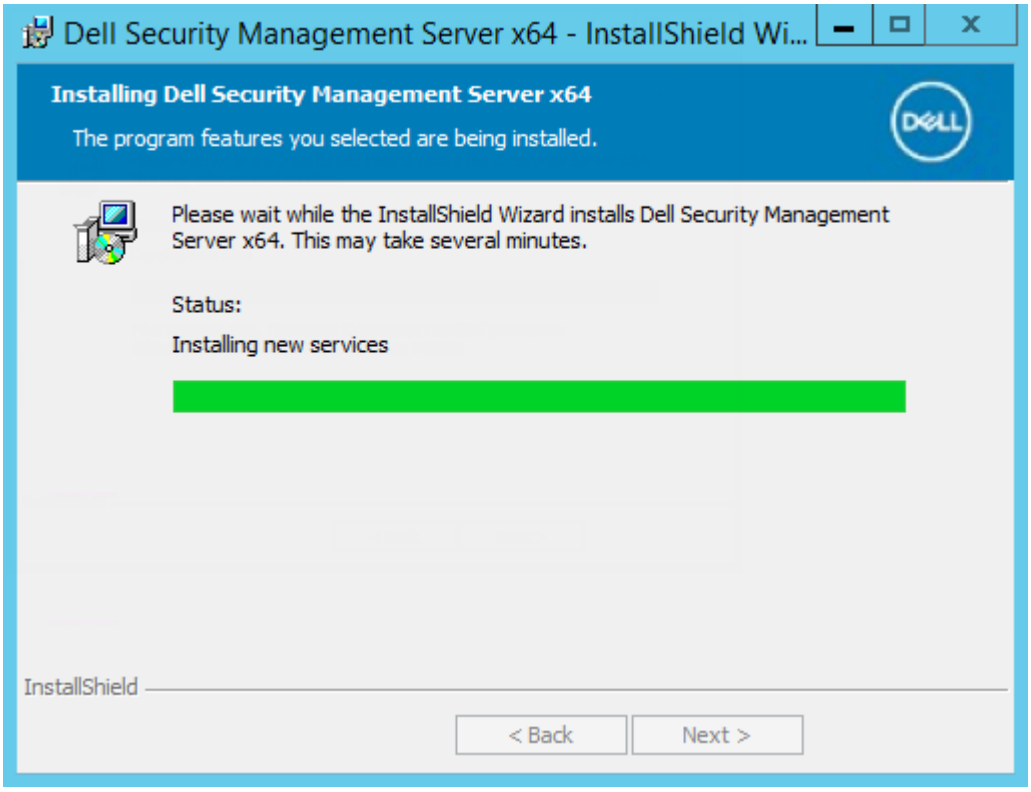




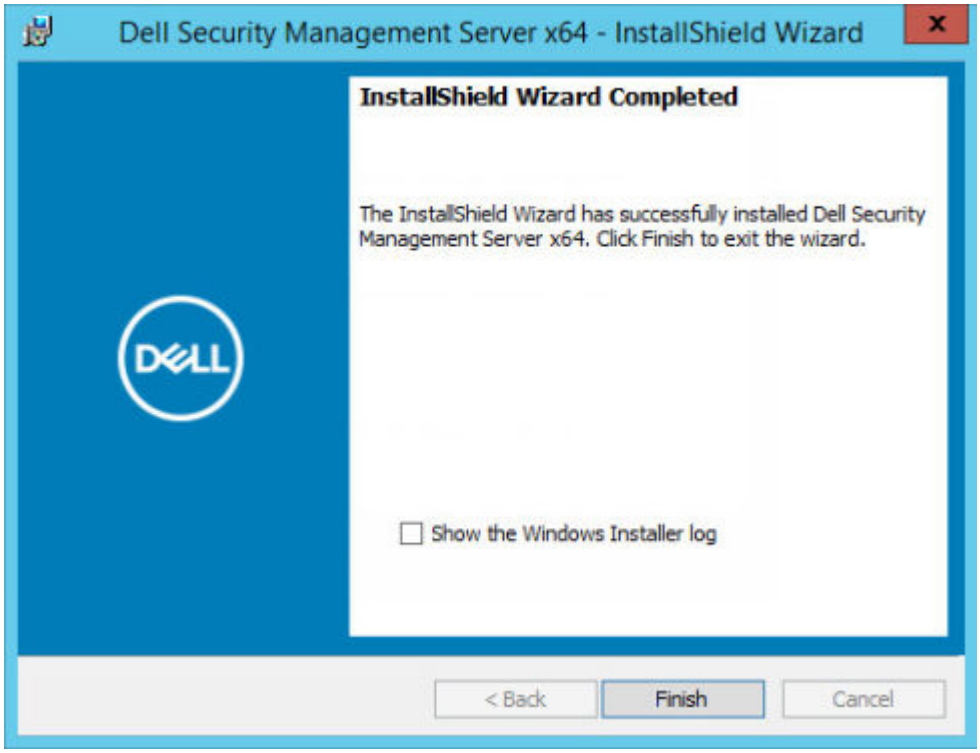
13. Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.



Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.



14. Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.



Die Front-End-Server-Installationsaufgaben wurden abgeschlossen.

Aktualisierung/Migration

Sie können Enterprise Server v9.2 und höher auf Security Management Server v10.x aktualisieren. Wenn Ihre Dell Server-Version älter als v9.2 ist, müssen Sie zuerst auf v9.2 und anschließend auf höhere Versionen aktualisieren.

Vor der Aktualisierung oder Migration

Bevor Sie beginnen, stellen Sie sicher, dass die Vorinstallationskonfiguration komplett durchgeführt wurde.

Lesen Sie die *Technischen Tipps für Security Management Server*, um sich über aktuelle Lösungen oder bekannte Probleme hinsichtlich der Installation von *Security Management Server* zu informieren.

Das Benutzerkonto, über das die Installation durchgeführt wird, muss über Datenbankbesitzerrechte für die SQL-Datenbank verfügen. Wenn Sie sich unsicher sind in Bezug auf die Zugriffsberechtigungen oder die Konnektivität zur Datenbank, bitten Sie Ihren Datenbankadministrator um Auskunft, bevor Sie mit der Installation beginnen.

Dell empfiehlt, für die Dell Server-Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfall-Wiederherstellungsplan Ihres Unternehmens einzubeziehen.

Wenn Sie Dell-Komponenten in Ihre DMZ implementieren möchten, vergewissern Sie sich, dass sie ausreichend vor Angriffen geschützt sind.

Für Produktionsumgebungen empfiehlt Dell, die Installation von SQL Server auf einem dedizierten Server vorzunehmen.

Zur vollständigen Umsetzung der Richtlinien empfiehlt Dell, sowohl Security Management Server als auch die Clients auf die neuesten Versionen zu aktualisieren.

Security Management Server v10.x unterstützt:

- Encryption Enterprise:
  - Windows-Clients v8.x/v10.x
  - Mac-Clients v8.x/v10.x
  - SED Management v8.x/v10.x
  - BitLocker Manager v8.x/10.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprise v1.x/v2.x
- Upgrade/Migration von Security Management Server Version 9.2 oder späteren Versionen. (Beim Migrieren von Security Management Server vor v9.2 bitten Sie den Dell ProSupport um Hilfe.)

Beim Aktualisieren oder Migrieren von Security Management Server auf eine Version, die neu eingeführte Richtlinien enthält, müssen Sie nach der Aktualisierung oder Migration die aktualisierte Richtlinie bestätigen, damit anstelle der Standardwerte Ihre bevorzugten Richtlinieneinstellungen für die neuen Richtlinien implementiert werden.

Im Allgemeinen empfehlen wir als Aktualisierungspfad die Aktualisierung oder Migration von Security Management Server und seiner Komponenten, gefolgt von der Installation/Aktualisierung des Clients.

Richtlinienänderungen implementieren

1. Melden Sie sich als Dell Administrator bei der Verwaltungskonsole an.
2. Klicken Sie im linken Menü auf **Verwaltung** > **Bestätigen**.
3. Geben Sie in *Kommentar* eine Beschreibung der Änderung ein.
4. Klicken Sie auf **Richtlinien bestätigen**.
5. Melden Sie sich nach Abschluss der Bestätigung von der Verwaltungskonsole ab.

   Stellen Sie sicher, dass die Dell Services ausgeführt werden

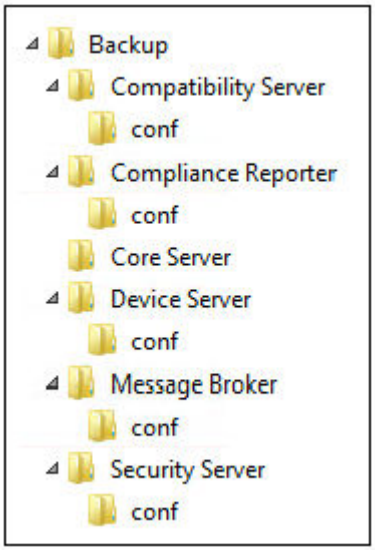
6. Klicken Sie im Windows-*Startmenü* auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Nachdem *Services* geöffnet wurde, navigieren Sie zu den einzelnen Dell Diensten, und klicken Sie bei Bedarf auf **Service starten**.

   Sichern der vorhandenen Installation

7. Sichern Sie die komplette vorhandene Installation an einem anderen Ort. Die Sicherung sollte die SQL Datenbank, secretKeyStore, und Konfigurationsdateien enthalten. Nach der Aktualisierung/Migration sind mehrere Dateien Ihrer bestehenden Installation erforderlich.

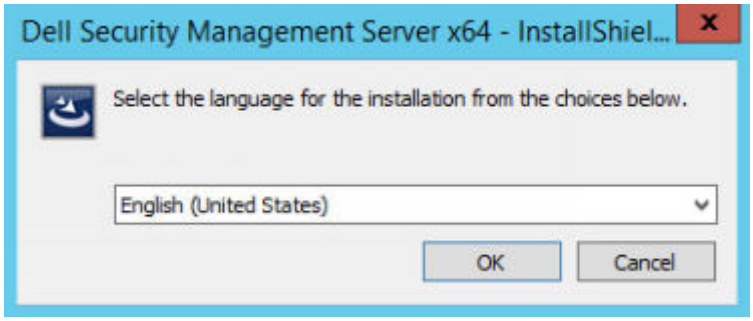
   ANMERKUNG:

   Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



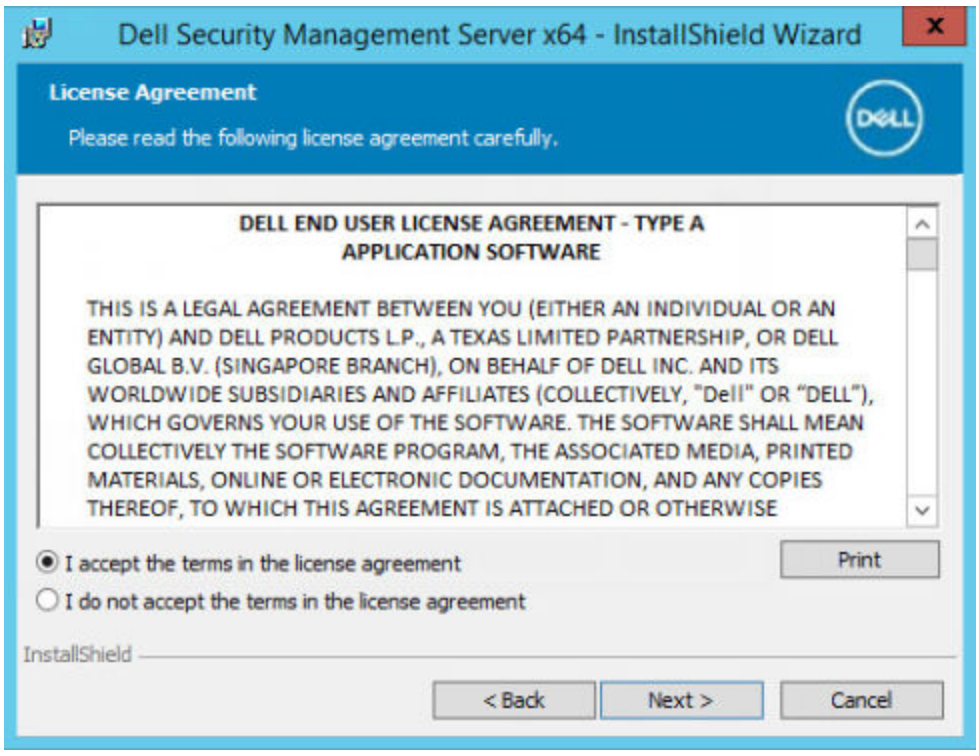
Back-End-Server-Aktualisierung/Migration

1. Wechseln Sie auf dem Dell Installationsmedium in das Security Management Server-Verzeichnis. **Entpacken** Sie (NICHT kopieren/einfügen oder ziehen) Security Management Server-x64 im Stammverzeichnis des Servers, auf dem Sie Security Management Server installieren. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***
2. Doppelklicken Sie auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.



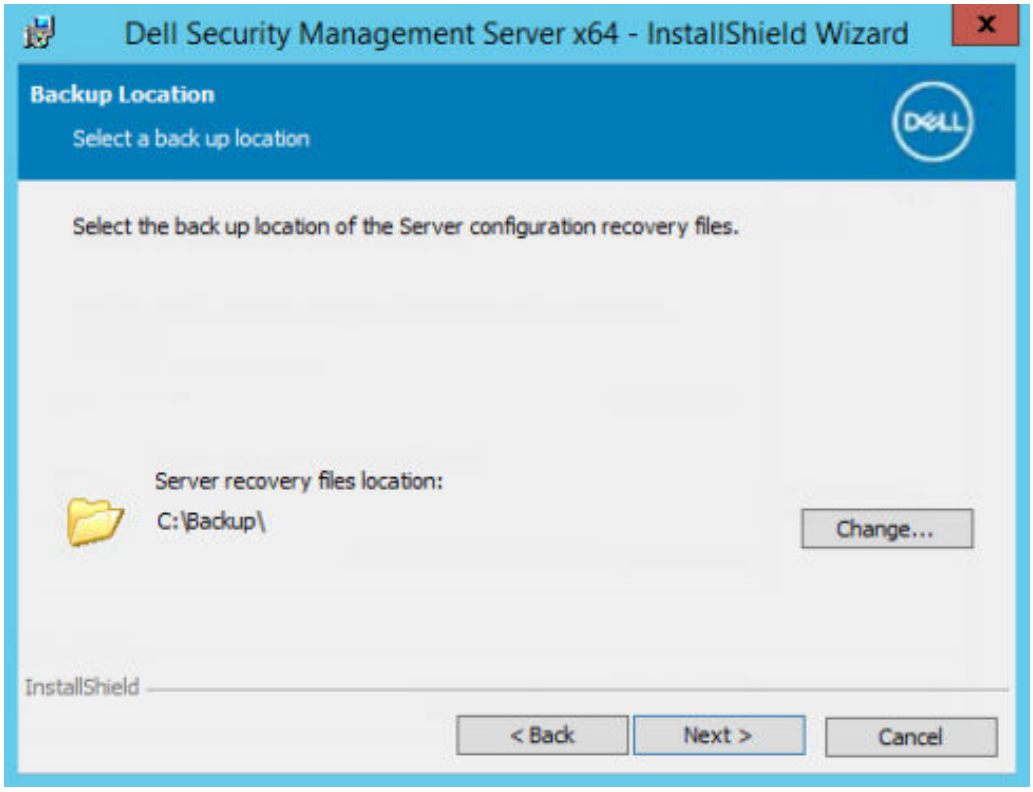
4. Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.

5. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen und klicken Sie auf **Weiter**.

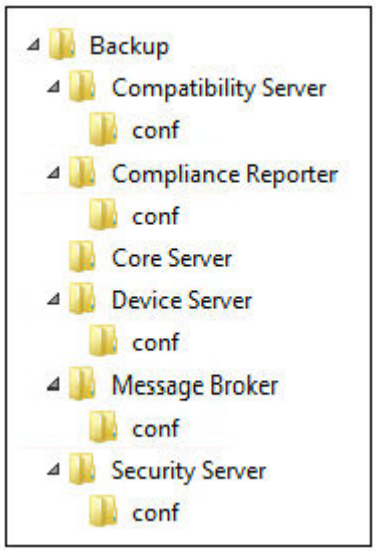


6. Klicken Sie zur Auswahl eines Speicherorts für zu speichernde Konfigurations-Sicherungsdateien auf **Ändern**, navigieren Sie zum gewünschten Ordner und klicken Sie anschließend auf **Weiter**.

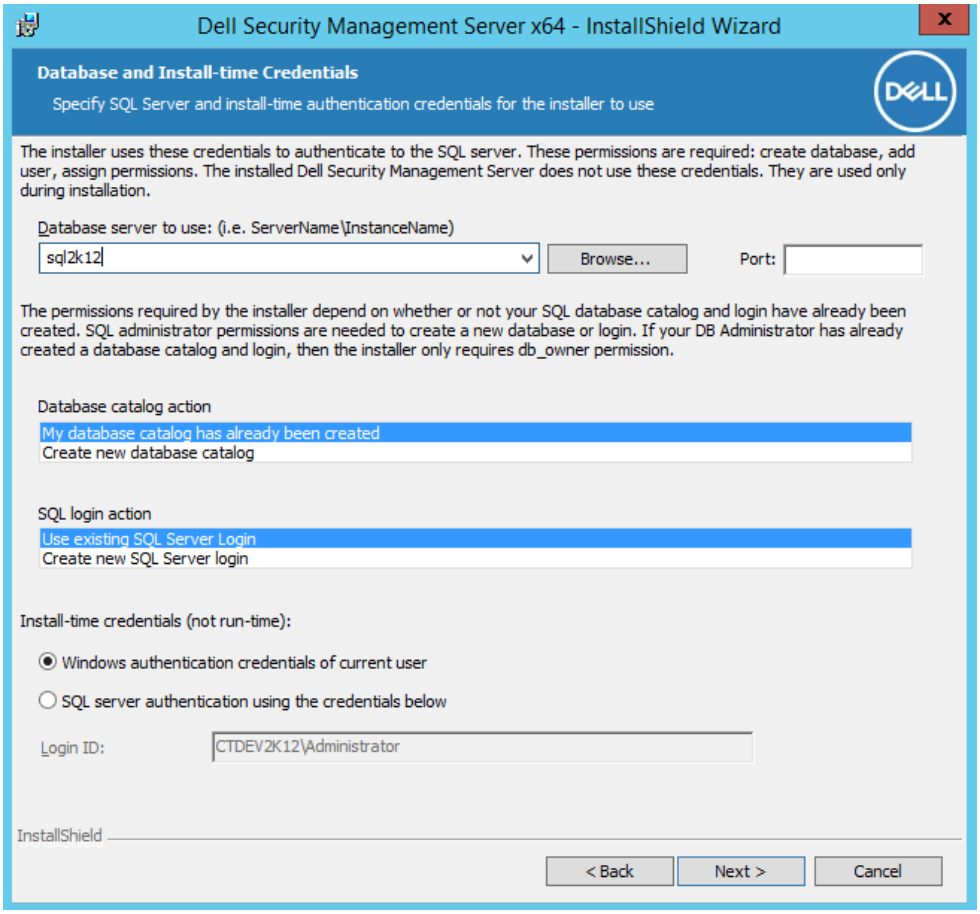
   Dell empfiehlt die Auswahl eines Remote-Netzwerkspeicherortes oder eines externen Sicherungslaufwerks.



Die durch das Installationsprogramm während der Installation erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.



7. Wenn das Installationsprogramm die vorhandene Datenbank ordnungsgemäß ermittelt, wird das Dialogfeld für Sie ausgefüllt.



Um die vorhandene Datenbank zu verbinden, geben Sie die zu verwendende Authentifizierungsmethode an. Nach der Installation verwendet das installierte Produkt nicht die hier angegebenen Anmeldeinformationen.

a. Wählen Sie den Datenbankauthentifizierungstyp aus:

- **Anmeldeinformationen für die Windows-Authentifizierung des aktuellen Benutzers**

  Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (*Benutzername* und *Kennwort* sind nicht bearbeitbar).

  Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die SQL Server-Rechte Default Schema: dbo und Database Role Membership: dbo_owner, public verfügen.

  ODER

- **SQL-Server-Authentifizierung über die unten angegebenen Anmeldeinformationen**

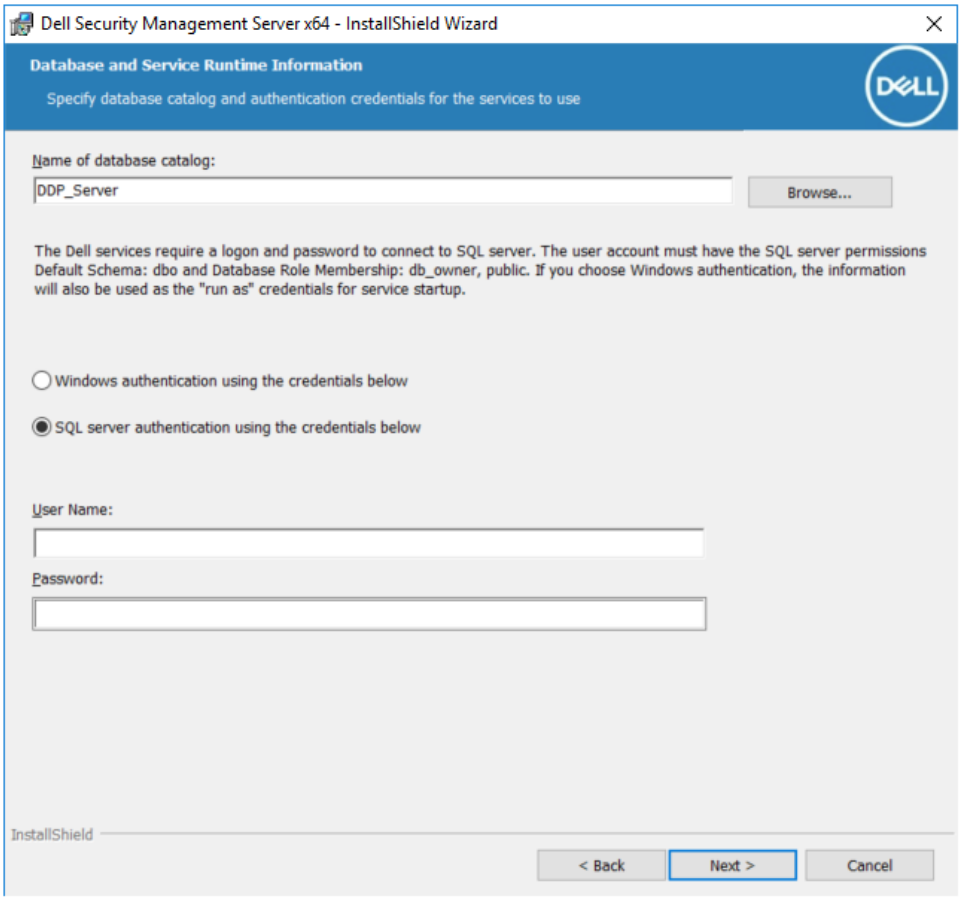
  Bei Verwendung der SQL-Authentifizierung muss das verwendete SQL-Konto auf dem SQL-Server über Systemadministratorberechtigungen verfügen.

  Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen.

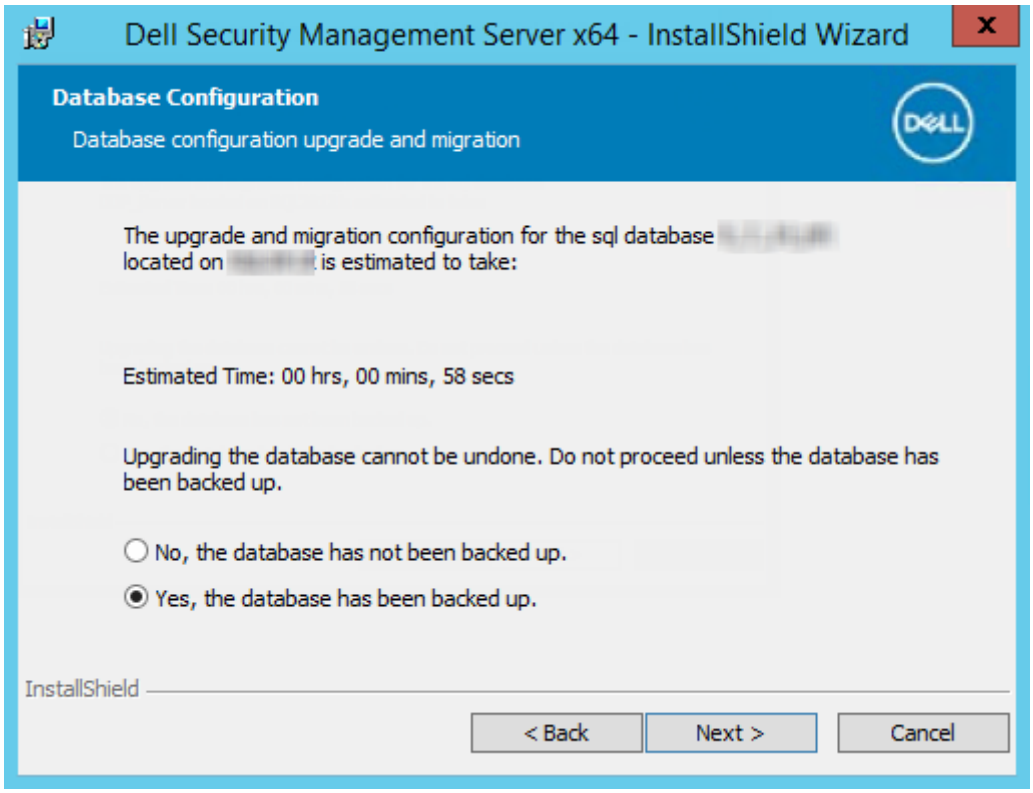
b. Klicken Sie auf **Weiter**.

8. Wenn das Dialogfenster für die Service-Laufzeit-Kontoangaben nicht automatisch ausgefüllt wird, geben Sie nach der Installation die Authentifizierungsmethode für das zu verwendende Produkt an.
   a. Wählen Sie den Authentifizierungstyp aus.
   b. Geben Sie den Benutzernamen und das Kennwort des Domänendienstkontos ein, das die Dell Dienste für den Zugriff auf den SQL-Server verwenden, und klicken Sie auf **Weiter**.

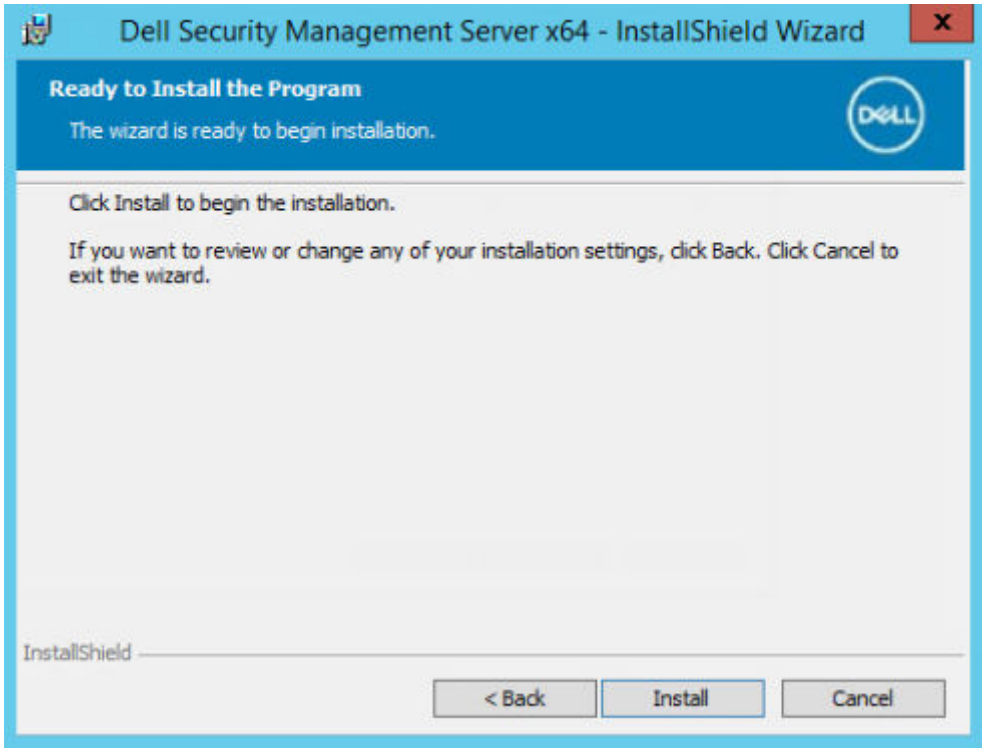
      Das Benutzerkonto muss im Format DOMAIN\Username vorliegen und das Default Schema: dbo und Database Role Membership: dbo_owner, public aufweisen.



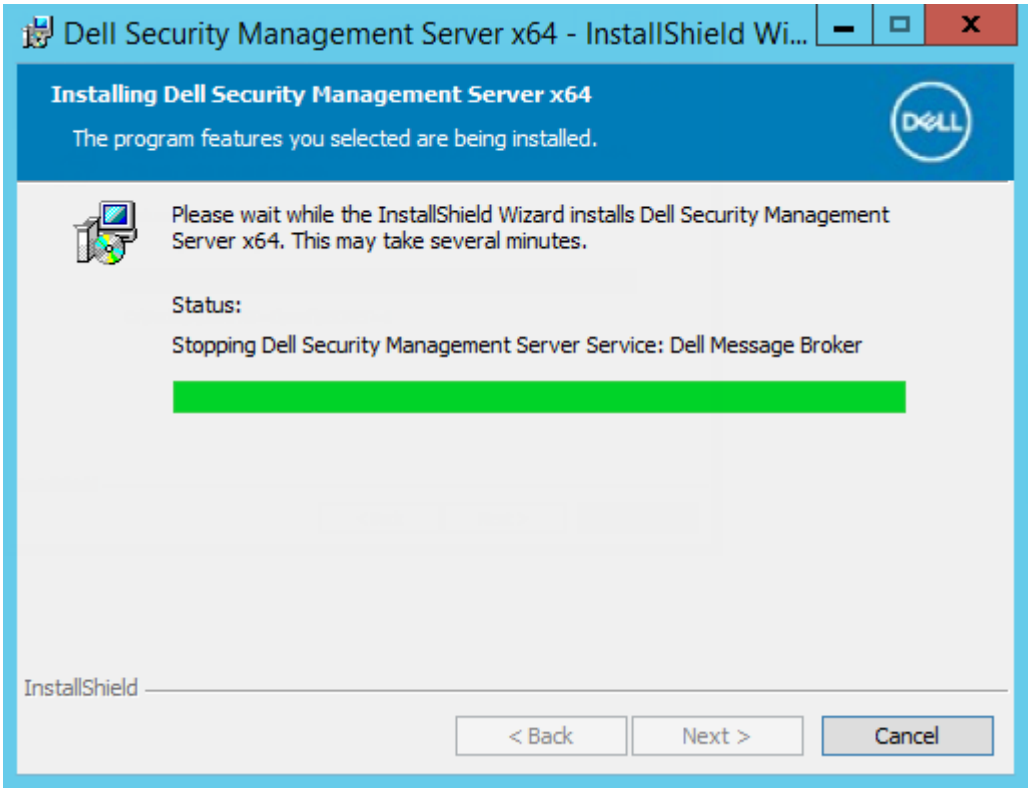
9. Falls die Datenbank noch nicht gesichert wurde, ***müssen*** Sie sie unbedingt sichern, bevor Sie mit der Installation fortfahren. ***Datenbankaktualisierung kann nicht rückgängig gemacht werden.*** Wählen Sie erst nach Sicherung der Datenbank **Ja**, **die Datenbank wurde gesichert** und klicken Sie auf **Weiter**.



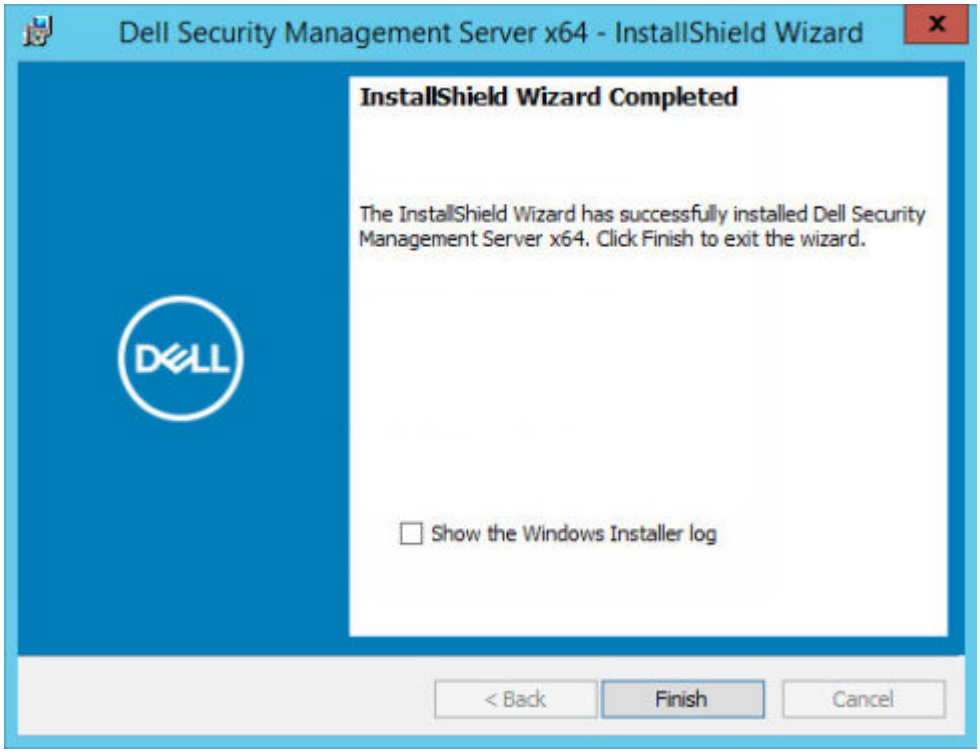
10. Klicken Sie auf **Installieren**, um mit der Installation zu beginnen.



Ein Fortschritts-Dialogfeld zeigt während des gesamten Aktualisierungsvorgangs den Status an.



11. Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.



Die Dell Services werden am Ende der Migration neu gestartet. Es ist nicht erforderlich, den Dell Server neu zu starten.

Das Installationsprogramm führt die Schritte 12-13 für Sie aus. Es hat sich bewährt, diese Werte zu überprüfen, um sicherzustellen, dass die Änderungen ordnungsgemäß vorgenommen wurden.

12. Kopieren Sie nun von der Sicherungsinstallation <Compatibility Server install dir>\conf\secretKeyStore, und fügen Sie alles in der neuen Installation ein:

    <Kompatibilitätsserver-Installationsverzeichnis>\conf\secretKeyStore

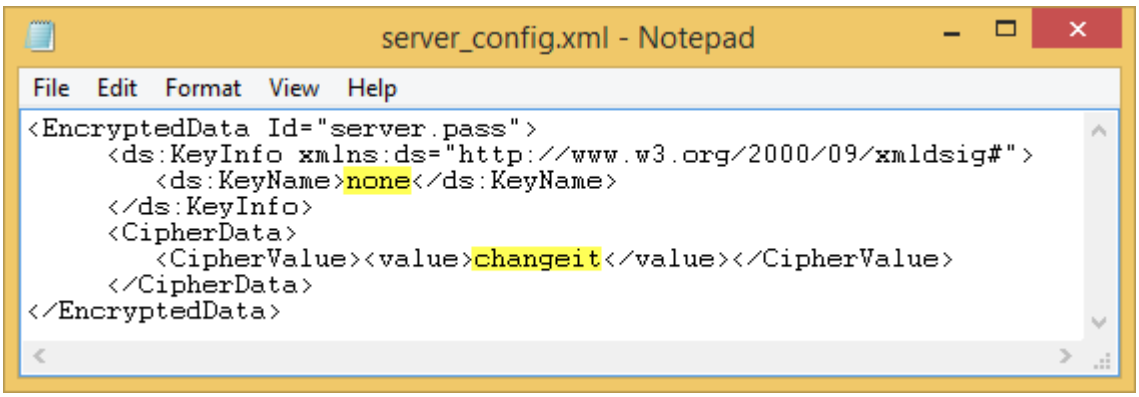
13. Öffnen Sie in der Neuinstallation <Kompatibilitätsserver-Installationsverzeichnis>\conf\server_config.xml, und ersetzen Sie den Wert für **server.pass** wie folgt durch den Wert der Sicherungsinstallation <Kompatibilitätsserver-Installationsverzeichnis>\conf \server_config.xml:

    Anleitung für server.pass:

    Wenn Sie das Passwort kennen, orientieren Sie sich an der Beispieldatei „server_config.xml“, und nehmen Sie die folgenden Änderungen vor:

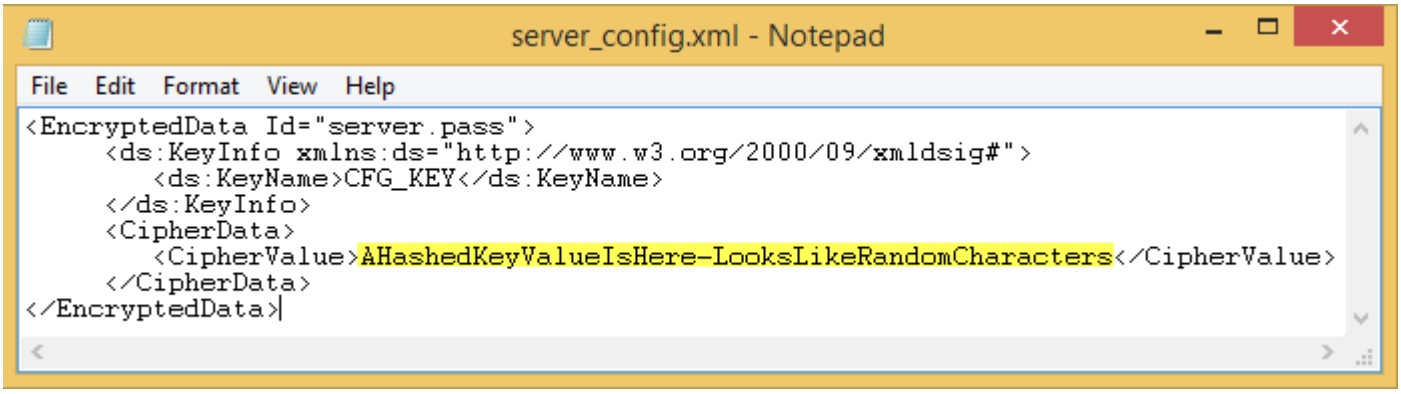
    - Ändern Sie *KeyName* vom Wert **CFG_KEY** in den Wert **Keiner**.
    - Geben Sie das Klartextpasswort ein, und schließen Sie es zwischen <value> </value> ein, in diesem Beispiel *<value>changeit</ value>*.
    - Beim Starten des Security Management Server wird das Klartextpasswort verschlüsselt. Dieser Schlüsselwert ersetzt den Klartext.

    Bekanntes Passwort:



Falls Sie das Passwort nicht kennen, schneiden Sie den Abschnitt in der gesicherten Datei „<Compatibility Server install dir>\conf \server_config.xml“ aus (vergleiche Abbildung 4-2), und fügen Sie ihn in den entsprechenden Abschnitt in der neuen Datei *server_config.xml* ein.

Unbekanntes Passwort:



Speichern und schließen Sie die Datei.

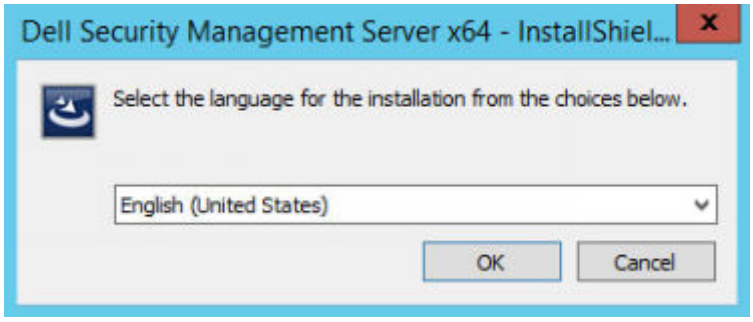
ANMERKUNG:

Versuchen Sie keinesfalls, das Passwort für den Security Management Server durch Bearbeiten von server.pass value in server_config.xml zu ändern. Wenn Sie diesen Wert ändern, können Sie nicht mehr auf die Datenbank zugreifen.

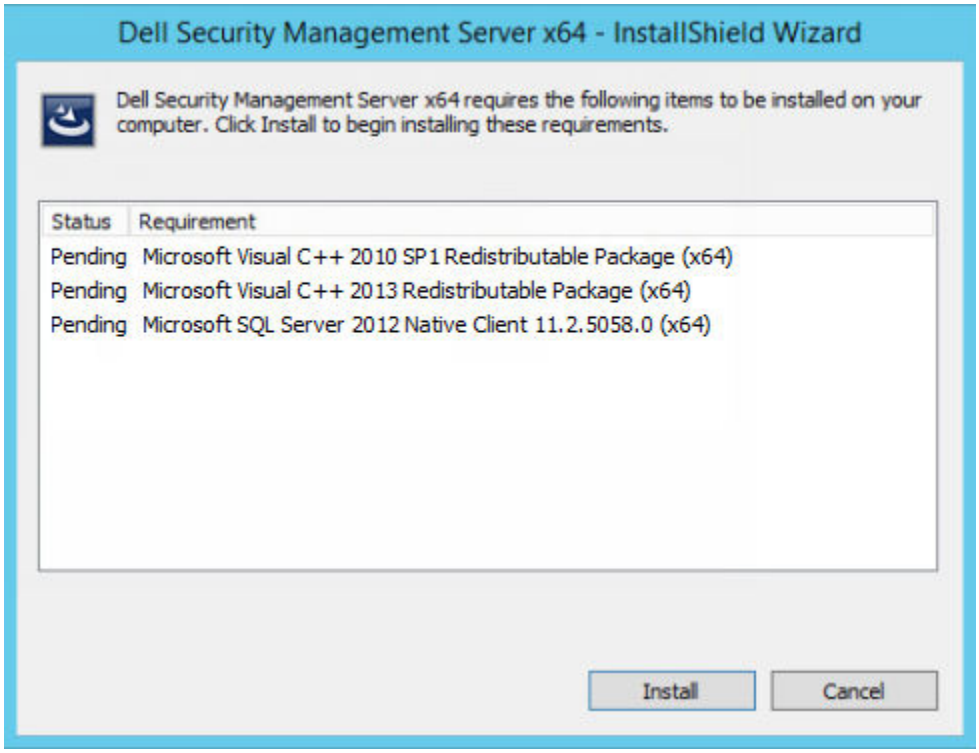
Die Back-End-Server Migrationsaufgaben wurden abgeschlossen.

Front-End-Server Aktualisierung/Migration

1. Wechseln Sie auf dem Dell Installationsmedium in das Security Management Server-Verzeichnis. **Entpacken** Sie (NICHT kopieren/einfügen oder ziehen) Security Management Server-x64 im Stammverzeichnis des Servers, auf dem Sie Security Management Server installieren. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***
2. Doppelklicken Sie auf **setup.exe**.
3. Wählen Sie die Sprache für die Installation aus und klicken Sie auf **OK**.



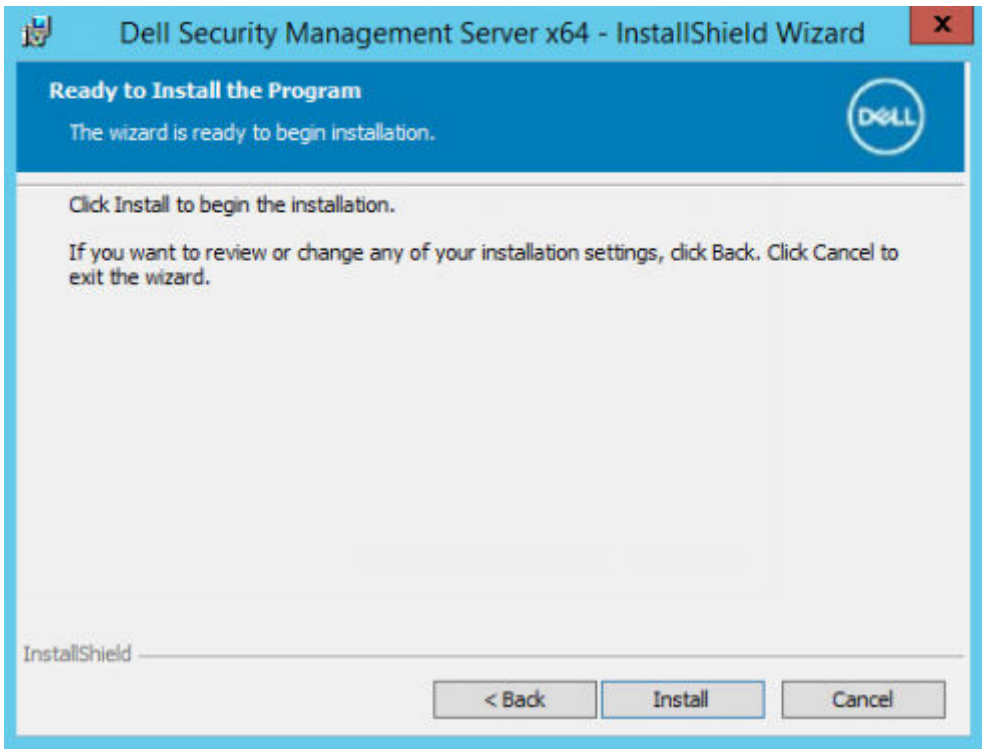
4. Wenn die Voraussetzungen noch nicht installiert wurden, wird eine Meldung angezeigt, die Sie darüber informiert, welche Voraussetzungen installiert werden Klicken Sie auf **Installieren**.



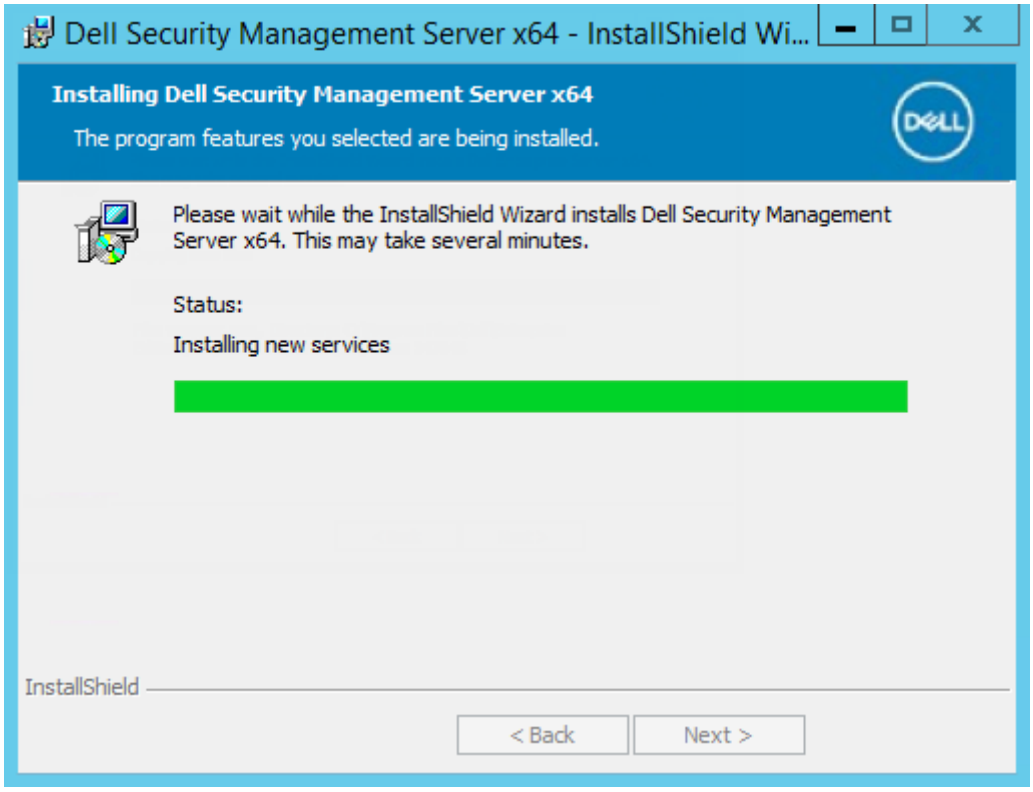
5. Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.

6. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie die Bedingungen und klicken Sie auf **Weiter**.

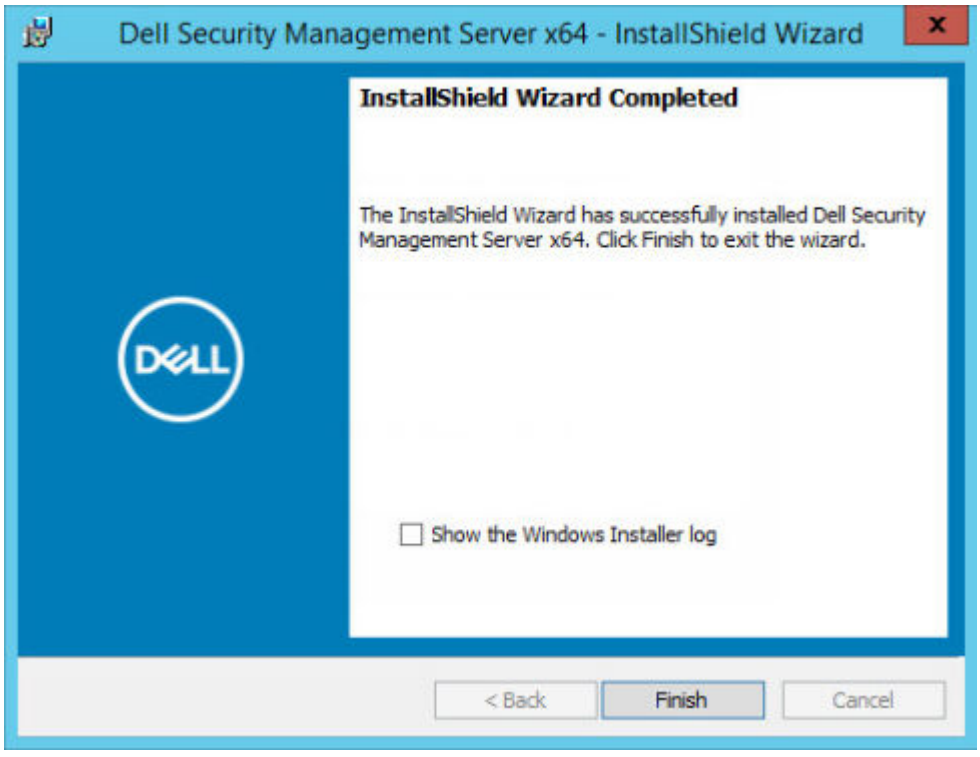
7. Klicken Sie im Dialogfeld *Bereit zur Installation des Programms* auf **Installieren**.



Ein Fortschritts-Dialogfeld zeigt während des gesamten Installationsvorgangs den Status an.



8. Wenn die Installation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.



9. Richten Sie den Back-End-Server für die Kommunikation mit dem Front-End-Server ein.
   a. Wechseln Sie auf dem Back-End-Server zu <Security Server install dir>\conf\, und öffnen Sie die Datei „application.properties“.
   b. Suchen Sie „publicdns.server.host“ und legen Sie den Namen auf einen extern auflösbaren Hostnamen fest.
   c. Suchen Sie „publicdns.server.port“, und legen Sie den Port fest (die Standardeinstellungen lautet 8443).

   Die Dell Services werden am Ende der Installation neu gestartet. Ein Neustart des Dell Server ist bis zum Abschluss der Konfigurationsaufgaben nach der Installation nicht erforderlich.

Installation im getrennten Modus

Der getrennte Modus isoliert Security Management Server aus dem Internet und einem ungesicherten LAN oder anderen Netzwerk. Nachdem Security Management Server im getrennten Modus installiert wurde, verbleibt er im getrennten Modus und kann nicht mehr auf den verbundenen Modus umgestellt werden.

Security Management Server wird im getrennten Modus über die Befehlszeile installiert .

Die folgende Tabelle zeigt die verfügbaren Switches.

Schalter	Erläuterung
/v	Gibt Variablen an die .msi-Datei innerhalb der *.exe-Datei weiter.
/s	Im Hintergrund

Die folgende Tabelle zeigt die verfügbaren Anzeigeoptionen.

Option	Erläuterung
/q	Kein Fortschrittsdialogfeld, führt nach Abschluss der Installation selbstständig einen Neustart durch
/qb	Dialogfeld mit der Schaltfläche **Abbrechen** fortführen
/qn	Keine Benutzeroberfläche

Die folgende Tabelle umfasst die für die Installation verfügbaren Parameter. Diese Parameter können an der Befehlszeile angegeben oder aus einer Datei unter Verwendung der folgenden Eigenschaft aufgerufen werden:

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

Parameter
AGREE_TO_LICENSE=Yes – Der Wert muss „Yes“ (Ja) lauten.
PRODUCT_SN=xxxxx – Optional, wenn sich die Lizenzinformationen am standardmäßigen Ort befinden; andernfalls müssen Sie sie hier eingeben.
INSTALLDIR=<path> – Optional.
BACKUPDIR=<path> – Dort werden die Wiederherstellungsdateien gespeichert. **ANMERKUNG:** Die durch das Installationsprogramm während des Installationsschritts erstellte Ordnerstruktur (Beispiel siehe unten) muss unverändert bleiben.
AIRGAP=1 – Zum Installieren von Security Management Server im getrennten Modus muss der Wert „1“ lauten.
SSL_TYPE=n – Wobei n zum Importieren eines vorhandenen Zertifikats, das von einer CA-Zertifizierungsstelle erworben wurde, „1“ und zum Erstellen eines selbstsignierten Zertifikats „2“ lautet. Der Wert SSL_TYPE bestimmt, welche SSL-Eigenschaften erforderlich sind. Mit SSL_TYPE=1 sind folgende Eigenschaften erforderlich: SSL_CERT_PASSWORD=xxxxx SSL_CERT_PATH=xxxxx Mit SSL_TYPE=2 sind folgende Eigenschaften erforderlich: SSL_CITYNAME SSL_DOMAINNAME SSL_ORGNAME

Parameter
SSL_UNITNAME SSL_COUNTRY – Optional, Standard = „US“ SSL_STATENAME
SSOS_TYPE=n – Wobei n zum Importieren eines vorhandenen Zertifikats, das von einer CA-Zertifizierungsstelle erworben wurde, „1“ und zum Erstellen eines selbstsignierten Zertifikats „2“ lautet. Der Wert SSOS_TYPE bestimmt, welche SSOS-Eigenschaften erforderlich sind. Mit SSOS_TYPE=1 sind folgende Eigenschaften erforderlich: SSOS_CERT_PASSWORD=xxxxx SSOS_CERT_PATH=xxxxx Mit SSOS_TYPE=2 sind folgende Eigenschaften erforderlich: SSOS_CITYNAME SSOS_DOMAINNAME SSOS_ORGNAME SSOS_UNITNAME SSOS_COUNTRY – Optional, Standard = „US“ SSOS_STATENAME
DISPLAY_SQLSERVER – Dieser Wert wird geparst, um Server-, Instanz- und Portinformationen zu erhalten. Beispiel: DISPLAY_SQLSERVER=SQL_server\Server_instance, Port
IS_AUTO_CREATE_SQLSERVER=FALSE – Optional. Der Standardwert ist FALSCH, was bedeutet, dass die Datenbank nicht erstellt wird. Die Datenbank muss bereits auf dem Server vorhanden sein. Setzen Sie diesen Wert zum Erstellen einer neuen Datenbank auf WAHR.
IS_SQLSERVER_AUTHENTICATION=0 – Optional. Der Standardwert ist 0 und gibt an, dass die Windows-Anmeldeinformationen für die Authentifizierung des aktuell angemeldeten Benutzers zur Authentifizierung des SQL-Servers genutzt werden. Wenn Sie die SQL-Authentifizierung verwenden möchten, setzen Sie diesen Wert auf 1. **ANMERKUNG:** Das Installationsprogramm muss sich anhand der folgenden Berechtigungen auf dem SQL Server authentifizieren: Datenbank erstellen, Benutzer hinzufügen, Berechtigungen zuweisen. Die Anmeldeinformationen sind Installations-Anmeldeinformationen, nicht Laufzeit-Anmeldeinformationen. Wenn die SQL-Authentifizierung verwendet wird, ist Folgendes erforderlich: IS_SQLSERVER_USERNAME IS_SQLSERVER_PASSWORD
EE_SQLSERVER_AUTHENTICATION – Erforderlich. Wählen Sie die Authentifizierungsmethode für das zu verwendende Produkt aus. Dieser Schritt verbindet ein Konto mit dem Produkt. Diese Anmeldeinformationen werden auch von den Dell Diensten verwendet, da sie mit dem Security Management Server funktionieren. Um die Windows-Authentifizierung zu verwenden, setzen Sie den Wert auf 0. Um die SQL-Authentifizierung zu verwenden, setzen Sie den Wert auf 1. **ANMERKUNG:** Stellen Sie sicher, dass das Konto über Administratorberechtigungen und die Fähigkeit zur Verwaltung des SQL-Servers verfügt. Das Benutzerkonto muss über die folgenden SQL Server-Berechtigungen verfügen Default Schema: dbo und Database Role Membership: db_owner, public. SQL_EE_USERNAME – Erforderlich. Verwenden Sie mit Windows-Authentifizierung dieses Format: DOMÄNE\Benutzername. Geben Sie mit SQL-Authentifizierung den Benutzernamen an. SQL_EE_PASSWORD – Erforderlich. Geben Sie das zum Windows- oder SQL-Benutzernamen gehörende Kennwort ein. Wenn die SQL-Authentifizierung verwendet wird (EE_SQLSERVER_AUTHENTICATION= 1) ist Folgendes gültig: RUNAS_KEYSERVER_USER – Verwenden Sie den Windows-Benutzernamen für Key Server „run as“ in diesem Format: Domain \Benutzer. Dies muss ein Windows-Benutzerkonto sein.

Parameter
RUNAS_KEYSERVER_PSWD – Windows-Kennwort für Windows-Benutzerkonto für Key Server "run as" festlegen.
SQL_ADD_LOGIN=T – Optional. Die Standardeinstellung ist Null (diese Art der Anmeldung ist nicht hinzugefügt worden). Wenn der Wert T eingestellt ist und der SQL_EE_USERNAME keine Anmeldung oder kein Benutzer für die Datenbank ist, versucht das Installationsprogramm die SQL-Anmeldeinformationen des Benutzers zur Authentifizierung hinzuzufügen und Berechtigungen festzulegen, damit die Anmeldedaten vom Produkt verwendet werden können.
Nachfolgend finden Sie Hostname-Parameter. Bearbeiten Sie Hostnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen. Das Format muss **`server.domain.com`** lauten. **ANMERKUNG:** Im Hostnamen darf kein Unterstrich (_) enthalten sein.
CORESERVERHOST – Optional. Hostname des Core Servers.
RMIHOST – Optional. Hostname des Compatibility-Servers.
REPORTERHOST – Optional. Hostname des Compliance Reporter.
DEVICEHOST – Optional. Hostname des Geräteservers.
KEYSERVERHOST – Optional. Hostnamen des Key Servers.
TIGAHOST – Optional. Hostname des Security Servers.
SMTP_HOST – Optional. SMTP-Hostname.
ACTIVEMQHOST – Optional. Hostname des Message Broker.
Im Folgenden finden Sie Portparameter. Bearbeiten Sie Portnamen nur bei Bedarf. Dell empfiehlt die Verwendung der Standardeinstellungen
SERVERPORT_CLIENTAUTH – Optional.
REPORTERPORT – Optional.
DEVICEPORT – Optional.
KEYSERVERPORT – Optional.
GKPORT – Optional.
TIGAPORT – Optional.
SMTP_PORT – Optional.
ACTIVEMQ_TCP – Optional.
ACTIVEMQ_STOMP – Optional.

Security Management Server im getrennten Modus installieren

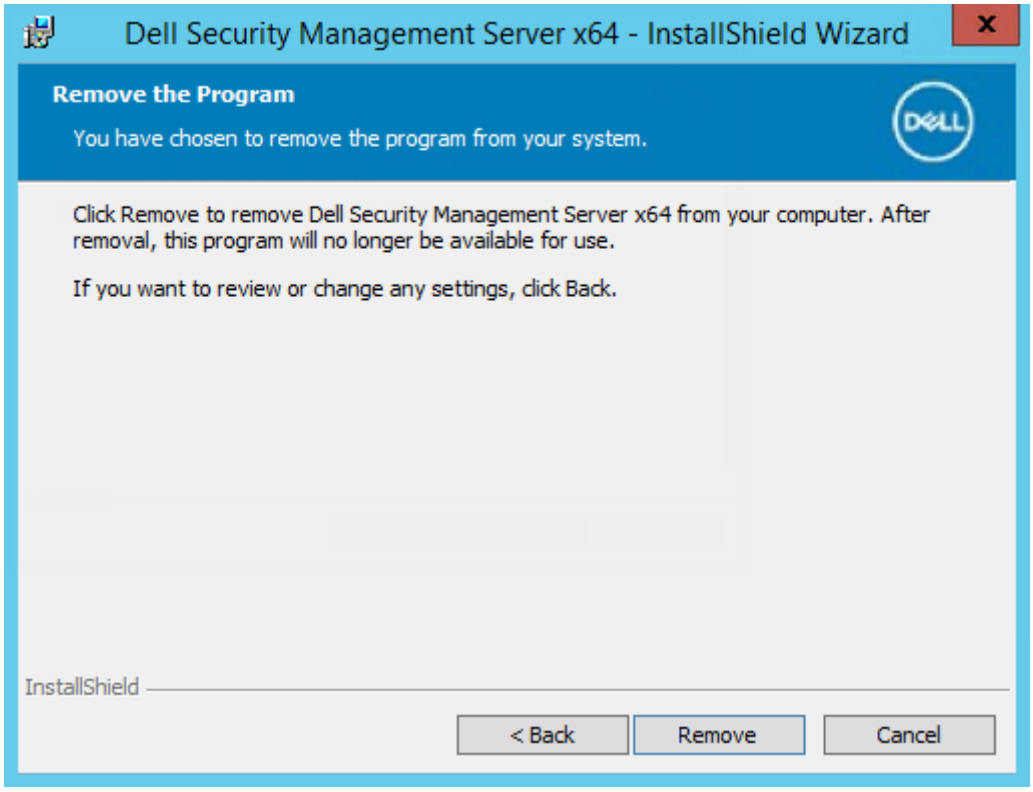
Im folgenden Beispiel wird Security Management Server unter Verwendung von Installationparametern, die in der Datei `C:\mysetups\eeoptions.txt\" "` aufgeführt sind, installiert

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

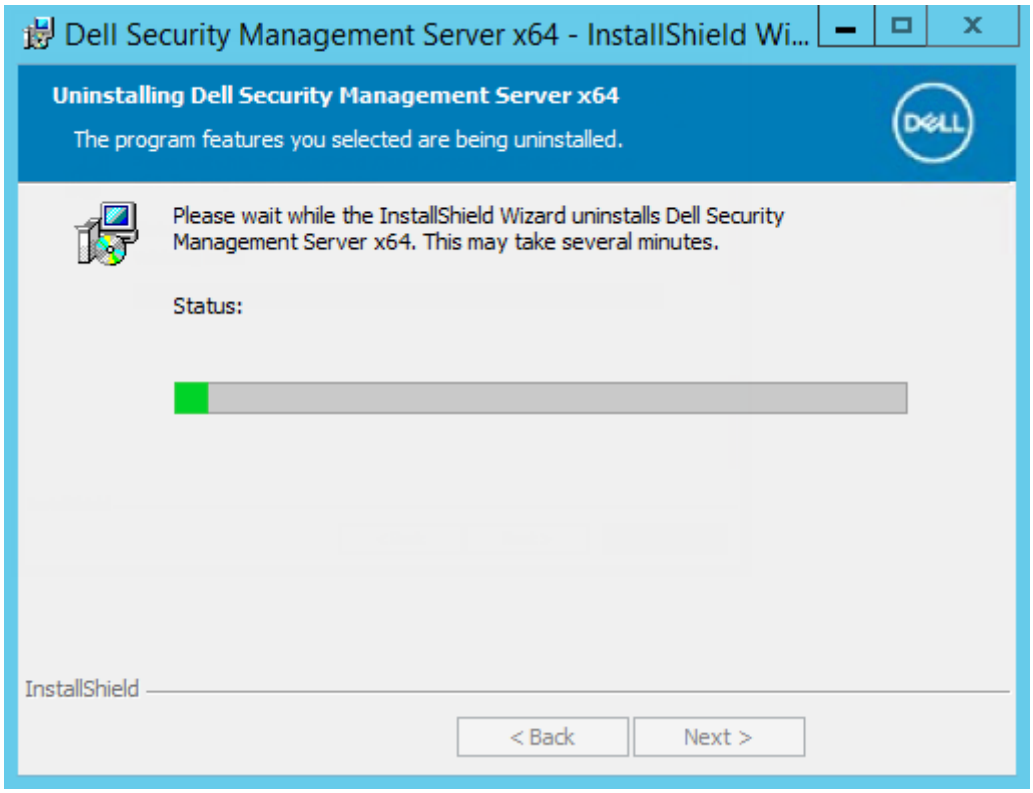
Deinstallation von Security Management Server

1. Wechseln Sie auf dem Dell Installationsmedium in das Security Management Server-Verzeichnis. **Entpacken** Sie (NICHT kopieren/einfügen oder ziehen) Security Management Server-x64 im Stammverzeichnis des Servers, auf dem Sie Security Management Server deinstallieren möchten. ***Kopieren/Einfügen oder Ziehen führt zu Fehlern und einer nicht erfolgreichen Installation.***
2. Doppelklicken Sie auf **setup.exe**.
3. Klicken Sie im Dialogfeld *Willkommen* auf **Weiter**.

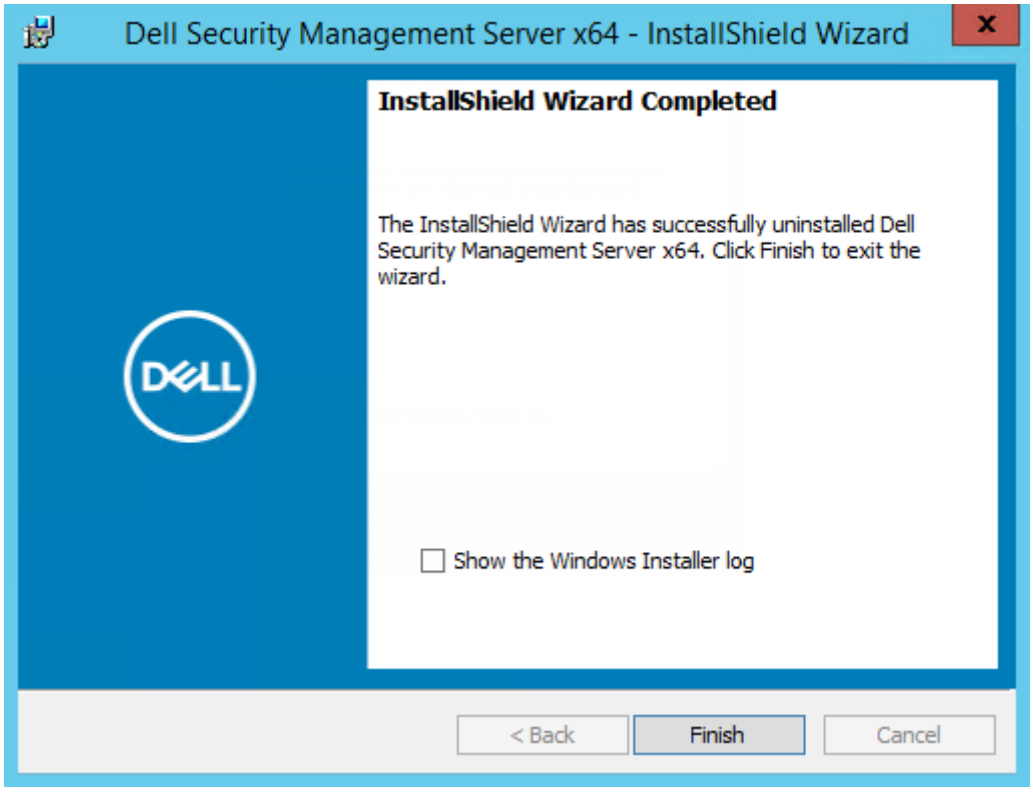
4. Klicken Sie im Dialogfeld *Programm entfernen* auf **Entfernen**.



Ein Fortschritts-Dialogfeld zeigt während des gesamten Deinstallationsvorgangs den Status an.



5. Wenn die Deinstallation abgeschlossen wurde, klicken Sie auf **Fertigstellen**.


Dell Security Management Server x64 - InstallShield Wizard
InstallShield Wizard Completed
The InstallShield Wizard has successfully uninstalled Dell Security Management Server x64. Click Finish to exit the wizard.
Show the Windows Installer log
< Back
Finish
Cancel

5

Konfiguration nach der Installation

Lesen Sie die *Security Management Server Technical Advisories* (Technischen Tipps für Security Management Server), um sich über aktuelle Lösungen oder bekannte Probleme hinsichtlich der Konfiguration von Security Management Server zu informieren.

Je nachdem, ob Sie Security Management Server zum ersten Mal installieren oder ob Sie eine Aktualisierung einer vorhandenen Installation durchführen, müssen Sie einige Komponenten Ihrer Umgebung konfigurieren.

Nach der Installation von Security Management Server müssen die folgenden Standardeinstellungen angepasst werden:

- Ändern Sie das Back-End-Server-Kennwort an folgendem Speicherort:

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

- Ändern Sie das Kennwort für jeden Front-End-Server in Ihrer Umgebung an folgendem Speicherort:

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

Das Kennwort wird wie folgt angezeigt: `proxy-server.password=ENC(<texthere>)`

So ändern Sie das Kennwort:

1. Wählen Sie: `ENC(<texthere>)`
2. Ändern Sie den ausgewählten Text zu: `CLR(<newpasswordhere>)`

   Nach einem Serviceneustart ändert sich die angepasste Zeile von `CLR` zu `ENC` und das Kennwort ist verschlüsselt.

HINWEIS: Der Proxy-Server-Benutzername wird möglicherweise auch geändert, dieser muss jedoch mit der application.properties-Datei des Nachrichtenbroker und allen aktiven Front-End-Servern übereinstimmen.

DMZ-Moduskonfiguration

Wenn der Security Server in einem DMZ und einem privaten Netzwerk bereitgestellt wird und nur der DMZ-Server über ein Domänenzertifikat von einer vertrauenswürdigen Zertifikatsstelle (CA) verfügt, müssen einige manuelle Schritte ausgeführt werden, um das vertrauenswürdige Zertifikat zu einem Java-Schlüsselspeicher auf dem Security Server des privaten Netzwerks hinzuzufügen.

Falls ein vertrauenswürdiges Zertifikat verwendet wird, überspringen Sie diesen Abschnitt.

ANMERKUNG: Wir empfehlen dringend, Domänenzertifikate einer vertrauenswürdigen Zertifikatsstelle für DMZ- und private Netzwerkserver zu verwenden.

Weitere Informationen über das Aktualisieren des Zertifikats für Dell Encryption mit einem vorhandenen Zertifikat im Microsoft-Keystore finden Sie unter http://www.dell.com/support/article/us/en/19/sln297240/.

Serverkonfigurationstool

Wenn nach Abschluss Ihrer Installation Konfigurationen in Ihrer Umgebung erforderlich sind, nehmen Sie die Änderungen mit dem Serverkonfigurationstool vor.

Mit dem Serverkonfigurationstool lassen sich folgende Aufgaben durchführen:

- Neue oder aktualisierte Zertifikate hinzufügen
- Dell Manager-Zertifikat importieren
- Identitätszertifikat importieren
- Einstellungen für Server SSL-Zertifikat konfigurieren
- Konfigurieren der SMTP Einstellungen für E-Mail-Dienste
- Datenbankname, Speicherort oder Anmeldeinformationen ändern
- Datenbank migrieren

Dell Core Server und Dell Compatibility Server dürfen nicht zusammen mit dem Serverkonfigurationstool ausgeführt werden. Halten Sie den Core Server-Dienst und den Compatibility Server-Dienst unter *Dienste* (**Start > Ausführen** an. Geben Sie ***services.msc*** ein) an, bevor Sie das Serverkonfigurationstool starten.

Um das Serverkonfigurationstool zu starten, gehen Sie zu **Start** > **Dell** > **Ausführen des Serverkonfigurationstools**.

Die vom Serverkonfigurationstool erstellten Protokolle werden im Ordner `C:\Programme\Dell\Enterprise Edition \Server Configuration Tool\Logs` gespeichert.

Neue oder aktualisierte Zertifikate hinzufügen

Sie können auswählen, welchen Zertifikatstyp Sie nutzen möchten: selbstsigniert oder signiert.

- **Selbstsignierte** Zertifikate werden durch den Ersteller signiert. Selbstsignierte Zertifikate eignen sich für Pilotprojekte, POCs usw. Für eine Produktionsumgebung empfiehlt Dell öffentliche, von einer Zertifizierungsstelle signierte oder Domänen-signierte Zertifikate.
- **Signierte** (öffentlich und von einer Zertifizierungsstelle oder Domäne signierte) Zertifikate werden von einer öffentlichen Zertifizierungsstelle oder einer Domäne signiert. Für Zertifikate, die von einer öffentlichen Zertifizierungsstelle signiert wurden, ist normalerweise ein Zertifikat der Zertifizierungsstelle im Microsoft-Zertifikatsspeicher vorhanden, und es wird automatisch eine Vertrauenskette erstellt. Für Zertifikate, die von einer Domäne und Zertifizierungsstelle signiert wurden, gilt Folgendes: Wurde die Workstation zur Domäne hinzugefügt, dann wurden das von der Domäne und Zertifizierungsstelle signierte Zertifikat zum Microsoft-Zertifikatsspeicher hinzugefügt und eine Vertrauenskette angelegt.

Komponenten, die durch Zertifikatskonfiguration beeinflusst werden:

- Java Services (zum Beispiel Device Server usw.)
- .NET-Anwendungen (Core Server)
- Die Validierung von Smart Cards wird für die Preboot-Authentifizierung verwendet (Security Server)
- Import privater Verschlüsselungscodes, die zum Signieren von Richtlinienpaketen genutzt werden, die ihrerseits an Dell Manager gesendet werden Dell Manager führt die SSL-Validierung für verwaltete Encryption-Clients mit selbstverschlüsselnden Laufwerken oder BitLocker Manager aus.
- Client-Workstations:
  - Workstations, auf denen BitLocker Manager ausgeführt wird
  - Workstations, auf denen Encryption Enterprise (Windows) ausgeführt wird
  - Workstations, auf denen Endpoint Security Suite Enterprise ausgeführt wird

Informationen zur Nutzung verschiedener Zertifikatstypen:

Die Preboot-Authentifizierung, die Smartcards verwendet, erfordert die SSL-Validierung durch den Security Server. Dell Manager führt beim Herstellen der Verbindung mit dem Dell Core Server eine SSL-Validierung durch. Für diese Verbindungen muss sich die signierende Zertifikatsstelle im Keystore befinden (entweder im Java-Keystore oder im Microsoft-Keystore, je nach Dell Server-Komponente). Falls selbstsignierte Zertifikate ausgewählt werden, stehen die folgenden Optionen zur Verfügung:

- Validierung von Smartcards, die für die Preboot-Authentifizierung verwendet werden:
  - Importieren Sie das Signierungszertifikat „Root Agency“ und die vollständige Vertrauenskette in den Java-Keystore des Security Servers. Die vollständige Vertrauenskette muss importiert werden.

Dell Manager:

- Fügen Sie das Signierungszertifikat „Root Agency“(vom selbstsignierten Zertifikat generiert) bei „Vertrauenswürdige Stammzertifizierungsstellen” (für „lokaler Computer“) der Workstation im Microsoft-Keystore ein.

  Der Security Management Server ist kompatibel mit der Microsoft Anforderung für die LDAP-Kanalbindung und LDAP-Signierung, wenn Active Directory verwendet wird.

  Um dies auf dem Security Management Server zu aktivieren, muss das Stammzertifikat für die Domänen-Controller-Zertifikate, die in den „Trusted Root“-Speicher importiert werden, im Microsoft Certificate Key Store liegen.
- Ändern Sie das Verhalten der serverseitigen SSL-Validierung. Wählen Sie zum Deaktivieren der serverseitigen SSL-Vertrauensvalidierung **Prüfung der Vertrauenskette deaktivieren** auf der Registerkarte „Einstellungen“.

Es gibt zwei Methoden für die Erstellung eines Zertifikats – *Express* und *Erweitert*.

Wählen Sie **eine** Methode aus:

- Express – Wählen Sie diese Methode aus, um ein selbstsigniertes Zertifikat für alle Komponenten zu generieren. Dies ist die einfachere Methode. Beachten Sie jedoch, dass selbstsignierte Zertifikate nur für Piloten, Machbarkeitsnachweise usw. angemessen sind. Für

Produktionsumgebungen empfiehlt Dell den Gebrauch von öffentlichen und von einer Zertifizierungsstelle oder Domäne signierten Zertifikaten.

- Erweitert – Wählen Sie diese Methode aus, um jede Komponente separat zu konfigurieren.

Express

1. Wählen Sie aus dem Hauptmenü **Aktionen** > **Zertifikate konfigurieren** aus.
2. Nachdem der Konfigurationsassistent gestartet wurde, wählen Sie **Express** aus, und klicken Sie auf **Weiter**. Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Security Management Server erstellt wurde.
3. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

Das Setup des Zertifikats ist vollständig. Im verbleibenden Teil dieses Abschnitts wird die erweiterte Methode für die Erstellung eines Zertifikats erläutert.

Erweitert

Es gibt zwei Pfade zur Erstellung eines Zertifikats – *Selbstsigniertes Zertifikat generieren* und *Aktuelle Einstellungen verwenden*. Wählen Sie **einen** dieser Pfade aus:

- Pfad 1 – Selbstsigniertes Zertifikat erstellen
- Pfad 2 – Aktuelle Einstellungen verwenden

Pfad 1 – Selbstsigniertes Zertifikat erstellen

1. Wählen Sie aus dem Hauptmenü **Aktionen** > **Zertifikate konfigurieren** aus.
2. Nachdem der Konfigurationsassistent gestartet wurde, wählen Sie **Erweitert** aus, und klicken auf **Weiter**.
3. Wählen Sie **Selbstsigniertes Zertifikat generieren** aus, und klicken Sie auf **Weiter**. Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Security Management Server erstellt wurde.
4. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

Das Setup des Zertifikats ist vollständig. Im verbleibenden Teil dieses Abschnitts wird die andere Methode für die Erstellung eines Zertifikats erläutert.

Pfad 2 – Aktuelle Einstellungen verwenden

1. Wählen Sie aus dem Hauptmenü **Aktionen** > **Zertifikate konfigurieren** aus.
2. Nachdem der Konfigurationsassistent gestartet wurde, wählen Sie **Erweitert** aus, und klicken auf **Weiter**.
3. Wählen Sie **Aktuelle Einstellungen verwenden** aus, und klicken Sie auf **Weiter**.
4. Wählen Sie im Fenster *SSL-Zertifikat für Compatibility Server* die Option **Selbstsigniertes Zertifikat generieren** aus, und klicken Sie auf **Weiter.** Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Security Management Server erstellt wurde.

   Klicken Sie auf **Weiter**.
5. Wählen Sie im Fenster „*SSL-Zertifikat für den Core Server*“ eine der folgenden Optionen aus:
   - *Zertifikat auswählen* – Wählen Sie diese Option, um ein vorhandenes Zertifikat zu verwenden. Klicken Sie auf **Weiter**.

     Navigieren Sie zum Speicherort des vorhandenen Zertifikats, geben Sie das zugehörige Passwort ein, und klicken Sie auf **Weiter**.

     Klicken Sie anschließend auf **Fertig stellen**.
   - *Selbstsigniertes Zertifikat generieren* – Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Security Management Server erstellt wurde. Wenn Sie diese Option auswählen, erscheint kein Fenster vom Typ „Zertifikat für die Nachrichtensicherheit“ (das Fenster wird jedoch angezeigt, wenn Sie die Option *Aktuelle Einstellungen verwenden* auswählen), und es wird das für den Dell Compatibility Server erstellte Zertifikat verwendet.

     Stellen Sie sicher, dass der vollständige Computername korrekt ist. Klicken Sie auf **Weiter**.

     Sie erhalten eine Warnmeldung, weil es bereits ein Zertifikat mit demselben Namen gibt. Wenn Sie gefragt werden, ob Sie es benutzen möchten, klicken Sie auf **Ja**.

Klicken Sie anschließend auf **Fertig stellen**.

- *Aktuelle Einstellungen verwenden* – Wählen Sie diese Option aus, um eine Einstellung für ein Zertifikat zu einem beliebigen Zeitpunkt nach der erstmaligen Konfiguration von Security Management Server zu ändern. Das bereits konfigurierte Zertifikat bleibt dabei erhalten. Wenn Sie diese Option auswählen, gelangen Sie zum Fenster „Zertifikat für die Nachrichtensicherheit“.

  Wählen Sie im Fenster Zertifikat für die Nachrichtensicherheit **eine** der folgenden Optionen aus:

  - *Zertifikat auswählen* – Wählen Sie diese Option, um ein vorhandenes Zertifikat zu verwenden. Klicken Sie auf **Weiter**.

    Navigieren Sie zum Speicherort des vorhandenen Zertifikats, geben Sie das zugehörige Passwort ein, und klicken Sie auf **Weiter**.

    Klicken Sie anschließend auf **Fertig stellen**.

  - *Selbstsigniertes Zertifikat generieren* – Falls verfügbar, werden die Informationen aus dem selbstsignierten Zertifikat verwendet, das im Rahmen der Installation von Security Management Server erstellt wurde.

    Klicken Sie auf **Weiter**.

    Klicken Sie anschließend auf **Fertig stellen**.

Das Setup des Zertifikats ist vollständig.

Wenn die Änderungen abgeschlossen wurden:

1. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.
2. Schließen Sie das Dell Server-Konfigurationstool.
3. Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Dell Manager-Zertifikat importieren

Falls Ihre Bereitstellung remote verwaltete Clients des Security Management Server mit Encryption Management Agents einschließt, müssen Sie Ihr neu erstelltes (oder vorhandenes) Zertifikat importieren. Das Dell Manager-Zertifikat wird dazu verwendet, den privaten Schlüssel zu schützen, der zum Signieren der Richtlinienpakete genutzt wird, die an remote verwaltete Security Management Server-Clients und den Encryption Management Agent gesendet werden. Dieses Zertifikat kann unabhängig von allen weiteren Zertifikaten genutzt werden. Außerdem kann dieser Schlüssel, wenn er beschädigt ist, durch einen neuen Schlüssel ersetzt werden. Dell Manager wird daraufhin einen neuen öffentlichen Schlüssel anfordern, wenn die Richtlinienpakete nicht entschlüsselt werden können.

1. Öffnen Sie die Microsoft Management Console.
2. Klicken Sie auf **Datei > Snapin hinzufügen/entfernen**.
3. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie im Fenster *Standalone-Snapin hinzufügen* **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
5. Wählen Sie **Computerkonto** aus und klicken Sie auf **Weiter**.
6. Wählen Sie im Fenster *Computer auswählen* **Lokaler Computer (der Computer, auf dem diese Konsole läuft)** und klicken Sie auf **Fertigstellen**.
7. Klicken Sie auf **Schließen**.
8. Klicken Sie auf **OK**.
9. Erweitern Sie im Ordner *Konsolenstamm* die *Zertifikate (Lokaler Computer)*.
10. Gehen Sie zum Ordner *Privat*, und suchen Sie das gewünschte Zertifikat.
11. Markieren Sie das gewünschte Zertifikat, und klicken Sie mit der rechten Maustaste auf **Alle Aufgaben > Exportieren**.
12. Sobald der Assistent „Zertifikat exportieren“ angezeigt wird, klicken Sie auf **Weiter**.
13. Wählen Sie **Ja, privaten Schlüssel exportieren** aus, und klicken Sie auf **Weiter**.
14. Wählen Sie **Privater Informationsaustausch - PKCS #12 (.PFX)** aus, und wählen Sie anschließend die Unteroptionen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren** aus. Klicken Sie auf **Weiter**.

15. Geben Sie das Passwort ein und bestätigen Sie es. Sie können das Passwort frei wählen. Wählen Sie ein Passwort, das nur Sie selbst sich leicht merken können, nicht aber andere. Klicken Sie auf **Weiter**.
16. Klicken Sie auf **Durchsuchen**, um zu dem Speicherort zu navigieren, auf dem Sie die Datei speichern möchten.
17. Geben Sie unter *Dateiname* einen Namen für die zu speichernde Datei ein. Klicken Sie auf **Speichern**.
18. Klicken Sie auf **Weiter**.
19. Klicken Sie auf **Fertigstellen**.
20. Sie erhalten die Meldung, dass der Export erfolgreich abgeschlossen wurde. Schließen Sie die MMC.
21. Kehren Sie zurück zum Dell Server-Konfigurationstool.
22. Wählen Sie aus dem Hauptmenü **Aktionen** > **DM-Zertifikat importieren** aus.
23. Navigieren Sie zu der Stelle, an der die exportierte Datei gespeichert wurde. Wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.
24. Geben Sie das mit dieser Datei verknüpfte Passwort ein, und klicken Sie auf **OK**.

Der Import des Dell Manager-Zertifikats ist nun abgeschlossen.

Wenn die Änderungen abgeschlossen wurden:

1. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.
2. Schließen Sie das Dell Server-Konfigurationstool.
3. Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn*Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Importieren des SSL/TLS-Zertifikats BETA

Wenn Ihre Implementierung die Serververschlüsselung umfasst, müssen Sie das neu erstellte (oder bestehende) Zertifikat importieren. Das SSL/TLS-Zertifikat BETA wird dazu verwendet, den privaten Schlüssel zu schützen, der zum Signieren der Richtlinienpakete genutzt wird, die an Client-Server gesendet werden.

1. Wählen Sie aus dem Hauptmenü **Aktionen** > **SSL/TLS-Zertifikat BETA importieren** aus.
2. Navigieren Sie zum Zertifikat, das Sie auswählen möchten, und klicken Sie auf **Weiter**.
3. Geben Sie bei der Aufforderung zur Eingabe des *Zertifikatkennworts* das Kennwort ein, das zum vorhandenen Zertifikat gehört.
4. Wählen Sie im Windows-Kontodialogfeld eine Option aus:
   a. Um die Anmeldeinformationen für das Identitätszertifikat zu ändern, wählen Sie **Andere Windows-Konto-Anmeldeinformationen mit dem Identitätszertifikat verwenden**.
   b. Um weiterhin die Anmeldeinformationen des angemeldeten Kontos zu verwenden, klicken Sie auf **Weiter**.
5. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.

Einstellungen für Server SSL-Zertifikat konfigurieren

Klicken Sie im Server Configuration Tool auf die Registerkarte **Einstellungen**.

Dell Manager:

Wählen Sie zum Deaktivieren der serverseitigen SSL-Vertrauensvalidierung für Dell Manager **Vertrauenskettenprüfung deaktivieren**.

SCEP:

Geben Sie bei Verwendung von Mobile Edition die URL des SCEP-Hostservers ein.

ANMERKUNG: Ab v9.8 wird Mobile Edition nicht mehr unterstützt.

Wenn die Änderungen abgeschlossen wurden:

1. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.
2. Schließen Sie das Dell Server-Konfigurationstool.
3. Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Konfigurieren von SMTP-Einstellungen

Klicken Sie im Server Configuration Tool auf die Registerkarte **SMTP**.

Diese Registerkarte konfiguriert SMTP-Einstellungen für Produkt-Bulletins, Benachrichtigungen und Threat Relay-Meldungen für Advanced Threat Prevention.

Wenn die Änderungen an der Konfiguration abgeschlossen sind, starten Sie den Sicherheitsserver-Dienst neu. Der Sicherheitsserver-Dienst muss neu gestartet werden, damit die Einstellungen aktualisiert werden.

Geben Sie die folgenden Informationen ein:

1. *Hostname*: Geben Sie den vollständigen Domainnamen des SMTP-Servers ein, z. B. smtpservername.domain.com
2. *Benutzername*: Geben Sie den Namen des Benutzers ein, der sich beim Mailserver anmelden wird. Das Format kann DOMAIN \hschmid“, „hschmid“ oder ein anderes, organisationsspezifisches Format sein.
3. Geben Sie in das Feld *Kennwort* das mit diesem Benutzernamen verknüpfte Kennwort ein.
4. *Absenderadresse*: Geben Sie die E-Mail-Adresse ein, von der die E-Mail abgeschickt wird. Sie können das mit dem Benutzernamen verknüpfte E-Mail-Konto (hschmidt@domain.com) oder ein anderes Konto angeben, auf das der Benutzer Zugriff hat (CloudRegistration@domain.com).
5. Geben Sie unter *Port* die Port-Nummer ein (in der Regel 25).
6. Wählen Sie im Menü *Authentifizierung* entweder *True* oder *False* aus.

ANMERKUNG: Der Benutzername und das Kennwort sollten leer bleiben, wenn die Authentifizierung auf „Falsch“ gesetzt ist.

Wenn die Änderungen abgeschlossen wurden:

1. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.
2. Schließen Sie das Dell Server-Konfigurationstool.
3. Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Datenbankname, Speicherort oder Anmeldeinformationen ändern

Klicken Sie im Serverkonfigurationstool auf die Registerkarte **Datenbank**.

1. Geben Sie unter *Servername* den vollständigen Domänennamen des Servers ein, auf dem die Datenbank gehostet wird (falls es einen Instanznamen gibt, nehmen Sie diesen mit auf). Beispiel: SQLTest.domain.com\DellDB.

   Dell empfiehlt die Verwendung eines vollständigen Domänennames, wenngleich eine IP-Adresse verwendet werden kann.
2. Geben Sie unter *Serverport* die Portnummer ein.

   Bei Verwendung einer nicht standardmäßigen SQL Server-Instanz müssen Sie im Feld *Port:* den dynamischen Port der Instanz angeben. Alternativ dazu aktivieren Sie den SQL Server Browser-Service und stellen Sie sicher, dass UDP-Port 1434 geöffnet ist. Weitere Informationen finden Sie unter https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.
3. Geben Sie unter *Datenbank* den Namen der Datenbank ein.
4. Wählen Sie unter *Authentifizierung* entweder **Windows-Authentifizierung** oder **SQL Server-Authentifizierung**. Bei Auswahl der Option „Windows-Authentifizierung“ werden zur Authentifizierung dieselben Anmeldeinformationen verwendet wie bei der Anmeldung bei Windows (*Benutzername* und *Kennwort* sind nicht bearbeitbar).
5. Geben Sie unter *Benutzername* den Namen des mit dieser Datenbank verbundenen Benutzers ein.

6. Geben Sie unter *Kennwort* das Kennwort für den unter „Benutzername“ aufgeführten Benutzer ein.
7. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.
8. Wählen Sie zum Testen der Datenbankkonfiguration **Aktionen** > **Datenbankkonfiguration testen** aus dem Hauptmenü. Daraufhin wird der Konfigurationsassistent gestartet.
9. Lesen Sie im Fenster *Konfigurationstest* die Testinformationen, und klicken Sie dann auf **Weiter**.
10. Wenn Sie auf der Registerkarte *Datenbank* die Option „Windows-Authentifizierung“ ausgewählt haben, können Sie alternative Anmeldeinformationen eingeben, damit die gleichen Anmeldeinformationen verwendet werden können wie für die Ausführung von Security Management Server. Klicken Sie auf **Weiter**.
11. Im Fenster *Konfiguration testen* werden die Ergebnisse für die Tests der Verbindungseinstellungen, der Kompatibilität und der Datenbankmigration angezeigt.
12. Klicken Sie auf **Fertigstellen**.

ANMERKUNG:

Falls entweder die SQL-Datenbank oder SQL-Instanz mit einer nicht standardmäßigen Sortierreihenfolge konfiguriert wird, muss bei der nicht-standardmäßigen Sortierung die Groß- und Kleinschreibung nicht beachtet werden. Eine Liste der Sortierreihenfolgen und Groß- und Kleinschreibung finden Sie unter https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Wenn die Änderungen abgeschlossen wurden:

1. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.
2. Schließen Sie das Dell Server-Konfigurationstool.
3. Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

Datenbank migrieren

Sie können eine Datenbank v9.2 oder höher mit dem neuesten Upgrade des Servers auf das neueste Schema migrieren.

Klicken Sie im Serverkonfigurationstool auf die Registerkarte **Datenbank**.

1. Wenn Sie noch keine Sicherungsdatei Ihrer bestehenden Dell Serverdatenbank angelegt haben, sollten Sie dies **jetzt** tun.
2. Wählen Sie aus dem Hauptmenü **Aktionen** > **Datenbank migrieren**. Daraufhin wird der Konfigurationsassistent gestartet.
3. Im Fenster *Enterprise-Datenbank migrieren* wird eine Warnung angezeigt. Bestätigen Sie, dass Sie die gesamte Datenbank gesichert haben bzw. dass eine Sicherung der vorhandenen Datenbank nicht erforderlich ist. Klicken Sie auf **Weiter**.

   Im Fenster *Datenbank wird migriert* zeigen informative Meldungen den Status der Migration an.

   Führen Sie nach der Initialisierung eine Fehlersuche durch.

   ANMERKUNG: Eine Fehlermeldung, die durch gekennzeichnet ist, weist darauf hin, dass eine Datenbankaufgabe fehlgeschlagen ist und dass Korrekturmaßnahmen erforderlich sind, damit die Datenbank ordnungsgemäß migriert werden kann. Klicken Sie auf Fertigstellen, beheben Sie die Datenbankfehler und führen Sie die Anweisungen in diesem Abschnitt erneut durch.
4. Klicken Sie auf **Fertigstellen**.

Wennd die Migration abgeschlossen ist:

1. Wählen Sie aus dem Hauptmenü **Konfiguration** > **Speichern** aus. Bestätigen Sie den Speichervorgang, wenn Sie dazu aufgefordert werden.
2. Schließen Sie das Dell Server-Konfigurationstool.
3. Klicken Sie auf **Start** > **Ausführen**. Geben Sie *services.msc* ein und klicken Sie auf **OK**. Wenn *Services* angezeigt wird, navigieren Sie zu den einzelnen Dell Services, und klicken Sie auf **Service starten**.

6

Administrative Aufgaben

Dell Administratorrolle zuweisen

1. Melden Sie sich als Administrator von Security Management Server Virtual an der Verwaltungskonsole an: https://server.domain.com:8443/webui/. Die Standard-Anmeldeinformationen lauten **superadmin/changeit**.
2. Klicken Sie im linken Bereich auf **Bestückung** > **Domänen**.
3. Klicken Sie auf eine Domäne, der ein Benutzer hinzugefügt werden soll.
4. Klicken Sie auf der Seite „Domänendetails“ auf die Registerkarte **Mitglieder**.
5. Klicken Sie auf **Benutzer hinzufügen**.
6. Geben Sie einen Filter ein, um den Benutzernamen nach allgemeinem Namen, UPN (Universal Principal Name) oder SAM-Kontonamen zu suchen. Der Platzhalter ist *.

   Auf dem Unternehmensverzeichnisserver muss für jeden Benutzer ein allgemeiner Name, ein UPN (Universal Principal Name) und ein SAM-Kontoname definiert sein. Wenn ein Benutzer einer Domäne oder Gruppe angehört, aber nicht in der Liste der Domänen- oder Gruppenmitglieder im Management angezeigt wird, überprüfen Sie, ob alle drei Namen für diesen Benutzer auf dem Unternehmensverzeichnisserver korrekt definiert sind.

   Bei der Abfrage wird automatisch zunächst nach dem allgemeinen Namen, dann nach dem UPN und dann nach dem SAM-Kontonamen gesucht, bis ein Treffer gefunden wurde.
7. Wählen Sie die Benutzer, die Sie zur Domäne hinzufügen möchten, aus der *Verzeichnisbenutzerliste* aus. Verwenden Sie <Umschalt><Klick> oder <Strg><Klick>, um mehrere Benutzer auszuwählen.
8. Klicken Sie auf **Hinzufügen**.
9. Klicken Sie in der Menüleiste auf die Registerkarte **Details und Aktionen** des angegebenen Benutzers.
10. Scrollen Sie durch die Menüleiste und wählen Sie die Registerkarte **Admin**.
11. Wählen Sie die Administratorrollen aus, die Sie diesem Benutzer zuweisen möchten.
12. Klicken Sie auf **Speichern**.

Mit Dell Administratorrolle anmelden

1. Melden Sie sich bei der Verwaltungskonsole ab.
2. Melden Sie sich mit den Anmeldeinformationen eines Domainbenutzers bei der Verwaltungskonsole an.

Hochladen der Client-Zugriffslizenz

Sie haben separat von den Installationsdateien Client-Zugriffslizenzen erhalten, entweder beim anfänglichen Kauf oder später, wenn Sie zusätzliche Client-Zugriffslizenzen hinzugefügt haben.

1. Klicken Sie im linken Fensterbereich auf **Verwaltung**.
2. Klicken Sie auf **Lizenzverwaltung**.
3. Klicken Sie auf **Datei auswählen**, um die Client-Lizenzdatei zu suchen und auszuwählen.

Richtlinien bestätigen

Wenn die Installation abgeschlossen ist, bestätigen Sie die Richtlinien.

Um Richtlinien nach der Installation oder später, nachdem die Richtlinienänderungen gespeichert sind, zu bestätigen, führen Sie die folgenden Schritte aus:

1. Klicken Sie im linken Fensterbereich auf **Verwaltung** > **Festlegen**.
2. Geben Sie in *Anmerkung* eine Beschreibung der Änderung ein.
3. Klicken Sie auf **Richtlinien bestätigen**.

Dell Compliance Reporter konfigurieren

1. Klicken Sie im linken Fensterbereich auf **Compliance Reporter**.
2. Wenn Dell Compliance Reporter gestartet wird, melden Sie sich mit den Standard-Anmeldeinformationen *superadmin/changeit* an.

Ausführen von Sicherungen

Zum Zwecke der Notfallwiederherstellung stellen Sie sicher, dass von den folgenden Speicherorten wöchentlich nächtliche differenzielle Sicherungen erstellt werden: Weitere Informationen zum Planen der Notfallwiederherstellung finden Sie unterhttp://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. Weitere Informationen zum Sichern der Daten von Compliance Reporter finden Sie unterhttp://www.dell.com/support/article/de/en/debsdt1/sln289096/how-to-backup-and-import-custom-compliance-reports-in-dell-security-management-server-dell-data-protection-enterprise-edition-server?lang=en.

Sicherungen von Security Management Server

Sichern Sie regelmäßig die Dateien an den Speicherorten, die Sie bei der Installation für die Sicherung von Konfigurationsdateien ausgewählt haben (Schritt 10 auf Seite 27) oder Aktualisierung/Migration (Schritt 6 auf Seite 68). Wöchentliche Sicherungen dieser Daten sind akzeptabel, da sie sich selten ändern und falls nötig manuell neu konfiguriert werden können. Die wichtigsten Dateien speichern Informationen, die zur Verbindungsaufnahme mit der Datenbank nötig sind:

<Installationsverzeichnis>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<Installationsverzeichnis>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<Installationsverzeichnis>\Enterprise Edition\Compatibility Server\conf\gkconfig.xml

SQL Server-Sicherungen

Führen Sie vollständige nächtliche Sicherungen mit aktivierter Transaktionsprotokollierung durch, und führen Sie differenzielle Datenbanksicherungen alle 3-4 Stunden durch. Falls eine Sicherungsdatenbank vorhanden ist, sollten Transaktionsprotokolle und/oder Protokollversandaufgaben alle 15 Minuten (oder in kürzeren Intervallen) ausgeführt werden. Wie immer empfehlen wir Ihnen, für die Dell Server-Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfall-Wiederherstellungsplan Ihres Unternehmens einzubeziehen.

Weitere Informationen zu bewährten Verfahren für SQL Server, die implementiert werden sollten, wenn Dell Security installiert ist, aber die Verfahren noch nicht implementiert sind, finden Sie in der folgenden Liste.

PostgreSQL Server-Sicherungen

Audit-Ereignisse werden in PostgreSQL-Server unter C:\ProgramData\Dell\PostgreSQL\10.7\data gespeichert, der routinemäßig gesichert werden sollte. Eine Anleitung zur Sicherung erhalten Sie unter /C:/ProgramData/Dell/PostgreSQL/10.7/data.

Dell empfiehlt, für die PostgreSQL-Datenbank die bewährten Verfahren für Datenbanken zu verwenden und Dell Software in den Notfallwiederherstellungsplan Ihres Unternehmens einzubeziehen.

7

Ports

In der folgenden Tabelle werden die einzelnen Komponenten mit ihren Funktionen aufgeführt.

Name	Standardport	Beschreibung
ACL-Dienst	TCP/ 8006	Verwaltet verschiedene Berechtigungen und Gruppenzugriffe für verschiedene Dell Sicherheitsprodukte. **ANMERKUNG:** Port 8006 ist derzeit nicht gesichert. Stellen Sie sicher, dass dieser Port ordnungsgemäß durch eine Firewall gefiltert ist. Dieser Port ist nur für die interne Verwendung.
Compliance Reporter	HTTP(S)/ 8084	Bietet eine umfassende Übersicht über die Umgebung für die Durchführung von Prüfverfahren und die Erstellung von Berichten über die Regelkonformität. **ANMERKUNG:** Port 8084 sollte durch eine Firewall gefiltert werden. Dell empfiehlt, dass dieser Anschluss nur intern verwendet wird.
Management Console	HTTP(S)/ 8443	Verwaltungskonsole und Befehlszentrale für die gesamte Unternehmensimplementierung.
Core Server	HTTPS/ 8888	Verwaltet den Richtlinienablauf, Lizenzen und die Registrierung für die Preboot-Authentifizierung, SED-Verwaltung, BitLocker Manager, Threat Protection und Advanced Threat Prevention. Verarbeitet Bestandslistendaten zur Verwendung durch den Compliance Reporter und die Verwaltungskonsole. Sammelt und speichert Authentifizierungsdaten Steuert den rollenbasierten Zugriff.
Device Server	HTTPS/ 8081	Unterstützt die Aktivierung und Wiederherstellung von Kennwörtern. Eine Komponente von Security Management Server. Erforderlich für Encryption Enterprise (Windows und Mac)
Security Server	HTTPS/ 8443	Kommuniziert mit Policy Proxy; verwaltet das Abrufen forensischer Schlüssel, Client-Aktivierungen, SED-PBA-Kommunikation und Full Disk Encryption-PBA-Kommunikation sowie Active

Name	Standardport	Beschreibung
		Directory für die Authentifizierung oder Abstimmung, einschließlich der Identitätsvalidierung für die Authentifizierung in der Remote Management-Konsole. Erfordert Zugriff auf die SQL-Datenbank.
Compatibility Server	TCP/ 1099	Ein Dienst für die Verwaltung der Unternehmensarchitektur. Sammelt und speichert anfängliche Bestandslistendaten während der Aktivierung und Richtliniendaten während Migrationen. Verarbeitet Daten auf Grundlage von Benutzergruppen. **ANMERKUNG:** Port 1099 sollte durch eine Firewall gefiltert werden. Dell empfiehlt, dass dieser Anschluss nur intern verwendet wird.
Message Broker-Service	TCP/ 61616 und STOMP/ 61613	Handhabt die Kommunikation zwischen Diensten von Dell Server. Stellt durch den Compatibility Server für Policy-Proxy-Warteschlangen erzeugte Richtlinieninformationen bereit. Erfordert Zugriff auf die SQL-Datenbank. **ANMERKUNG:** Port 61616 sollte durch eine Firewall gefiltert werden. Dell empfiehlt, dass dieser Anschluss nur intern verwendet wird. **ANMERKUNG:** Port 61613 sollte nur auf Security Management Servern geöffnet werden, die im Front-End-Modus konfiguriert sind.
Key Server	TCP/ 8050	Verhandlung, Authentifizierung und Verschlüsselung einer Client-Verbindung unter Verwendung von Kerberos APIs. Erfordert Zugriff auf die SQL-Datenbank, um die Schlüsseldaten abzurufen.
Policy Proxy	TCP/ 8000	Stellt einen netzwerkbasierten Kommunikationsweg bereit, über den Aktualisierungen der Sicherheitsrichtlinien und der Bestandsdaten übermittelt werden.
Postgres	TCP/ 5432	Lokale Datenbank, die für Ereignisdaten verwendet wird. **ANMERKUNG:** Port 5432 sollte durch eine Firewall gefiltert werden. Dell empfiehlt, dass dieser Anschluss nur intern verwendet wird.
LDAP	TCP/	Port 389 - Dieser Port wird für die Anforderung von Informationen aus dem

Name	Standardport	Beschreibung
	389/636 (lokaler Domänencontroller), 3268/3269 (globaler Katalog) TCP/ 135/ 49125+ (RPC)	lokalen Domänencontroller verwendet. LDAP-Anfragen, die an Port 389 gesandt wurden, können nur zur Suche nach Objekten innerhalb der Startdomäne des globalen Katalogs verwendet werden. Die anfordernde Anwendung kann jedoch alle Attribute für diese Objekte ermitteln. Eine Anfrage an Port 389 könnte beispielsweise zur Ermittlung des Departements eines Benutzers verwendet werden. Port 3268 – Dieser Port wird für Abfragen verwendet, die spezifisch für den globalen Katalog vorgesehen ist. LDAP-Anfragen, die an Port 3268 gesandt wurden, können zur Suche nach Objekten im ganzen Wald verwendet werden. Es können jedoch nur die Attribute zurückgegeben werden, die zur Replikation im globalen Katalog markiert sind. Das Departement eines Benutzers kann beispielsweise nicht unter Verwendung von Pport 3268 zurückgegeben werden, da dieses Attribut nicht in den globalen Katalog repliziert wurde.
Microsoft SQL-Datenbank	TCP/ 1433	Der Standardport für SQL Server ist 1433. Client-Ports wird ein zufälliger Wert zwischen 1024 und 5000 zugewiesen.
Client-Authentifizierung	HTTPS/ 8449	Ermöglicht Client-Servern die Authentifizierung bei Dell Server. Erforderlich für Server Encryption.

8

Bewährte Verfahren für SQL Server

Die folgende Liste erklärt die bewährten Verfahren für SQL Server, die implementiert werden sollten, wenn Dell Security installiert wird, falls sie noch nicht implementiert wurden.

1. Stellen Sie sicher, dass die Größe des NTFS-Blocks, der die Datendatei und Protokolldatei enthält, 64 KB beträgt. SQL Server Extents (Grundeinheit von SQL-Speicher) entspricht 64 KB.

   Weitere Informationen finden Sie in den TechNet-Artikeln von Microsoft für „Erläuterungen zu Seiten und Umfang".

2. Generell soll die maximale Größe des SQL-Server-Speichers 80% des installierten Speichers betragen.

   Weitere Informationen finden Sie in den TechNet-Artikeln von Microsoft für *Serverspeicher, Serverkonfigurationsoptionen*.

   - 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. Stellen Sie -t1222 in den Instanz-Starteigenschaften ein, um sicherzustellen, dass Deadlock-Informationen erfasst werden, falls sie eintreten.

   Weitere Informationen finden Sie in den TechNet-Artikeln von Microsoft für „Ablaufverfolgungsflags (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. Stellen Sie sicher, dass alle Indizes wöchentlich gewartet werden, um sie neu aufzubauen.

5. Überprüfen Sie, ob die Berechtigungen und Funktionen für die Datenbank geeignet sind, die vom Security Management Server verwendet werden. Weitere Informationen finden Sie im KB-Artikel SLN307771.

9

Zertifikate

In diesem Kapitel wird erläutert, wie Sie Zertifikate für die Verwendung des Security Management Server erhalten.

Weitere Informationen über die Konfiguration der SmartCard-Authentifizierung finden Sie unter http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en.

Weitere Informationen zu den Mindestanforderungen zum Anfordern von SSL/TLS-Zertifikaten für die Verwendung durch Dell Data Security Server finden Sie unter 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.

Weitere Informationen über das Aktualisieren des Zertifikats für Dell Encryption mit einem vorhandenen Zertifikat im Microsoft-Keystore finden Sie unter http://www.dell.com/support/article/us/en/19/sln297240/.

Erstellen eines selbstsignierten Zertifikats und Generieren einer Zertifikatssignieranforderung

In diesem Abschnitt werden die Schritte zum Erstellen eines selbstsignierten Zertifikats für die Java-basierten Komponenten beschrieben. Mit diesem Verfahren können **keine** selbstsignierten Zertifikate für .NET-basierte Komponenten erstellt werden.

Für Produktionsumgebungen wird die Verwendung selbstsignierter Zertifikate von Dell *nicht* empfohlen.

Falls Ihre Organisation ein SSL-Serverzertifikat benötigt oder Sie aus anderen Gründen ein Zertifikat erstellen müssen, wird in diesem Abschnitt das Verfahren zum Erstellen eines Java-Keystore mit Keytool beschrieben.

Wenn Ihre Organisation die Verwendung von Smart Cards für die Authentifizierung plant, müssen Sie Keytool verwenden, um die vollständige Zertifikatsvertrauenskette zu importieren, die im Zertifikat des Smart Card-Benutzers verwendet wird.

Keytool erstellt private Schlüssel, die im CSR-Format (Certificate Signing Request) an eine Zertifizierungsstelle wie VeriSign® oder Entrust® übertragen werden. Anhand dieser CSR erstellt die Zertifizierungsstelle dann ein Serverzertifikat und signiert es. Danach wird das Serverzertifikat zusammen mit dem Zertifikat der Zertifizierungsstelle in eine Datei heruntergeladen. Anschließend werden die Zertifikate in die cacerts-Datei importiert.

Neue Key-Paare und selbstsignierte Zertifikate erstellen

1. Navigieren Sie zum Verzeichnis **conf** von Compliance Reporter, Security Server oder Device Server.
2. Erstellen Sie eine Sicherungskopie der Standard-Zertifikatsdatenbank:

   Klicken Sie auf **Start** > **Ausführen** und geben Sie **`move cacerts cacerts.old`** ein.
3. Fügen Sie Keytool in den Systempfad ein. Geben Sie den folgenden Befehl in eine Eingabeaufforderung ein:

   `set path=%path%;<Dell Java Install Dir>\bin`
4. Führen Sie zum Erstellen eines Zertifikats Keytool wie folgt aus:

   `keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias` Dell **`-keystore .\cacerts`**
5. Geben Sie nach der entsprechenden Aufforderung in Keytool die folgenden Informationen ein.

   ANMERKUNG:

   Erstellen Sie vor der Bearbeitung von Konfigurationsdateien eine Sicherungskopie. Ändern Sie nur die angegebenen Parameter. Wenn Sie andere Daten in diesen Dateien ändern, beispielsweise Tags, kann dies zu einem Systemschaden und -ausfall führen. Dell kann nicht gewährleisten, dass sich Probleme als Folge nicht autorisierter Änderungen an diesen Dateien ohne Neuinstallation des Security Management Server beheben lassen.

- *Keystore-Passwort*: Geben Sie ein Passwort ein (die Zeichen <>;&" ' sind nicht zulässig), und setzen Sie die Variable in der Datei **conf** der Komponente auf denselben Wert, wie hier gezeigt:

<Compliance Reporter install dir>\conf\eserver.properties. Bestimmen Sie den Wert eserver.keystore.password =

<Device Server install dir>\conf\application.properties. Bestimmen Sie den Wert keystore.password =

<Security Server install dir>\conf\application.properties. Bestimmen Sie den Wert keystore.password =

- *Vollständiger Servername*: Geben Sie den vollständigen Namen des Servers ein, auf dem die Komponente, mit der Sie arbeiten, installiert ist. Zum vollständigen Namen gehören der Hostname und der Domänenname (Beispiel: server.domäne.com).
- *Organisationseinheit*: Geben Sie den entsprechenden Wert ein (Beispiel: Sicherheit).
- *Organisation*: Geben Sie den entsprechenden Wert ein (Beispiel: Dell).
- *Ort*: Geben Sie den entsprechenden Wert ein (Beispiel: München).
- *Bundesstaat bzw. Bundesland*: Geben Sie den Namen des Bundesstaats oder -landes ohne Abkürzungen ein (Beispiel: Bayern).
- Landescode mit zwei Buchstaben.
- Sie müssen im Dienstprogramm bestätigen, dass die Angaben stimmen. Ist dies der Fall, geben Sie **Ja** ein.

  Falls nicht, geben Sie **Nein** ein. Keytool zeigt jeden zuvor eingegebenen Wert an. Drücken Sie die Eingabetaste, um den Wert zu akzeptieren, oder ändern Sie den Wert und drücken Sie anschließend die **Eingabetaste**.
- *Schlüsselpasswort für Alias*: Wenn Sie hier kein anderes Passwort eingeben, wird automatisch das Keystore-Passwort verwendet.

Signierte Zertifikate von einer Zertifizierungsstelle anfordern

Verwenden Sie dieses Verfahren, um eine Anfrage zum Signieren von Zertifikaten (CSR) für das bei Neues Key-Paar und selbstsigniertes Zertifikat erstellen erstellte, selbstsignierte Zertifikat zu generieren.

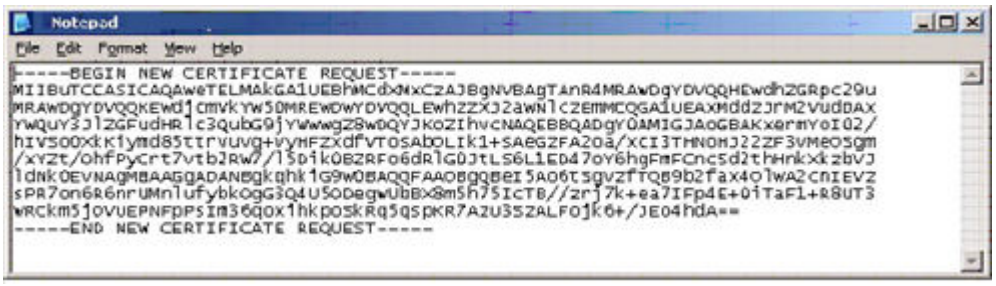
1. Verwenden Sie die denselben Wert wie zuvor für <**certificatealias**>:

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

   Beispiel: **keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file** Dell**.csr**

   Die .csr-Datei enthält ein BEGIN/END-Paar, das während der Erstellung des Zertifikats bei der Zertifizierungsstelle verwendet wird.

   Beispiel .CSR-Datei

2. Befolgen Sie Ihr Organisationsverfahren zum Erwerb eines SSL-Serverzertifikats bei einer Zertifizierungsstelle. Senden Sie den Inhalt von <CSR-Dateiname> zum Signieren.

   ANMERKUNG:

   Es gibt verschiedene Methoden zur Anforderung eines gültigen Zertifikats. Ein Beispiel finden Sie unter **Beispielmethode zur Anforderung eines Zertifikats**.
3. Speichern Sie das signierte Zertifikat nach Erhalt in einer Datei.
4. Wir empfehlen, immer eine Sicherungskopie dieses Zertifikats anzufertigen, falls beim Import ein Fehler auftritt. Die Sicherungskopie verhindert, dass der Vorgang noch einmal von vorn begonnen werden muss.

Stammzertifikate importieren

Wenn die Zertifizierungsstelle für das Stammzertifikat Verisign (aber nicht Verisign Test) ist, gehen Sie zum nächsten Verfahren weiter und importieren Sie das signierte Zertifikat.

Mit dem Stammzertifikat der Zertifizierungsstelle werden signierte Zertifikate validiert.

1. Führen Sie **eine** der folgenden Maßnahmen durch:
   - Laden Sie das Stammzertifikat der Zertifizierungsstelle herunter und speichern Sie es in einer Datei.
   - Rufen Sie das Stammzertifikat vom Unternehmensverzeichnisserver ab.
2. Führen Sie **eine** der folgenden Maßnahmen durch:
   - Wenn Sie SSL für Compliance Reporter, Security Server oder Device Server aktivieren möchten, wechseln Sie in das Komponentenverzeichnis **conf**.
   - Wenn Sie SSL zwischen dem Security Management Server und dem Unternehmensverzeichnisserver aktivieren möchten, wechseln Sie in das Verzeichnis <**Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (das Standardpasswort für JRE-Cacerts lautet **changeit**).
3. Führen Sie Keytool wie folgt aus, um das Stammzertifikat zu installieren:

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

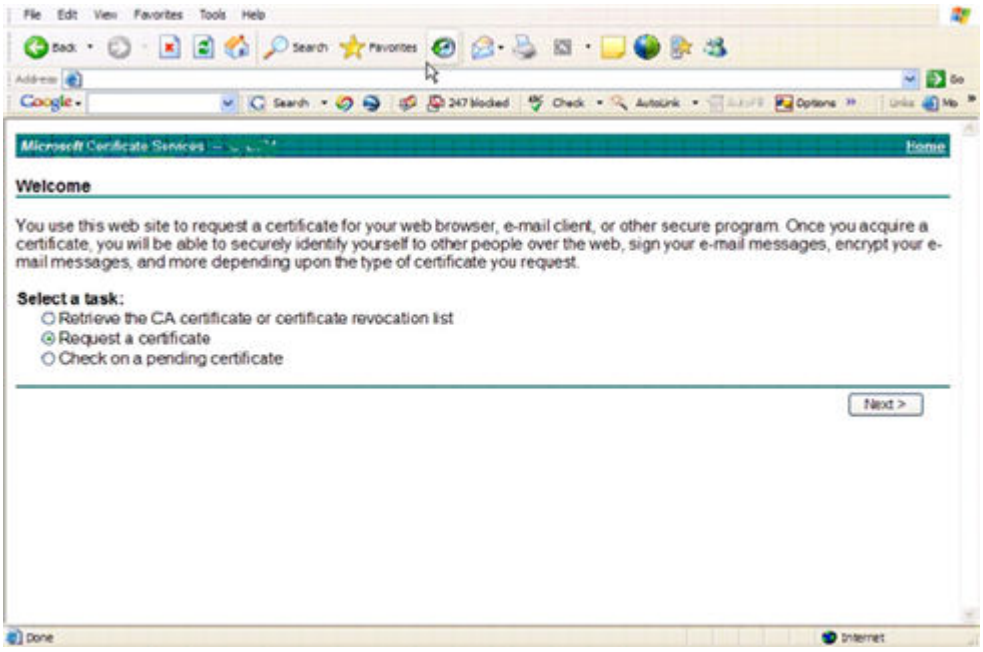
   Beispiel: **keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer**

Beispielmethode zur Anforderung eines Zertifikats

Eine Methode zur Anforderung eines Zertifikats besteht darin, über einen Webbrowser auf den Microsoft-Zertifizierungsstellenserver zuzugreifen, der intern von Ihrer Organisation eingerichtet wird.

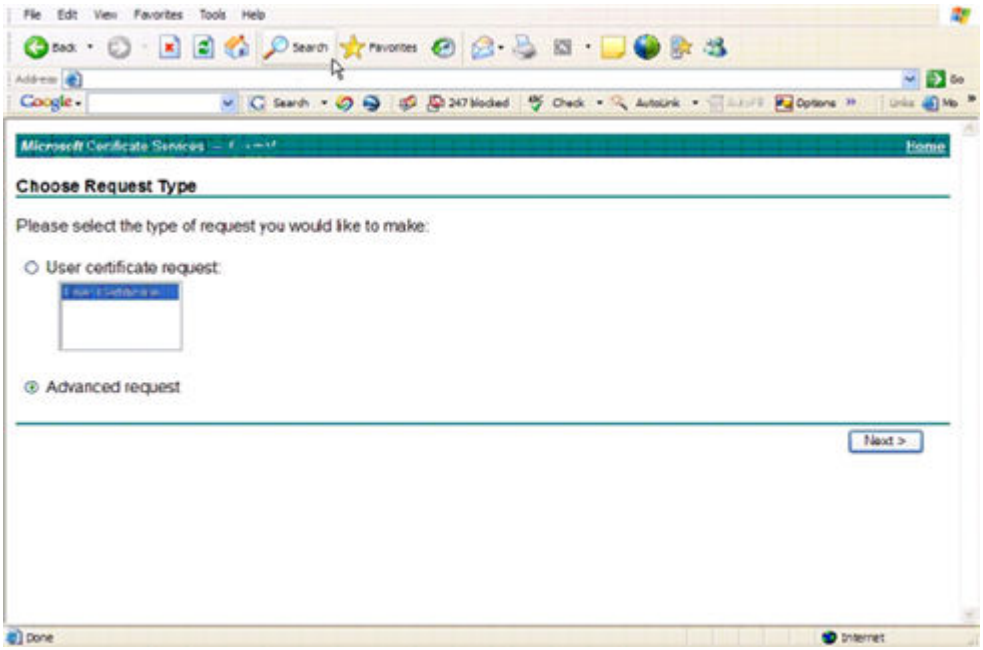
1. Navigieren Sie zum Microsoft-Zertifizierungsstellenserver. Die IP-Adresse wird von Ihrer Organisation bereitgestellt.
2. Wählen Sie **Zertifikat anfordern** aus, und klicken Sie auf **Weiter.**

   Microsoft-Zertifikatdienste



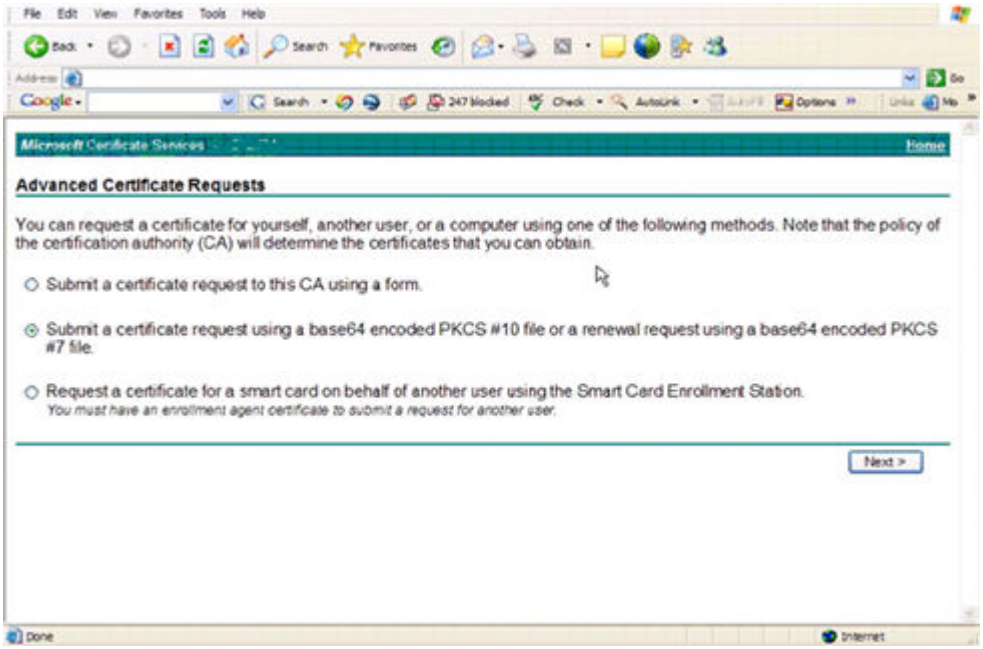
3. Wählen Sie **Erweiterte Anforderung** aus, und klicken Sie auf **Weiter**.

   Art der Anforderung auswählen



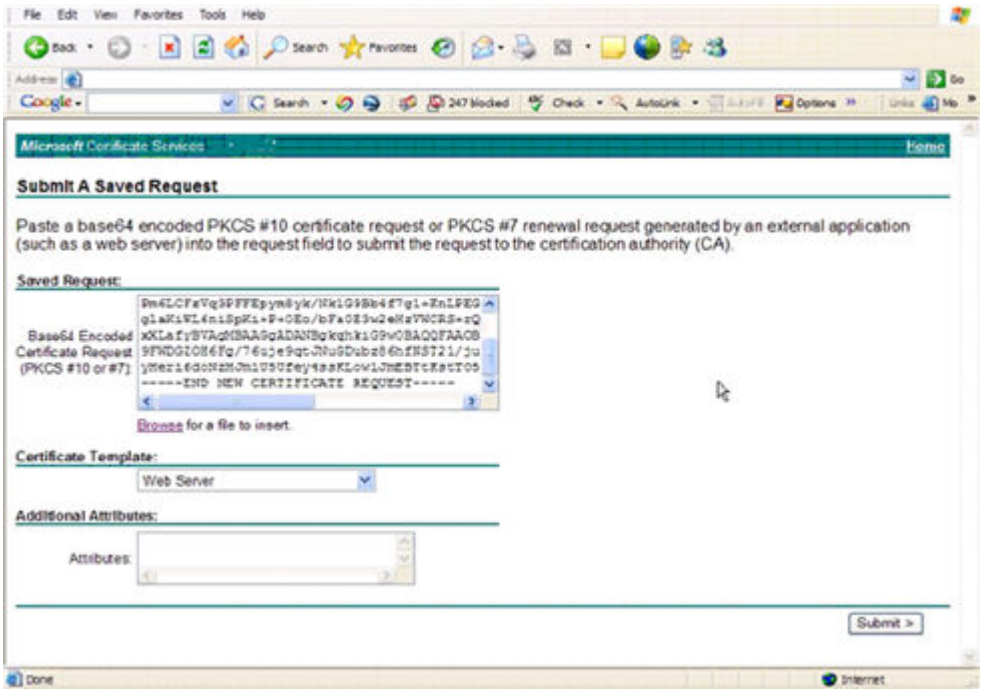
4. Wählen Sie die Option **Einreichen einer Zertifikatanforderung, die eine Base64-codierte PKCS #10-Datei verwendet**, und klicken Sie auf **Weiter**.

Erweiterte Zertifikatanforderung



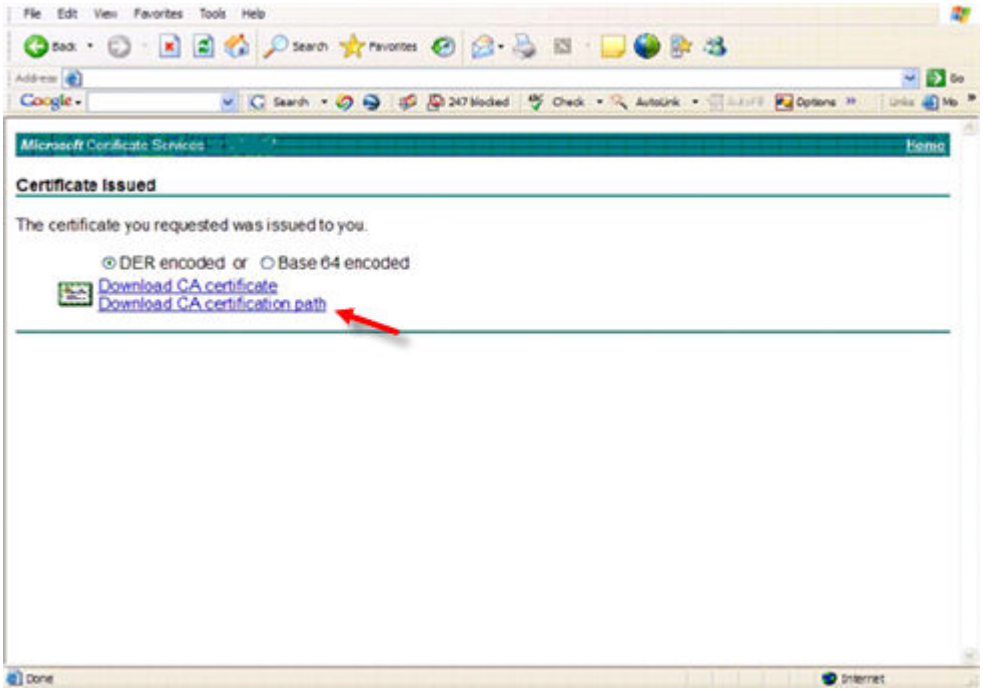
5. Kopieren Sie den Inhalt der CSR-Anforderung in das Textfeld. Wählen Sie die Zertifikatvorlage **Web Server** aus, und klicken Sie auf **Einreichen.**

Gespeicherte Anforderung senden



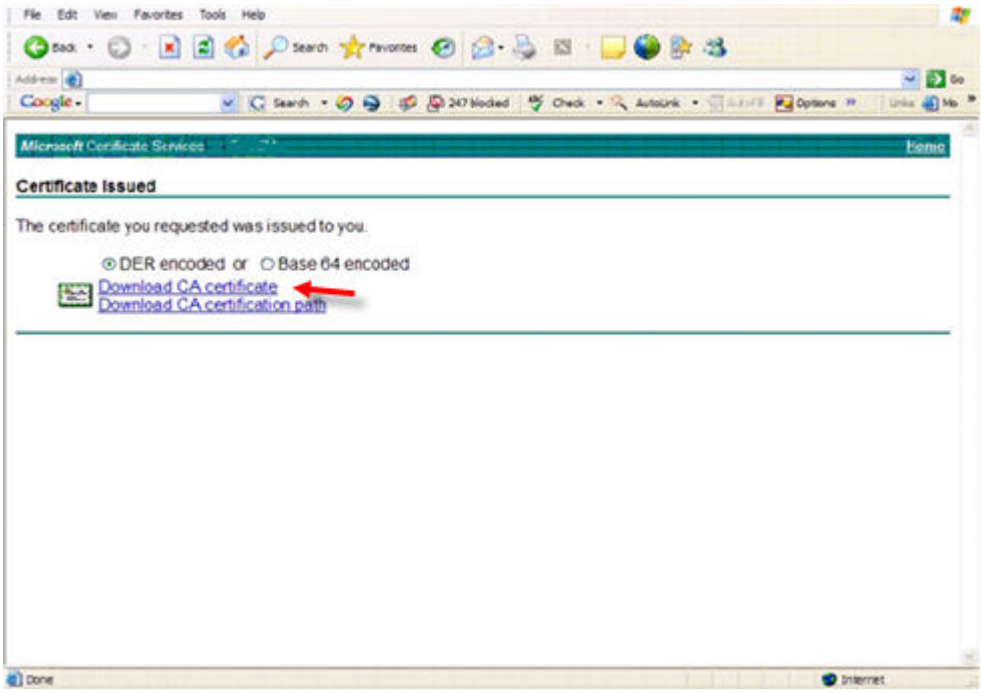
6. Speichern Sie das Zertifikat. Wählen Sie **DER-codiert** aus und klicken Sie auf **Download des Zertifizierungsstellenzertifikats**.

Download des Zertifizierungsstellenzertifikats



7. Speichern Sie das Zertifikat. Wählen Sie **DER-codiert** und klicken Sie auf **Download des Zertifizierungsstellenzertifikats**.

Download des Zertifizierungsstellen-Zertifizierungspfads



8. Importieren Sie das konvertierte Zertifikat der Zertifizierungsstelle. Zurück zur Eingabeaufforderung. Geben Sie Folgendes ein:

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

9. Nach dem Import des Zertifikats der Zertifizierungsstelle kann nun das Serverzertifikat importiert werden (die Zertifikatkette kann eingerichtet werden). Geben Sie Folgendes ein:

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

Verwenden Sie das Alias des selbstsignierten Zertifikats, um die CSR-Anforderung mit dem Serverzertifikat zu verknüpfen.

10. Eine Auflistung der Cacerts-Datei zeigt, dass das Serverzertifikat eine **Zertifikatkettenlänge** von **2** hat. Dies ist ein Hinweis darauf, dass das Zertifikat nicht selbstsigniert ist. Geben Sie Folgendes ein:

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

Der Zertifikat-Fingerabdruck des zweiten Zertifikats in der Kette ist das importierte Zertifikat der signierenden Zertifizierungsstelle (außerdem unter dem Serverzertifikat in der Auflistung aufgeführt).

Zertifikat unter Verwendung der Zertifikatverwaltungskonsole in das Format PFX exportieren

Sobald Ihnen ein Zertifikat in Form einer CRT-Datei im MMC vorliegt, muss diese für die Kompatibilität mit Keytool in eine PFX-Datei konvertiert werden, wenn Sie Dell Security Server im DMZ-Modus verwenden *und* ein Dell Manager-Zertifikat in das Serverkonfigurationstool importieren möchten.

1. Öffnen Sie die Microsoft Management Console.
2. Klicken Sie auf **Datei > Snapin hinzufügen/entfernen**.
3. Klicken Sie auf **Hinzufügen**.
4. Wählen Sie im Fenster *Standalone-Snapin hinzufügen* **Zertifikate** aus und klicken Sie dann auf **Hinzufügen**.
5. Wählen Sie **Computerkonto** aus und klicken Sie auf **Weiter**.
6. Wählen Sie im Fenster *Computer auswählen* **Lokaler Computer (der Computer, auf dem diese Konsole läuft)** und klicken Sie auf **Fertigstellen**.
7. Klicken Sie auf **Schließen**.

8. Klicken Sie auf **OK**.
9. Erweitern Sie im Ordner *Konsolenstamm* die *Zertifikate (Lokaler Computer)*.
10. Gehen Sie zum Ordner *Privat*, und suchen Sie das gewünschte Zertifikat.
11. Markieren Sie das gewünschte Zertifikat, und klicken Sie mit der rechten Maustaste auf **Alle Aufgaben > Exportieren**.
12. Sobald der Assistent „Zertifikat exportieren“ angezeigt wird, klicken Sie auf **Weiter**.
13. Wählen Sie **Ja, privaten Schlüssel exportieren** aus, und klicken Sie auf **Weiter**.
14. Wählen Sie **Privater Informationsaustausch - PKCS #12 (.PFX)** aus, und wählen Sie anschließend die Unteroptionen **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen** und **Alle erweiterten Eigenschaften exportieren** aus. Klicken Sie auf **Weiter**.
15. Geben Sie das Passwort ein und bestätigen Sie es. Sie können das Passwort frei wählen. Wählen Sie ein Passwort, das nur Sie selbst sich leicht merken können, nicht aber andere. Klicken Sie auf **Weiter**.
16. Klicken Sie auf **Durchsuchen**, um zu dem Speicherort zu navigieren, auf dem Sie die Datei speichern möchten.
17. Geben Sie unter *Dateiname* einen Namen für die zu speichernde Datei ein. Klicken Sie auf **Speichern**.
18. Klicken Sie auf **Weiter**.
19. Klicken Sie auf **Fertigstellen**.

    Sie erhalten die Meldung, dass der Export erfolgreich abgeschlossen wurde. Schließen Sie die MMC.

Vertrauenswürdiges, signiertes Zertifikat zum Security Server hinzufügen, wenn ein nicht vertrauenswürdiges Zertifikat für SSL verwendet wurde

1. Wenn der Security Server-Service ausgeführt wird, halten Sie ihn an.
2. Sichern Sie die Cacerts-Datei unter <Security Server install dir>\conf\.

   Verwenden Sie Keytool, um die folgenden Schritte auszuführen:

3. Vertrauenswürdige PFX-Datei in eine Textdatei exportieren und den Aliasnamen dokumentieren:

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

4. PFX-Datei in die Cacerts-Datei nach <Security Server install dir>\conf\. importieren

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

5. Ändern Sie den Wert für „keystore.alias.signing“ unter <Security Server install dir>\conf\application.properties.

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

   Starten Sie den Security Server-Service.