


# Dell Security Management Server

Guia de instalação e migração v10.2.12

## Notas, avisos e advertências

 **NOTA:** Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

 **CUIDADO:** um AVISO indica possíveis danos ao hardware ou a possibilidade de perda de dados e informa como evitar o problema.

 **ATENÇÃO:** uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.

<b>Capítulo 1: Introdução.....</b>	<b>5</b>
Sobre o Security Management Server.....	5
Entre em contato com o Dell ProSupport.....	5
<b>Capítulo 2: Requisitos e arquitetura.....</b>	<b>6</b>
Design da arquitetura do Security Management Server.....	6
Requirements.....	7
Hardware.....	8
Software.....	9
Suporte a idiomas do Management Console.....	12
<b>Capítulo 3: Configuração de pré-instalação.....</b>	<b>13</b>
Configuração.....	13
<b>Capítulo 4: Instalar ou fazer upgrade/migrar.....</b>	<b>17</b>
Antes de iniciar a instalação ou Atualizar/Migrar.....	17
Nova instalação.....	17
Instalar um servidor de back-end e um novo banco de dados.....	18
Instalar um servidor de back-end com um banco de dados existente.....	32
Instalar servidor front-end.....	48
Atualizar/Migrar.....	57
Antes de iniciar o processo de Atualizar/Migrar.....	58
Fazer upgrade/migrar servidor(es) de back-end.....	59
Atualizar/migrar servidor(es) de front-end.....	66
Instalação em modo Desconectado.....	70
Desinstalar o Security Management Server.....	72
<b>Capítulo 5: Configuração pós-instalação.....</b>	<b>75</b>
Configuração do Modo DMZ.....	75
Ferramenta de configuração do servidor.....	75
Adicionar certificados novos ou atualizados.....	76
Importar o Certificado do Dell Manager.....	78
Importar certificado SSL/TLS BETA.....	79
Definir as configurações do certificado do SSL Server.....	79
Definir as configurações do SMTP.....	79
Alterar nome, local ou credenciais do banco de dados.....	80
Migrar o banco de dados.....	81
<b>Capítulo 6: Tarefas administrativas.....</b>	<b>82</b>
Atribuir a função de administrador Dell.....	82
Login com função de administrador Dell.....	82
Carregar licença de acesso do cliente.....	82
Confirmar políticas.....	82
Configurar o Dell Compliance Reporter.....	83

Realizar backups.....	83
Backups do Security Management Server.....	83
SQL Server Backups.....	83
Backups do PostgreSQL Server.....	83
<b>Capítulo 7: Portas.....</b>	<b>84</b>
<b>Capítulo 8: Práticas recomendadas do SQL.....</b>	<b>87</b>
<b>Capítulo 9: Certificados.....</b>	<b>88</b>
Criar um certificado autoassinado e gerar uma solicitação de assinatura de certificado.....	88
Gerar um novo par de chaves e um certificado auto-assinado.....	88
Solicitar um certificado assinado em uma Autoridade de Certificação.....	89
Importar um certificado raiz.....	90
Método de exemplo para solicitar um certificado.....	90
Exportar um certificado para o formato .PFX usando o Console de gerenciamento do certificado.....	93
Adicionar um Certificado de assinatura confiável ao Security Server quando um certificado não confiável foi usado para SSL.....	94

# Introdução

## Sobre o Security Management Server

O Security Management Server tem os seguintes recursos:

- Gerenciamento centralizado de dispositivos, usuários e política de segurança
- Auditoria e relatórios de compatibilidade centralizados
- Separação de deveres administrativos
- Criação e gerenciamento de política de segurança baseada em função
- Distribui as políticas de segurança quando os clientes se conectam
- Recuperação de dispositivo auxiliado pelo administrador
- Caminhos confiáveis para comunicação entre os componentes
- Geração de chave de criptografia exclusiva e depósito de chave de segurança

## Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell.

Há também disponível o serviço de suporte on-line para os produtos Dell no site [dell.com/support](http://dell.com/support). O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone fora dos Estados Unidos, veja [Números de telefone internacionais do Dell ProSupport](#).

# Requisitos e arquitetura

Esta seção aborda detalhadamente as recomendações de design de arquitetura e os requisitos de hardware e software para a implementação do Dell Security Management Server.

## Design da arquitetura do Security Management Server


As soluções do Encryption Enterprise e Endpoint Security Suite Enterprise são produtos altamente dimensionáveis, de acordo com a quantidade de pontos de extremidade que se deseja criptografar em sua organização.

### Componentes da arquitetura

Abaixo estão as configurações sugeridas de hardware que atendem à maioria dos ambientes.

#### **Servidor de gerenciamento de segurança**

- Sistema operacional: Windows Server 2012 R2 (Standard, Datacenter 64 bits), Windows Server 2016 (Standard, Datacenter 64 bits), Windows Server 2019 (Standard, Datacenter)
- Máquina virtual/física
- CPU: 4 núcleos
- RAM: 16 GB
- Unidade C: 30 GB de espaço em disco disponível para os registros e bases de dados da aplicação


 **NOTA:** Até 10 GB podem ser consumidos para um banco de dados de evento local armazenado no PostgreSQL.

#### **Servidor proxy**

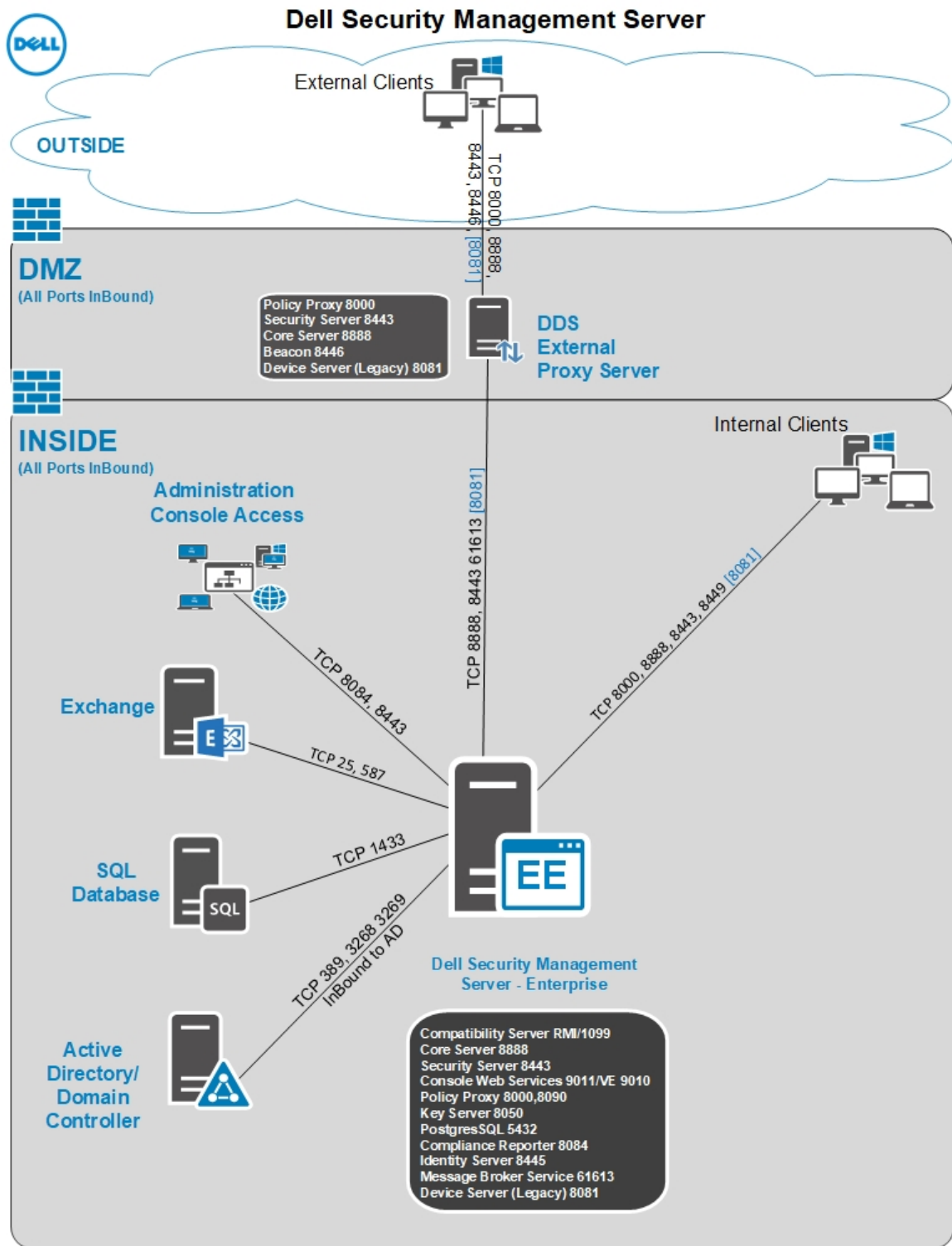
- Sistema operacional: Windows Server 2012 R2 (Standard, Datacenter 64 bits), Windows Server 2016 (Standard, Datacenter 64 bits), Windows Server 2019 (Standard, Datacenter)
- Máquina virtual/física
- CPU: 2 núcleos
- RAM: 8 GB
- Unidade C: 20 GB de espaço em disco disponível para os registros

#### **Especificações do hardware do SQL Server**

- CPU: 4 núcleos
- RAM: 24 GB
- Unidade de dados: 100 - 150 GB de espaço em disco disponível (pode variar de acordo com ambiente)
- Unidade de registro: 50 GB de espaço em disco disponível (pode variar de acordo com ambiente)

 **NOTA:** A Dell recomenda que se siga as [Melhores práticas do SQL Server](#), apesar das informações acima mencionadas cobrirem a maioria dos ambientes.

Abaixo encontra-se uma implementação básica para o Dell Security Management Server.



**NOTA:** Se a organização tiver mais de 20.000 endpoints, entre em contato com o Dell ProSupport para obter assistência.


## Requirements

Os pré-requisitos de hardware e software para instalação do software Security Management Server estão incluídos abaixo.

**Antes de começar a instalação, certifique-se de que todos os patches e as atualizações estejam aplicadas nos servidores usados para a instalação.**

## Hardware

A tabela a seguir detalha os requisitos de hardware *mínimos* para o Security Management Server. Consulte [Design da arquitetura do Dell Security Management Server](#) para obter mais informações sobre dimensionamento com base no tamanho da implementação.

<b>Requisitos de hardware</b>
<b>Processador</b> CPU Quad-Core moderna (1,5 GHz+)
<b>RAM</b> 16 GB
<b>Espaço livre em disco</b> 20 GB de espaço livre em disco  <b>NOTA:</b> Até 10 GB podem ser consumidos para um banco de dados de evento local armazenado no PostgreSQL
<b>Placa de rede</b> 10/100/1000 ou melhor
<b>Diversos</b> Ambiente IPv4 ou IPv6 ou híbrido IPv4/IPv6 necessário

A tabela a seguir detalha os requisitos *mínimos* de hardware para um Security Management Server Front-end/Servidor Proxy.

<b>Requisitos de hardware</b>
<b>Processador</b> CPU Dual-Core moderna
<b>RAM</b> 8GB
<b>Espaço livre em disco</b> 20 GB de espaço livre em disco para os arquivos de log
<b>Placa de rede</b> 10/100/1000 ou melhor
<b>Diversos</b> Ambiente IPv4 ou IPv6 ou híbrido IPv4/IPv6 necessário

## Virtualização

O Security Management Server pode ser instalado em um ambiente virtual. Apenas os ambientes a seguir são recomendados.

O Security Management Server v10.2.11 foi validado nas plataformas abaixo.

Hyper-V Server instalado como uma instalação Completa ou Principal ou como uma função no Windows Server 2012, Windows Server 2016 ou Windows Server 2019.

- Hyper-V Server
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado

- O hardware precisa estar em conformidade com os requisitos mínimos do Hyper-V
- Mínimo de 4 GB de RAM para recurso dedicado de imagem
- Deve ser executado como uma máquina virtual da geração 1
- Consulte <https://technet.microsoft.com/en-us/library/hh923062.aspx> para obter mais informações

O Security Management Server v10.2.11 foi validado com o VMWare ESXi 6.0, VMware ESXi 6.5 e VMware ESXi 6.5.

**i** **NOTA:** Se você for executar o VMware ESXi e o Windows Server 2012 R2, o Windows Server 2016 ou o Windows Server 2019, é recomendável usar adaptadores Ethernet VMXNET3.

- VMware ESXi 6.0
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Consulte a página <http://www.vmware.com/resources/compatibility/search.php> para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte <http://pubs.vmware.com/vsphere-60/index.jsp> para obter mais informações
- VMware ESXi 6.5
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Consulte a página <http://www.vmware.com/resources/compatibility/search.php> para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte <http://pubs.vmware.com/vsphere-65/index.jsp> para obter mais informações
- VMware ESXi 6.7
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Consulte a página <http://www.vmware.com/resources/compatibility/search.php> para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte <http://pubs.vmware.com/vsphere-65/index.jsp> para obter mais informações

**i** **NOTA:** O banco de dados do SQL Server que hospeda o Security Management Server deve ser executado em um computador separado por motivo de desempenho.

## SQL Server

Em ambientes maiores, é altamente recomendável que o servidor de Banco de Dados SQL seja executado em um sistema redundante, como um SQL Cluster, para garantir a disponibilidade e a continuidade dos dados. É recomendável também realizar backups completos e diários com o registro das transações ativado, a fim de garantir que todos os códigos recém-gerados através da ativação de usuários/dispositivos sejam recuperáveis.

As tarefas de manutenção de banco de dados precisam conter a recriação dos índices de bancos de dados e a coleta de estatísticas.

## Software

A tabela a seguir detalha os requisitos de software do Security Management Server e servidor proxy.

**i** **NOTA:** Devido à natureza confidencial dos dados que o Security Management Server retém e para alinhá-lo com a regra de privilégios mínimos, é recomendada a instalação do Security Management Server em seu próprio sistema operacional dedicado ou como parte de um servidor do aplicativo que tenha funções e direitos limitados ativados para ajudar a garantir um ambiente seguro. Essa recomendação inclui não fazer a instalação do Security Management Server em servidores de infraestrutura privilegiados.

Consulte <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models> para obter mais informações sobre a implementação da regra de privilégios mínimos.

**NOTA:** O UAC (Universal Account Control, controle de conta universal) deve ser desativado quando a instalação ocorrer em um diretório protegido. Após desativar o UAC, é preciso reinicializar o servidor para que essa alteração seja aplicada.

**NOTA:** Locais de registro para Policy Proxy (se estiver instalado): HKLM\SOFTWARE\Wow6432Node\Dell

**NOTA:** Local de registro para Windows Servers: HKLM\SOFTWARE\Dell

### Pré-requisitos

- **Pacote redistribuível do Visual C++ 2010**

Se ele ainda não tiver sido instalado, o instalador fará isso para você.

- **Pacote redistribuível do Visual C++ 2013**

Se ele ainda não tiver sido instalado, o instalador fará isso para você.

- **Pacote redistribuível do Visual C++ 2015**

Se ele ainda não tiver sido instalado, o instalador fará isso para você.

- **.NET Framework versão 4.6.1**

- **.NET Framework versão 4.5**

A Microsoft publicou as atualizações de segurança para o .NET Framework versões 4.6.1 e 4.5.

- **.NET Framework versão 3.5 SP1**

- **SQL Native Client 2012**

Se estiver usando o SQL Server 2012 ou o SQL Server 2016.

Se ele ainda não tiver sido instalado, o instalador fará isso para você.

### Security Management Server - Servidor de back-end e servidor de front-end Dell

- **Windows Server 2012 R2**

- Standard Edition

- Datacenter Edition

- **Windows Server 2016**

- Standard Edition

- Datacenter Edition

- **Windows Server 2019**

- Standard Edition

- Datacenter Edition

**NOTA:** No momento o Security Management Server da Dell instalado em uma configuração de back-end ou de front-end não oferece suporte a atualizações de sistema operacional do Windows Server.

### Repositório do LDAP

- Active Directory 2008 R2

- Active Directory 2012 R2

- Active Directory 2016

**NOTA:** O Security Management Server é compatível com o requisito da Microsoft de vinculação de canal LDAP e assinatura LDAP quando o Active Directory está em uso.

## Management Console e Compliance Reporter

- Mozilla Firefox 41.x ou posterior
- Google Chrome 46.x ou posterior
- Microsoft Edge (Chromium)
- Microsoft Edge


 **NOTA:** Seu navegador precisa aceitar cookies.

## Ambientes virtuais recomendados para componentes do Security Management Server

O Security Management Server pode ser instalado em um ambiente virtual.


Atualmente, a Dell oferece suporte à hospedagem do Dell Security Management Server ou Dell Security Management Server Virtual dentro de um ambiente de IaaS (Infraestrutura as a Service, infraestrutura como serviço) hospedado na nuvem, tal como Amazon Web Services, Azure e vários outros provedores. O suporte para esses ambientes é limitado à funcionalidade do Security Management Server. A administração e a segurança dessas máquinas virtuais ficam a cargo do administrador da solução de IaaS (Infraestrutura as a Service, infraestrutura como serviço).

Requisitos de infraestrutura adicionais. Os requisitos de infraestrutura adicionais, como Active Directory e SQL Server, ainda são necessários para a funcionalidade adequada.

 **NOTA:** O banco de dados do SQL Server que hospeda o Security Management Server deve ser executado em um computador separado.

## Banco de dados

- **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


 **NOTA:** Express Editions não são suportados para ambientes de produção. Express Editions podem ser usados apenas em POC e avaliações.

Com base na sua versão do SQL Server, o Security Management Server **requer** que um dos seguintes esteja ativado:

- Indexação de texto completo
- Filtro de texto completo
- Extrações semânticas e de teste completo para pesquisa

Para obter mais informações sobre os erros identificados quando os recursos mencionados acima não estão habilitados para o SQL Server em uso, consulte o artigo da base de conhecimento [SLN308557](#).

Para obter mais informações sobre a configuração das permissões e recursos do Microsoft SQL Server para o Security Management Server, consulte o artigo da base de conhecimento [SLN307771](#).

 **NOTA:** Abaixo, são apresentados os requisitos para as permissões do SQL. O usuário que executa a instalação e os serviços deve ter direitos de administrador local. Além disso, os direitos de administrador local são necessários para a conta de serviço que gerencia os serviços do Dell Security Management Server.

Digite	Ação	Cenário	Privilegio SQL necessário
Back-end	Upgrade	Por definição, upgrades já têm DB e login/usuário estabelecidos.	db_owner
Back-end	Restaurar e instalar	A restauração envolve o DB e login existentes.	db_owner
Back-end	Nova instalação	Usar o DB existente	db_owner
Back-end	Nova instalação	Criar um novo DB	dbcreator, db_owner

Digite	Ação	Cenário	Privilégio SQL necessário
Back-end	Nova instalação	Usar o login existente.	db_owner
Back-end	Nova instalação	Criar novo login.	securityadmin
Back-end	Desinstalar o	NA	NA
Proxy front-end	Qualquer	NA	NA

**NOTA:** Se o UAC (Controle de conta de usuário) estiver ativado, você precisará desativá-lo antes de fazer a instalação no Windows Server 2012 R2 quando estiver instalando em C:\Program Files. O servidor precisa ser reiniciado para que essa alteração tenha efeito.

Durante a instalação, as credenciais de Autenticação do Windows ou SQL são exigidas para configurar o banco de dados. Independentemente de qual tipo de credenciais forem usadas, a conta precisa ter os privilégios apropriados para a ação que está sendo executada. A tabela anterior detalha os privilégios necessários para cada tipo de instalação. Além disso, a conta usada para criar e configurar o banco de dados deve ter seu esquema padrão predefinido como dbo.

Esses privilégios são necessários apenas durante a instalação para configurar o banco de dados. Depois que o Security Management Server estiver instalado, a conta usada para gerenciar o acesso SQL poderá ser restrita às funções db\_owner e público.

Se você não tiver certeza sobre os privilégios de acesso ou conectividade ao banco de dados, peça a seu administrador de banco de dados que confirme isso antes de você começar a instalação.

## Suporte a idiomas do Management Console

O Management Console é compatível com interfaces de usuário multi-idiomas (MUI) e oferece suporte para os seguintes idiomas:

Suporte a idiomas	
EN - Inglês	JA - Japonês
ES - Espanhol	KO - Coreano
FR - Francês	PT-BR - Português, Brasil
IT - Italiano	PT-PT - Português, Portugal (ibérico)
DE - Alemão	

# Configuração de pré-instalação

Antes de começar, leia os *conselhos técnicos do Security Management Server* para conhecer qualquer solução temporária ou problemas conhecidos relacionado ao Security Management Server.

A configuração de pré-instalação do(s) servidor(es) onde você deseja instalar o Security Management Server é muito importante. Preste atenção especial a esta seção para garantir uma instalação perfeita do Security Management Server.

## Configuração

### Acessar o console de gerenciamento

Como o Internet Explorer não é mais compatível, você deve instalar um navegador de terceiros para acessar corretamente o Management Console.

Se o Internet Explorer for necessário para validar o Management Console, você deverá desativar a configuração de segurança reforçada do Internet Explorer para o tipo de conta que corresponde ao administrador conectado.

### Configuração de porta e firewall

#### Comunicação entre cliente e servidor com o público (saída)

Os serviços e as portas abaixo são requeridos para que o servidor da Dell se comunique com os endpoints gerenciados. Essas portas e serviços devem ser capazes de realizar comunicações de saída. Caso os serviços de inspeção e proxy SSL estejam em uso, os URLs exigem exclusões.

- Validação inicial de direitos
  - URL de destino
    - cloud.dell.com
  - Porta
    - 443
  - Dispositivo de saída
    - Security Management Server ou Security Management Server Virtual na configuração de back-end
  - Serviço de origem
    - Dell Security Server
  - Porta de origem
    - 8443
- Comunicação de clients Advanced Threat Prevention
  - URLs de destino
    - América do Norte
      - login.cylance.com
      - protect.cylance.com
      - data.cylance.com
      - update.cylance.com
      - api.cylance.com
      - protect-api.cylance.com
      - download.cylance.com
    - América do Sul
      - 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
- Oriente Médio e Ásia
  - 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
- Japão, Austrália e Nova Zelândia
  - 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
- Porta
  - 443
- Dispositivo de saída
  - Todos os endpoints gerenciados
- Serviço de saída
  - CylanceSVC
- Porta de origem
  - 443

#### **Comunicação pública com o servidor de front-end (se necessário)**

Refere-se a informações que transitam da Internet para o servidor de front-end. A configuração de firewall ou roteamento deve ter portas definidas como entrada de uma conexão pública ou de Internet com um ou mais servidores de front-end ou balanceadores de carga.

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

#### **Comunicação de DMZ ou front-end com o servidor de back-end (se necessário)**

Os serviços e portas abaixo se comunicam de qualquer Security Management Server configurado no modo Front-End com o Security Management Server configurado no modo Back-End. A configuração de firewall ou roteamento deve ter portas definidas como entrada de um ou mais servidores de front-end ou balanceadores de carga para o servidor de back-end.

- Dell Policy Proxy de front-end e Dell Beacon Server para Dell Message Broker de back-end: STOMP/61613
- Dell Security Server Proxy de front-end para Dell Security Server de back-end: HTTPS/8443
- Dell Core Server Proxy de front-end para Dell Core Server de back-end: HTTPS/8888
- Dell Device Server de front-end para Dell Security Server de back-end: HTTPS/8443

#### **Servidor de back-end para rede interna**

Os serviços e portas abaixo são usados para comunicação interna com os respectivos serviços por clients no domínio ou conectados pela VPN. A Dell Technologies recomenda que vários desses serviços não sejam encaminhados fora da rede, ou que o serviço seja filtrado na

configuração do servidor de front-end por padrão. A configuração de firewall ou roteamento deve ter estas portas definidas como entrada da rede interna para o Security Management Server de back-end.

- Console de gerenciamento hospedado no Dell Security Server: HTTPS/8443
- Relatórios entregues por meio do Dell Compliance Reporter: HTTP(S)/8084
  - NOTA:** Esse serviço fica desabilitado por padrão. Em vez disso, use Relatórios gerenciados, que estão disponíveis no Management Console hospedado pelo Dell Security Server. Para obter informações sobre como ativar o Dell Compliance Reporter para relatórios de histórico, consulte o artigo da base de conhecimento [SLN314792](#).
- Dell Core Server: HTTPS/8888
- Dell Device Server: HTTP(S)/8081
  - NOTA:** Esse serviço preexistente só é necessário para clients Dell Encryption anteriores à versão 8.x. Esse serviço poderá ser desativado com segurança se todos os clients dentro do ambiente forem da versão 8.0 ou posterior.
- Key Server: TCP/8050
- Dell Policy Proxy: TCP/8000
- Dell Security Server: HTTPS/8443
- Autenticação baseada em certificado, hospedada pelo Dell Security Server: HTTPS/8449
  - NOTA:** Os clients do Dell Encryption instalados nos sistemas operacionais do Windows Server ou clients instalados no modo de servidor usam essa função. Para obter informações adicionais sobre a instalação de clients no modo de servidor, consulte o [Guia de instalação avançada do Encryption Enterprise](#).

### Comunicação de infraestrutura

- Active Directory utilizado para autenticação de usuário com o Dell Encryption TCP/389/636 (controlador de domínio local), TCP/3268/3269 (catálogo global), TCP/135/49125+ (RPC)
- Comunicação por e-mail (opcional): 25/587
- Microsoft SQL Server: 1433 (porta padrão)

### Criação e gerenciamento do banco de dados Microsoft SQL

Criar o banco de dados do servidor Dell:

Estas instruções são opcionais. Se um banco de dados não existir, o instalador o criará por padrão. Se você preferir configurar um banco de dados antes de instalar o Security Management Server, siga as instruções abaixo para criar o banco de dados e o usuário SQL no SQL Management Studio. Certifique-se de que as permissões apropriadas estejam definidas para bancos de dados SQL que não sejam criados automaticamente durante a instalação do Security Management Server. Para ver uma lista de permissões necessárias, consulte os [Requisitos de software](#).

Ao pré-criar o banco de dados, siga as instruções em [Instalar um servidor de back-end com um banco de dados existente](#).

O Security Management Server está configurado para autenticação SQL e do Windows.

- NOTA:** O agrupamento não-padrão esperado compatível com seu banco de dados SQL ou instância SQL é o agrupamento "SQL\_Latin1\_General\_CP1\_CI\_AS". O agrupamento não pode diferenciar maiúsculas de minúsculas, mas precisa diferenciar acentos.

### Pré-requisitos de instalação

Os pré-requisitos são instalados por padrão durante a instalação do Security Management Server nos sistemas operacionais Windows Server. Os pré-requisitos abaixo podem ser instalados opcionalmente antes da instalação do Security Management Server para ignorar os requisitos de reinicialização.

#### Instalar os pacotes redistribuíveis Visual C++

Se ainda não estiverem instalados, instale os pacotes redistribuíveis Visual C++ 2010, 2013 e 2015 (ou posteriores). Se desejar, você pode permitir que o instalador do Security Management Server instale esses componentes.

- NOTA:** A instalação dos pacotes redistribuíveis Microsoft Visual C++ pode requerer uma reinicialização.

Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019- <https://support.microsoft.com/en-US/help/2977003/the-latest-supported-visual-c-downloads>

#### Instalar o .NET Framework 4.5

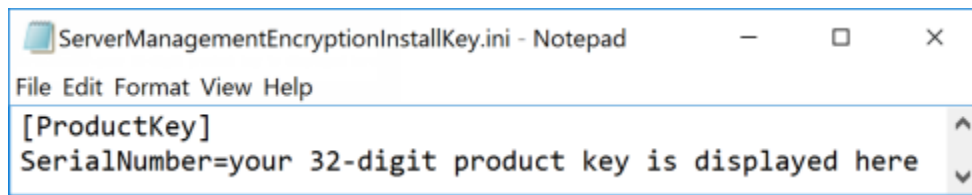
O .NET Framework 4.5 é pré-instalado no Windows Server 2012 R2 e posterior como um recurso do Server Manager.

#### Instalar o SQL Native Client 2012

Se estiver usando SQL Server 2012 ou o SQL Server 2016, instale o SQL Native Client 2012. Se desejar, você pode permitir que o instalador do Security Management Server instale esse componente. <http://www.microsoft.com/en-us/download/details.aspx?id=35580>

#### Importar a licença de instalação do servidor

**Para uma nova instalação** – copie a Chave do produto (o nome do arquivo é *EnterpriseServerInstallKey.ini*) para C:\Windows para preencher automaticamente a Chave de produto de 32 caracteres no instalador do Security Management Server.



**NOTA:** O EnterpriseServerInstallKey.ini está presente no pacote de download do Security Management Server, disponível [aqui](#).

A configuração da pré-instalação do servidor está completa. Continue para [Instalar](#) ou [Atualizar/migrar](#).

# Instalar ou fazer upgrade/migrar

O capítulo fornece instruções sobre o seguinte:

- [Nova instalação](#) - Instalar um novo Security Management Server.
- [Atualização/migração](#) - Fazer upgrade de um Enterprise Server v9.2 ou posterior existente e funcional.
- [Desinstalar o Security Management Server](#) - Para remover a instalação atual, caso seja necessário.

Se sua instalação precisar conter mais de um servidor principal (back-end), entre em contato com seu representante Dell ProSupport.

## Antes de iniciar a instalação ou Atualizar/Migrar

Antes de começar, certifique-se de que as etapas aplicáveis da [Configuração de pré-instalação](#) foram concluídas.

Leia os *relatórios técnicos do Security Management Server* para conhecer qualquer solução atual ou problema conhecido relacionado à instalação do Security Management Server.

O antivírus e o antimalware devem ser desativados durante a instalação ou atualização do Security Management Server para evitar que os instaladores do tempo de execução do Microsoft C++, atividades Java (criação e manipulação de certificados) e criação e modificação de PostgreSQL sejam afetados. Todos esses itens são acionados por executáveis ou scripts.

Como solução alternativa, exclua:

- [CAMINHO DA INSTALAÇÃO]:\Dell\Enterprise Edition
- C:\Windows\Installer
- O caminho do arquivo a partir do qual o instalador é executado

A Dell recomenda que as boas práticas de bancos de dados sejam usadas para o banco de dados do servidor da Dell e que o software seja incluído no plano de recuperação de desastres da sua organização.

Se você pretende implementar componentes da Dell no DMZ, verifique se eles estão devidamente protegidos contra ataques.

Para produção, a Dell recomenda a instalação do SQL Server em um servidor dedicado.

É recomendável instalar o servidor de back-end antes de instalar e configurar um servidor de front-end.

Os arquivos de log da instalação estão localizado neste diretório: C:\Users\

## Nova instalação

Escolha uma das duas opções para a instalação do servidor de back-end:

- [Instalar um servidor de back-end e um novo banco de dados](#) - Para instalar um novo Security Management Server e um novo banco de dados.
- [Instalar um servidor de back-end com banco de dados existente](#) - Para instalar um novo Security Management Server e se conectar a um banco de dados SQL criado durante a [Configuração de pré-instalação](#) ou a um banco de dados SQL existente com a versão 9.x ou mais recente, quando a versão do esquema corresponde à versão do Security Management Server a ser instalada. Um banco de dados v9.2 ou posterior precisa ser migrado para o esquema mais recente com a última versão da Server Configuration Tool. Para obter instruções sobre a migração do banco de dados com a Server Configuration Tool, consulte [Migrar o banco de dados](#). Para obter a Server Configuration Tool mais recente ou para migrar um banco de dados de versão anterior para a versão 9.2, entre em contato com a Dell ProSupport para obter assistência.

### NOTA:

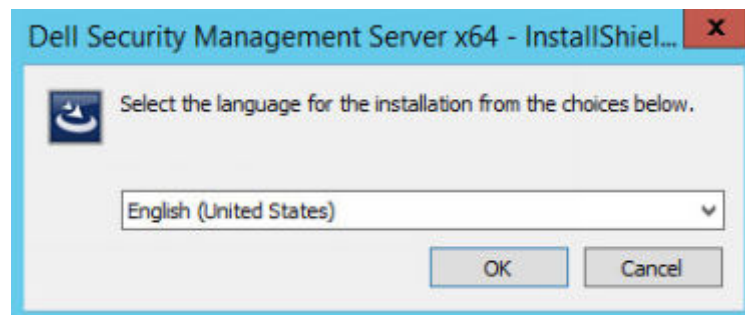
Se você tiver um Enterprise Server v9.2 ou posterior funcional, consulte as instruções em [Atualizar/Migrar o\(s\) servidor\(es\) de back-end](#).

Se você instalar um servidor de front-end, execute essa instalação após a instalação do servidor de back-end:

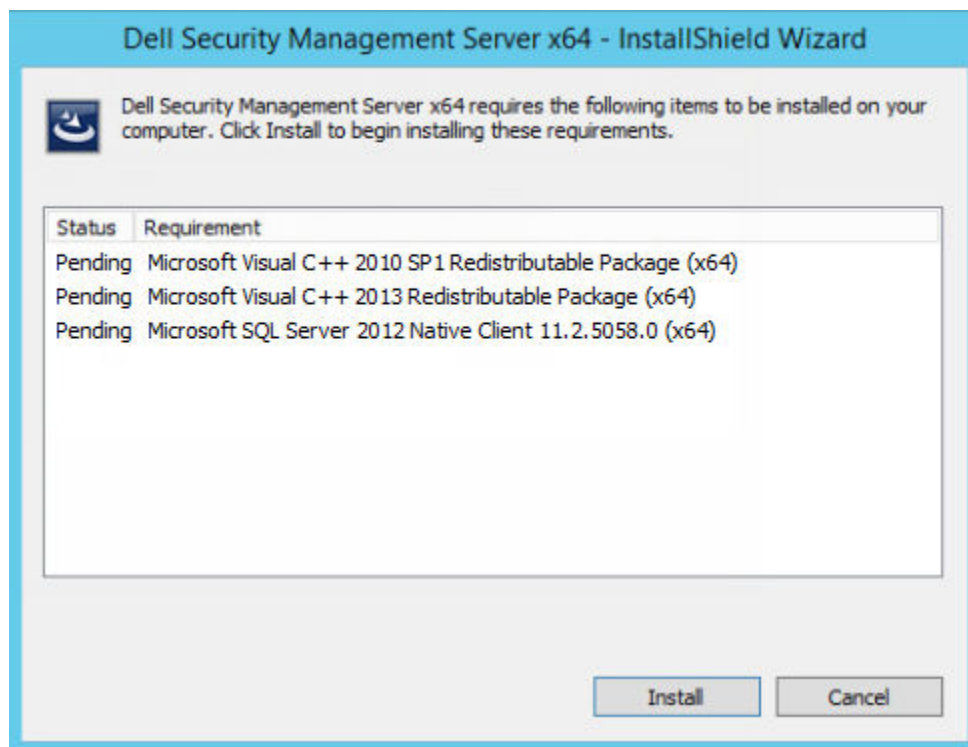
- [Instalar um servidor de front-end](#) - Instalar um servidor de front-end para se comunicar com um servidor de back-end.

## Instalar um servidor de back-end e um novo banco de dados

1. Na mídia de instalação Dell, navegue até o diretório do Security Management Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Security Management Server-x64 no diretório raiz do servidor onde você está instalando o Security Management Server. **Copiar/colar ou arrastar/soltar produz erros e causa uma instalação malsucedida.**
2. Clique duas vezes em **setup.exe**.
3. Selecione o idioma para a instalação e clique em **OK**.



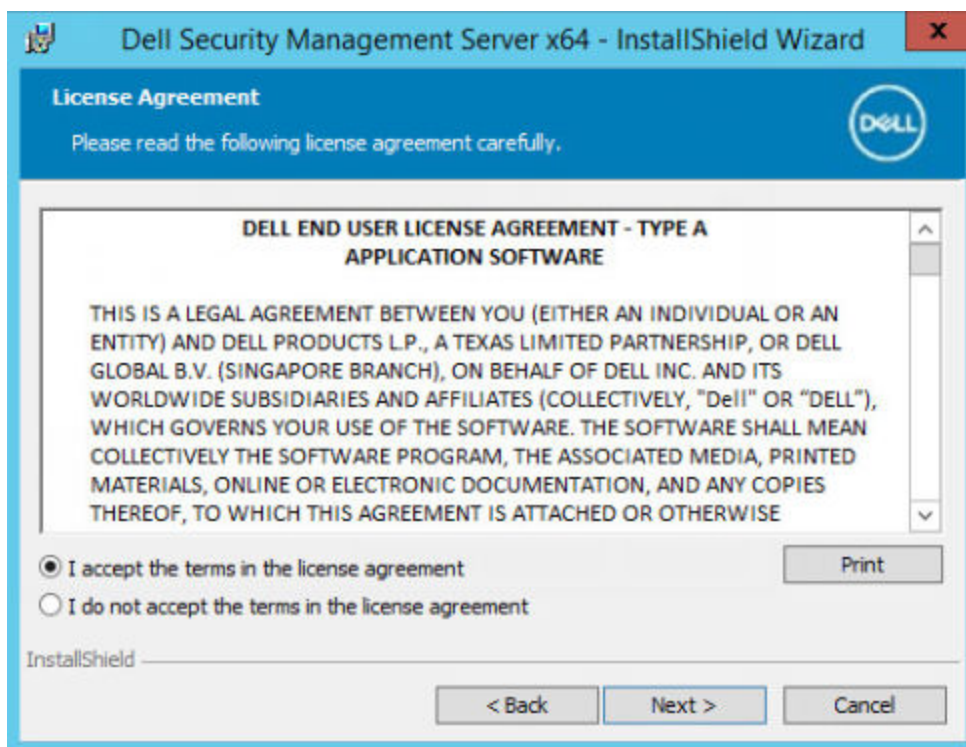
4. Se os pré-requisitos ainda não estiverem instalados, será mostrada uma mensagem informando quais pré-requisitos serão instalados. Clique em **Instalar**.



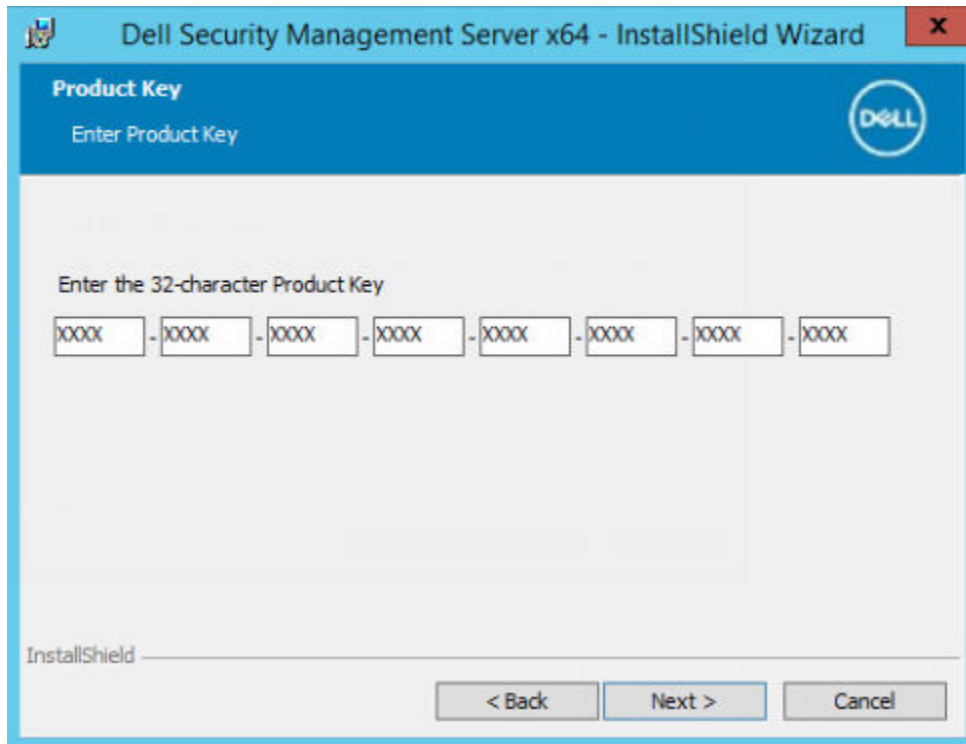
5. Na caixa de diálogo *Bem-vindo*, clique em **Avançar**.



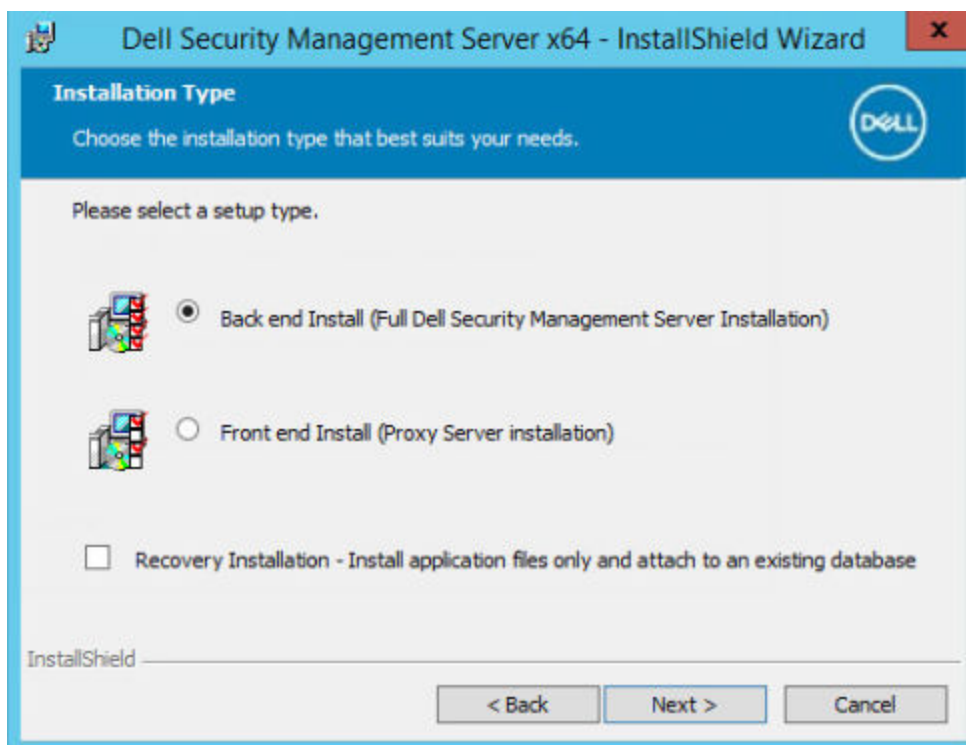
6. Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.



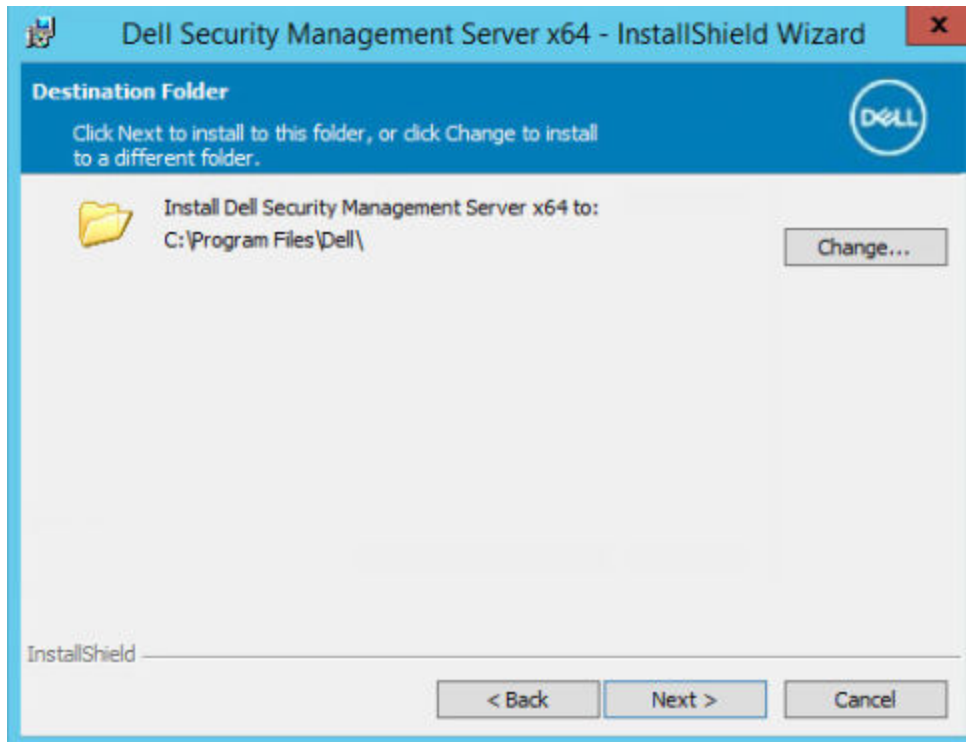
7. Se você, opcionalmente, copiou o arquivo EnterpriseServerInstallKey system.ini para C:\Windows conforme explicado em [Configuração de pré-instalação](#), clique em **Avançar**. Caso contrário, digite a Chave do Produto de 32 caracteres e clique em **Avançar**. A Chave do Produto está localizada no arquivo EnterpriseServerInstallKey.ini.



8. Selecione **Instalação do back-end** e clique em **Avançar**.

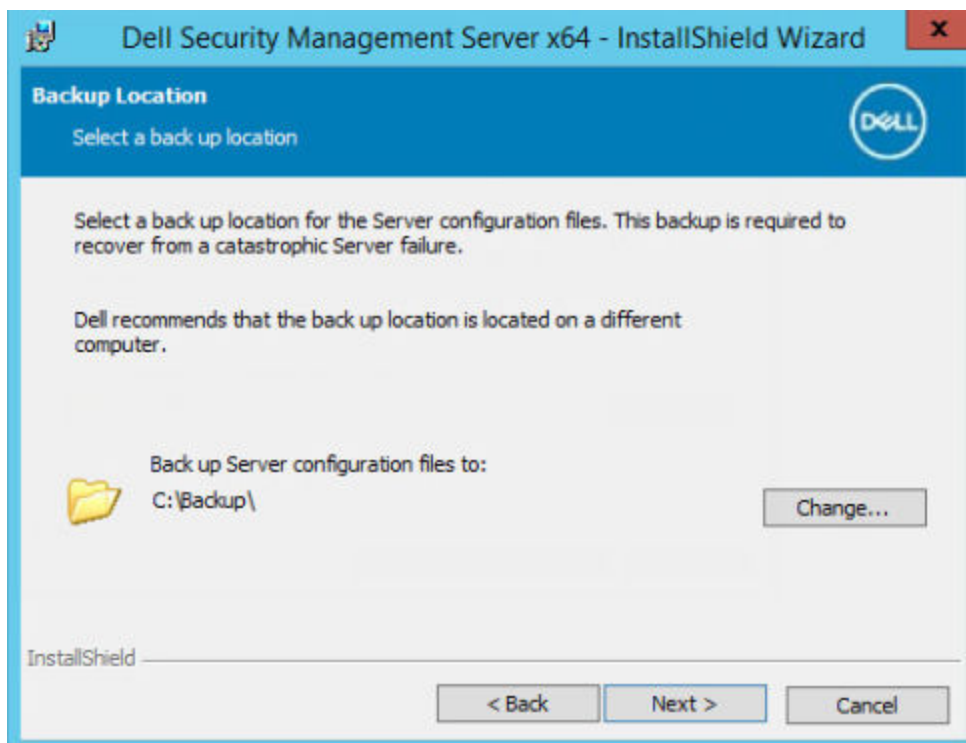


9. Para instalar o Security Management Server no local padrão C:\Program Files\Dell, clique em **Avançar**. Caso contrário, clique em **Alterar** para selecionar outro local e clique em **Avançar**.



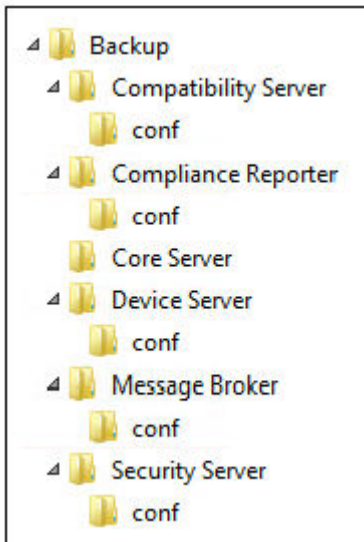
10. Para selecionar um local de armazenamento do backup dos arquivos de configuração, clique em **Alterar**, navegue até a pasta desejada e clique em **Avançar**.

**A Dell recomenda que você selecione um local de rede remoto ou uma unidade externa para o backup.**



Após a instalação, quaisquer alterações aos arquivos de configuração, inclusive alterações feitas com a Server Configuration Tool, precisarão ser manualmente copiadas para essas pastas. Os arquivos de configuração são uma parte importante do total de informações usadas para restaurar manualmente o servidor da Dell, se necessário.

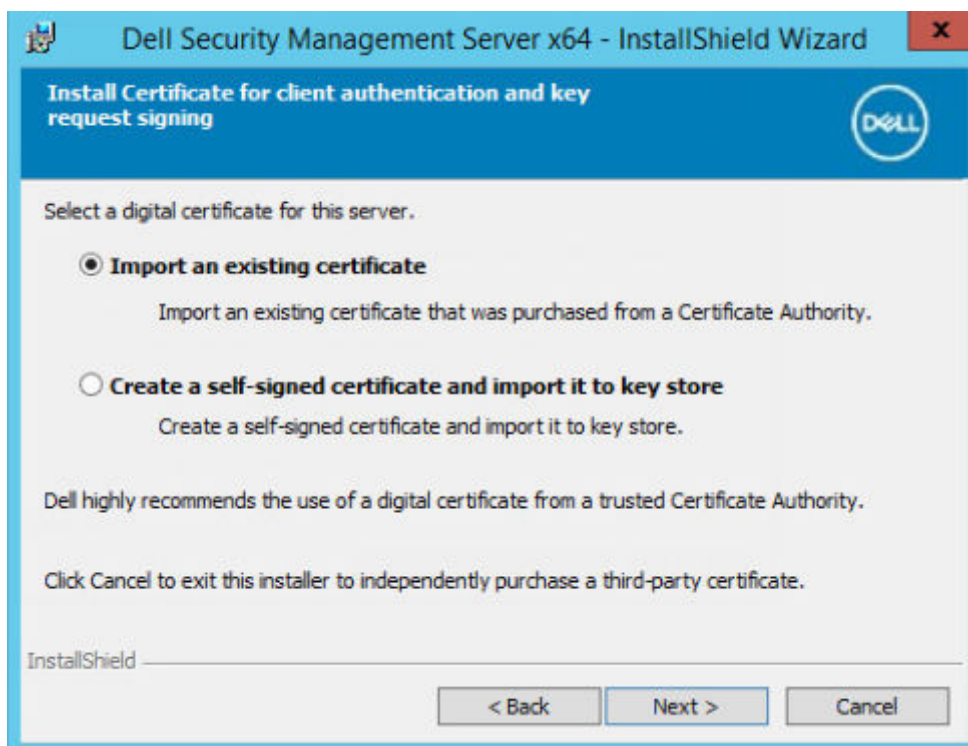
**NOTA:** A estrutura de pastas criada pelo instalador durante esta etapa de instalação (exemplo mostrado abaixo) precisa permanecer inalterada.



11. Você pode escolher entre alguns tipos de certificados digitais para usar. **É extremamente recomendado o uso de um certificado digital de uma autoridade de certificação confiável.**

Selecione a opção “a” ou “b” abaixo:

- a. Para usar um certificado existente que foi comprado de uma autoridade de certificação, selecione **Importar um certificado existente** e clique em **Avançar**.



Clique em **Procurar** para digitar o caminho do certificado.

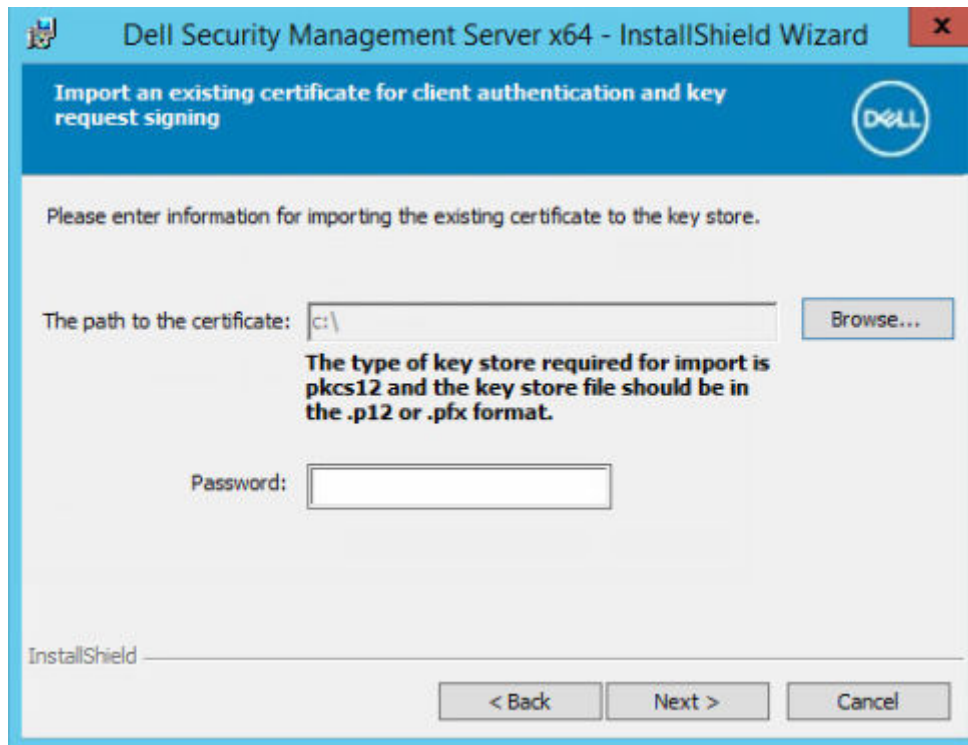
Digite a senha associada a esse certificado. O arquivo de armazenamento de chaves deve ser .p12 ou pfx. Consulte [Exportar um certificado para .PFX usando o console de gerenciamento de certificados](#) para obter instruções.

Clique em **Avançar**.

**NOTA:**

Para usar essa configuração, o certificado CA exportado que está sendo importado precisa ter a cadeia de confiança completa. Se não tiver certeza, exporte novamente o certificado CA e verifique se as seguintes opções estão selecionadas no “Assistente para exportação de certificados”:

- Troca de informações pessoais - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades estendidas



OU

- b. Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para o armazenamento de chaves** e clique em **Avançar**.

Na caixa de diálogo *Criar certificado autoassinado*, digite as informações a seguir:

Nome do computador totalmente qualificado (exemplo: nomedocomputador.domínio.com)

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Estado (nome completo)

País: abreviação com duas letras

Clique em **Avançar**.

**NOTA:** Por padrão, o certificado expira em um 10 anos.

12. Para o Server Encryption, você pode escolher dentre alguns tipos de certificados digitais para usar. É extremamente recomendado o uso de um certificado digital de uma autoridade de certificação confiável.

Selecione a opção “a” ou “b” abaixo:

- a. Para usar um certificado existente que foi comprado de uma autoridade de certificação, selecione **Importar um certificado existente** e clique em **Avançar**.

Clique em **Procurar** para digitar o caminho do certificado.

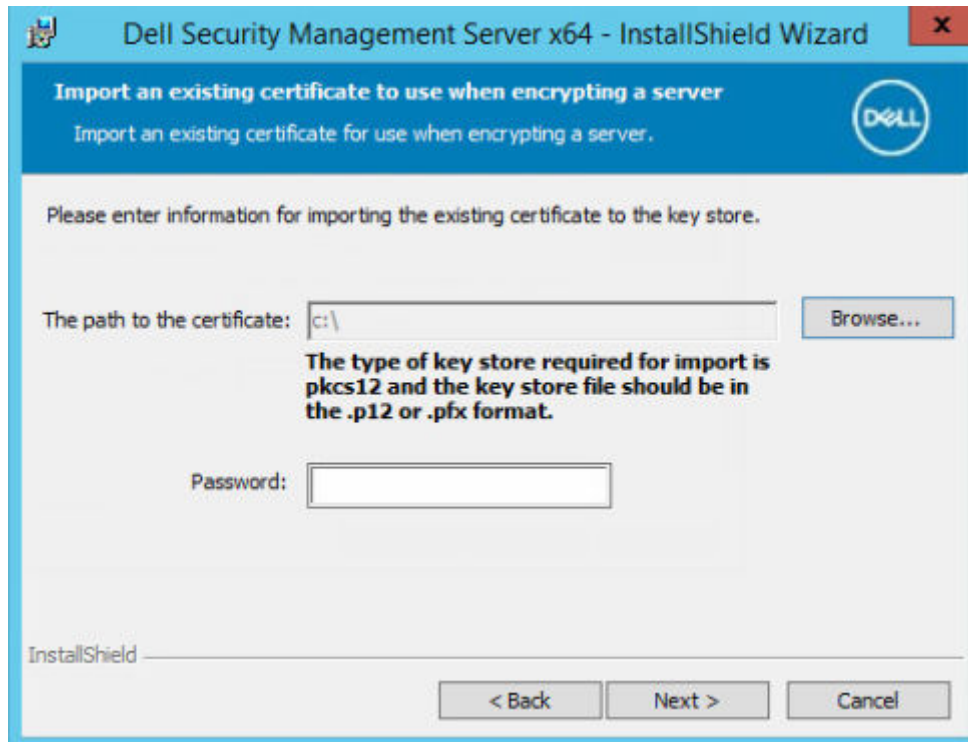
Digite a senha associada a esse certificado. O arquivo de armazenamento de chaves deve ser .p12 ou pfx. Consulte [Exportar um certificado para .PFX usando o console de gerenciamento de certificados](#) para obter instruções.

Clique em **Avançar**.

**NOTA:**

Para usar essa configuração, o certificado CA exportado que está sendo importado precisa ter a cadeia de confiança completa. Se não tiver certeza, exporte novamente o certificado CA e verifique se as seguintes opções estão selecionadas no “Assistente para exportação de certificados”:

- Troca de informações pessoais - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades estendidas



OU

- b. Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para o armazenamento de chaves e clique em Avançar**.

Na caixa de diálogo *Criar certificado autoassinado*, digite as informações a seguir:

Nome do computador totalmente qualificado (exemplo: nomedocomputador.domínio.com)

Organização

Unidade organizacional (exemplo: Segurança)

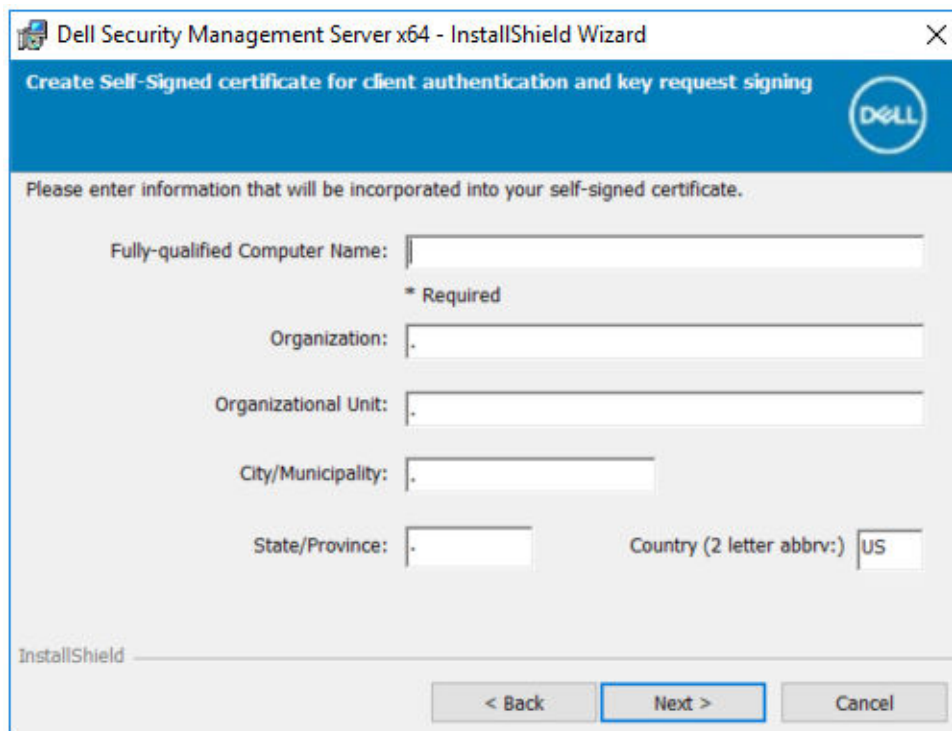
Cidade

Estado (nome completo)

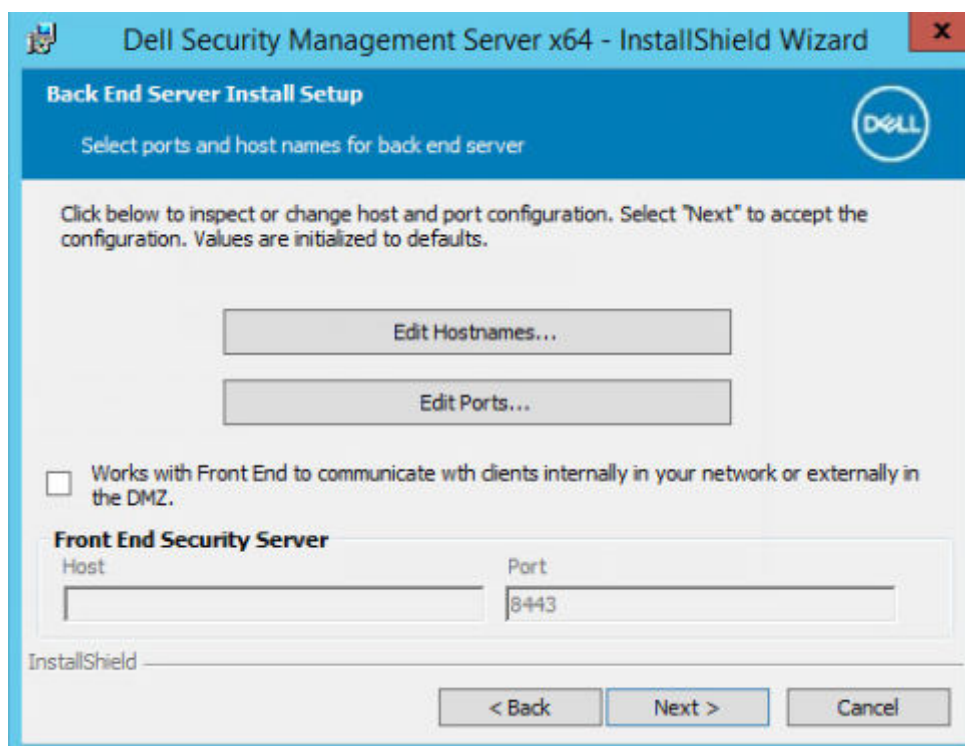
País: abreviação com duas letras

Clique em **Avançar**.

**NOTA:** Por padrão, o certificado expira em um 10 anos.



13. Na caixa de diálogo *Configuração de instalação do servidor de back-end*, você pode ver ou editar os nomes de host e as portas.
- Para aceitar os nomes de host e as portas padrão, na caixa de diálogo *Configuração de instalação do servidor de back-end*, clique em **Avançar**.
  - Se você estiver usando um servidor de front-end, selecione **Trabalha com o front-end para se comunicar com clientes internamente em sua rede ou externamente no DMZ** e digite o nome de host do Front End Security Server (por exemplo, server.domain.com).



- Para ver ou editar os nomes de host, clique em **Editar nomes de host**. Edite os nomes de host apenas se necessário. A Dell recomenda usar as configurações padrão.

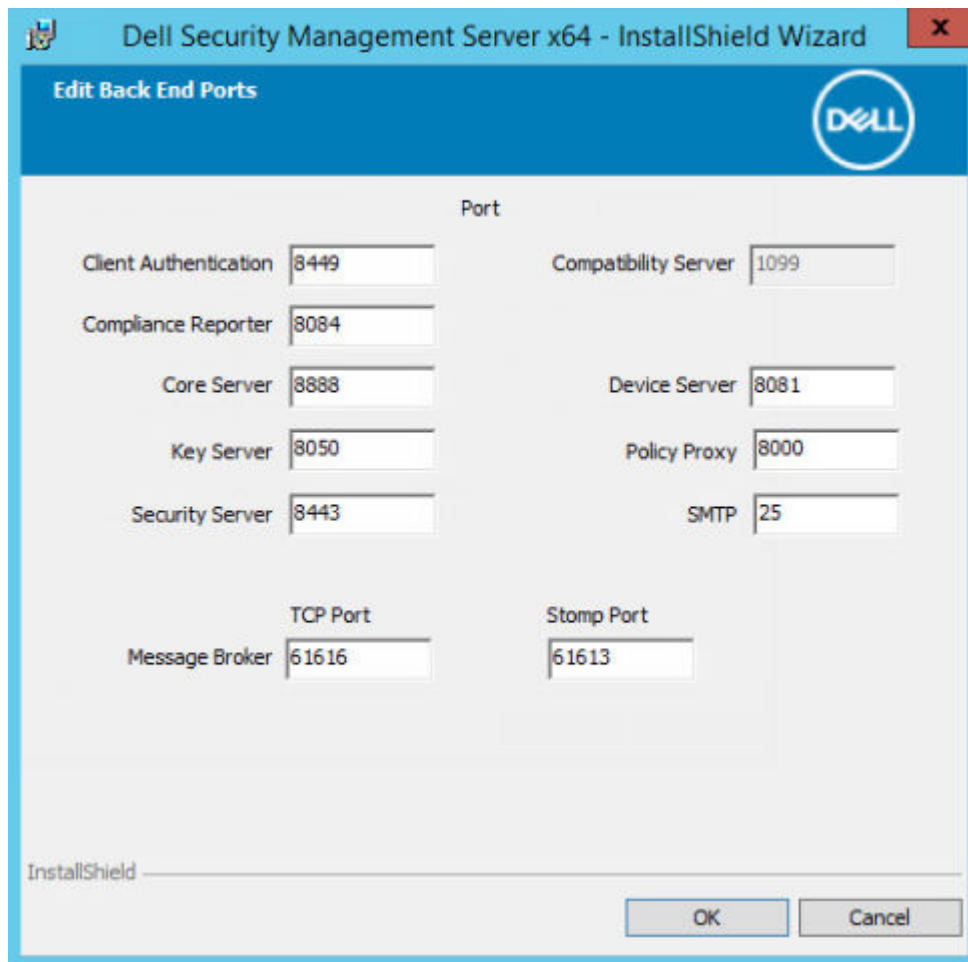
**NOTA:** Um nome de host não pode conter um caractere sublinhado ("\_").

Quando concluído, clique em **OK**.

The screenshot shows a Windows-style dialog box titled "Dell Security Management Server x64 - InstallShield Wizard" with a red close button in the top right corner. Below the title bar is a blue header with the text "Edit Back End Hostnames" and the Dell logo. The main area of the dialog is light gray and contains a list of server roles, each with a corresponding text input field. The roles and their values are: Core Server (server.domain.com), Compatibility Server (server.domain.com), Compliance Reporter (server.domain.com), Device Server (server.domain.com), Key Server (server.domain.com), Security Server (server.domain.com), Policy Proxy (Not applicable), SMTP (server.domain.com), and Message Broker (server.domain.com). At the bottom left, the text "InstallShield" is visible. At the bottom right, there are two buttons: "OK" and "Cancel".

Role	Hostname
Core Server	server.domain.com
Compatibility Server	server.domain.com
Compliance Reporter	server.domain.com
Device Server	server.domain.com
Key Server	server.domain.com
Security Server	server.domain.com
Policy Proxy	(Not applicable)
SMTP	server.domain.com
Message Broker	server.domain.com

- Para ver ou editar as portas, clique em **Editar portas**. Edite as portas apenas se necessário. A Dell recomenda usar as configurações padrão. Quando concluído, clique em **OK**.

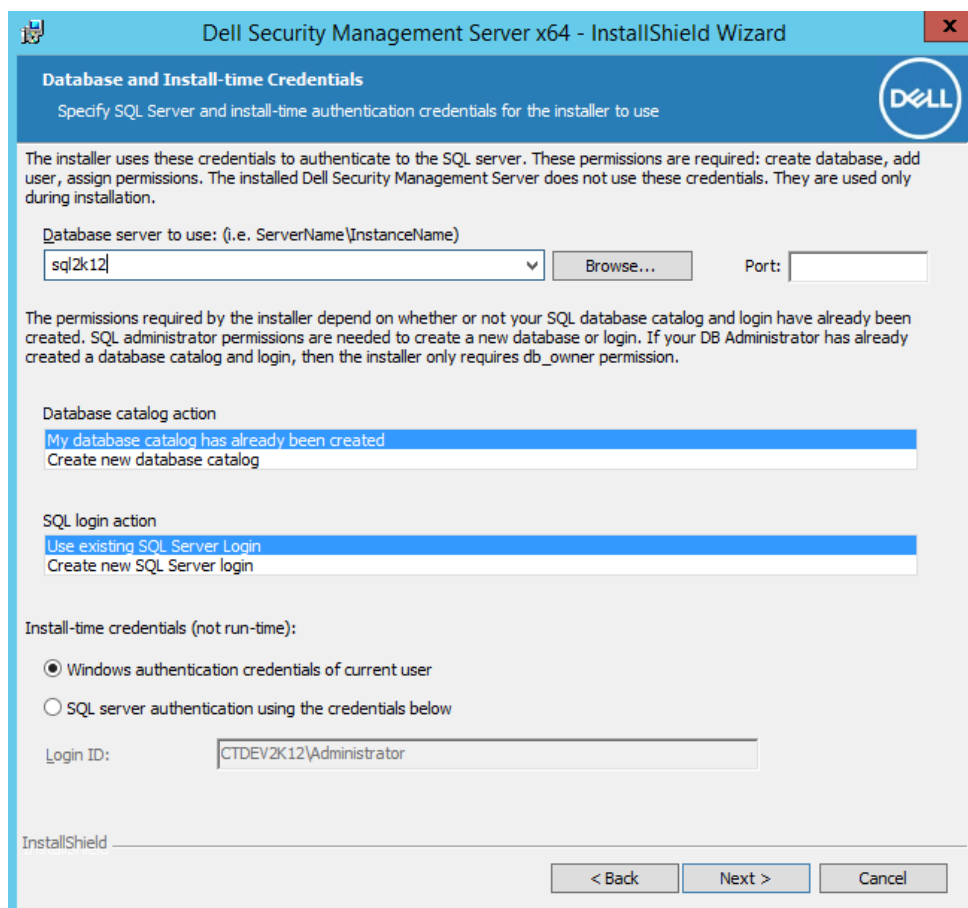


14. Para criar um novo banco de dados, siga estas instruções:

- Clique em **Procurar** para selecionar o servidor no qual será instalado o banco de dados.
- Selecione o método de autenticação a ser usado pelo instalador para configurar o banco de dados do Dell Server. Após a instalação, o produto instalado não usa as credenciais aqui especificadas.

- **Credenciais de autenticação do Windows do usuário atual**

Se você escolher Autenticação do Windows, as mesmas credenciais usadas para fazer login no Windows são usadas para autenticação (os campos *Nome de usuário* e *Senha* não podem ser editados). Confirme que a conta tenha direitos de administrador de sistema e a capacidade de gerenciar o SQL Server.



OU

- **Autenticação do SQL Server usando as credenciais abaixo**

Se você usar a autenticação SQL, a conta SQL usada precisa ter direitos de administrador do sistema no SQL Server.

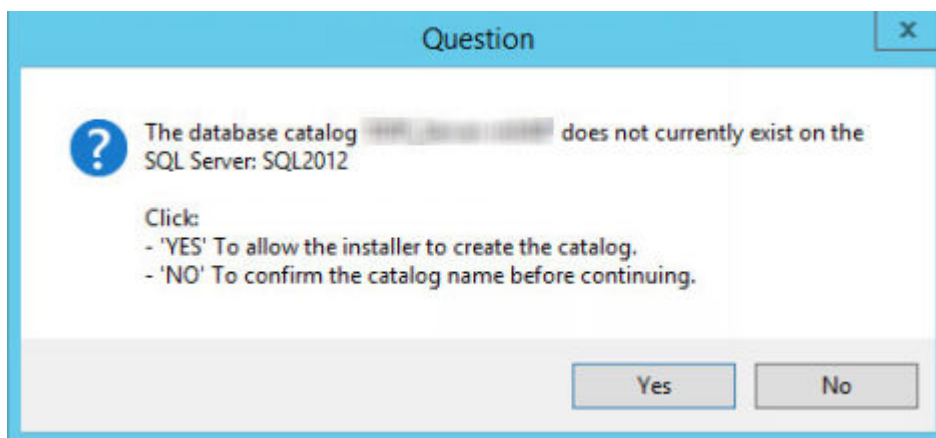
O instalador precisa ser autenticado para o SQL Server com estas permissões: criar banco de dados, adicionar usuário, atribuir permissões.

c. Identifique o catálogo de banco de dados:

Digite o nome para o novo catálogo de banco de dados. Na próxima caixa de diálogo, o sistema solicitará que você crie o novo catálogo.

d. Clique em **Avançar**.

e. Para confirmar que você quer que o instalador crie um banco de dados, clique em **Sim**. Para retornar à tela anterior para fazer alterações, clique em **Não**.



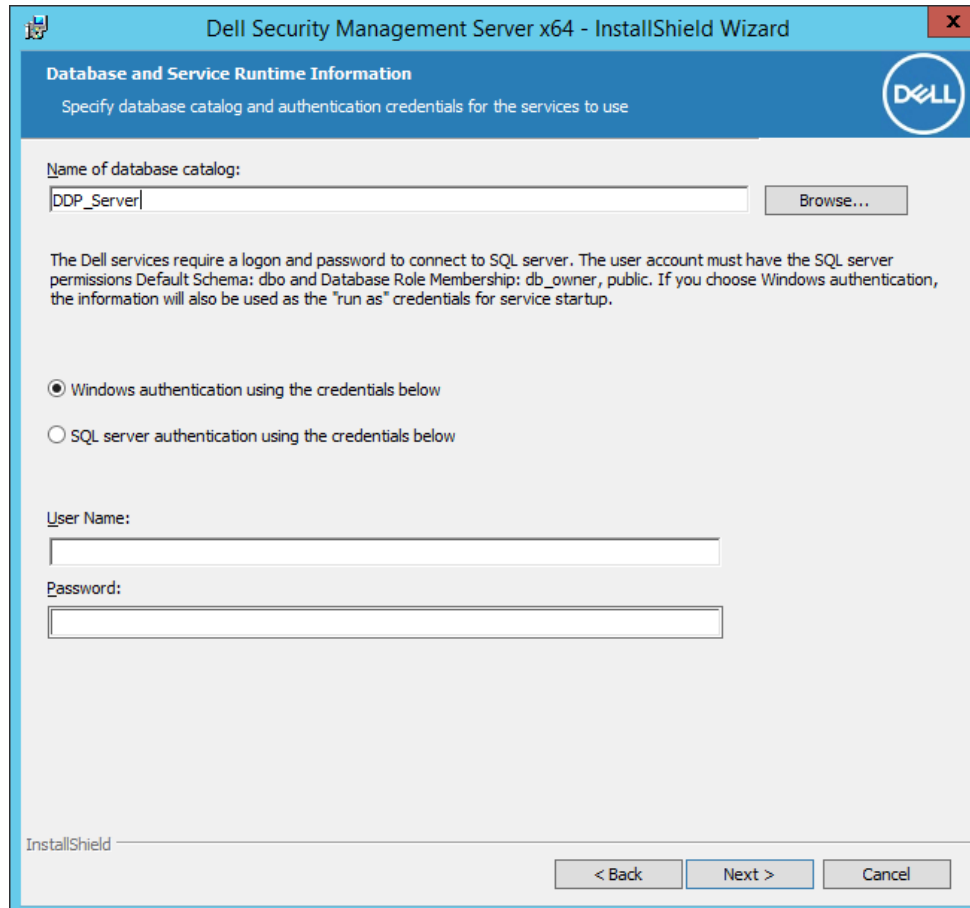
15. Selecione o método de autenticação a ser usado pelo produto. Esta etapa conecta uma conta ao produto.

- **Autenticação do Windows**

Selecione **Autenticação do Windows usando as credenciais abaixo**, insira as credenciais que o produto deve usar e clique em **Avançar**.

Confirme que a conta tenha direitos de administrador de sistema e a capacidade de gerenciar o SQL Server. A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Associação à função de banco de dados: dbo\_owner, público.

Essas credenciais são usadas, também, pelos serviços Dell, para operar com o Security Management Server.

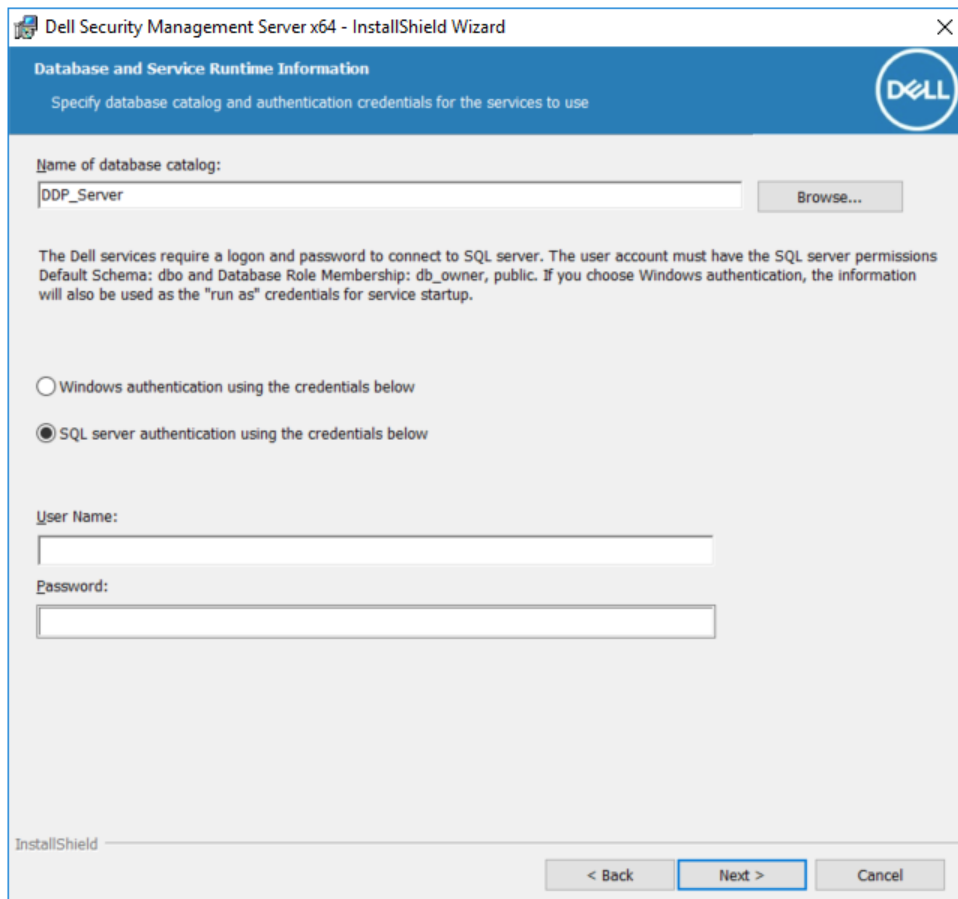


OU

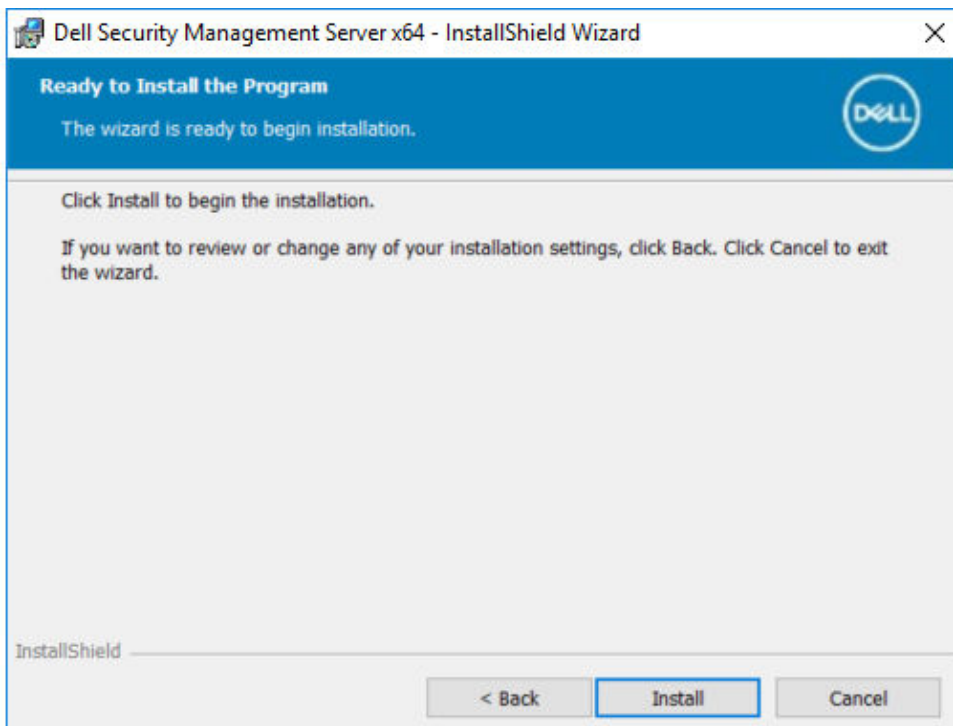
- **Autenticação do SQL Server**

Selecione **Autenticação do SQL Server usando as credenciais abaixo**, digite as credenciais do SQL Server que os serviços Dell usarão para funcionar com o Security Management Server e clique em **Avançar**.

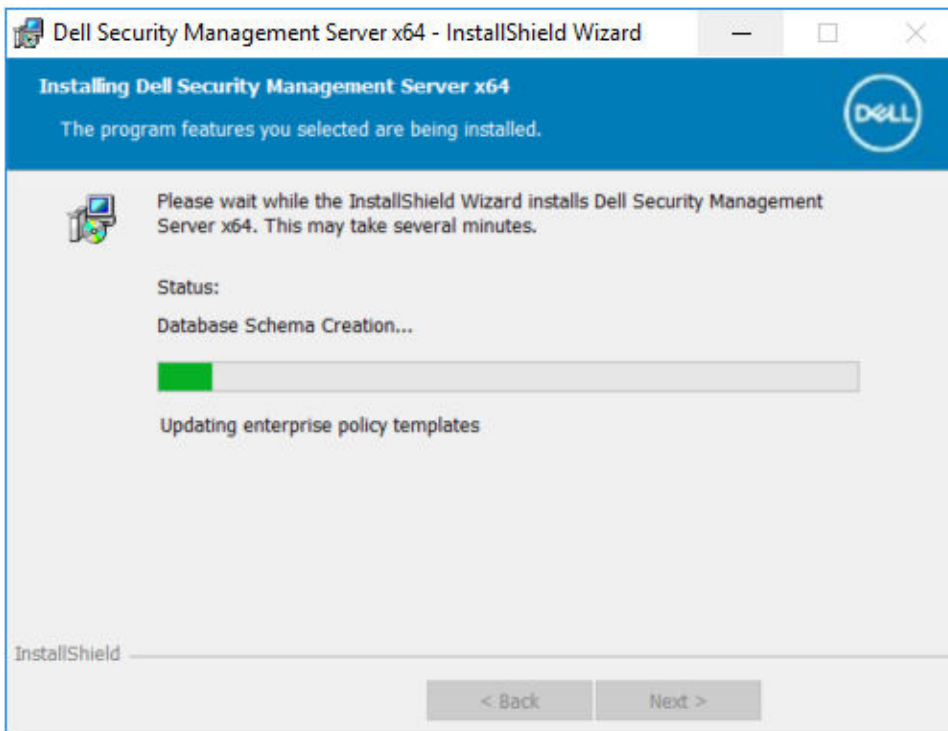
A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Associação à função de banco de dados: dbo\_owner, público.



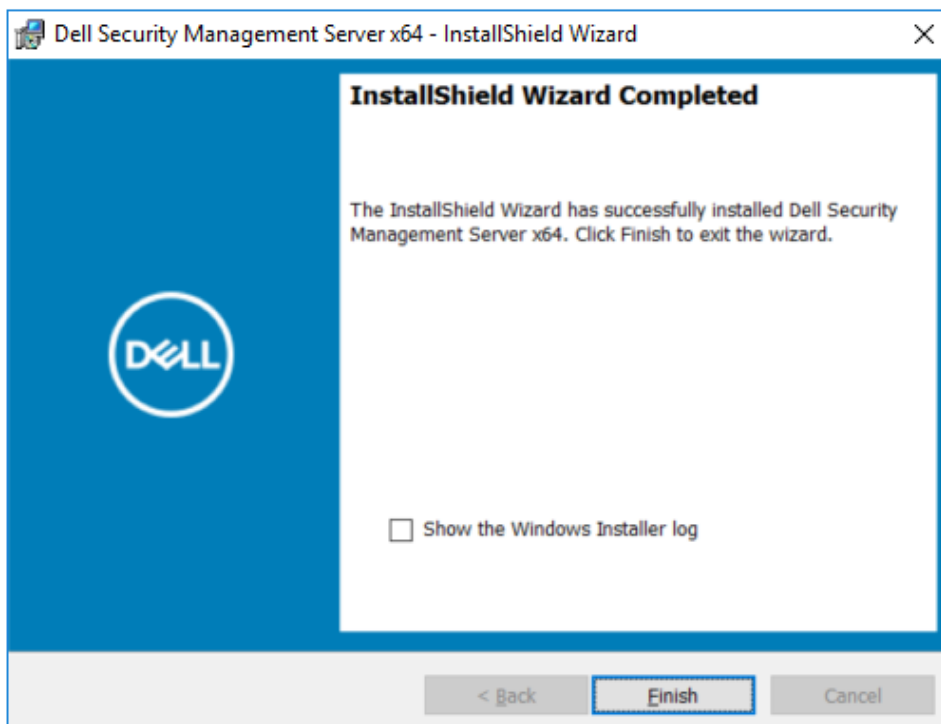
16. Na caixa de diálogo *Pronto para instalar o programa*, clique em **Instalar**.



Uma caixa de diálogo do progresso mostra o status de todo o processo de instalação.



17. Ao terminar a instalação, clique em **Concluir**.



As tarefas de instalação do servidor de back-end estão concluídas.

Os Serviços Dell são reiniciados ao final da instalação. Não é necessário reinicializar o Dell Server.

## Instalar um servidor de back-end com um banco de dados existente

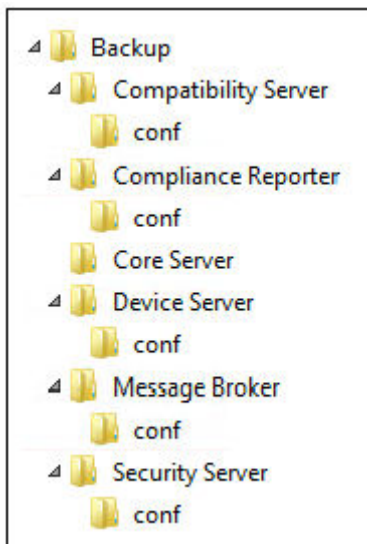
### NOTA:

Se você tiver um Dell Server v9.2 ou posterior funcional, consulte as instruções em [Atualizar/Migrar o\(s\) servidor\(es\) de back-end](#).

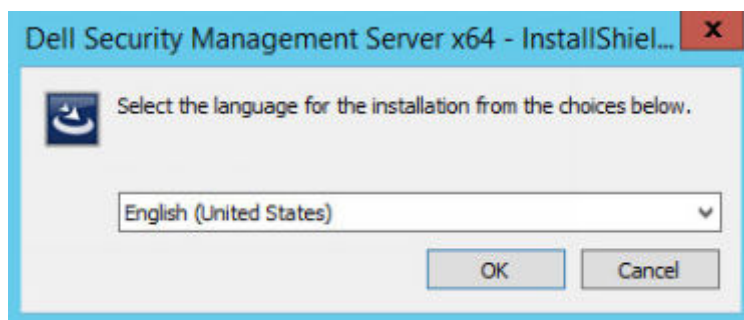
Você pode instalar um novo Security Management Server e se conectar a um banco de dados SQL criado durante a [Configuração de pré-instalação](#) ou a um banco de dados SQL existente com a versão 9.x ou mais recente, quando a versão do esquema corresponde à versão do Security Management Server a ser instalada.

A conta do usuário a partir da qual a instalação é executada precisa ter privilégios de proprietário do banco de dados para o banco de dados SQL. Se você não tiver certeza sobre os privilégios de acesso ou conectividade ao banco de dados, peça a seu administrador de banco de dados que confirme isso antes de você começar a instalação.

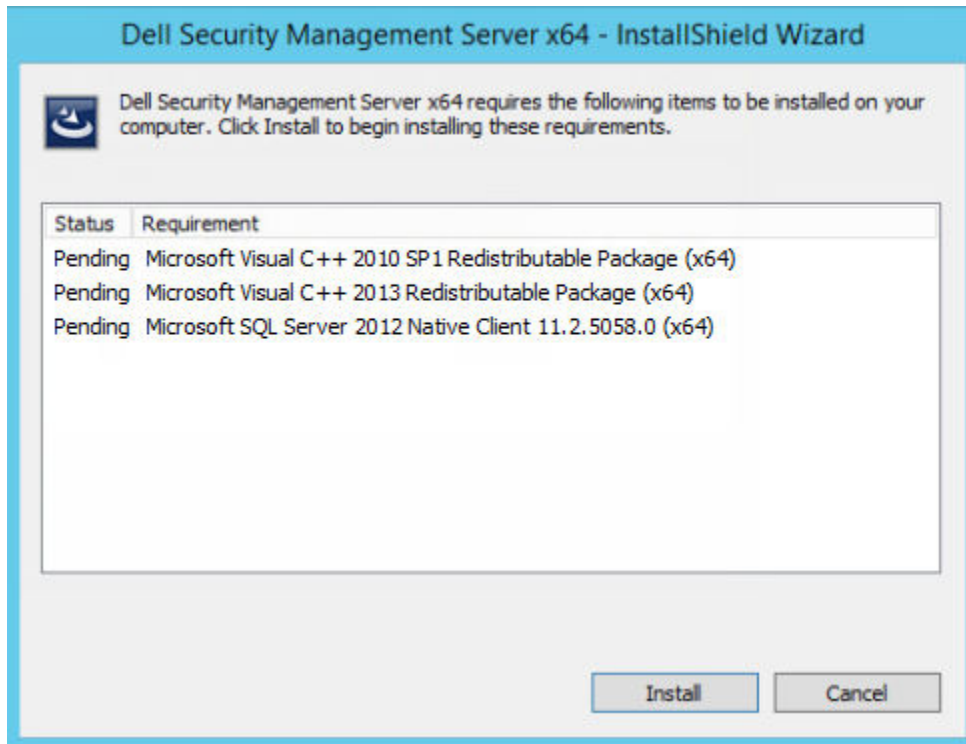
Se o banco de dados existente tiver sido anteriormente instalado com o Security Management Server, antes de iniciar a instalação, verifique se há um backup do banco de dados, dos arquivos de configuração e do secretKeyStore que possa ser acessada a partir do servidor no qual você está instalando o Security Management Server. O acesso a esses arquivos é necessário para configurar o Security Management Server e o banco de dados existente. A estrutura de pastas criada pelo instalador durante a instalação (exemplo mostrado abaixo) precisa permanecer inalterada.



1. Na mídia de instalação Dell, navegue até o diretório do Security Management Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Security Management Server-x64 no diretório raiz do servidor onde você está instalando o Security Management Server. **Copiar/colar ou arrastar/soltar produz erros e causa uma instalação malsucedida.**
2. Clique duas vezes em **setup.exe**.
3. Selecione o idioma para a instalação e clique em **OK**.



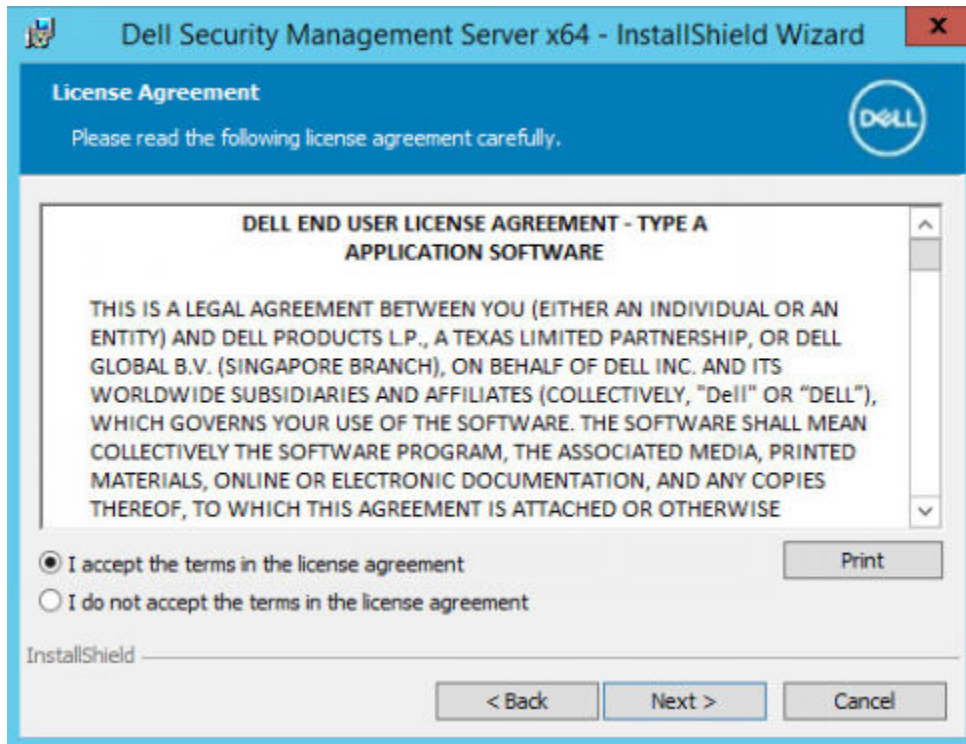
4. Se os pré-requisitos ainda não estiverem instalados, será mostrada uma mensagem informando quais pré-requisitos serão instalados. Clique em **Instalar**.



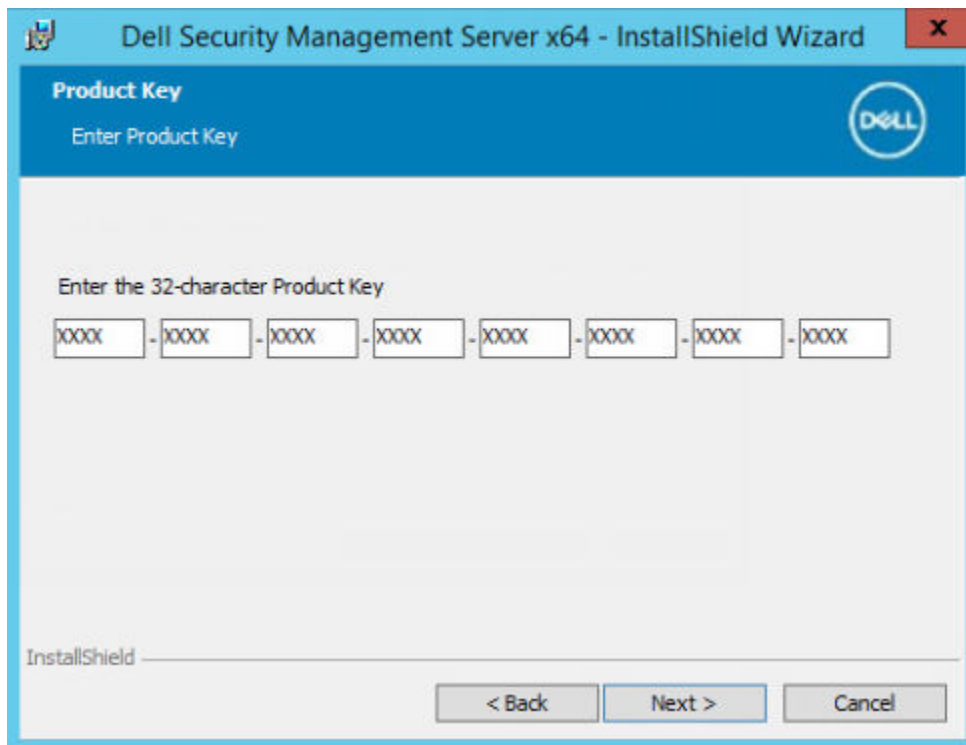
5. Na caixa de diálogo *Bem-vindo*, clique em **Avançar**.



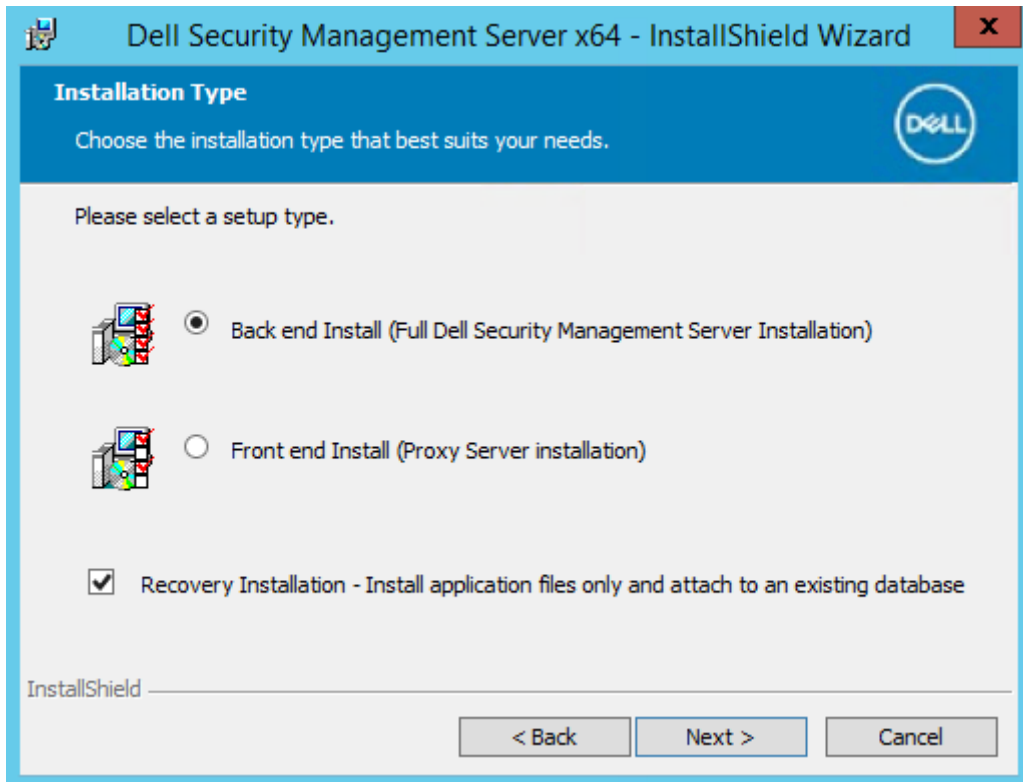
6. Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.



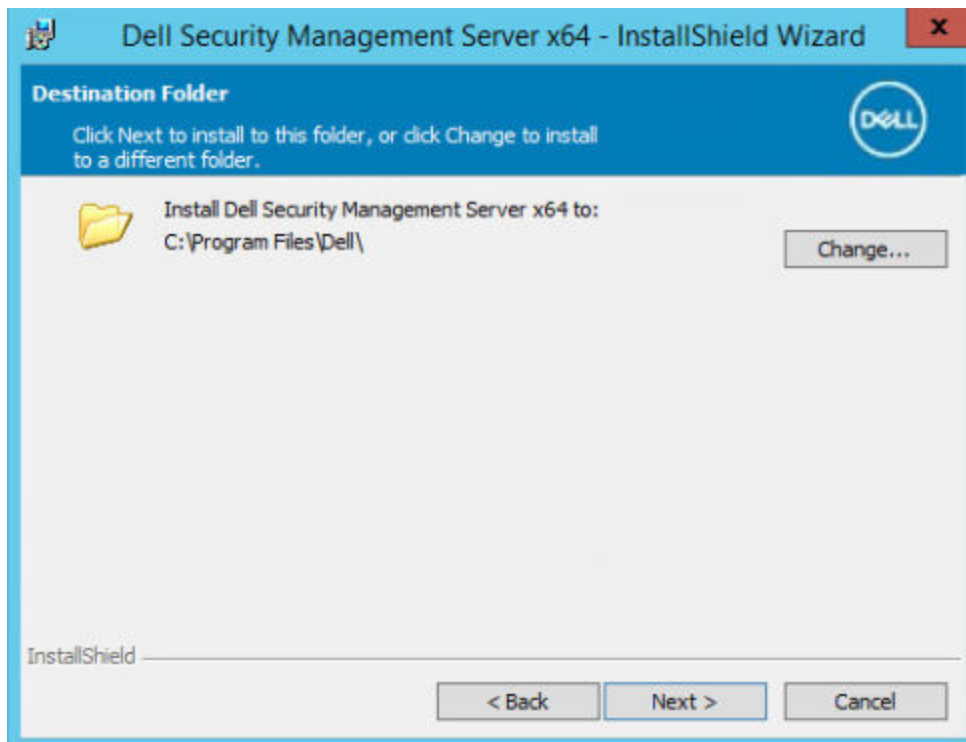
7. Se você, opcionalmente, copiou o arquivo EnterpriseServerInstallKey system.ini para C:\Windows conforme explicado em [Configuração de pré-instalação](#), clique em **Avançar**. Caso contrário, digite a Chave do Produto de 32 caracteres e clique em **Avançar**. A Chave do Produto está localizada no arquivo EnterpriseServerInstallKey.ini.



8. Selecione **Instalação do back-end** e **Instalação de recuperação** e clique em **Avançar**.

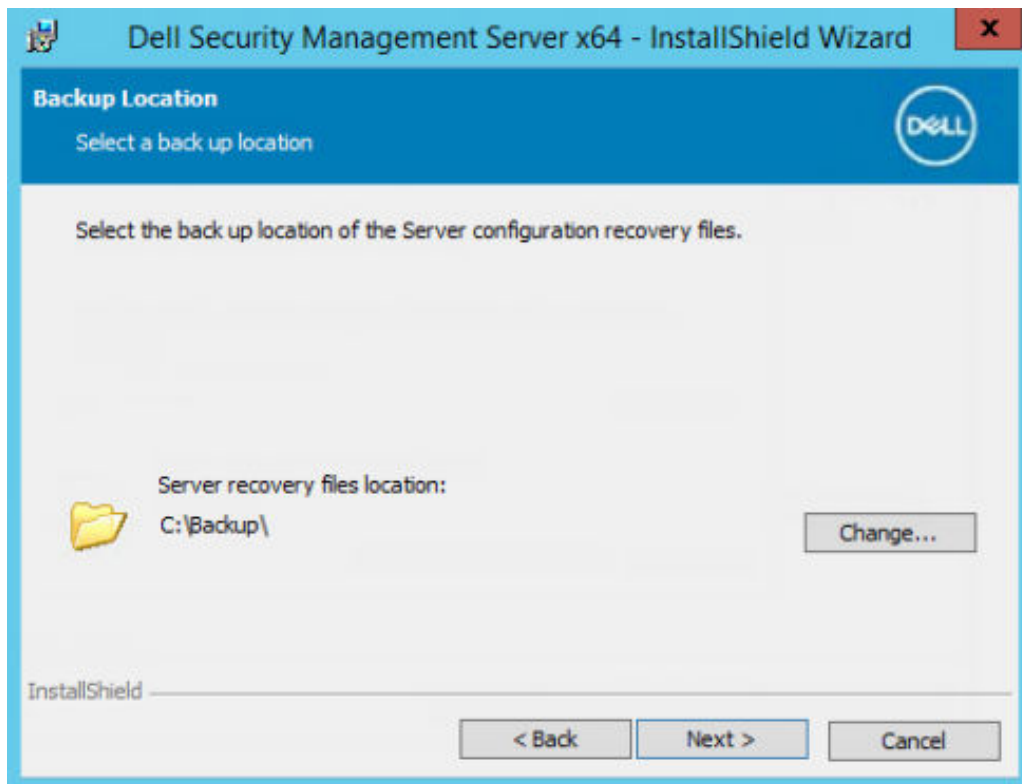


9. Para instalar o Security Management Server no local padrão C:\Program Files\Dell, clique em **Avançar**. Caso contrário, clique em **Alterar** para selecionar outro local e clique em **Avançar**.



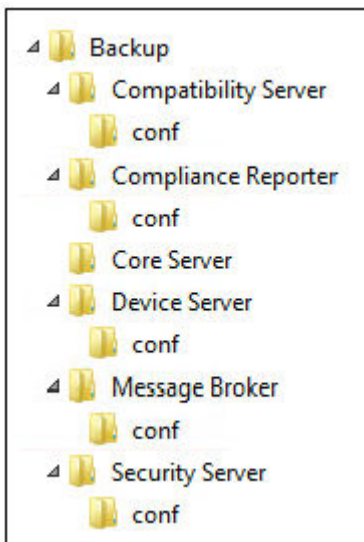
10. Para selecionar um local de armazenamento do backup dos arquivos de recuperação de configuração, clique em **Alterar**, navegue até a pasta desejada e clique em **Avançar**.

**A Dell recomenda que você selecione um local de rede remoto ou uma unidade externa para o backup.**



Após a instalação, quaisquer alterações aos arquivos de configuração, inclusive alterações feitas com a Server Configuration Tool, precisarão ser manualmente copiadas para essas pastas. Os arquivos de configuração são uma parte importante do total de informações usadas para restaurar manualmente o Dell Server.

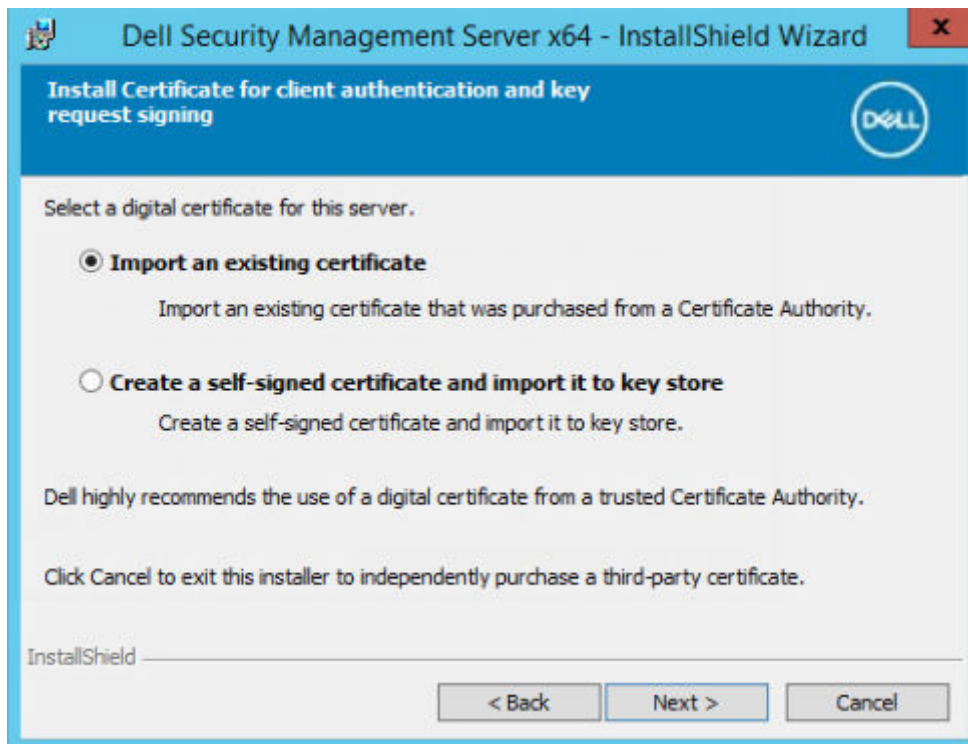
**NOTA:** A estrutura de pastas criada pelo instalador durante a instalação (exemplo mostrado abaixo) precisa permanecer inalterada.



11. Você pode escolher entre alguns tipos de certificados digitais para usar. **É extremamente recomendado o uso de um certificado digital de uma autoridade de certificação confiável.**

Selecione a opção “a” ou “b” abaixo:

a. Para usar um certificado existente que foi comprado de uma autoridade de certificação, selecione **Importar um certificado existente** e clique em **Avançar**.



Clique em **Procurar** para digitar o caminho do certificado.

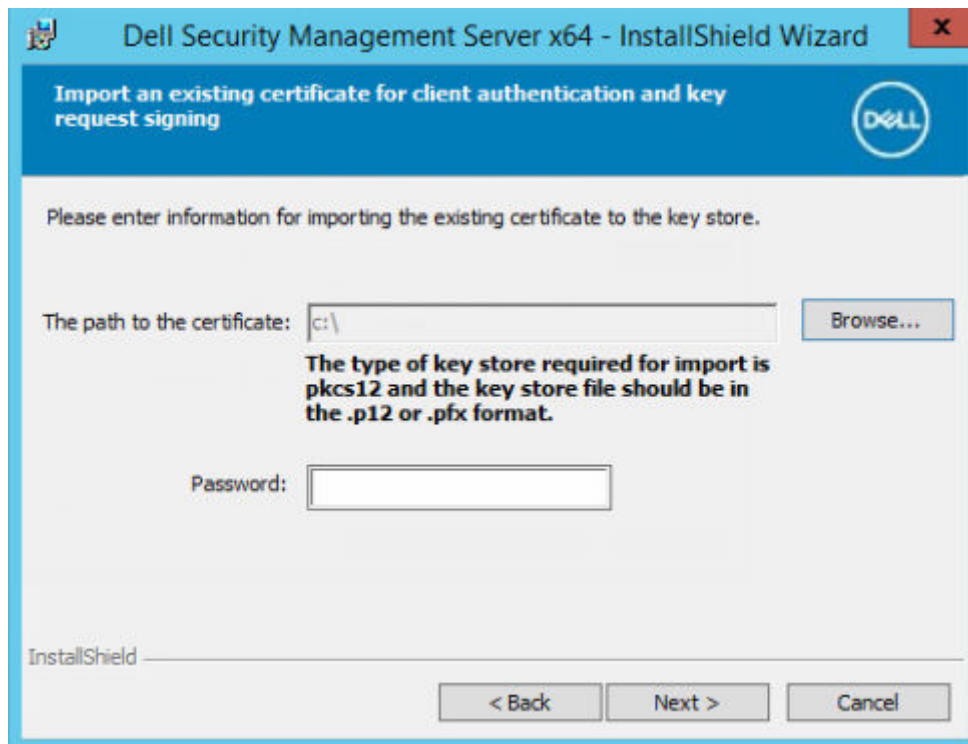
Digite a senha associada a esse certificado. O arquivo de armazenamento de chaves deve ser .p12 ou pfx. Consulte [Exportar um certificado para .PFX usando o console de gerenciamento de certificados](#) para obter instruções.

Clique em **Avançar**.

**NOTA:**

Para usar essa configuração, o certificado CA exportado que está sendo importado precisa ter a cadeia de confiança completa. Se não tiver certeza, exporte novamente o certificado CA e verifique se as seguintes opções estão selecionadas no "Assistente para exportação de certificados":

- Troca de informações pessoais - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades estendidas



OU

- b. Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para o armazenamento de chaves e clique em Avançar.**

Na caixa de diálogo *Criar certificado autoassinado*, digite as informações a seguir:

Nome do computador totalmente qualificado (exemplo: nomedocomputador.domínio.com)

Organização

Unidade organizacional (exemplo: Segurança)

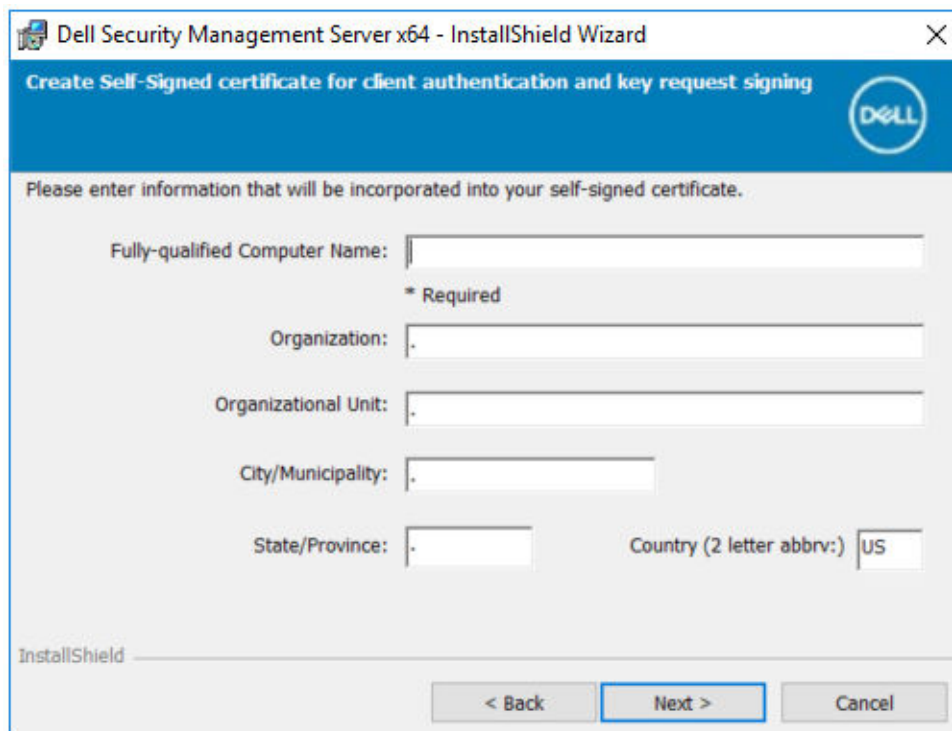
Cidade

Estado (nome completo)

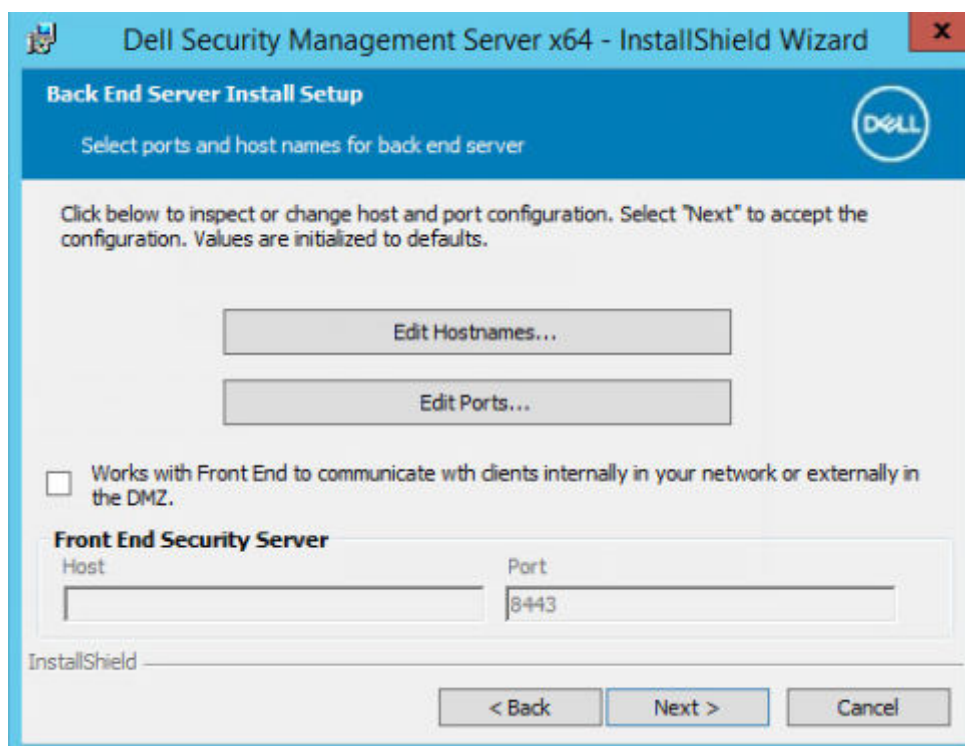
País: abreviação com duas letras

Clique em **Avançar**.

**i** **NOTA:** Por padrão, o certificado expira em um 10 anos.



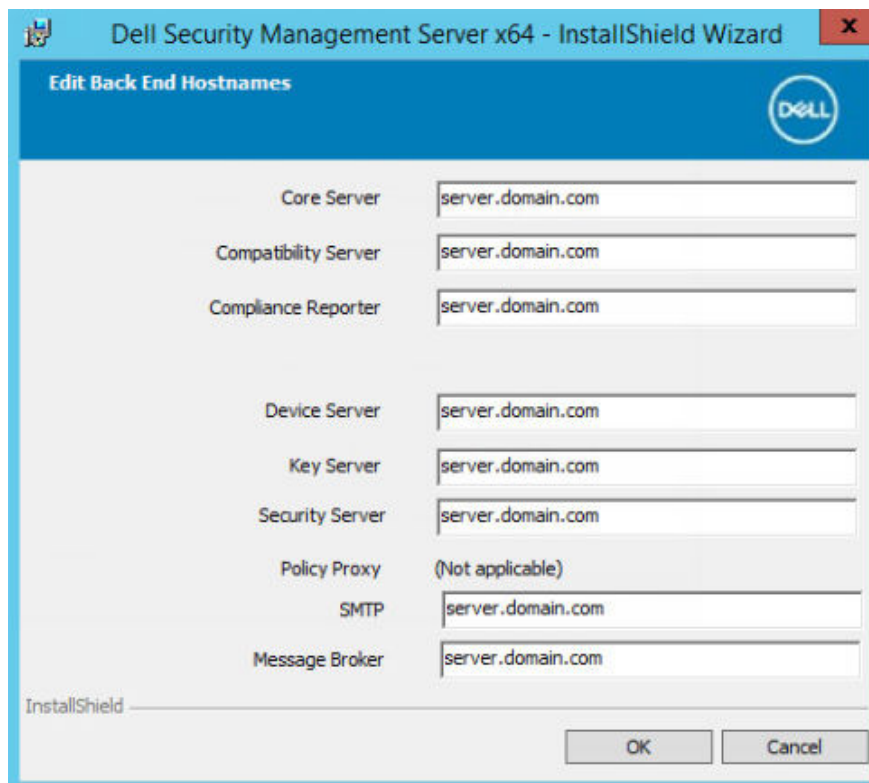
12. Na caixa de diálogo *Configuração de instalação do servidor de back-end*, você pode ver ou editar os nomes de host e as portas.
- Para aceitar os nomes de host e as portas padrão, na caixa de diálogo *Configuração de instalação do servidor de back-end*, clique em **Avançar**.
  - Se você estiver usando um servidor de front-end, selecione **Trabalha com o front-end para se comunicar com clientes internamente em sua rede ou externamente no DMZ** e digite o nome de host do Front End Security Server (por exemplo, server.domain.com).



- Para ver ou editar os nomes de host, clique em **Editar nomes de host**. Edite os nomes de host apenas se necessário. A Dell recomenda usar as configurações padrão.

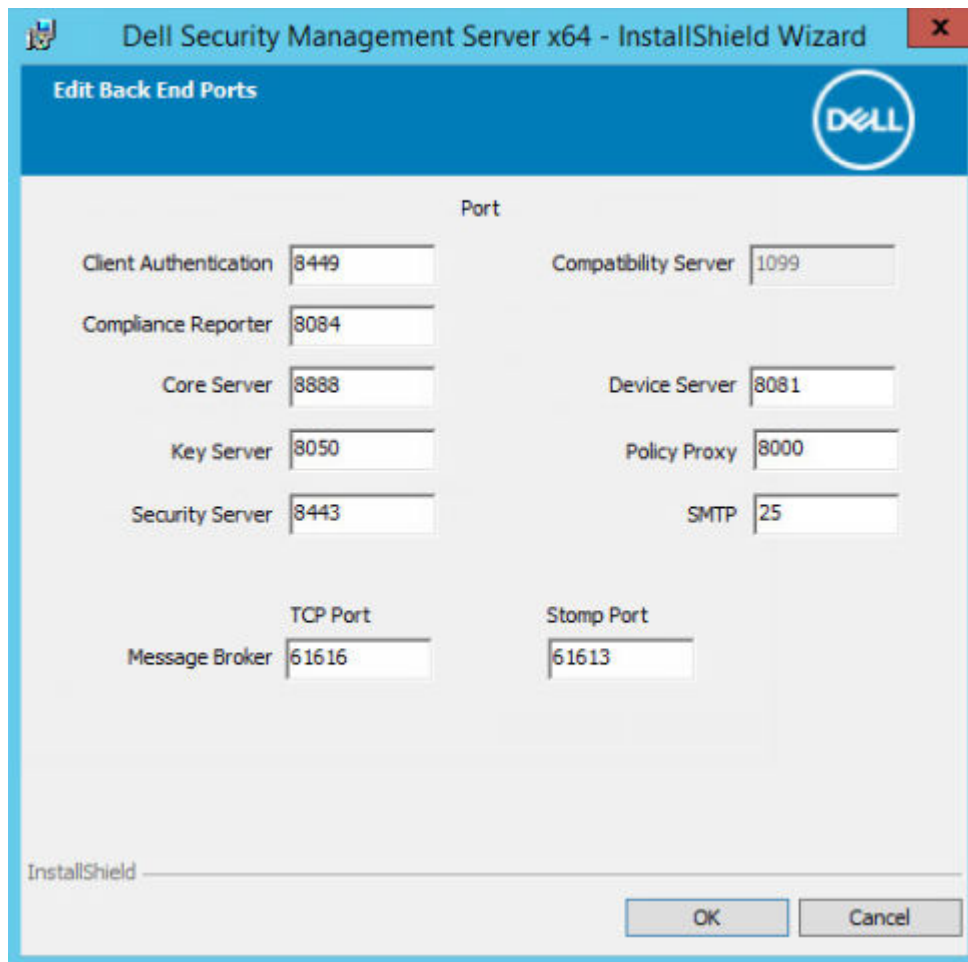
**NOTA:** Um nome de host não pode conter um caractere sublinhado ("\_").

Quando concluído, clique em **OK**.



Role	Hostname
Core Server	server.domain.com
Compatibility Server	server.domain.com
Compliance Reporter	server.domain.com
Device Server	server.domain.com
Key Server	server.domain.com
Security Server	server.domain.com
Policy Proxy	(Not applicable)
SMTP	server.domain.com
Message Broker	server.domain.com

- Para ver ou editar as portas, clique em **Editar portas**. Edite as portas apenas se necessário. A Dell recomenda usar as configurações padrão. Quando concluído, clique em **OK**.

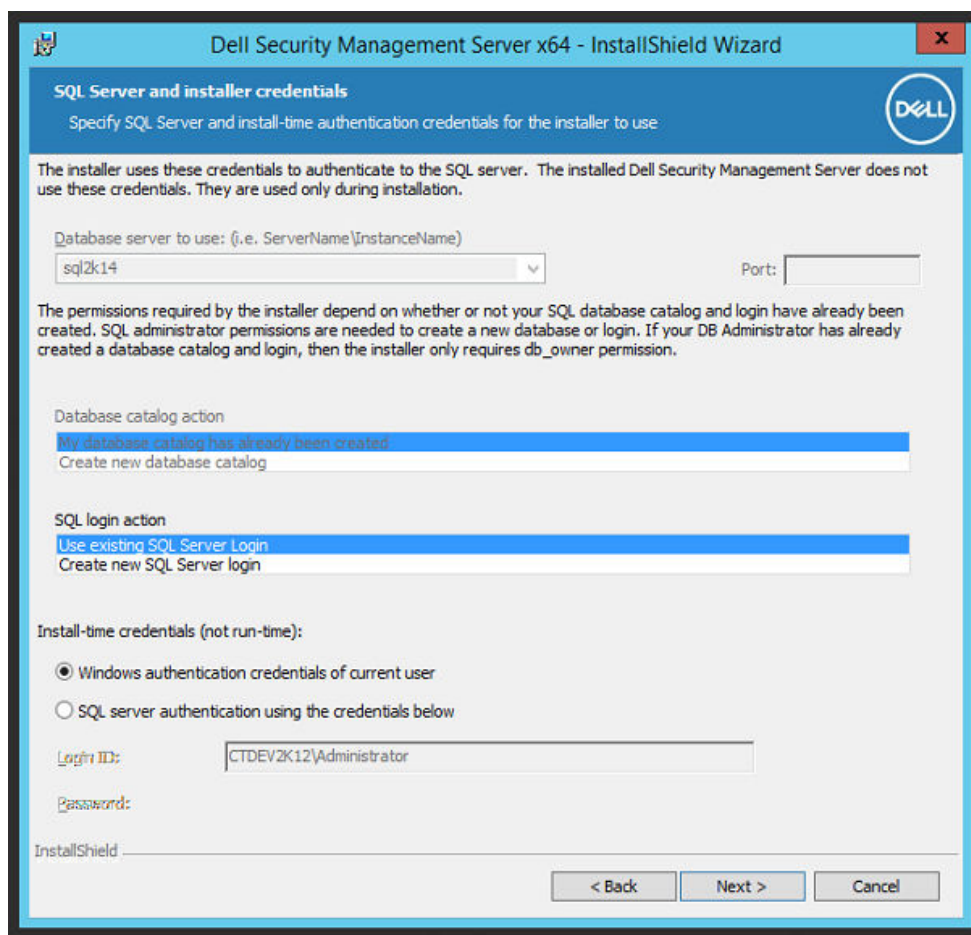


13. Especifique o método de autenticação a ser usado pelo instalador.

- a. Clique em **Procurar** para selecionar o servidor em que o banco de dados reside.
- b. Selecione o tipo de autenticação.

- **Credenciais de autenticação do Windows do usuário atual**

Se você escolher Autenticação do Windows, as mesmas credenciais usadas para fazer log-in no Windows são usadas para autenticação (os campos *Nome de usuário* e *Senha* não podem ser editados). Confirme que a conta tenha direitos de administrador de sistema e a capacidade de gerenciar o SQL Server.



OU

- **Autenticação do SQL Server usando as credenciais abaixo**

Se você usar a autenticação SQL, a conta SQL usada precisa ter direitos de administrador do sistema no SQL Server.

O instalador precisa ser autenticado para o SQL Server com estas permissões: criar banco de dados, adicionar usuário, atribuir permissões.

c. Clique em **Procurar** para selecionar o nome do catálogo do banco de dados existente.

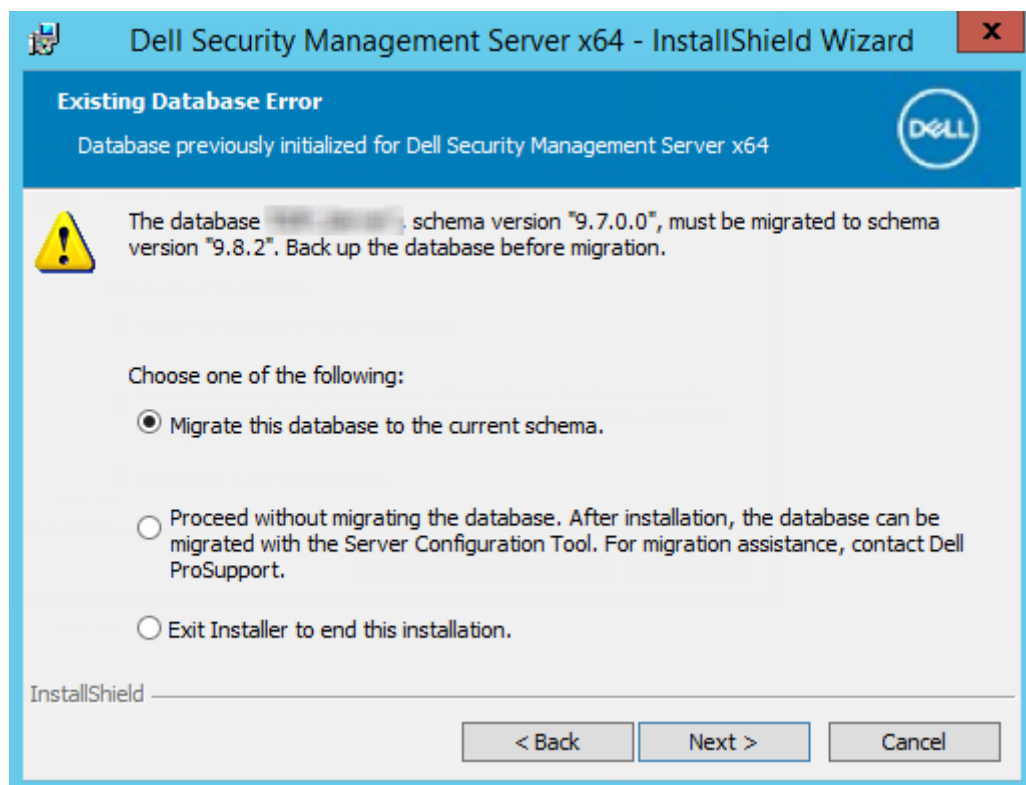
d. Clique em **Avançar**.

14. Se a caixa de diálogo Erro de banco de dados existente for exibida, selecione a opção apropriada.

Se o instalador detectar um problema com o banco de dados, será exibida uma caixa de diálogo de *Erro de banco de dados existente*. As opções na caixa de diálogo dependem das circunstâncias:

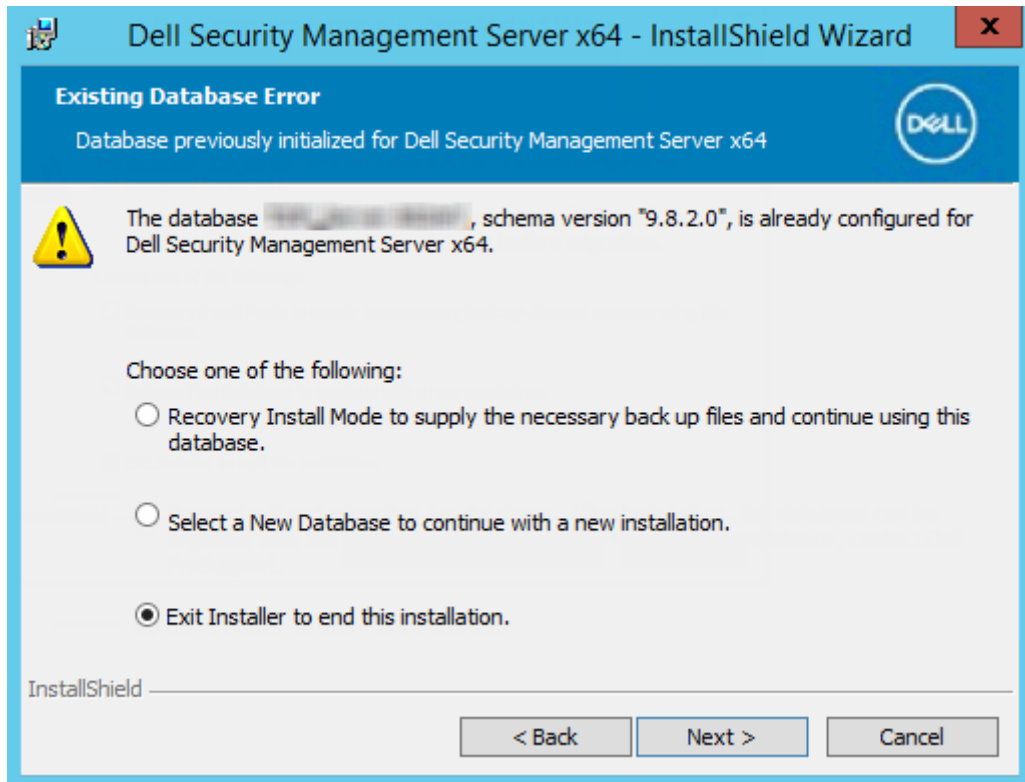
- O esquema do banco de dados é de uma versão anterior. (Consulte a etapa a.)
- O banco de dados já tem um esquema de banco de dados que corresponde à versão que está sendo instalada no momento. (Consulte a etapa b.)

a. Quando o esquema do banco de dados for de uma versão anterior, selecione **Sair do instalador para encerrar esta instalação**. Em seguida, você precisa fazer o backup do banco de dados.



As opções a seguir **PRECISAM** ser usadas somente com a ajuda do Dell ProSupport:

- A opção **Migrar este banco de dados para o esquema atual** é usada para recuperar um banco de dados em bom estado de uma implementação de servidor com falha. Esta opção usa os arquivos de recuperação na pasta \Backup para reconectar ao banco de dados e, em seguida, migra o banco de dados para o esquema atual. Esta opção deveria ser usada *somente* depois de tentar, primeiro, reinstalar a versão correta do Security Management Server e, em seguida, executar o instalador mais recente para atualizar a versão.
  - A opção **Prosseguir sem migrar o banco de dados** instala os arquivos do Security Management Server sem configurar completamente o banco de dados. A configuração do banco de dados precisa ser concluída posteriormente, manualmente, usando a Server Configuration Tool, e precisa de alterações manuais adicionais.
- b. Quando o esquema do banco de dados já tem o esquema da versão atual, mas não está conectado a um back-end do Security Management Server, isso é considerado uma *Recuperação*. Se **Instalação de recuperação** não foi selecionado *nesta etapa*, a caixa de diálogo a seguir será exibida:
- Selecione **Modo de instalação de recuperação** para continuar a instalação com o banco de dados selecionado.
  - Selecione **Selecionar um novo banco de dados** para escolher outro banco de dados.
  - Selecione **Sair do Instalador para encerrar esta instalação**.
- c. Clique em **Avançar**.



15. Selecione o método de autenticação a ser usado pelo produto. Esta é a conta que o produto usará para operar com o banco de dados e os serviços Dell.

- **Para usar a autenticação do Windows**

Selecione **Autenticação do Windows usando as credenciais abaixo**, insira as credenciais da conta que o produto pode usar e clique em Avançar.

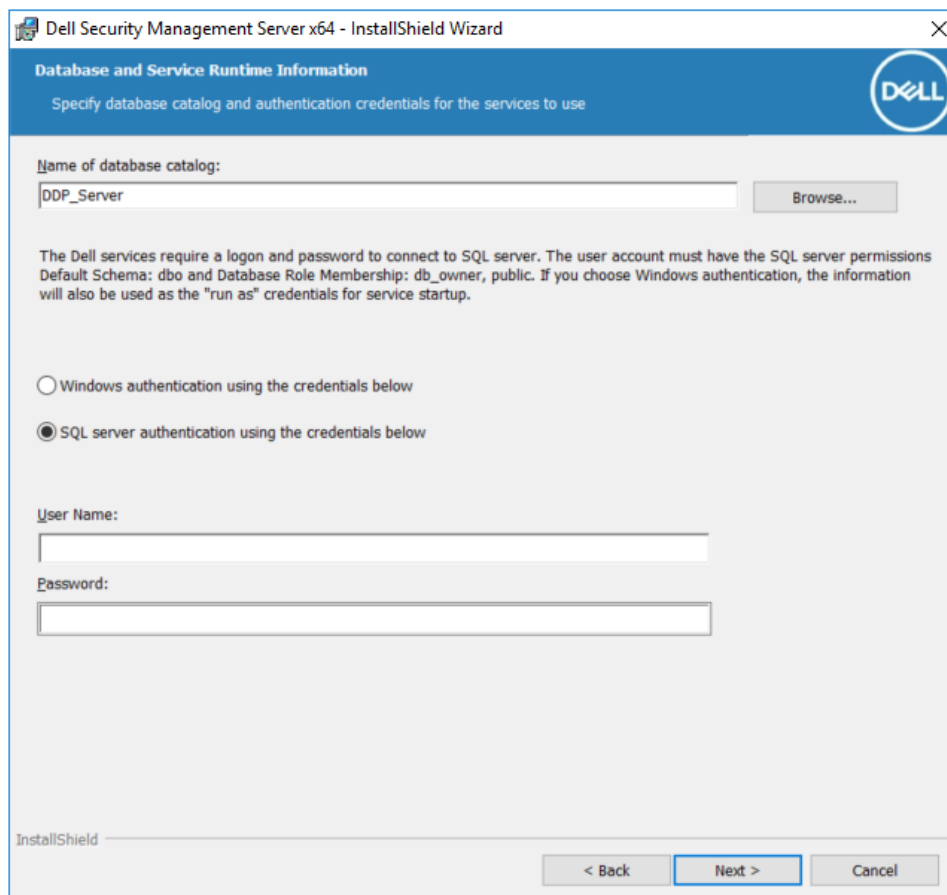
Confirme que a conta tenha direitos de administrador de sistema e a capacidade de gerenciar o SQL Server. A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Associação à função de banco de dados: dbo\_owner, público.

OU

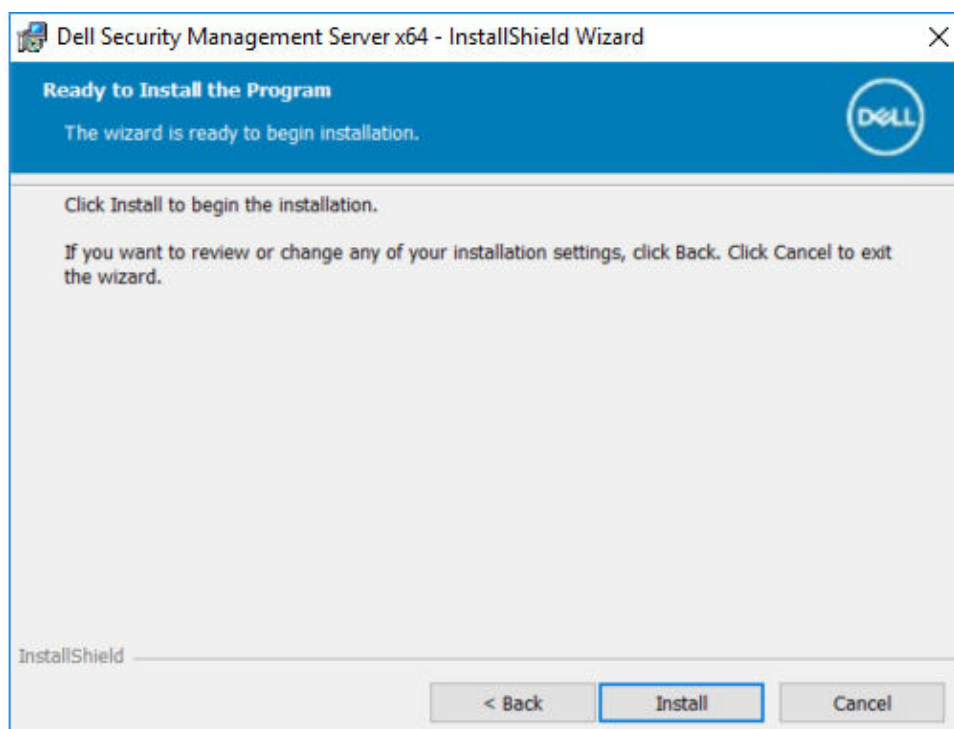
- **Para usar a autenticação do SQL Server**

Selecione **autenticação do SQL usando as credenciais abaixo**, digite as credenciais do SQL Server e, em seguida, clique em **Avançar**.

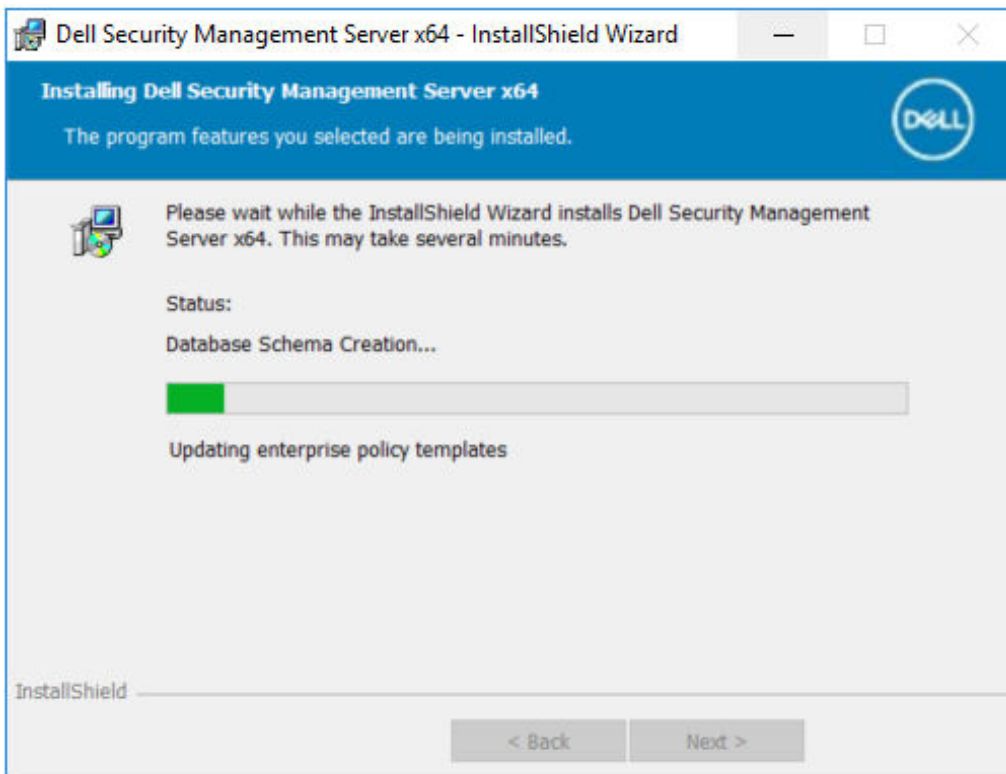
A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Associação à função de banco de dados: dbo\_owner, público.



16. Na caixa de diálogo *Pronto para instalar o programa*, clique em **Instalar**.



Uma caixa de diálogo do progresso mostra o status de todo o processo de instalação.



Ao terminar a instalação, clique em **Concluir**.



As tarefas de instalação do servidor de back-end estão concluídas.

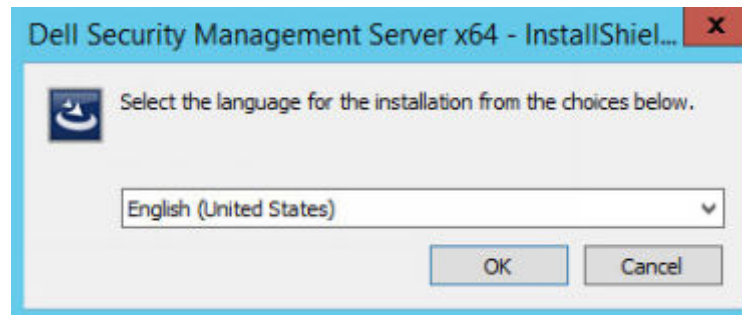
Os Serviços Dell são reiniciados ao final da instalação. Não é necessário reinicializar o servidor.

## Instalar servidor front-end

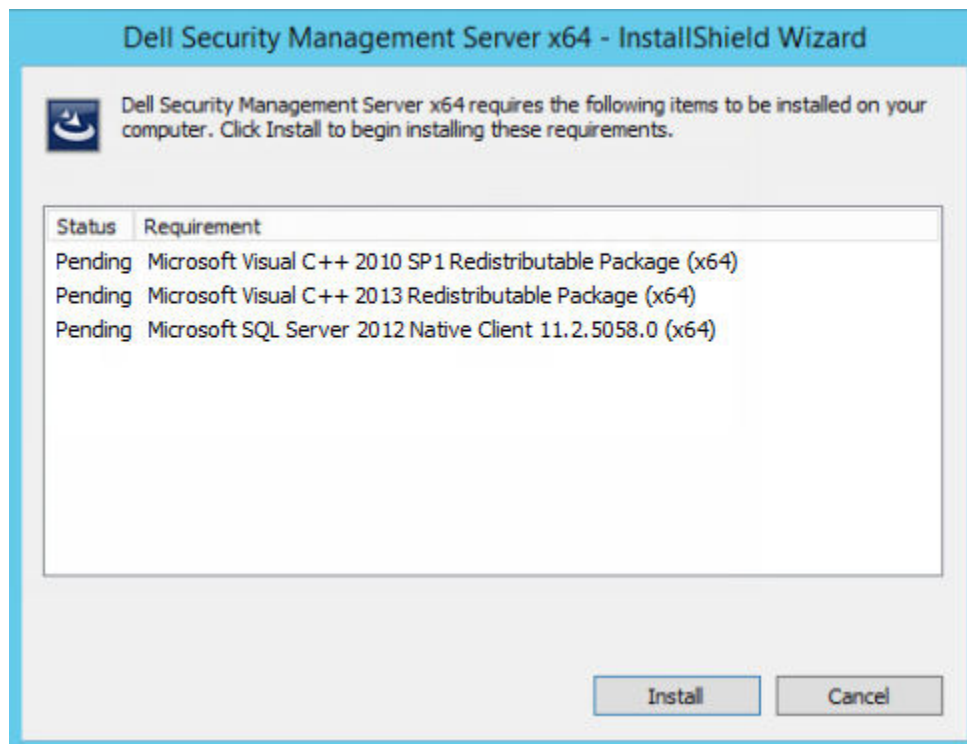
Instalação de servidor front-end fornece uma opção de front-end (Modo DMZ) para uso com o Security Management Server. Se você pretende implementar componentes da Dell no DMZ, verifique se eles estão devidamente protegidos contra ataques.

Para executar a instalação, é necessário ter o nome de host totalmente qualificado do servidor DMZ.

1. Na mídia de instalação Dell, navegue até o diretório do Security Management Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Security Management Server-x64 no diretório raiz do servidor onde você está instalando o Security Management Server. **Copiar/colar ou arrastar/soltar produz erros e causa uma instalação malsucedida.**
2. Clique duas vezes em **setup.exe**.
3. Selecione o idioma para a instalação e clique em **OK**.



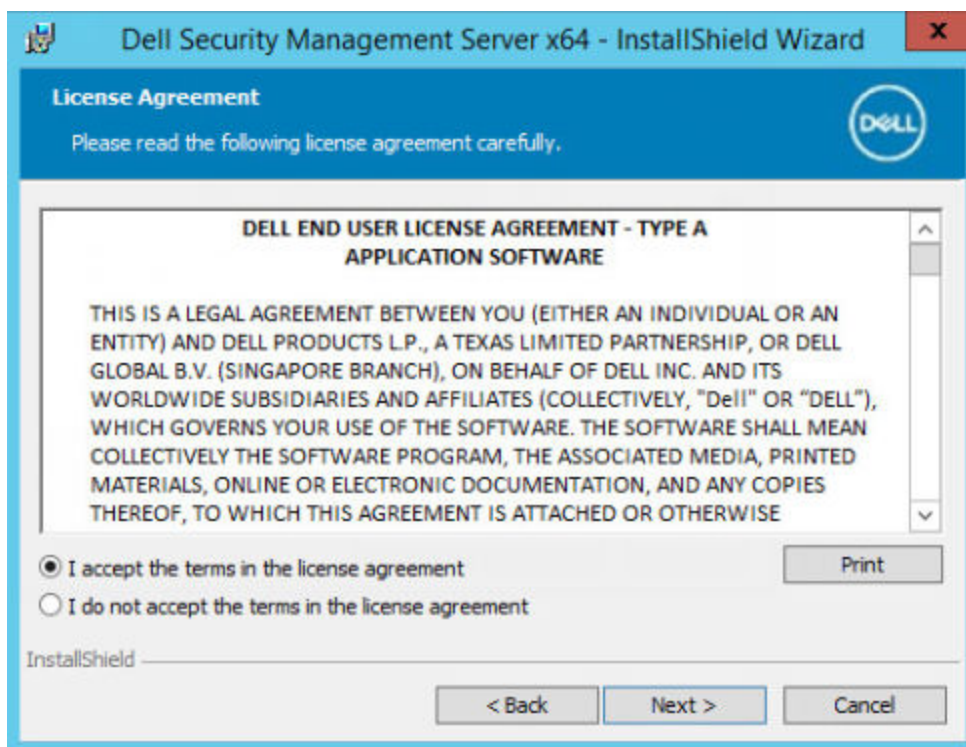
4. Se os pré-requisitos ainda não estiverem instalados, será mostrada uma mensagem informando quais pré-requisitos serão instalados. Clique em **Instalar**.



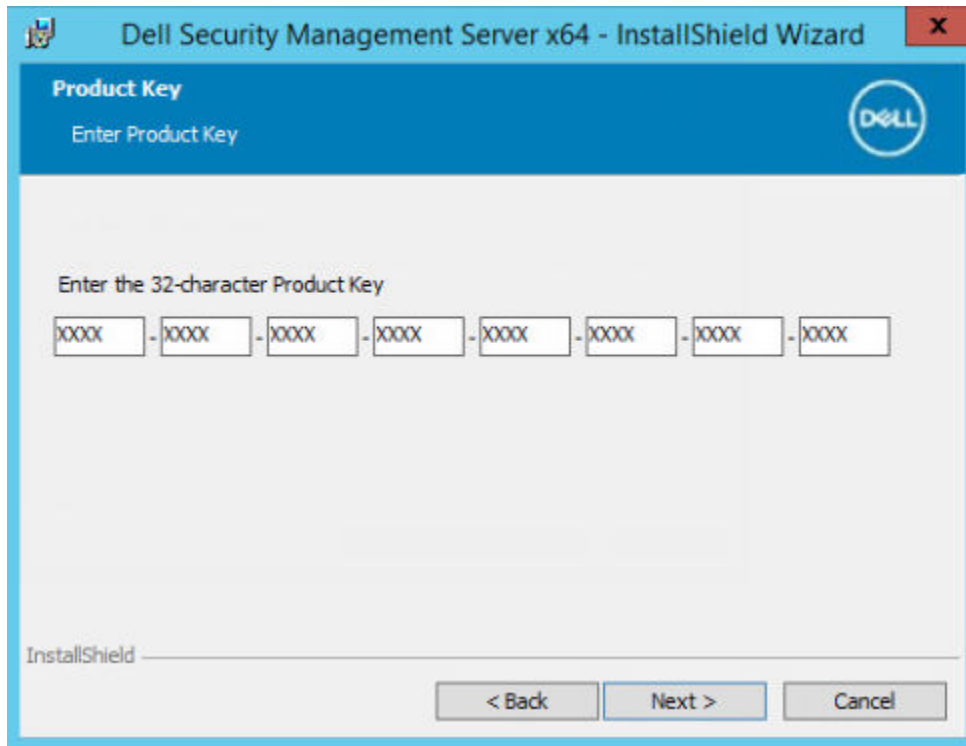
5. Clique em **Avançar** na caixa de diálogo de Boas-vindas.



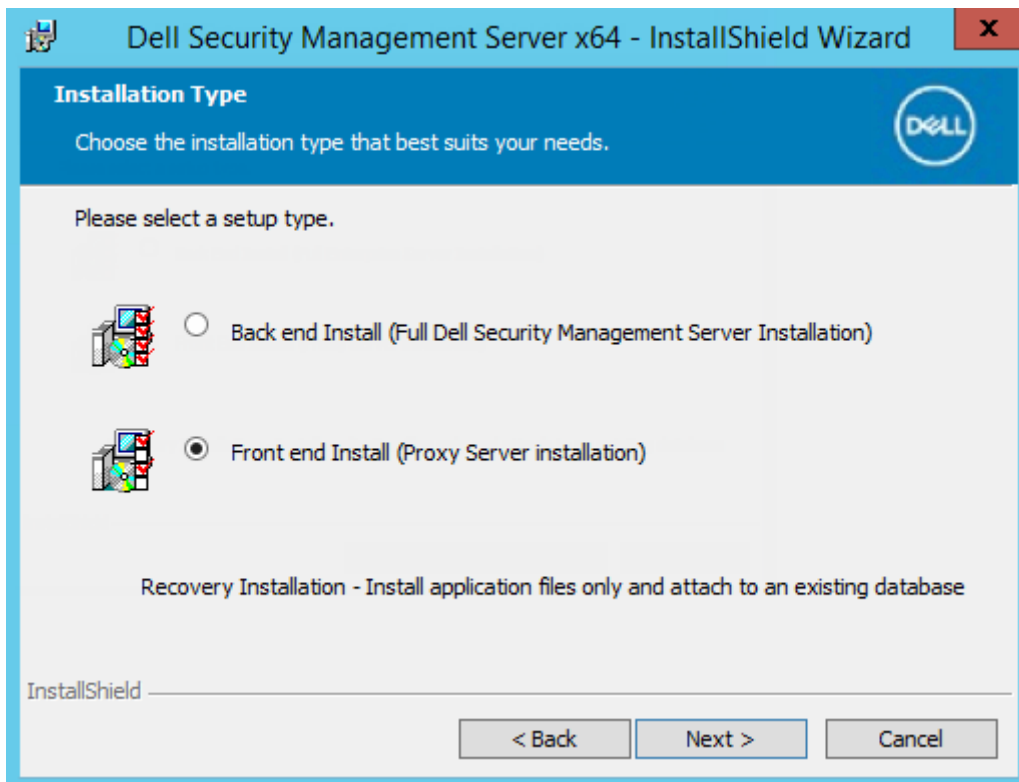
6. Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.



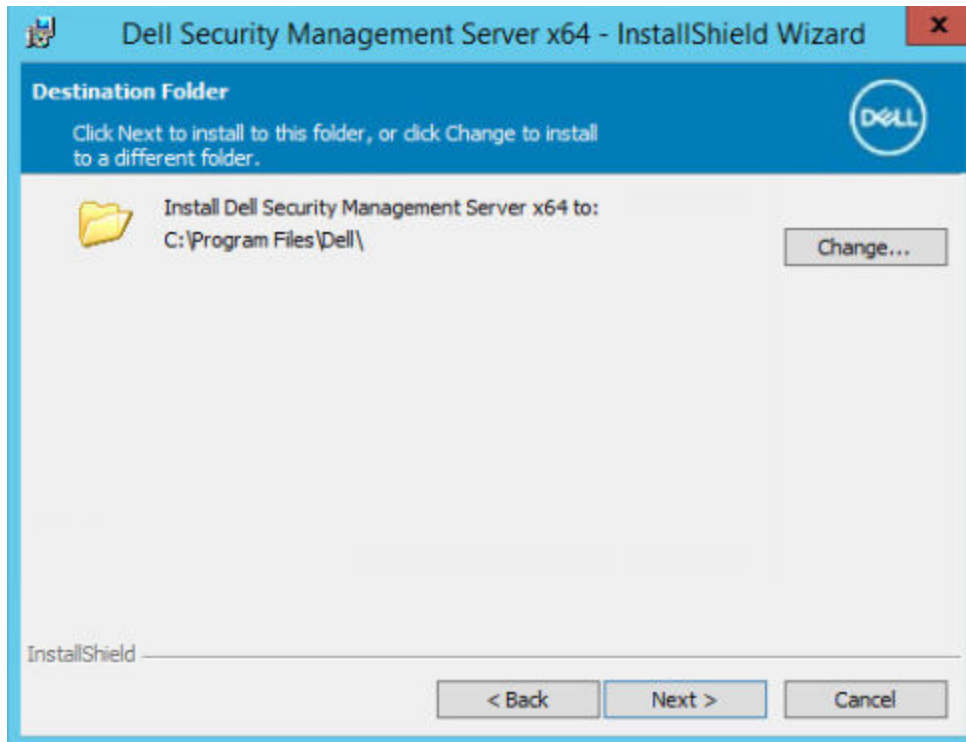
7. Se você, opcionalmente, copiou o arquivo EnterpriseServerInstallKey system.ini para C:\Windows conforme explicado em [Configuração de pré-instalação](#), clique em **Avançar**. Caso contrário, digite a Chave do Produto de 32 caracteres e clique em **Avançar**. A Chave do Produto está localizada no arquivo EnterpriseServerInstallKey.ini.



8. Selecione **Instalação do front-end** e clique em **Avançar**.



9. Para instalar o servidor de front-end no local padrão `C:\Program Files\Dell`, clique em **Avançar**. Caso contrário, clique em **Alterar** para selecionar outro local e clique em **Avançar**.

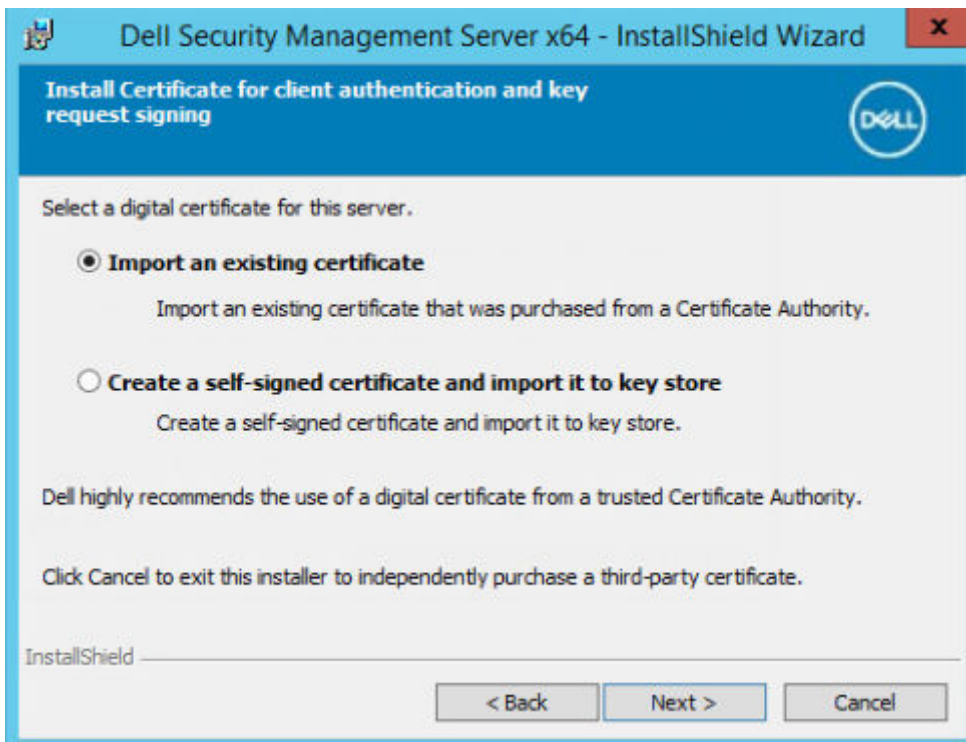


10. Você pode escolher entre alguns tipos de certificados digitais para usar.

**NOTA:** É extremamente recomendado o uso de um certificado digital de uma autoridade de certificação confiável.

Selecione a opção “a” ou “b” abaixo:

- a. Para usar um certificado existente que foi comprado de uma autoridade de certificação, selecione **Importar um certificado existente** e clique em **Avançar**.



Clique em **Procurar** para digitar o caminho do certificado.

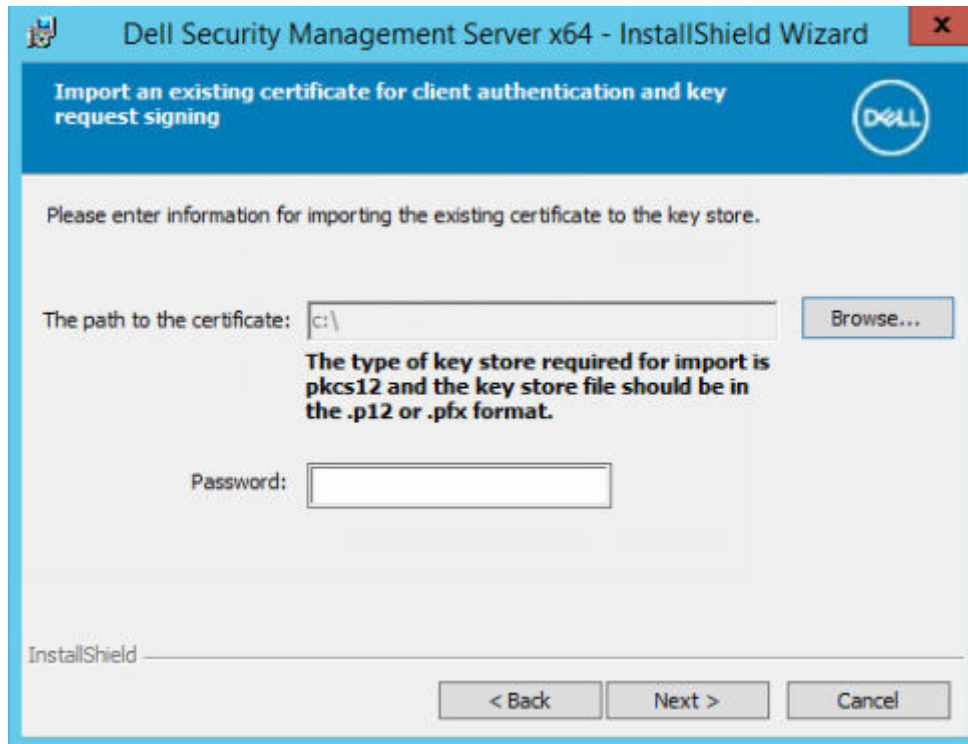
Digite a senha associada a esse certificado. O arquivo de armazenamento de chaves deve ser .p12 ou pfx. Consulte [Exportar um certificado para .PFX usando o console de gerenciamento de certificados](#) para obter instruções.

Clique em **Avançar**.

**i** **NOTA:**

Para usar essa configuração, o certificado CA exportado que está sendo importado precisa ter a cadeia de confiança completa. Se não tiver certeza, exporte novamente o certificado CA e verifique se as seguintes opções estão selecionadas no “Assistente para exportação de certificados”:

- Troca de informações pessoais - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades estendidas



- b. Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para o armazenamento de chaves e clique em Avançar**.

Na caixa de diálogo *Criar certificado autoassinado*, digite as informações a seguir:

Nome do computador totalmente qualificado (exemplo: nomedocomputador.domínio.com)

Organização

Unidade organizacional (exemplo: Segurança)

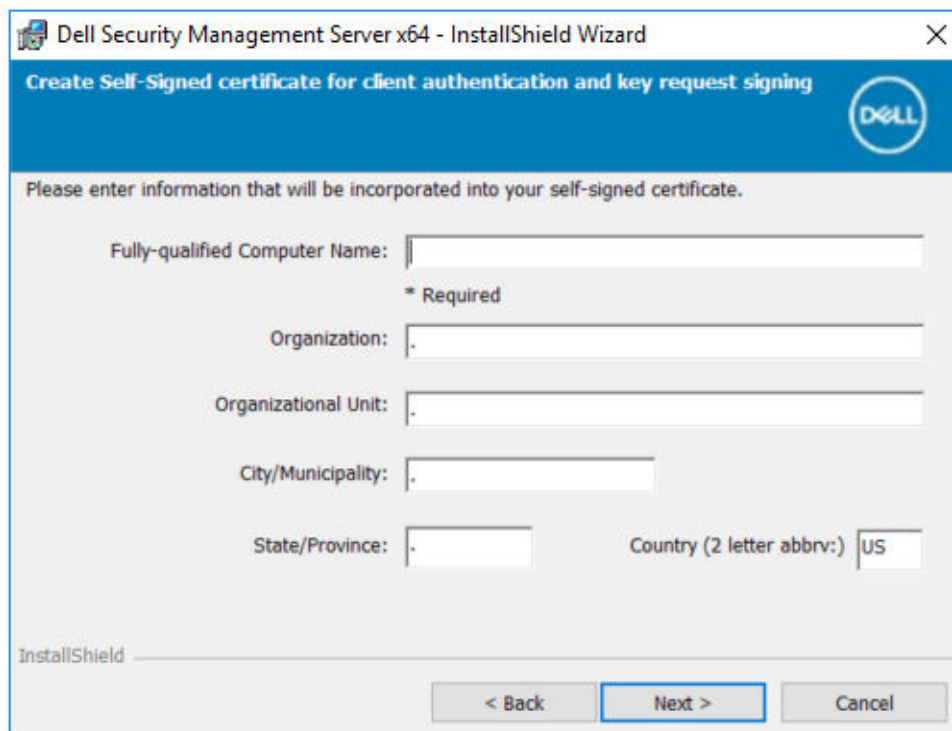
Cidade

Estado (nome completo)

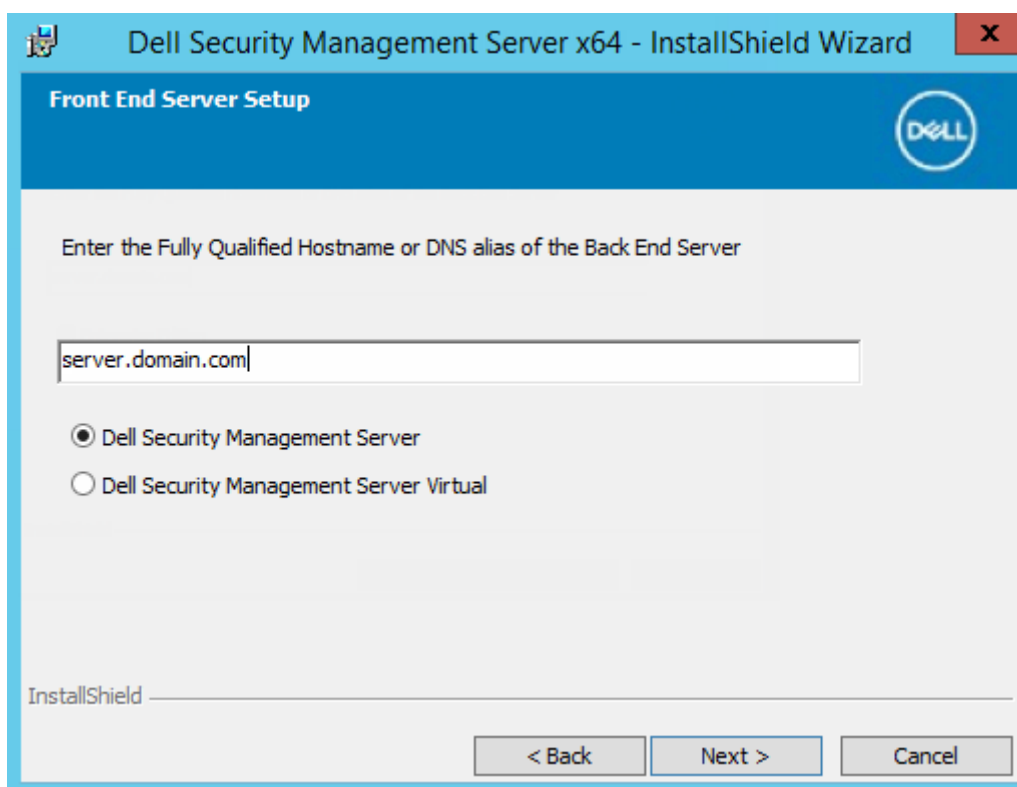
País: abreviação com duas letras

Clique em **Avançar**.

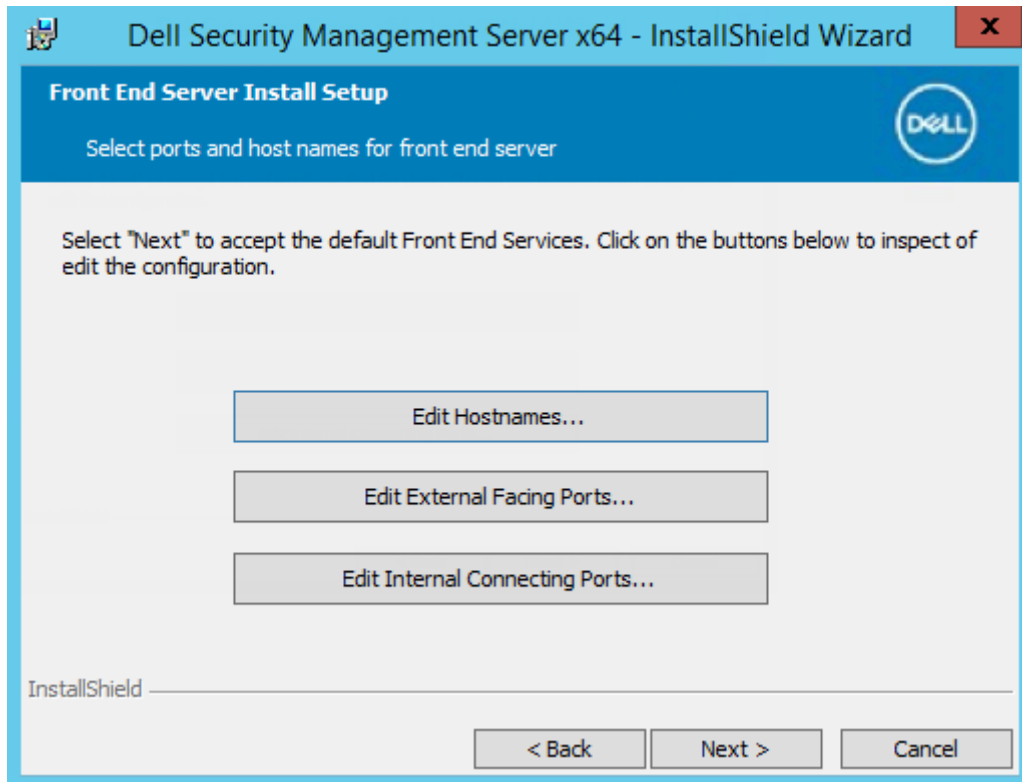
**i** **NOTA:** Por padrão, o certificado expira em um 10 anos.



11. Na caixa de diálogo *Configuração do servidor de front-end*, digite o nome de host ou o alias do DNS do servidor de back-end, selecione **Dell Security Management Server** e clique em **Avançar**.



12. Na caixa de diálogo *Configuração de instalação do servidor de front-end*, você pode ver ou editar os nomes de host e as portas.
  - Para aceitar os nomes de host e as portas padrão, na caixa de diálogo *Configuração de instalação do servidor de front-end*, clique em **Avançar**.



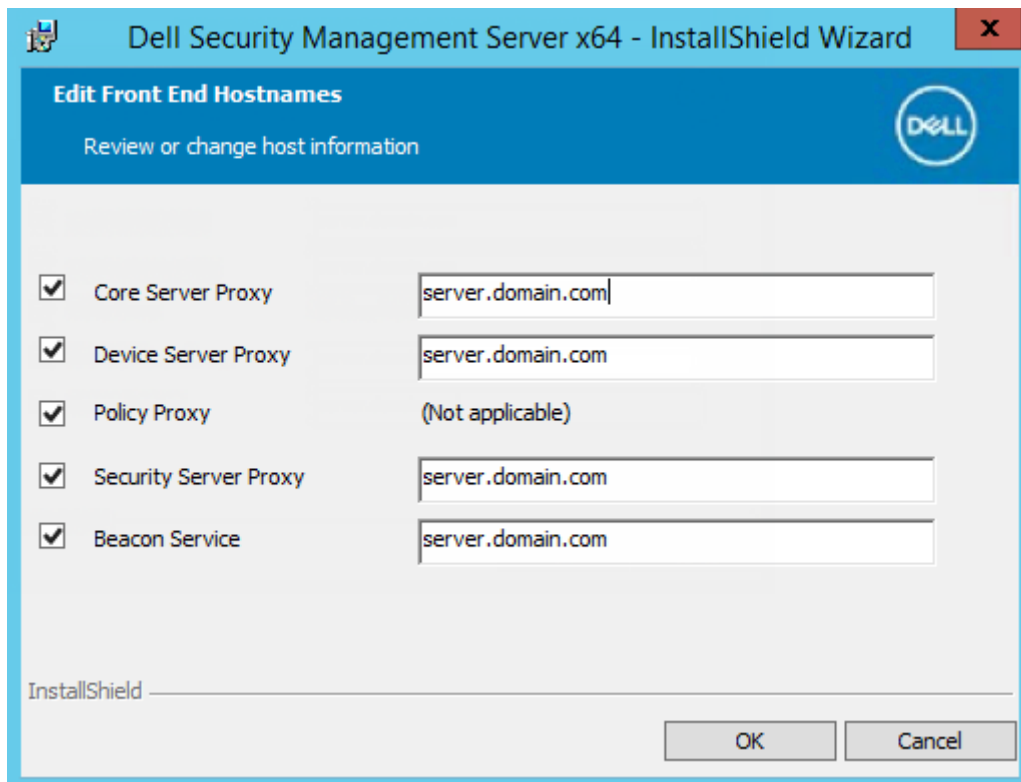
- Para ver ou editar os nomes de host, na caixa de diálogo *Configuração do servidor de front-end*, clique em **Editar nomes de host**. Edite os nomes de host apenas se necessário. A Dell recomenda usar as configurações padrão.

**NOTA:**

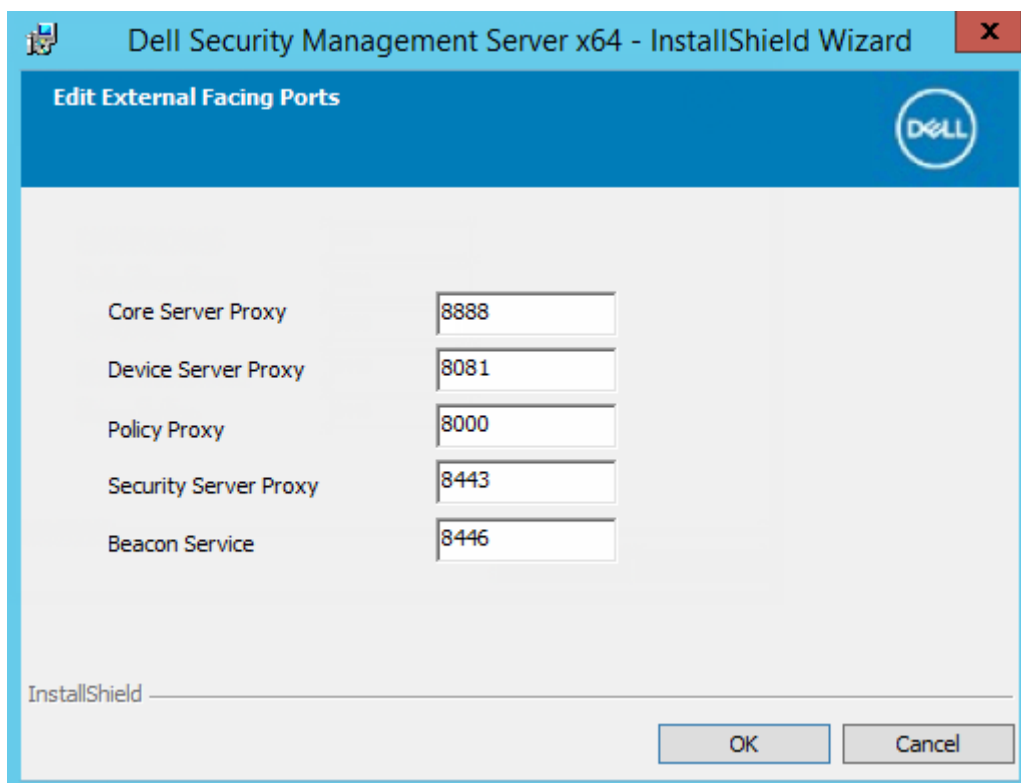
Um nome de host não pode conter um caractere sublinhado ( "\_").

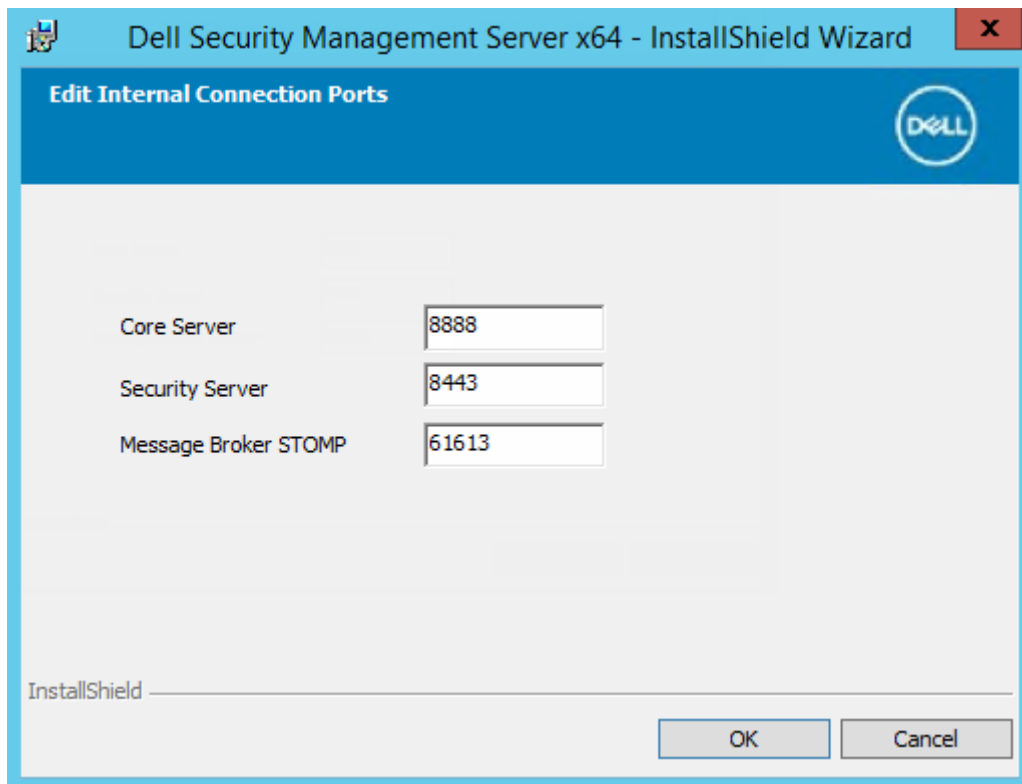
Desmarque um proxy apenas se tiver certeza de que não quer configurá-lo para instalação. Se você desmarcar um proxy nessa caixa de diálogo, ele não é instalado.

Quando concluído, clique em **OK**.

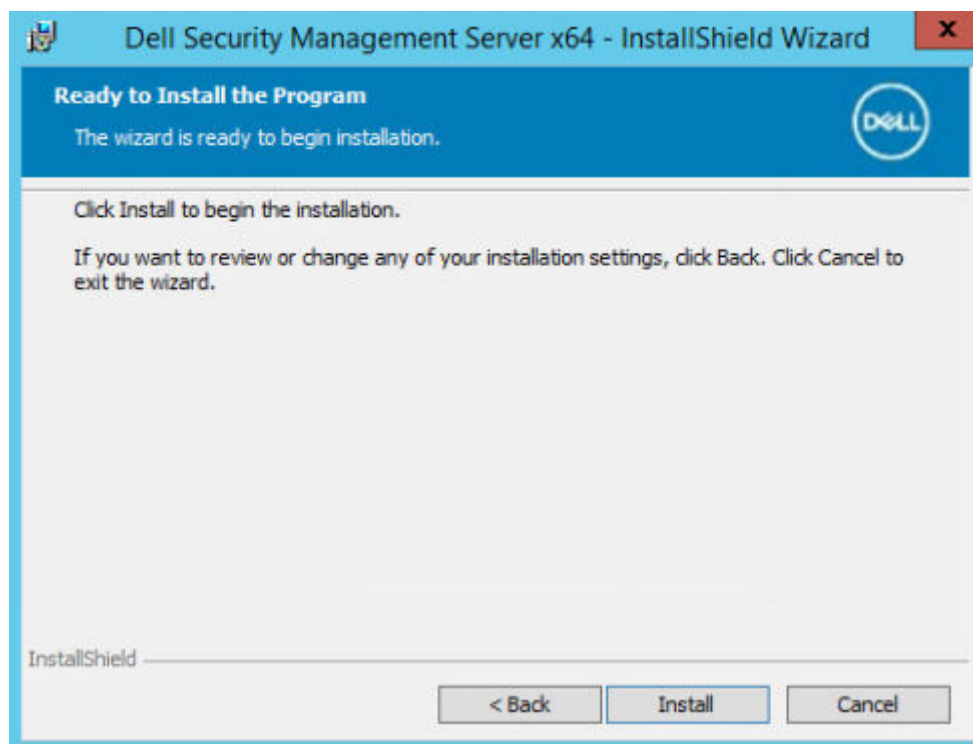


- Para ver ou editar as portas, na caixa de diálogo *Configuração do servidor de front-end* clique em **Editar portas externas** ou **Editar portas de conexão internas**. Edite as portas apenas se necessário. A Dell recomenda usar as configurações padrão. Se você desmarcar um proxy na caixa de diálogo *Editar nomes de host do front-end*, sua porta não será mostrada nas caixas de diálogo *Portas externas* ou *Portas internas*. Quando concluído, clique em **OK**.

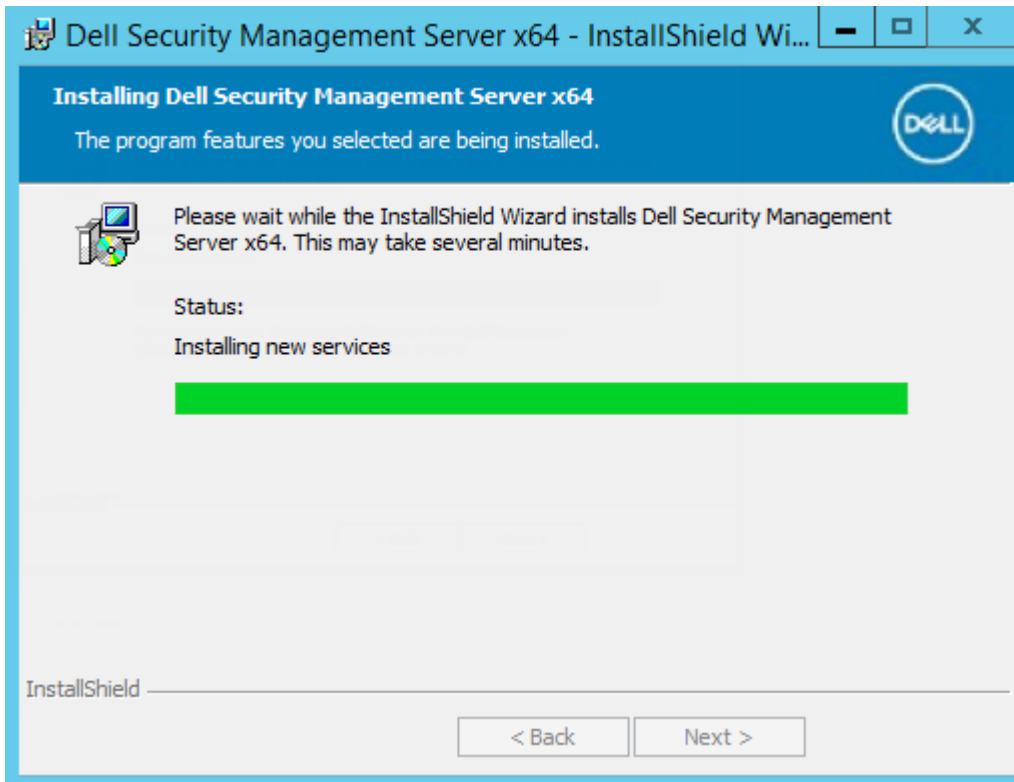




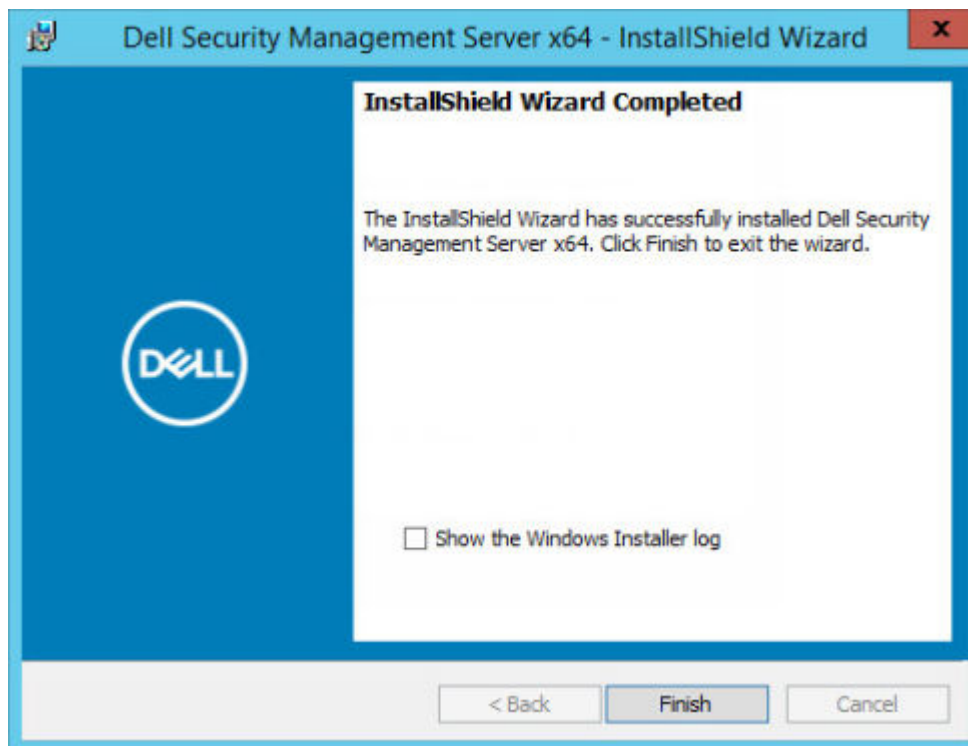
13. Na caixa de diálogo *Pronto para instalar o programa*, clique em **Instalar**.



Uma caixa de diálogo do progresso mostra o status de todo o processo de instalação.



14. Ao terminar a instalação, clique em **Concluir**.



As tarefas de instalação do servidor de front-end estão concluídas.

## Atualizar/Migrar

Você pode fazer o upgrade do Enterprise Server v9.2 ou posterior para o Security Management Server v10.x. Se a sua versão do Dell Server for anterior a v9.2, primeiramente você precisará fazer o upgrade para a v9.2 e, em seguida, para as versões posteriores.

## Antes de iniciar o processo de Atualizar/Migrar

Antes de começar, certifique-se de que toda a [Configuração de pré-instalação](#) foi concluída.

Leia os *relatórios técnicos do Security Management Server* para conhecer qualquer solução atual ou problema conhecido relacionado à instalação do Security Management Server.

A conta do usuário a partir da qual a instalação é executada precisa ter privilégios de proprietário do banco de dados para o banco de dados SQL. Se você não tiver certeza sobre os privilégios de acesso ou conectividade ao banco de dados, peça a seu administrador de banco de dados que confirme isso antes de você começar a instalação.

A Dell recomenda que as boas práticas de bancos de dados sejam usadas para o banco de dados do servidor da Dell e que o software seja incluído no plano de recuperação de desastres da sua organização.

Se você pretende implementar componentes da Dell no DMZ, verifique se eles estão devidamente protegidos contra ataques.

Para produção, a Dell recomenda a instalação do SQL Server em um servidor dedicado.

Para aproveitar os recursos completos das políticas, a Dell recomenda atualizar para as versões mais recentes do Security Management Server e clientes.

O Security Management Server v10.x suporta:

- Encryption Enterprise:
  - Clients Windows v8.x/v10.x
  - 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
- Atualização/migração do Security Management Server versão 9.2 ou superior. (Ao migrar de uma versão anterior para a versão 9.2 do Security Management Server, entre em contato com o Dell ProSupport para obter assistência.)

Ao fazer upgrade/migração do Security Management Server para um versão que inclui novas políticas que são introduzidas nessa versão, confirme a política atualizada após o upgrade/migração, para garantir que as configurações preferenciais de políticas sejam implementadas para as novas políticas, em vez dos valores padrão.

Geralmente, nosso caminho de upgrade recomendado é fazer o(a) upgrade/migração do Security Management Server e seus componentes, seguido da instalação/upgrade do Client.

### Aplicar as alterações da política

1. Como um administrador Dell, faça log-in no Console de gerenciamento.
2. No menu à esquerda, clique em **Gerenciamento > Confirmar**.
3. Em *Comentário*, digite uma descrição da alteração.
4. Clique em **Confirmar políticas**.
5. Quando a confirmação for concluída, faça logoff do Management Console.

#### Confirmar se os Serviços Dell estão funcionando

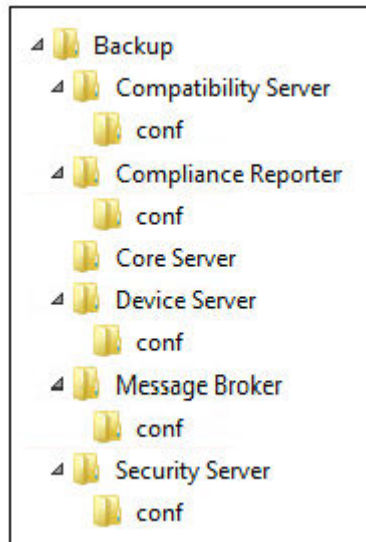
6. No menu *Iniciar* do Windows, clique em **Iniciar > Executar**. Digite `services.msc` e clique em **OK**. Quando Serviços abrir, navegue até cada Serviço da Dell e clique em **Iniciar o serviço**.

#### Fazer backup da instalação existente

7. Faça backup de toda a instalação existente para um local alternativo. O backup deve conter o banco de dados SQL, o secretKeyStore e os arquivos de configuração. Vários arquivos da instalação existente são necessários após a conclusão do processo de upgrade/migração.

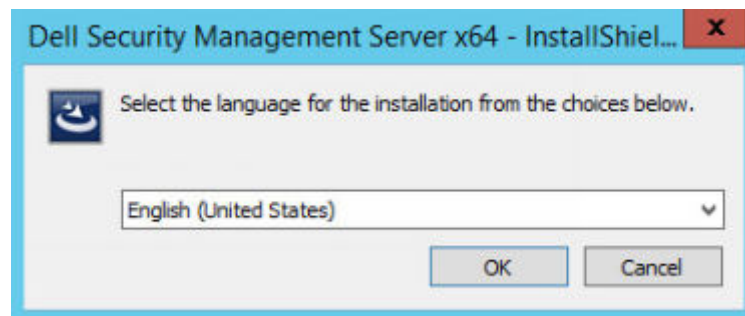
#### **NOTA:**

A estrutura de pastas criada pelo instalador durante a instalação (exemplo mostrado abaixo) precisa permanecer inalterada



## Fazer upgrade/migrar servidor(es) de back-end

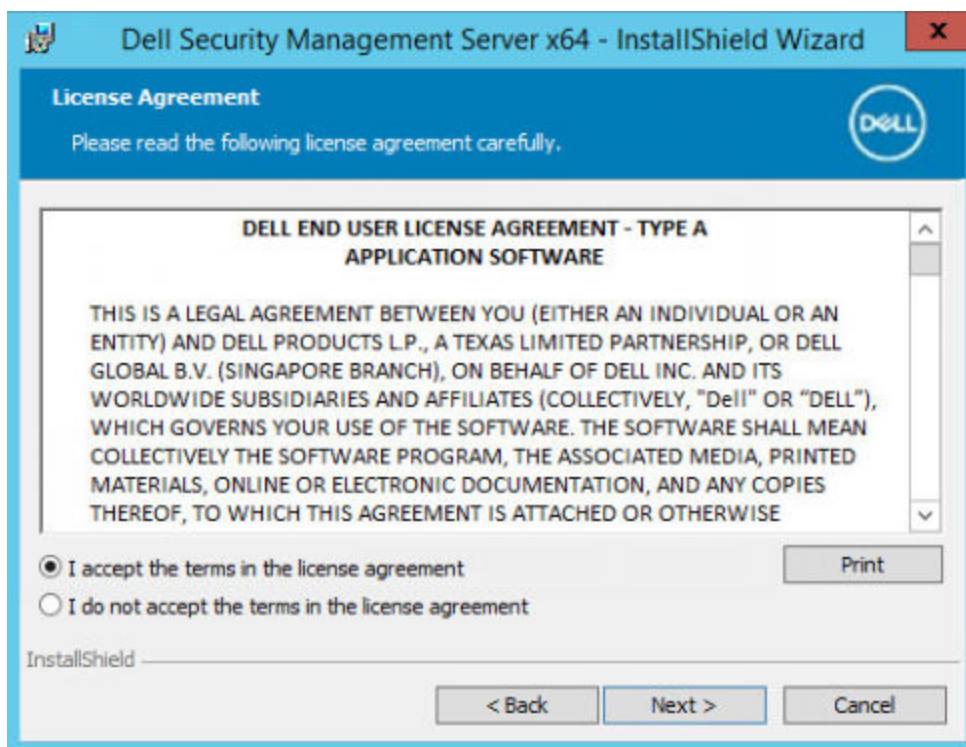
1. Na mídia de instalação Dell, navegue até o diretório do Security Management Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Security Management Server-x64 no diretório raiz do servidor onde você está instalando o Security Management Server. **Copiar/colar ou arrastar/soltar produz erros e causa uma instalação malsucedida.**
2. Clique duas vezes em **setup.exe**.
3. Selecione o idioma para a instalação e clique em **OK**.



4. Na caixa de diálogo *Bem-vindo*, clique em **Avançar**.

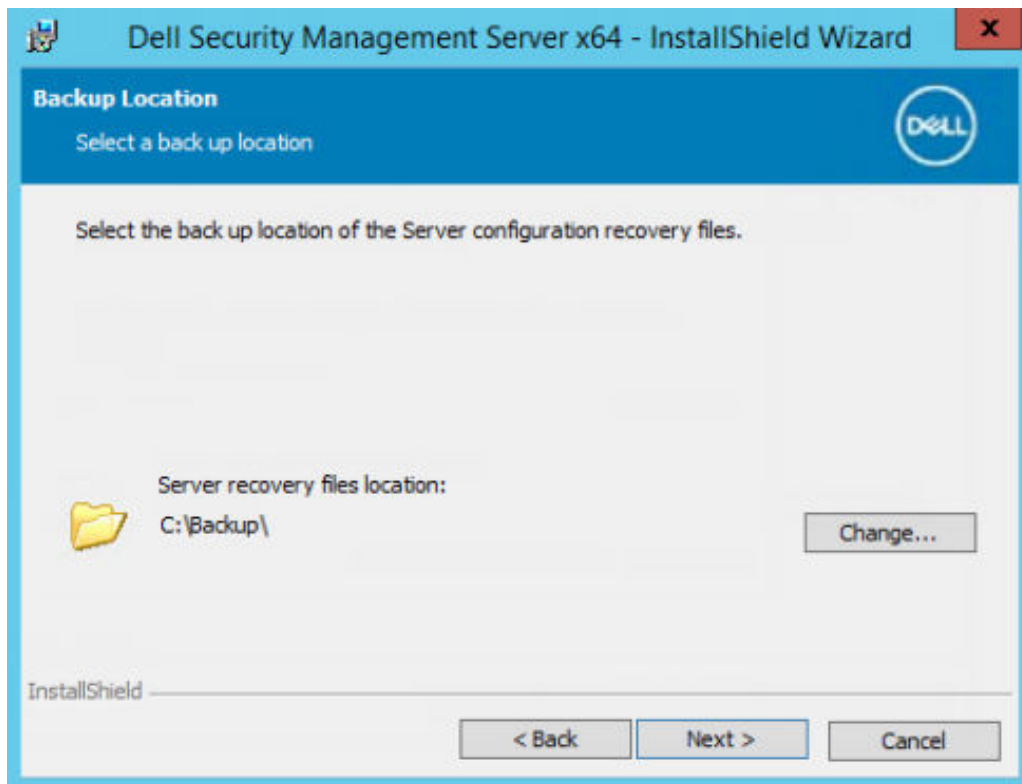


5. Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.

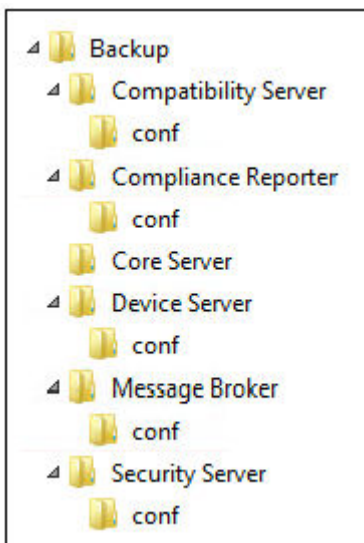


6. Para selecionar um local de armazenamento do backup dos arquivos de configuração, clique em **Alterar**, navegue até a pasta desejada e clique em **Avançar**.

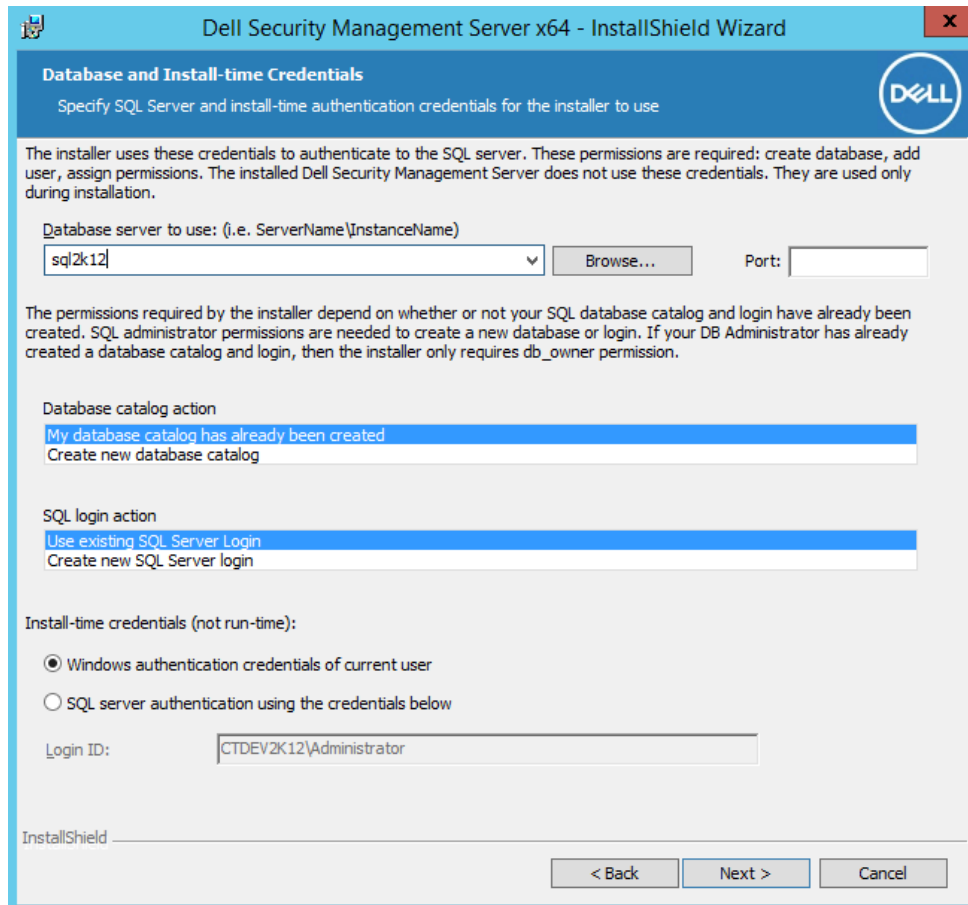
A Dell recomenda que você selecione um local de rede remoto ou uma unidade externa para o backup.



A estrutura de pastas criada pelo instalador durante a instalação (exemplo mostrado abaixo) precisa permanecer inalterada.



7. Quando o instalador localiza corretamente o banco de dados existente, a caixa de diálogo é preenchida para você.



Para conectar-se ao banco de dados existente, especifique o método de autenticação a ser usado. Após a instalação, o produto instalado não usa credenciais aqui especificadas.

a. Selecione o tipo de autenticação do banco de dados:

- **Credenciais de autenticação do Windows do usuário atual**

Se você escolher Autenticação do Windows, as mesmas credenciais usadas para fazer login no Windows são usadas para autenticação (os campos *Nome de usuário* e *Senha* não podem ser editados).

Confirme que a conta tenha direitos de administrador de sistema e a capacidade de gerenciar o SQL Server. A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: *dbo* e Associação à função de banco de dados: *dbo\_owner*, público.

**OU**

- **Autenticação do SQL Server usando as credenciais abaixo**

Se você usar a autenticação SQL, a conta SQL usada precisa ter direitos de administrador do sistema no SQL Server.

O instalador precisa ser autenticado para o SQL Server com estas permissões: criar banco de dados, adicionar usuário, atribuir permissões.

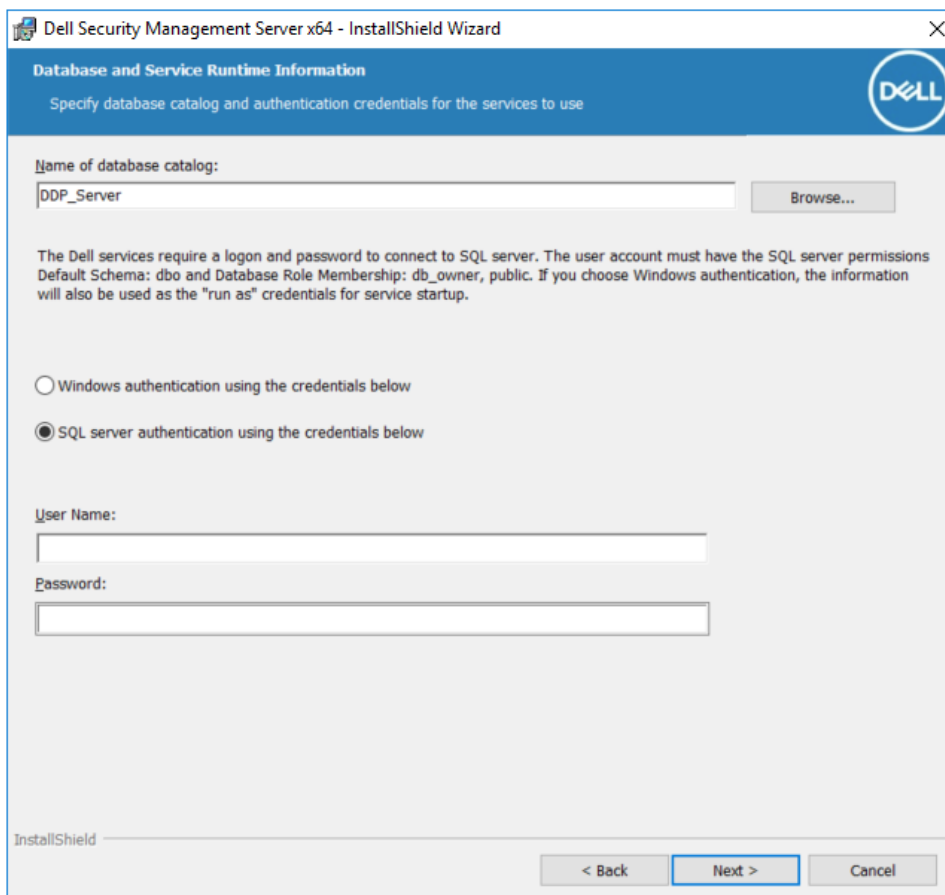
b. Clique em **Avançar**.

8. Se a caixa de diálogo Informações da conta de tempo de execução do serviço não for preenchida automaticamente, especifique o método de autenticação que o produto deve usar após a instalação.

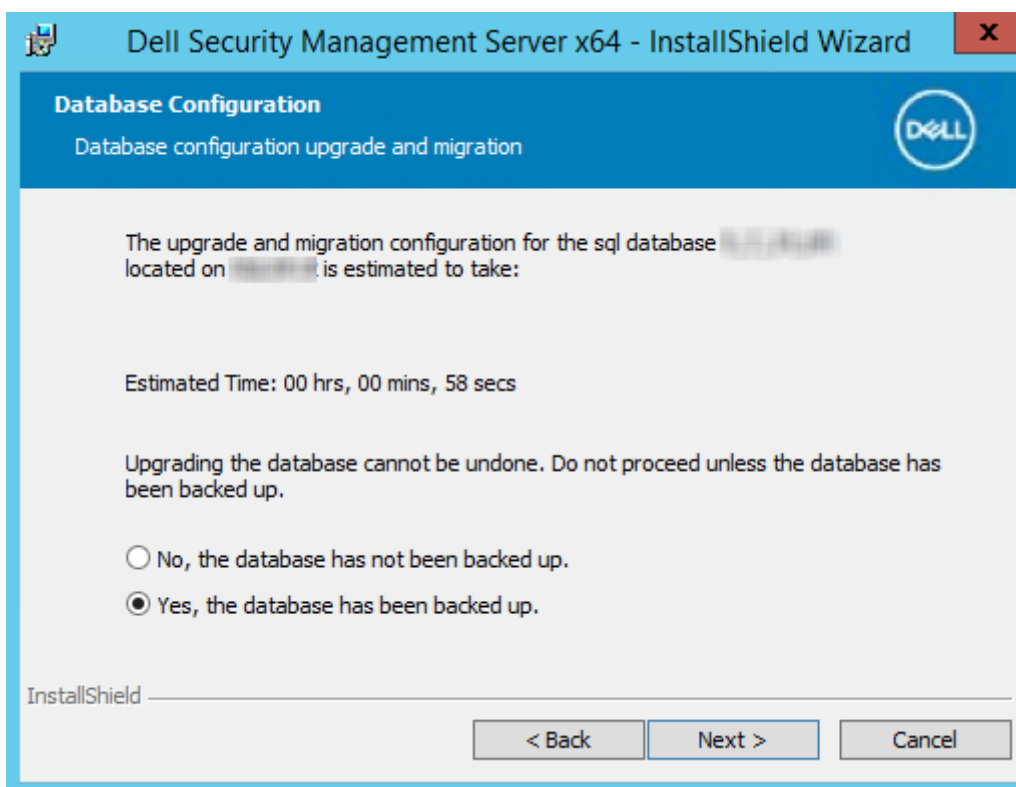
a. Selecione o tipo de autenticação.

b. Insira o nome de usuário e a senha da conta de serviço de domínio que os serviços Dell usarão para acessar o SQL Server, e clique em **Avançar**.

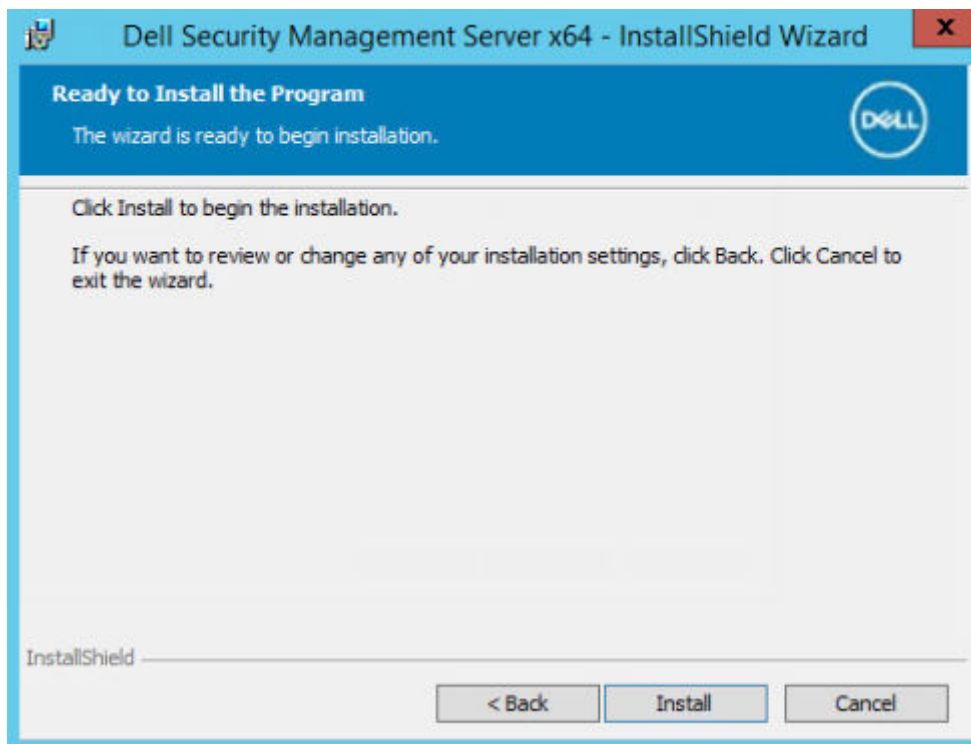
A conta de usuário precisa estar no formato *DOMAIN\Username* e ter o esquema padrão de permissões do SQL Server: *dbo* e a Associação à função de banco de dados: *dbo\_owner*, público.



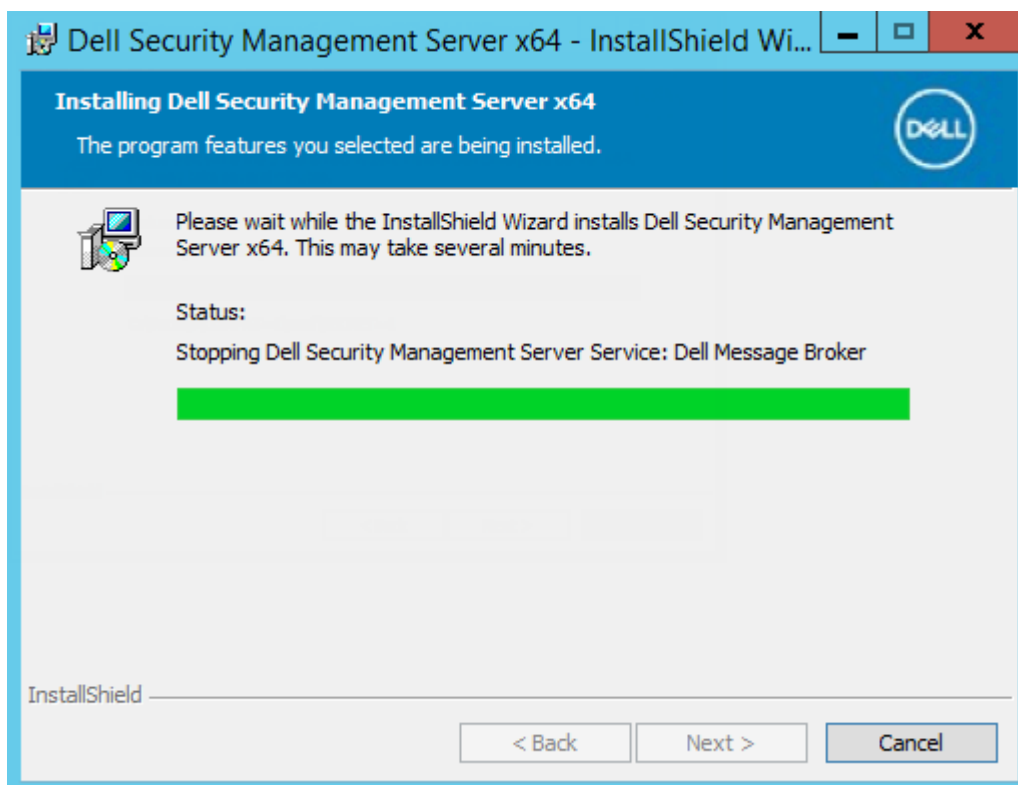
9. Se o backup do banco de dados não tiver sido feito, você **precisará** fazer o backup dele antes de continuar a instalação. **O upgrade do banco de dados não poderá ser revertido.** Apenas após a realização do backup do banco de dados, selecione **Sim, foi realizado o backup do banco de dados** e clique em **Avançar**.



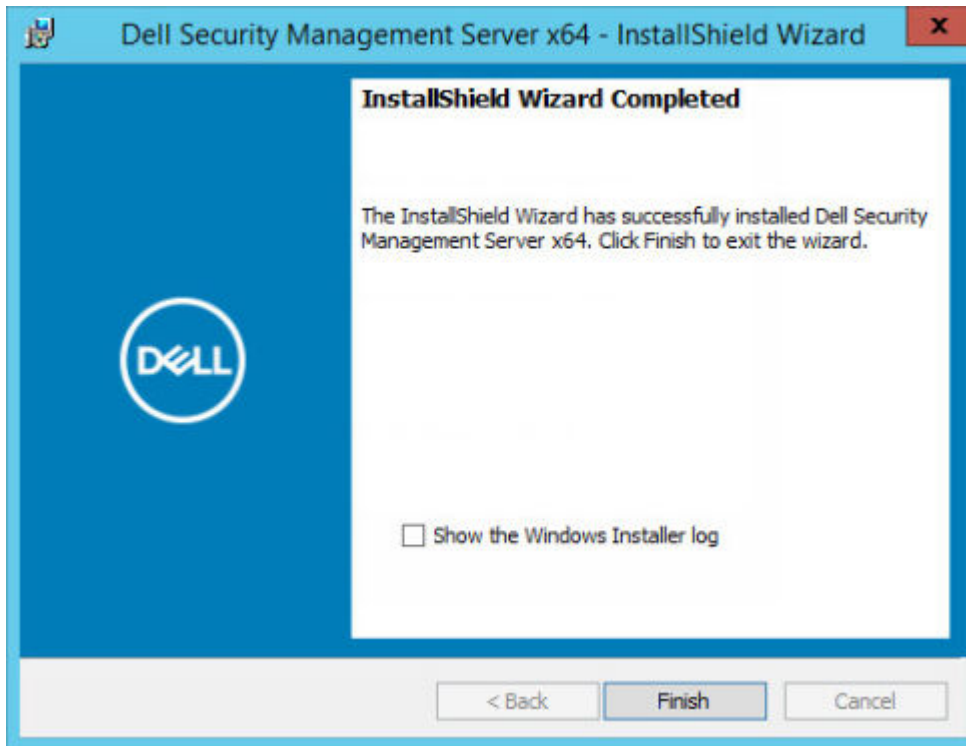
10. Clique em **Instalar** para iniciar a instalação.



Uma caixa de diálogo do progresso mostra o status de todo o processo de upgrade.



11. Ao terminar a instalação, clique em **Concluir**.



Os Serviços Dell são reiniciados ao final da migração. Não é necessário reinicializar o Dell Server.

O instalador executa as etapas de 12 a 13 para você. É uma prática recomendada verificar esses valores para assegurar que as alterações tenham sido feitas corretamente.

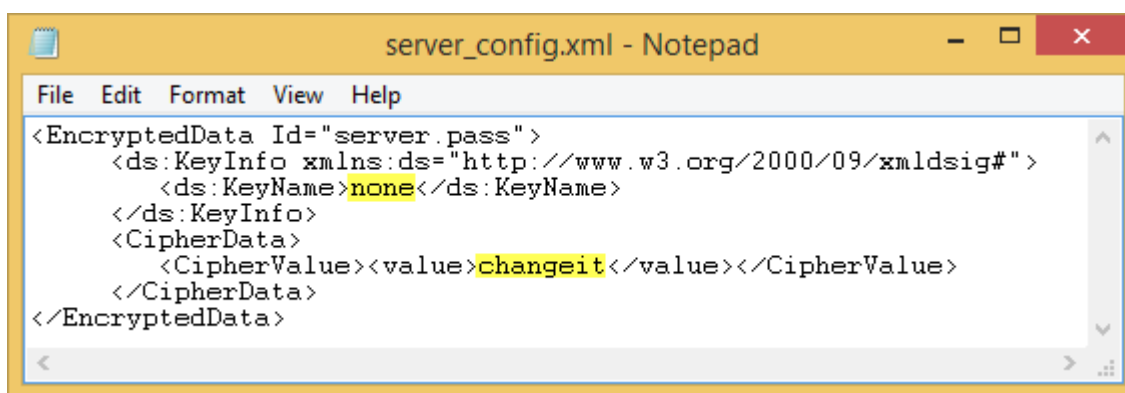
12. Na sua instalação armazenada, copie/cole: <diretório de instalação do Compatibility Server>\conf\secretKeyStore na nova instalação:  
<diretório de instalação do Compatibility Server>\conf\secretKeyStore
13. Na nova instalação, abra <diretório de instalação do Compatibility Server>\conf\server\_config.xml e substitua o valor **server.pass** pelo valor do <diretório de instalação do Compatibility Server>\conf\server\_config.xml, do qual foi feito backup, da seguinte forma:

**Instruções para server.pass:**

**Se você souber a senha**, consulte o arquivo server\_config.xml de exemplo e faça as seguintes alterações:

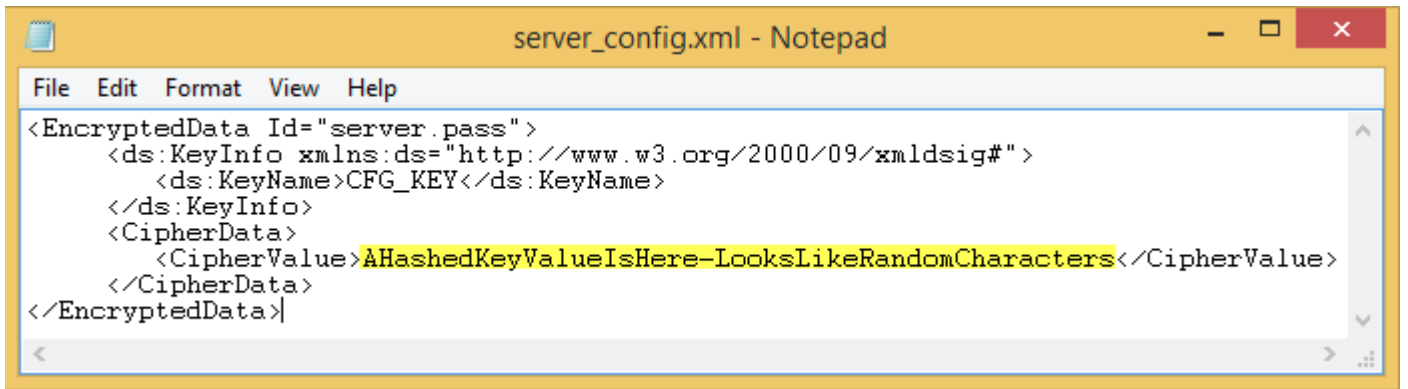
- Edite o *KeyName* do valor **CFG\_KEY** para **none**.
- Digite a senha com texto sem formatação e coloque-a entre <value> </value>, que neste exemplo é <value>changeit</value>
- Quando o Security Management Server for iniciado, a senha com texto sem formatação terá hash, e o valor de hash substituirá o texto sem formatação.

**Senha Conhecida**



**Se você não souber a senha**, recorte e cole a seção similar à seção mostrada na Figura 4-2 do arquivo <diretório de instalação do Compatibility Server>\conf\server\_config.xml armazenado na seção correspondente do novo arquivo server\_config.xml.

**Senha Desconhecida**



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

Salve e feche o arquivo.

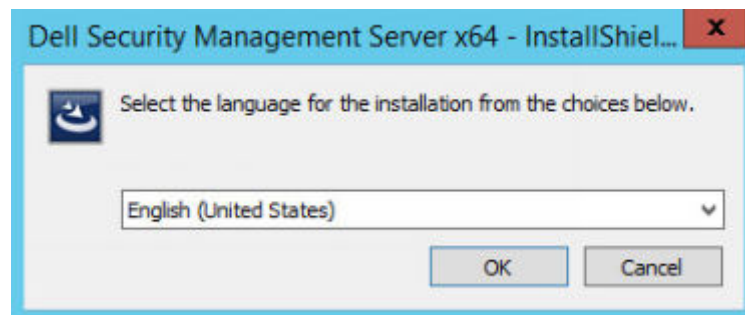
**NOTA:**

Não tente alterar a senha do Security Management Server editando o valor `server.pass` no `server_config.xml` em nenhum outro momento. Se você alterar esse valor, perderá o acesso ao banco de dados.

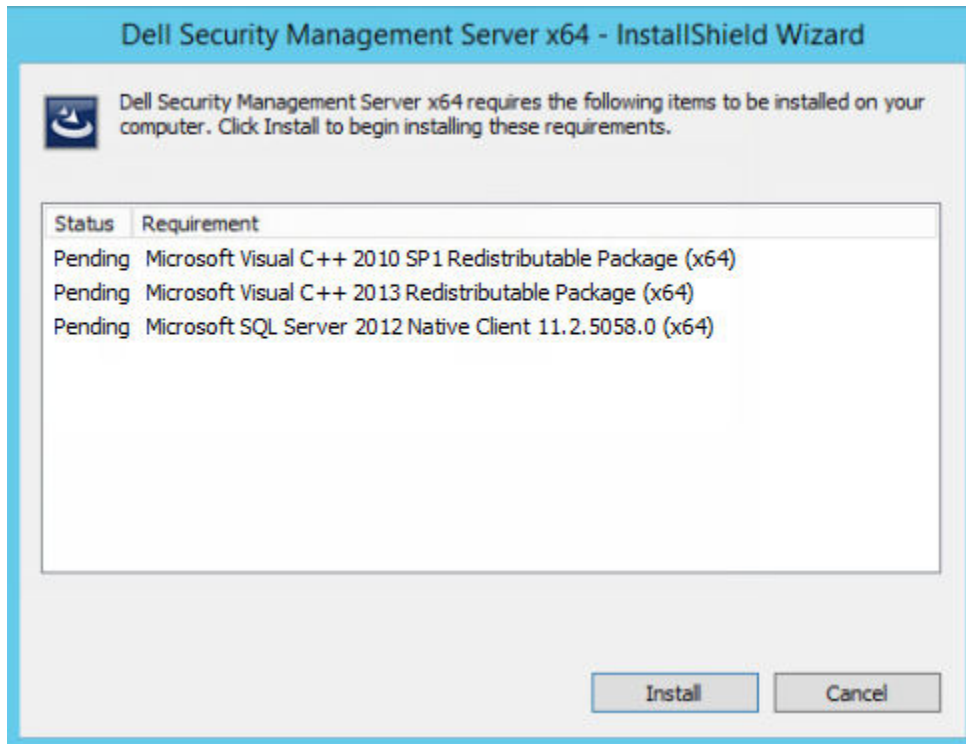
As tarefas de migração do servidor de back-end estão concluídas.

## Atualizar/migrar servidor(es) de front-end

1. Na mídia de instalação Dell, navegue até o diretório do Security Management Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Security Management Server-x64 no diretório raiz do servidor onde você está instalando o Security Management Server. **Copiar/colar ou arrastar/soltar produz erros e causa uma instalação malsucedida.**
2. Clique duas vezes em **setup.exe**.
3. Selecione o idioma para a instalação e clique em **OK**.



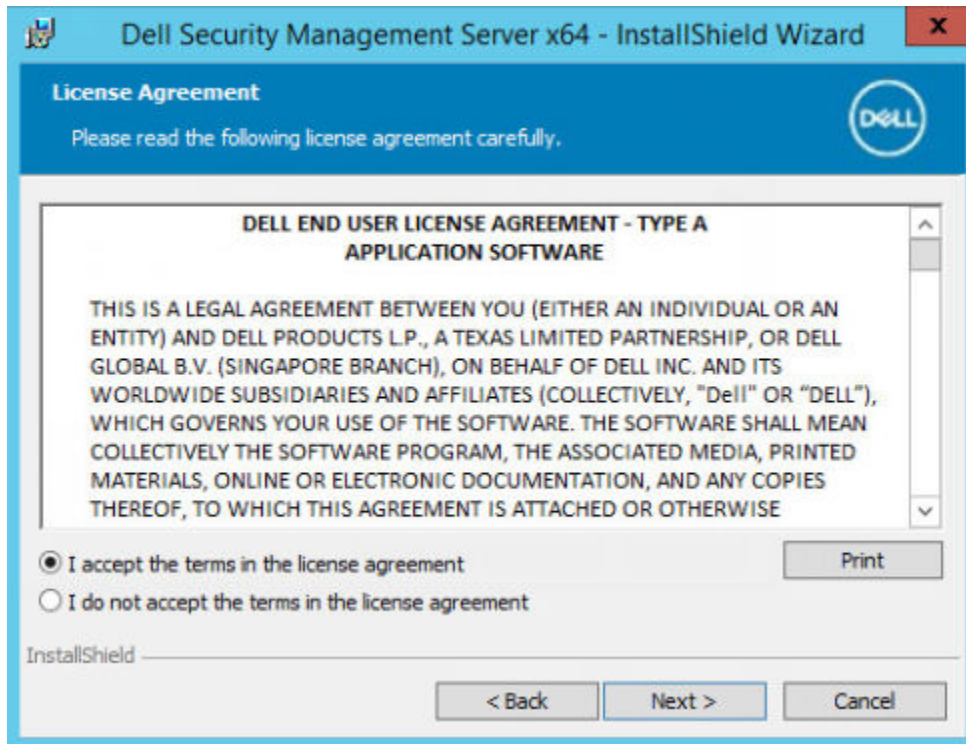
4. Se os pré-requisitos ainda não estiverem instalados, será mostrada uma mensagem informando quais pré-requisitos serão instalados. Clique em **Instalar**.



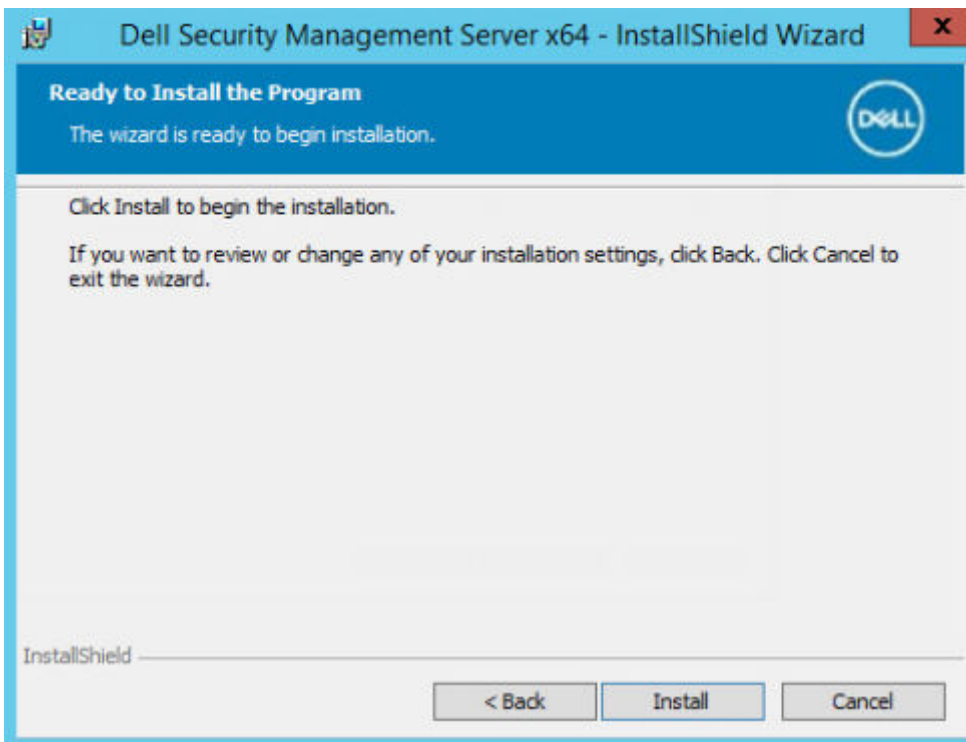
5. Na caixa de diálogo *Bem-vindo*, clique em **Avançar**.



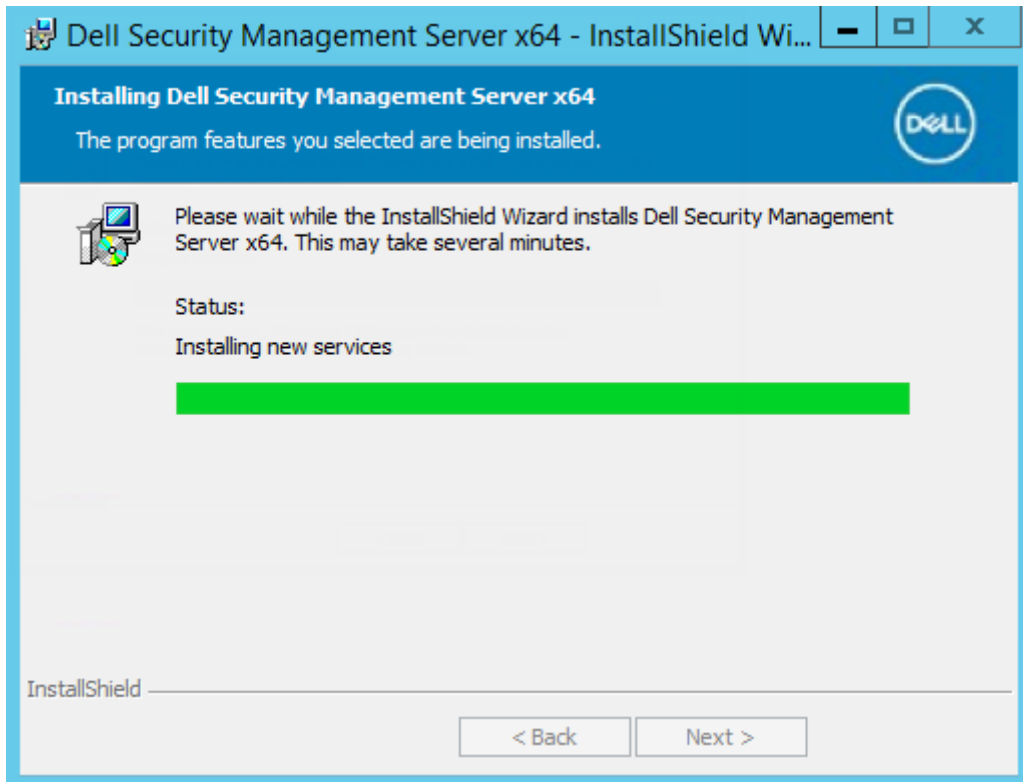
6. Leia o contrato de licença, aceite os termos e condições e clique em **Avançar**.



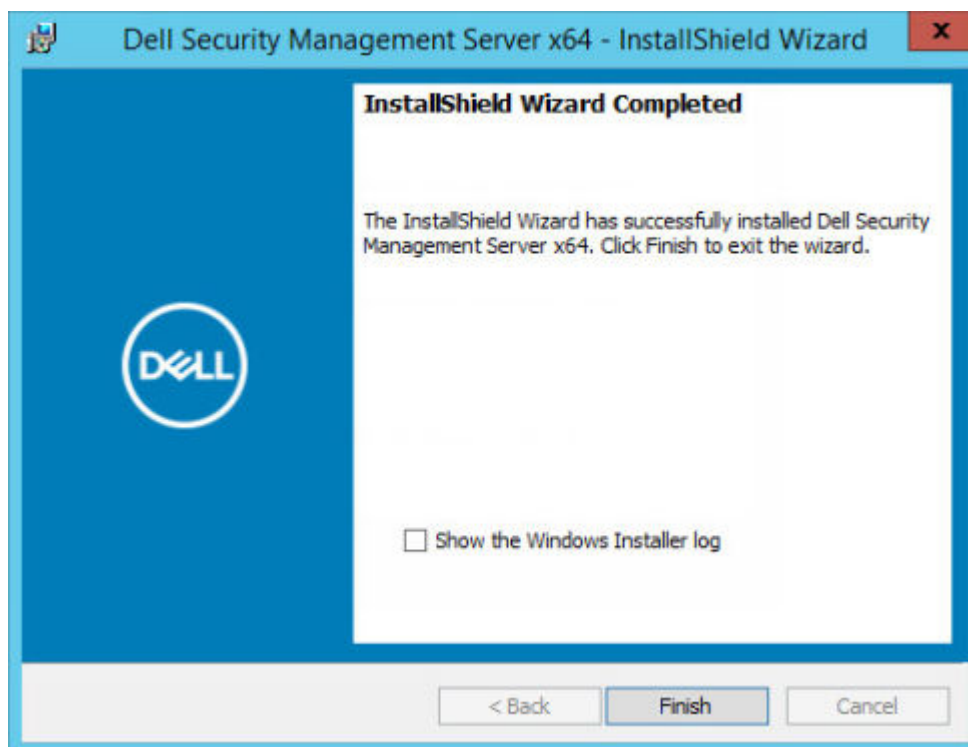
7. Na caixa de diálogo *Pronto para instalar o programa*, clique em **Instalar**.



Uma caixa de diálogo do progresso mostra o status de todo o processo de instalação.



8. Ao terminar a instalação, clique em **Concluir**.



9. Configure o servidor de back-end para comunicar-se com o servidor de front-end.
- No servidor de back-end, vá para <diretório de instalação do Security Server>\conf\ e abra o arquivo application.properties.
  - Localize publicdns.server.host e defina o nome para um hostname resolvido externamente.
  - Localize publicdns.server.port e defina a porta (o padrão é 8443).

Os Serviços Dell são reiniciados ao final da instalação. Não é necessário reinicializar o Dell Server até que as tarefas de configuração pós-instalação sejam concluídas.

# Instalação em modo Desconectado

O modo Desconectado isola o Security Management Server da Internet e de uma LAN não protegida ou outra rede. Após o Security Management Server ser instalado em modo Desconectado, ele permanecerá nesse modo e não poderá voltar para o modo Conectado.

O Security Management Server é instalado em modo Desconectado na linha de comando.

A tabela a seguir mostra os switches disponíveis.


Switch	Significado
/v	Passa as variáveis para o .msi dentro do *.exe
/s	Modo silencioso

A tabela a seguir mostra as opções de exibição disponíveis.

Opção	Significado
/q	Não há caixa de diálogo de andamento, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de andamento com o botão <b>Cancelar</b>
/qn	Sem interface do usuário

A tabela a seguir detalha os parâmetros disponíveis para a instalação. Esses parâmetros podem ser especificados na linha de comando ou invocados a partir de um arquivo, usando a propriedade:

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

Parâmetros
AGREE_TO_LICENSE=Yes - Esse valor deve ser "Sim".
PRODUCT_SN=xxxxx - Opcional se você tiver as informações da licença no local padrão; caso contrário, digite-o aqui.
INSTALLDIR=<path> - Opcional.
BACKUPDIR=<path> - Os arquivos de recuperação são armazenados neste local.
 <b>NOTA:</b> A estrutura de pastas criada pelo instalador durante esta etapa de instalação (exemplo mostrado abaixo) precisa permanecer inalterada.
AIRGAP=1 - Este valor deve ser "1" para instalar o Security Management Server em modo Desconectado.
SSL_TYPE=n - Onde n é 1 para importar um certificado existente que foi comprado a partir de uma autoridade CA e 2 para criar um certificado autoassinado. O valor SSL_TYPE determina quais propriedades de SSL são obrigatórias. Os itens a seguir são obrigatórios com SSL_TYPE=1: SSL_CERT_PASSWORD=xxxxx SSL_CERT_PATH=xxxxx Os itens a seguir são obrigatórios com SSL_TYPE=2: SSL_CITYNAME SSL_DOMAINNAME SSL_ORGNAME SSL_UNITNAME SSL_COUNTRY - Opcional, padrão = "US" SSL_STATENAME

## Parâmetros

SSOS\_TYPE=n - Onde n é 1 para importar um certificado existente que foi comprado a partir de uma autoridade CA e 2 para criar um certificado autoassinado. O valor SSOS\_TYPE determina quais propriedades de SSOS são obrigatórias.

Os itens a seguir são obrigatórios com SSOS\_TYPE=1:

SSOS\_CERT\_PASSWORD=xxxxx

SSOS\_CERT\_PATH=xxxxx

Os itens a seguir são obrigatórios com SSOS\_TYPE=2:

SSOS\_CITYNAME

SSOS\_DOMAINNAME

SSOS\_ORGNAME

SSOS\_UNITNAME

SSOS\_COUNTRY - Opcional, padrão = "US"

SSOS\_STATENAME

DISPLAY\_SQLSERVER - Este valor é analisado para obter informações do servidor SQL, da instância e da porta.

Exemplo:

DISPLAY\_SQLSERVER=SQL\_server\Server\_instance, port

IS\_AUTO\_CREATE\_SQLSERVER=FALSE - Opcional. O valor padrão é FALSE, o que significa que o banco de dados não é criado. O banco de dados já deve existir no servidor.

Para criar um novo banco de dados, defina esse valor como TRUE.

IS\_SQLSERVER\_AUTHENTICATION=0 - Opcional. O valor padrão é 0, o que especifica que as credenciais de autenticação do Windows do usuário atual conectado são usadas para fazer autenticação no SQL Server. Para usar autenticação SQL, defina esse valor como 1.

**NOTA:** O instalador precisa ser autenticado para o SQL Server com estas permissões: criar banco de dados, adicionar usuário, atribuir permissões. As credenciais são credenciais de instalação, não credenciais de tempo de uso.

Se a autenticação SQL for usada, o seguinte é obrigatório:

IS\_SQLSERVER\_USERNAME

IS\_SQLSERVER\_PASSWORD

EE\_SQLSERVER\_AUTHENTICATION - Obrigatório. Especifique o método de autenticação a ser usado pelo produto. Esta etapa conecta uma conta ao produto. Essas credenciais são usadas, também, pelos serviços Dell, para operar com o Security Management Server. Para usar autenticação do Windows, defina esse valor como 0. Para usar autenticação SQL, defina o valor como 1.

**NOTA:** Confirme que a conta tenha direitos de administrador de sistema e a capacidade de gerenciar o SQL Server. A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Associação à função de banco de dados: dbo\_owner, público.

SQL\_EE\_USERNAME - Obrigatório. Com autenticação do Windows, utilize o seguinte formato: DOMÍNIO\Nomedusuário. Com a autenticação SQL, especifique o nome do usuário.


SQL\_EE\_PASSWORD - Obrigatório. Especifique a senha associada ao nome de usuário do Windows ou SQL.

Se a autenticação SQL for usada (EE\_SQLSERVER\_AUTHENTICATION=1), o seguinte é válido:

RUNAS\_KEYSERVER\_USER - Defina o Key Server para "executar como" nome de usuário do Windows neste formato: Domínio \Usuário. Precisa ser uma conta de usuário do Windows.

RUNAS\_KEYSERVER\_PSWD - Defina o Key Server para "executar como" senha do Windows associada à conta de usuário do Windows.

SQL\_ADD\_LOGIN=T - Opcional. O padrão é "null" (esse login não é adicionado). Quando o valor é definido como T, se o SQL\_EE\_USERNAME não for um log-in ou usuário do banco de dados, o instalador tenta adicionar as credenciais de autenticação SQL do usuário e definir privilégios para permitir que as credenciais sejam usadas pelo produto.

Parâmetros
Veja a seguir os parâmetros de nome de host. Edite os nomes de host apenas se necessário. A Dell recomenda usar as configurações padrão. O formato deve ser <b>servidor.domínio.com</b> .
 <b>NOTA:</b> Um nome de host não pode conter um caractere sublinhado ("_").
CORESERTERHOST - Opcional. Hostname do Core Server.
RMIHOST - Opcional. Hostname do Compatibility Server.
REPORTERHOST - Opcional. Hostname do Compliance Reporter.
DEVICEHOST - Opcional. Hostname do Device Server.
KEYSERVERHOST - Opcional. Hostname do Key Server.
TIGAHOST - Opcional. Hostname do Security Server.
SMTP_HOST - Opcional. Hostname do SMTP.
ACTIVEMQHOST - Opcional. Hostname do Message Broker.
Veja a seguir os parâmetros de porta. Edite as portas apenas se necessário. A Dell recomenda usar as configurações padrão
SERVERPORT_CLIENTAUTH - Opcional.
REPORTERPORT - Opcional.
DEVICEPORT - Opcional.
KEYSERVERPORT - Opcional.
GKPORT - Opcional.
TIGAPORT - Opcional.
SMTP_PORT - Opcional.
ACTIVEMQ_TCP - Opcional.
ACTIVEMQ_STOMP - Opcional.

## Instalar o Security Management Server em modo Desconectado

O exemplo a seguir instala o Security Management Server no modo silencioso com uma caixa de diálogo de andamento, usando parâmetros de instalação listados no arquivo, C:\mysetups\eeoptions.txt " "

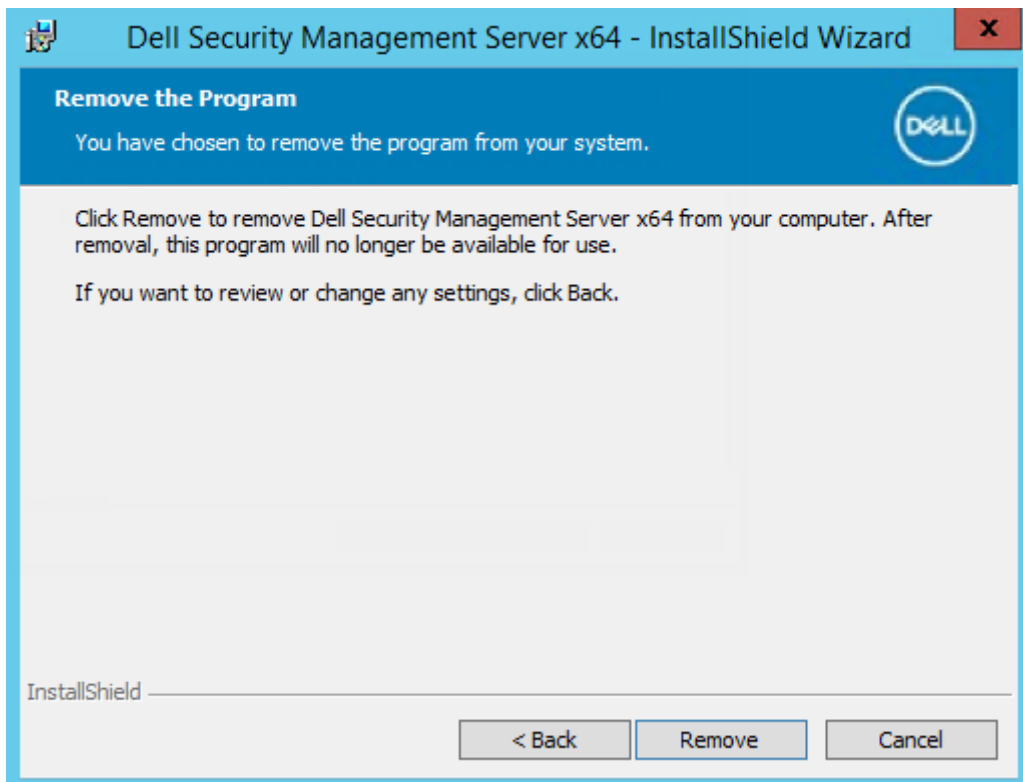
```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE="C:\mysetups\eeoptions.txt" " "
```

## Desinstalar o Security Management Server

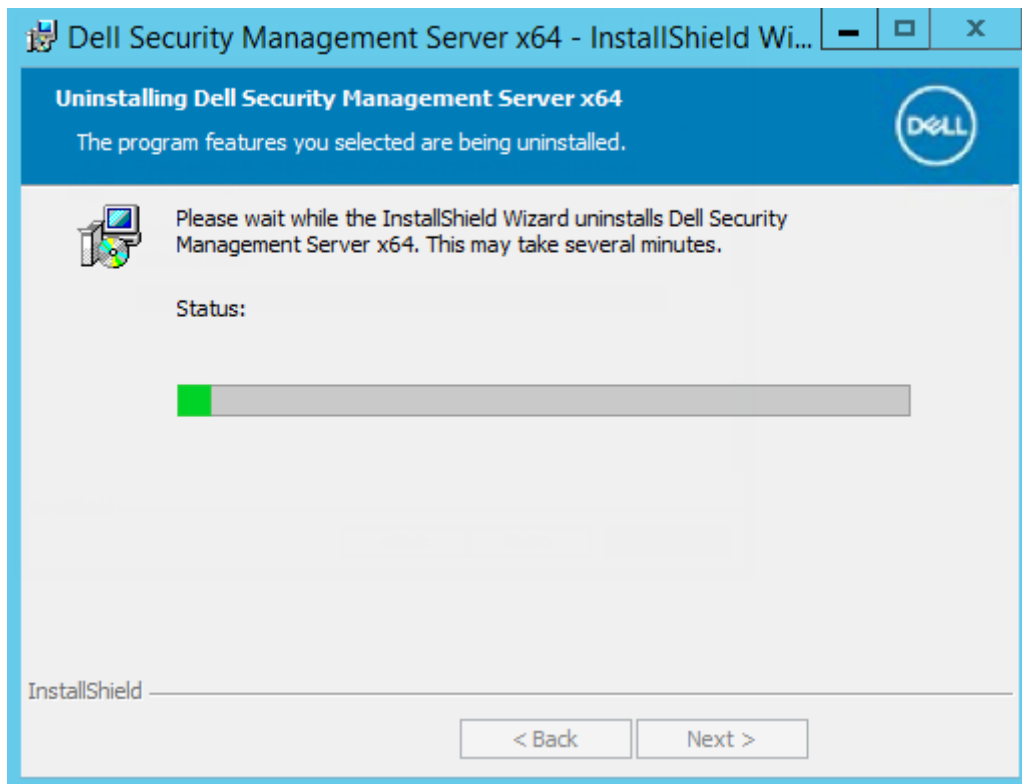
1. Na mídia de instalação Dell, navegue até o diretório do Security Management Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Security Management Server-x64 no diretório raiz do servidor de onde você está desinstalando o Security Management Server. **Copiar/colar ou arrastar/soltar produz erros e causa uma instalação malsucedida.**
2. Clique duas vezes em **setup.exe**.
3. Na caixa de diálogo *Bem-vindo*, clique em **Avançar**.



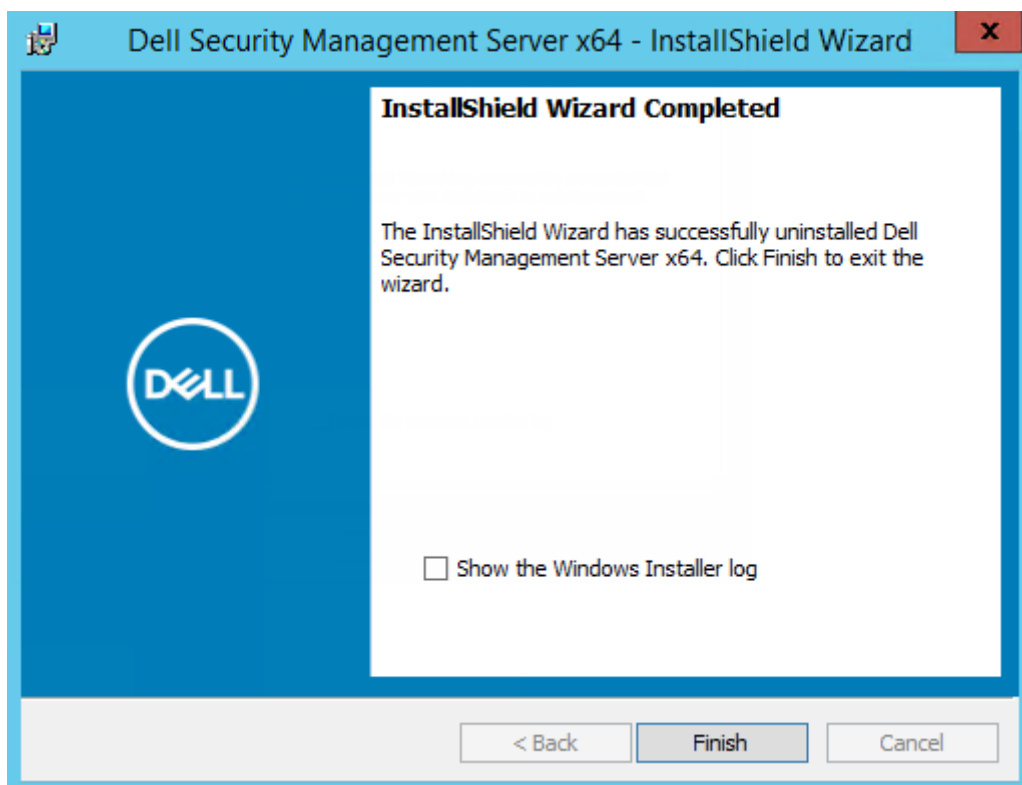
4. Na caixa de diálogo *Remover o programa*, clique em **Remover**.



Uma caixa de diálogo do progresso mostra o status de todo o processo de desinstalação.



5. Ao terminar a instalação, clique em **Concluir**.



## Configuração pós-instalação

Leia os relatórios técnicos do *Security Management Server* para conhecer qualquer solução atual ou problema conhecido relacionado à configuração do Security Management Server.

Se você estiver instalando o Security Management Server pela primeira vez ou se estiver fazendo o upgrade de uma instalação existente, alguns componentes do seu ambiente devem ser configurados.

Depois de instalar o Security Management Server, os seguintes padrões devem ser alterados:

- Alterar a senha do servidor de back-end no seguinte local:

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

- Alterar a senha de cada servidor de front-end em seu ambiente no seguinte local:

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

A senha é exibida da seguinte forma: `proxy-server.password=ENC (<textthere>)`

Para alterar a senha:

1. Selecione: `ENC (<textthere>)`
2. Altere o texto selecionado para: `CLR (<newpasswordhere>)`


Após o serviço reiniciar, a linha é alterada para `ENC` de `CLR` e a senha é criptografada.

**NOTA:** o `proxy-server.username` também pode ser modificado, mas isto deve corresponder ao arquivo `application.properties` do Message Broker e a todos os servidores de front-end ativos.

## Configuração do Modo DMZ

Se o Security Server for implementado em uma DMZ e uma rede privada, e apenas o servidor de DMZ tiver um certificado de domínio de uma Autoridade de Certificação (CA) confiável, algumas etapas manuais serão necessárias para adicionar o certificado confiável ao armazenamento de chaves Java da rede privada do Security Server.

Se um certificado confiável estiver sendo usado, desconsidere esta seção.

 **NOTA:** A Dell recomenda fortemente o uso de certificados de domínio de uma Autoridade de Certificação confiável para os servidores DMZ e de rede privada.

Para obter informações sobre a atualização do certificado do Dell Encryption com um certificado existente no armazenamento de chaves da Microsoft, consulte <http://www.dell.com/support/article/us/en/19/sln297240/>.

## Ferramenta de configuração do servidor

Quando for necessário configurar seu ambiente depois de terminar sua instalação, use o Server Configuration Tool para fazer as alterações.

O Server Configuration Tool permite:

- [Adicionar certificados novos ou atualizados](#)
- [Importar o Certificado do Dell Manager](#)
- [Importar certificado de identidade](#)
- [Definir as configurações para o certificado SSL do servidor](#)
- [Definir configurações de SMTP para serviços de e-mail](#)
- [Alterar nome, local ou credenciais do banco de dados](#)
- [Migrar o banco de dados](#)

O Dell Core Server e o Compatibility Server não podem ser executados simultaneamente com o Server Configuration Tool. Pare o serviço Core Server e o serviço Compatibility Server em *Serviços* (**Iniciar > Executar**. Digite **services.msc**) antes de iniciar o Server Configuration Tool.

Para abrir a Server Configuration Tool, vá para **Iniciar > Dell > Executar Server Configuration Tool**.

Os logs da Server Configuration Tool são salvos em C:\Program Files\Dell\Enterprise Edition\Server Configuration Tool\Logs.

## Adicionar certificados novos ou atualizados

Você tem a opção do tipo de certificado que deseja usar - autoassinado ou assinado:

- **Autoassinados** são assinados pelo próprio criador. Certificados autoassinados são apropriados para pilotos, POCs e assim por diante. Para um ambiente de produção, a Dell recomenda certificados assinados por CA pública ou assinados por domínio.
- **Assinados** (assinados por CA pública ou assinados por domínio) são assinados por uma CA pública ou um domínio. Para certificados assinados por uma autoridade de certificação (CA) pública, o certificado da CA, normalmente, já existe no armazenamento de certificados da Microsoft e, portanto, a cadeia de confiança será automaticamente estabelecida. Nos certificados assinados por autoridade de certificação de domínio, se a estação de trabalho tiver se aderido ao domínio, o certificado da autoridade de certificação do domínio terá sido adicionada ao armazenamento de certificados da Microsoft da estação de trabalho, criando assim também uma cadeia de confiança.

Os componentes que serão afetados pela configuração do certificado:

- Serviços Java (por exemplo, Device Server, e assim por diante)
- Aplicativos .NET (Core Server)
- Validação de smart cards usados para Autenticação de Pré-Inicialização (Security Server)
- Importação de uma chave de criptografia privada a ser usada em pacotes de políticas de assinatura enviados ao Dell Manager O Dell Manager executa a validação SSL para clients Encryption gerenciados com unidades de autcriptografia ou BitLocker Manager.
- Estações de trabalho de client:
  - Estações de trabalho que executam BitLocker Manager
  - Estações de trabalho que executam o Encryption Enterprise (Windows)
  - Estações de trabalho que executam o Endpoint Security Suite Enterprise

### **Informações sobre os tipos de certificados a serem usados:**

A autenticação de pré-inicialização usando smart cards exige validação de SSL com o Security Server. O Dell Manager executa a validação do SSL ao conectar-se ao Dell Core Server. Para esses tipos de conexão, a CA assinante deve estar no armazenamento de chaves (seja do Java ou da Microsoft, dependendo do componente do Dell Server em questão). Se forem escolhidos certificados autoassinados, as seguintes opções estarão disponíveis:

- Validação dos cartões inteligentes usados para a Autenticação de Pré-Inicialização:
  - Importe o certificado de assinatura "Agência Raiz" e a cadeia de confiança completa para o armazenamento de chaves do Java do Security Server. A cadeia de confiança completa precisa ser importada.

Dell Manager:

- Insira o certificado de assinatura "Agência Raiz" (do certificado autoassinado gerado) nas "Autoridades de certificação raiz confiáveis" da estação de trabalho (para "computador local") no armazenamento de chaves da Microsoft.

O Security Management Server é compatível com o requisito da Microsoft de vinculação de canal LDAP e assinatura LDAP quando o Active Directory está em uso.

Para ativar isso no Security Management Server, ele deve ter o certificado de emissão da raiz para os certificados do controlador de domínio importados para o armazenamento de "Raiz confiável" dentro do armazenamento de chaves de certificados da Microsoft.

- Modifique o comportamento da validação de SSL do lado do servidor. Para desativar a validação do SSL do lado do servidor, selecione **Desativar verificação da cadeia de confiança** na guia Configurações.

Há dois métodos para criar um certificado – *Expresso* e *Avançado*.

Escolha **um** método:

- **Expresso** – Escolha este método para gerar um certificado autoassinado para todos os componentes. Este é o método mais fácil, mas os certificados autoassinados são adequados apenas para pilotos, POCs, e assim por diante. Para um ambiente de produção, a Dell recomenda certificados assinados por CA pública e assinados por domínio.

- **Avançado** – Escolha este método para configurar cada componente separadamente.

### Expresso

1. No menu superior, selecione **Ações > Configurar certificados**.
2. Quando o Assistente de configuração abrir, selecione **Expresso** e clique em **Avançar**. As informações do certificado autoassinado que foi criado durante a instalação do Security Management Server são usadas, se estiverem disponíveis.
3. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.

A configuração do certificado está concluída. O resto desta seção detalha o método Avançado de criação de um certificado.

### Avançado

Há dois caminhos para criar um certificado – *Gerar certificado autoassinado* e *Usar configurações atuais*. Escolha **um** caminho:

- **Caminho 1 – Gerar certificado autoassinado**
- **Caminho 2 – Usar configurações atuais**

#### Caminho 1 – Gerar certificado autoassinado

1. No menu superior, selecione **Ações > Configurar certificados**.
2. Quando o Assistente de configuração abrir, selecione **Avançado** e clique em **Avançar**.
3. Selecione **Gerar certificado autoassinado** e clique em **Avançar**. As informações do certificado autoassinado que foi criado durante a instalação do Security Management Server são usadas, se estiverem disponíveis.
4. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.

A configuração do certificado está concluída. O resto desta seção detalha o outro método de criação de um certificado.

#### Caminho 2 – Usar configurações atuais

1. No menu superior, selecione **Ações > Configurar certificados**.
2. Quando o Assistente de configuração abrir, selecione **Avançado** e clique em **Avançar**.
3. Selecione **Usar configurações atuais** e clique em **Avançar**.
4. Na janela *Certificado SSL do Compatibility Server*, selecione **Gerar certificado autoassinado** e clique em **Avançar**. As informações do certificado autoassinado que foi criado durante a instalação do Security Management Server são usadas, se estiverem disponíveis. Clique em **Avançar**.
5. Na janela *Certificado SSL do Core Server*, selecione uma das seguintes opções:
  - **Selecionar certificado** - selecione essa opção para usar um certificado existente. Clique em **Avançar**.  
Vá até o local do certificado existente, digite a senha associada ao certificado existente e clique em **Avançar**.  
Clique em **Concluir** quando terminar.
  - **Gerar certificado autoassinado** – As informações do certificado autoassinado que foi criado durante a instalação do Security Management Server são usadas, se estiverem disponíveis. Se essa opção for selecionada, a janela Certificado de segurança de mensagens não aparecerá (a janela aparece se você selecionar a opção *Usar configurações atuais*) e o certificado criado para o Dell Compatibility Server será usado.  
Verifique se o nome do computador totalmente qualificado está correto. Clique em **Avançar**.  
Uma mensagem de aviso é mostrada, informando que o nome já existe. Quando for perguntado se quer usá-lo, clique em **Sim**.  
Clique em **Concluir** quando terminar.
  - **Usar configurações atuais** – selecione essa opção para alterar uma configuração em um certificado a qualquer momento após a configuração inicial do Security Management Server. A seleção dessa opção não altera o certificado já configurado. A seleção dessa opção leva para a janela Certificado de segurança de mensagens.  
Em Certificado de segurança de mensagens, selecione **uma** das seguintes opções:
    - **Selecionar certificado** - selecione essa opção para usar um certificado existente. Clique em **Avançar**.  
Vá até o local do certificado existente, digite a senha associada ao certificado existente e clique em **Avançar**.  
Clique em **Concluir** quando terminar.

- *Gerar certificado autoassinado* – As informações do certificado autoassinado que foi criado durante a instalação do Security Management Server são usadas, se estiverem disponíveis.

Clique em **Avançar**.

Clique em **Concluir** quando terminar.

A configuração do certificado está concluída.

Quando as alterações forem concluídas:

1. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.
2. Feche a Dell Server Configuration Tool.
3. Clique em **Iniciar > Executar**. Digite *services.msc* e clique em **OK**. Quando *Serviços* abrir, acesse cada Serviço da Dell e clique em **Iniciar o serviço**.

## Importar o Certificado do Dell Manager

Se a sua implementação inclui clientes Security Management Server gerenciados remotamente com Encryption Management Agents, você precisa importar seu certificado recém-criado (ou já existente). O certificado do Dell Manager é usado como um meio de proteger a chave privada usada para assinar os pacotes de política que são enviados aos clientes Security Management Server remotamente gerenciados e ao Encryption Management Agent. Esse certificado pode ser independente de qualquer outro certificado. Além disso, se essa chave estiver comprometida, ela pode ser substituída por uma nova chave, e o Dell Manager solicitará uma nova chave pública caso não possa descriptografar os pacotes de política.

1. Abra o Console de Gerenciamento Microsoft.
2. Clique em **Arquivo > Adicionar/remover snap-in**.
3. Clique em **Adicionar**.
4. Na janela *Adicionar snap-in autônomo*, selecione **Certificados** e clique em **Adicionar**.
5. Selecione **Conta de computador** e clique em **Avançar**.
6. Na janela *Selecionar computador*, selecione **Computador local (o computador no qual o console está sendo executado)** e clique em **Concluir**.
7. Clique em **Fechar**.
8. Clique em **OK**.
9. Na pasta *Raiz do console* expanda *Certificados (computador local)*.
10. Acesse a pasta *Pessoal* e encontre o certificado desejado.
11. Selecione o certificado desejado, clique com o botão direito em **Todas as tarefas > Exportar**.
12. Quando o Assistente para Exportação de Certificados abrir, clique em **Avançar**.
13. Selecione **Sim, exportar a chave privada** e clique em **Avançar**.
14. Selecione **Troca de Informações Pessoais - PKCS #12 (.PFX)** e selecione as subopções **Incluir todos os certificados no caminho de certificação, se possível** e **Exportar todas as propriedades estendidas**. Clique em **Avançar**.
15. Digite e confirme uma senha. Você pode escolher qualquer senha. Escolha uma senha fácil de lembrar, mas difícil de ser descoberta por outras pessoas. Clique em **Avançar**.
16. Clique em **Procurar** para ir até o local onde deseja salvar o arquivo.
17. No campo *Nome do arquivo*, digite um nome para salvar o arquivo. Clique em **Salvar**.
18. Clique em **Avançar**.
19. Clique em **Concluir**.
20. Será mostrada uma mensagem informando que a exportação foi bem-sucedida. Feche o Console de Gerenciamento Microsoft.
21. Volte para a Dell Server Configuration Tool.
22. No menu superior, selecione **Ações > Importar certificado de DM**.

23. Navegue até o local em que o arquivo exportado foi salvo. Selecione o arquivo e clique em **Abrir**.
24. Digite a senha associada ao arquivo e clique em **OK**.

A importação do certificado do Dell Manager agora está concluída.

Quando as alterações forem concluídas:

1. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.
2. Feche a Dell Server Configuration Tool.
3. Clique em **Iniciar > Executar**. Digite *services.msc* e clique em **OK**. Quando *Serviços* abrir, navegue até cada Serviço da Dell e clique em **Iniciar o serviço**.

## Importar certificado SSL/TLS BETA

Se a sua implementação inclui o Server Encryption, você precisará importar seu certificado recém-criado (ou existente). O certificado SSL/TLS BETA protege a chave privada usada para assinar os pacotes de políticas enviados aos servidores client.

1. No menu superior, selecione **Ações > Importar certificado SSL/TLS BETA**.
2. Selecione um certificado e clique em **Avançar**.
3. No prompt *Senha do certificado*, digite a senha associada ao certificado existente.
4. Na caixa de diálogo Conta do Windows, escolha uma opção:
  - a. Para alterar as credenciais associadas ao certificado de identidade, selecione **Usar credenciais diferentes da conta do Windows com o certificado de identidade**.
  - b. Para continuar usando as credenciais da conta na qual você está conectado, clique em **Avançar**.
5. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.

## Definir as configurações do certificado do SSL Server

No Server Configuration Tool, clique na guia **Configurações**.

### Dell Manager:

Para desativar a validação de confiança de SSL do Dell Manager no lado do servidor, selecione **Desativar a verificação da cadeia de confiança**.

### SCEP:

Se estiver usando o Mobile Edition, digite o URL do servidor que hospeda o SCEP.

 **NOTA:** A partir da v9.8, o Mobile Edition não é mais suportado.

Quando as alterações forem concluídas:

1. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.
2. Feche a Dell Server Configuration Tool.
3. Clique em **Iniciar > Executar**. Digite *services.msc* e clique em **OK**. Quando *Serviços* abrir, navegue até cada Serviço da Dell e clique em **Iniciar o serviço**.

## Definir as configurações do SMTP


No Server Configuration Tool, clique na guia **SMTP**.

Essa guia define as configurações de SMTP para o informativos de produtos, notificações e mensagens de retransmissão de ameaça do Advanced Threat Prevention.

Quando as alterações de configuração estiverem concluídas, reinicie o serviço do Servidor de Segurança. O serviço do Servidor de Segurança deve ser reiniciado para que as configurações sejam atualizadas.

Insira as seguintes informações:

1. Em *Nome do host*, digite o FQDN do seu servidor SMTP, como `nomedoservidoresmtp.domínio.com`
2. Em *Nome de usuário*, digite o nome de usuário que fará log-in no servidor de e-mail. O formato pode ser `DOMÍNIO\jdoe`, `jdoe` ou o formato que sua organização exigir.
3. Em *Senha*, digite a senha associada a esse nome de usuário.
4. Em *Endereço de origem*, digite o endereço de e-mail de origem. Pode ser igual ao da conta do nome de usuário (`jdoe@domain.com`), mas também pode ser de outra conta que o nome de usuário especificado tem acesso para enviar e-mail (`CloudRegistration@domain.com`).
5. Em *Porta*, digite o número da porta (normalmente 25).
6. No menu *Autenticação*, selecione *Verdadeiro* ou *Falso*.

 **NOTA:** O nome de usuário e a senha devem ficar em branco se a autenticação estiver definida como false.

Quando as alterações forem concluídas:

1. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.
2. Feche a Dell Server Configuration Tool.
3. Clique em **Iniciar > Executar**. Digite `services.msc` e clique em **OK**. Quando *Serviços* abrir, navegue até cada Serviço da Dell e clique em **Iniciar o serviço**.

## Alterar nome, local ou credenciais do banco de dados

No Server Configuration Tool, clique na guia **Banco de dados**.

1. Em *Nome do servidor*: digite o nome do domínio totalmente qualificado (se houver o nome de uma instância, inclua-o) do servidor que hospeda o banco de dados. Por exemplo, `SQLTest.domain.com\DellDB`.  
A Dell recomenda o uso de um nome de domínio totalmente qualificado, embora um endereço IP possa ser usado.
2. Em *Porta do servidor*, insira o número da porta.  
Ao usar uma instância do SQL Server que não seja a instância padrão, você precisa especificar a porta dinâmica da instância no campo *Porta*:. Como alternativa, ative o serviço SQL Server Browser e confirme que a porta UDP 1434 está aberta. Para obter mais informações, consulte [https://msdn.microsoft.com/en-us/library/hh510203\(v=sql.120\).aspx](https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx).
3. Em *Banco de dados*:, digite o nome do banco de dados.
4. Em *Autenticação*, selecione **Autenticação do Windows** ou **Autenticação do SQL Server**. Se você escolher Autenticação do Windows, as mesmas credenciais usadas para fazer login no Windows são usadas para autenticação (os campos *Nome de usuário* e *Senha* não podem ser editados).
5. Em *Nome do usuário*:, digite o nome de usuário apropriado associado a este banco de dados.
6. Em *Senha*:, digite a senha do nome de usuário listado no campo Nome do usuário.
7. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.
8. Para testar a configuração do banco de dados, no menu superior, selecione **Ações > Testar configuração do banco de dados**. O assistente de configuração é iniciado.
9. Na janela *Teste de configuração*, leia as informações de teste e clique em **Avançar**.
10. Se você escolher Autenticação do Windows na guia *Banco de dados*, poderá digitar credenciais alternativas para permitir o uso das mesmas credenciais que são usadas para executar o Security Management Server. Clique em **Avançar**.
11. Na janela *Testar Configuração*, são mostrados os resultados das configurações de conexão do teste, do teste de compatibilidade e do teste do banco de dados migrado.
12. Clique em **Concluir**.

 **NOTA:**

Se o banco de dados SQL ou a instância SQL estiverem configurados com um agrupamento que seja diferente do padrão, esse agrupamento não pode diferenciar maiúsculas de minúsculas. Para obter uma lista de agrupamentos e diferenciação de maiúsculas e minúsculas, consulte [https://msdn.microsoft.com/en-us/library/ms144250\(v=sql.105\).aspx](https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx).

Quando as alterações forem concluídas:

1. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.
2. Feche a Dell Server Configuration Tool.
3. Clique em **Iniciar > Executar**. Digite `services.msc` e clique em **OK**. Quando *Serviços* abrir, navegue até cada Serviço da Dell e clique em **Iniciar o serviço**.

## Migrar o banco de dados

Você pode migrar um banco de dados da versão 9.2 ou posterior para o esquema mais recente com a versão mais recente do servidor.

No Server Configuration Tool, clique na guia **Banco de dados**.

1. Se você ainda não tiver feito o backup do banco de dados do Dell Server existente, **faça-o agora**.
2. No menu superior, selecione **Ações > Inicializar banco de dados**. O assistente de configuração é iniciado.
3. Na janela *Migrar banco de dados do Enterprise*, um aviso é mostrado. Confirme se foi feito backup de todo o banco de dados ou se não é necessário fazer backup do banco de dados existente. Clique em **Avançar**.

Na janela *Migrando Banco de Dados*, as mensagens informativas mostram o status da migração.

Ao concluir, verifique se há algum erro.



**NOTA:** Uma mensagem de erro identificada por , significa que uma tarefa do banco de dados falhou, e uma ação corretiva deve ser tomada antes de o banco de dados ser devidamente migrado. Clique em **Concluir**, corrija os erros do banco de dados e reinicie as instruções nesta seção.

4. Clique em **Concluir**.

Quando a migração estiver concluída:

1. No menu superior, selecione **Configuração > Salvar**. Se solicitado, confirme o salvamento.
2. Feche a Dell Server Configuration Tool.
3. Clique em **Iniciar > Executar**. Digite `services.msc` e clique em **OK**. Quando *Serviços* abrir, navegue até cada Serviço da Dell e clique em **Iniciar o serviço**.

## Tarefas administrativas

### Atribuir a função de administrador Dell

1. Como administrador virtual do Security Management Server, faça login no Management Console: <https://server.domain.com:8443/webui/>. As credenciais padrão são **superadmin/changeit**.
2. No painel à esquerda, clique em **Populações > Domínios**.
3. Clique em um domínio para adicionar um usuário.
4. Na página Detalhes de domínios, clique na guia **Membros**.
5. Clique em **Adicionar usuário**.
6. Insira um filtro para pesquisar o nome de usuário por Nome comum, Nome principal universal ou sAMAccountName. O caractere curinga é \*.

Um Nome comum, Nome principal universal e sAMAccountName precisam ser definidos no servidor de diretório corporativo para cada usuário. Se um usuário for membro de um Domínio ou Grupo, mas não for exibido na lista de Membros do Domínio ou do Grupo no gerenciamento, verifique se todos os três nomes estão adequadamente definidos para o usuário no servidor de diretório corporativo.

A consulta pesquisará automaticamente o nome comum e, em seguida, o UPN e o nome sAMAccount até que uma correspondência seja encontrada.

7. Selecione os usuários na *Lista de Usuários do Diretório* para adicionar ao Domínio. Use <Shift><clique> ou <Ctrl><clique> para selecionar múltiplos usuários.
8. Clique em **Adicionar**.
9. A partir da barra de menu, clique na guia **Detalhe e Ações** do usuário específico.
10. Role pela barra de menu e selecione a guia **Admin**.
11. Selecione as funções de administrador que serão adicionadas a este usuário.
12. Clique em **Salvar**.

### Login com função de administrador Dell

1. Faça logout do Management Console.
2. Faça log-in no Management Console e faça log-in com as credenciais de usuário do Domínio.

### Carregar licença de acesso do cliente

Você recebeu licenças de acesso do cliente separadamente dos arquivos de instalação, na compra inicial ou posteriormente, caso tenha adicionado outras licenças de acesso do cliente.

1. No painel à esquerda, clique em **Gerenciamento**.
2. Clique em **Gerenciamento de licenças**.
3. Clique em **Selecionar arquivo** para localizar e selecionar o arquivo de licença do cliente.

### Confirmar políticas

Confirme as políticas quando a instalação for concluída.

Para confirmar as políticas após a instalação, ou, mais tarde, após as modificações da política serem salvas, siga estas instruções:

1. No painel à esquerda, clique em **Gerenciamento > Confirmar**.

2. Em *Comentário*, digite uma descrição da alteração.
3. Clique em **Confirmar políticas**.

## Configurar o Dell Compliance Reporter

1. No painel à esquerda, clique em **Compliance Reporter**.
2. Quando o Dell Compliance Reporter for aberto, faça login usando as credenciais padrão de superadmin/changeit.

## Realizar backups

Para fins de recuperação de desastres, certifique-se de que os seguintes locais tenham um backup efetuado semanalmente, com diferenciais noturnos. Para obter mais informações sobre o planejamento para a recuperação de desastres, consulte <http://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>. Para obter mais informações sobre como fazer o backup de dados do Compliance Reporter, consulte <http://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>.

## Backups do Security Management Server

Regularmente, faça um backup dos arquivos que estão armazenados no local que você selecionou para o backup de arquivos de configuração durante a instalação (*etapa 10 na página 27*) ou atualização/migração (*etapa 6 na página 68*). Backups semanais desses dados são aceitáveis, já que eles raramente mudam e podem ser reconfigurados manualmente, se necessário. Os arquivos mais críticos armazenam informações necessárias para a conexão com o banco de dados:

<Pasta de instalação>\Enterprise Edition\Compatibility Server\conf\server\_config.xml

<Pasta de instalação>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<Pasta de instalação>\Enterprise Edition\Compatibility Server\conf\gkconfig.xml

## SQL Server Backups

Execute os backups completos noturnos com registro de transação ativado e crie backups de bancos de dados diferenciais a cada 3 a 4 horas. Se um banco de dados estiver disponível, então a recomendação seria que os logs de transação e/ou tarefas de envio de log sejam realizadas em intervalos de 15 minutos (ou intervalos menores se possível). Como sempre, a Dell recomenda que as boas práticas de bancos de dados sejam usadas para o banco de dados do Dell Server e que o software da Dell seja incluído no plano de recuperação de desastres da sua organização.

Para obter informações adicionais sobre boas práticas do SQL Server, consulte a [lista](#) a seguir, que precisam ser implementadas quando o Dell Security for instalado, caso ainda não tenham sido implementadas.

## Backups do PostgreSQL Server

Eventos de auditoria são armazenados no PostgreSQL Server em C:\ProgramData\Dell\PostgreSQL\10.7\data, cujo backup deve ser realizado regularmente. Para obter instruções de backup, consulte </C:/ProgramData/Dell/PostgreSQL/10.7/data>.

A Dell recomenda que as boas práticas de bancos de dados sejam usadas para o banco de dados PostgreSQL e que o software da Dell seja incluído no plano de recuperação de desastres da sua organização.

## Portas

A tabela a seguir descreve cada componente e sua função.

Nome	Porta padrão	Descrição
Serviço ACL	TCP/ 8006	Gerencia várias permissões e acesso de grupo para vários produtos do Dell Security.  <i>NOTA:</i> A porta 8006 não está protegida no momento. Certifique-se de que essa porta seja filtrada corretamente por meio de um firewall. Esta porta é apenas interna.
Compliance Reporter	HTTP(S)/ 8084	Fornecer uma visão completa do ambiente para auditoria e geração de relatórios de conformidade.  <i>NOTA:</i> A porta 8084 deve ser filtrada por um firewall. A Dell recomenda que essa porta seja apenas interna.
Management Console	HTTP(S)/ 8443	A central de controles e o console de administração da implantação de toda a empresa.
Core Server	HTTPS/ 8888	Gerencia o fluxo de política, as licenças, o registro para Preboot Authentication, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa os dados de inventário para uso pelo Compliance Reporter e pelo Management Console. Coleta e armazena os dados de autenticação. Controla o acesso baseado em função.
Device Server	HTTPS/ 8081	Suporta ativações e a recuperação de senha.  Um componente do Security Management Server.  Necessário para Encryption Enterprise (Windows e Mac)
Security Server	HTTPS/ 8443	Comunica-se com o Policy Proxy; gerencia as recuperações de chave forense, ativações dos clientes, comunicação SED-PBA e Full Disk Encryption-PBA e Active Directory para autenticação e reconciliação, incluindo validação da identidade para a autenticação no Management Console. Precisa de acesso ao banco de dados SQL.

Nome	Porta padrão	Descrição
Compatibility Server	TCP/ 1099	Um serviço para gerenciar a arquitetura corporativa. Coleta e armazena os dados iniciais de inventário durante a ativação e os dados de política durante as migrações. Processa os dados baseados em grupos de usuário.  <b>i</b> <b>NOTA:</b> A porta 1099 deve ser filtrada por um firewall. A Dell recomenda que essa porta seja apenas interna.
Message Broker Service	TCP/ 61616 e STOMP/ 61613	Lida com a comunicação entre os serviços do Dell Server. Armazena as informações de políticas criadas pelo Compatibility Server para o enfileiramento do Policy Proxy.  Precisa de acesso ao banco de dados SQL.  <b>i</b> <b>NOTA:</b> A porta 61616 deve ser filtrada por um firewall. A Dell recomenda que essa porta seja apenas interna.  <b>i</b> <b>NOTA:</b> A porta 61613 só deve ser aberta para os Security Management Servers configurados no modo Front-End.
Key Server	TCP/ 8050	Negocia, autentica e criptografa uma conexão de um cliente usando APIs Kerberos.  Precisa de acesso ao banco de dados SQL para obter os dados de chave.
Policy Proxy	TCP/ 8000	Fornecer um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário.
PostGres	TCP/ 5432	Banco de dados local usado para dados de eventos.  <b>i</b> <b>NOTA:</b> A porta 5432 deve ser filtrada por um firewall. A Dell recomenda que essa porta seja apenas interna.
LDAP	TCP/ 389/636 (controlador de domínio local), 3268/3269 (catálogo global)  TCP/ 135/ 49125+	Porta 389 – Esta porta é usada para solicitar informações a partir do controlador de domínio local. As solicitações de LDAP enviadas para a porta 389 podem ser usadas para buscar objetos apenas dentro do domínio doméstico do catálogo global. No entanto, o aplicativo de solicitação pode obter todos os atributos para esses objetos. Por exemplo, uma solicitação à porta 389 poderia ser usada para obter um departamento do usuário.

Nome	Porta padrão	Descrição
	(RPC)	Porta 3268 – Esta porta é usada para filas especificamente voltadas ao catálogo global. As solicitações de LDAP enviadas para a porta 3268 podem ser usadas para buscar objetos em toda a floresta. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, o departamento de um usuário poderia não ser devolvido usando a porta 3268 já que esse atributo não é replicado para o catálogo global.
Microsoft SQL Database	TCP/ 1433	A porta padrão do SQL Server é 1433, e as portas client recebem um valor aleatório entre 1024 e 5000.
Client Authentication	HTTPS/ 8449	Permite que os servidores client sejam autenticados com o Dell Server. Necessário para Server Encryption.

# Práticas recomendadas do SQL

A lista a seguir explica as boas práticas do SQL Server que precisam ser implementadas quando o Dell Security for instalado, caso ainda não tenham sido implementadas.

1. Certifique-se de que o tamanho de bloco do NTFS onde residem os arquivos de dados e o arquivo de registro é de 64 KB. As extensões do SQL Server (unidade básica do SQL Storage) são de 64 KB.

Para obter mais informações, procure por "Compreendendo páginas e extensões" nos artigos da TechNet da Microsoft.

2. Como diretriz geral, defina a quantidade máxima de memória do SQL Server como 80% da memória instalada.

Para obter mais informações, procure por *Opções de configuração de memória do servidor* nos artigos da TechNet da Microsoft.

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

3. Defina -t1222 nas propriedades de inicialização de instância para garantir que, na ocorrência de um deadlock, as respectivas informações sejam capturadas.

Para obter mais informações, procure por "Sinalizadores de rastreamento (Transact-SQL)" nos artigos da TechNet da Microsoft.

- 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. Certifique-se de que todos os índices estejam cobertos por uma rotina de manutenção semanal que os reconstrua.

5. Confirme se as permissões e os recursos são apropriados para o banco de dados aproveitado pelo Security Management Server. Para obter mais informações, consulte o artigo da base de conhecimento [SLN307771](#).

## Certificados

Este capítulo explica como para obter certificados para uso com o Security Management Server.

Para obter informações sobre como configurar a autenticação do SmartCard, consulte <http://www.dell.com/support/article/us/en/19/sln303783/dell-data-protection-sed-management-smartcard-setup-guide?lang=en>.

Para obter informações sobre os requisitos mínimos para solicitação de certificado SSL/TLS para uso pelo servidor Dell Data Security, consulte <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>.

Para obter informações sobre a atualização do certificado do Dell Encryption com um certificado existente no armazenamento de chaves da Microsoft, consulte <http://www.dell.com/support/article/us/en/19/sln297240/>.

### Criar um certificado autoassinado e gerar uma solicitação de assinatura de certificado

Esta seção detalha as etapas necessárias para criar um certificado autoassinado para componentes baseados em Java. Este processo **não pode** ser usado para criar um certificado autoassinado para componentes baseados em .NET.

A Dell recomenda um certificado autoassinado *apenas* em um ambiente que não seja de produção.

Se sua organização precisar de um certificado do servidor SSL, ou se você precisar criar um certificado por outros motivos, esta seção descreverá o processo de criação de um armazenamento de chaves java usando o Keytool.

Se sua organização desejar usar smart cards para autenticação, você precisará usar o Keytool para importar a cadeia confiável de certificados completa que é usada no certificado do usuário de smart cards.

O Keytool cria chaves privadas passadas no formato de uma CSR (Certificate Signing Request - Solicitação de assinatura de certificado) para uma CA (Autoridade de certificação), como VeriSign® ou Entrust®. Baseado nessa CSR, a CA criará um certificado de servidor que ela assina. Aí então o certificado de servidor pode ser baixado em um arquivo com o certificado de autoridade de assinatura. Os certificados são importados no arquivo cacerts.

### Gerar um novo par de chaves e um certificado auto-assinado

1. Navegue até o diretório **conf** do Compliance Reporter, Security Server ou Device Server.
2. Faça o backup do banco de dados de certificado padrão:  
Clique em **Iniciar > Executar** e digite **move cacerts cacerts.old**.
3. Adicione Keytool ao caminho do sistema. Digite o seguinte comando em um prompt de comando:  
**set path=%path%;< Diretório de instalação Dell do Java>\bin**
4. Para gerar um certificado, execute o Keytool conforme exibido:  
**keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell -keystore .\cacerts**
5. Insira as seguintes informações conforme o Keytool solicita.

#### **NOTA:**

Sempre faça um backup dos arquivos de configuração antes de editá-los. Altere somente os parâmetros especificados. Alterar outros dados nesses arquivos, incluindo tags, pode causar falhas e corromper o sistema. A Dell não pode garantir que os problemas resultantes de alterações não autorizadas nesses arquivos possam ser resolvidos sem a reinstalação do Security Management Server.

- *Senha do armazenamento de chaves:* digite uma senha (os caracteres incompatíveis são <>:&" ') e defina a variável no arquivo do componente **conf** para o mesmo valor, da seguinte forma:

<diretório de instalação do Compliance Reporter>\conf\eserver.properties. Defina o valor eserver.keystore.password =  
<diretório de instalação do Device Server>\conf\application.properties. Defina o valor keystore.password =  
<diretório de instalação do Security Server>\conf\application.properties. Defina o valor keystore.password =

- *Nome do servidor totalmente qualificado*: digite o nome totalmente qualificado do servidor onde o componente com o qual você está trabalhando está instalado. Este nome totalmente qualificado inclui o nome do host e o nome do domínio (por exemplo: domínio.com).
- *Unidade organizacional*: digite o valor apropriado (por exemplo, Segurança).
- *Organização*: digite o valor apropriado (por exemplo, Dell).
- *Cidade ou localidade*: digite o valor apropriado (por exemplo, Dallas).
- *Estado ou província*: digite o nome do estado ou da província sem abreviação (por exemplo, Texas).
- *Código do país com duas letras*.
- O utilitário solicita confirmação sobre as informações. Em caso afirmativo, digite **sim**.

Caso contrário, digite **não**. O Keytool exibe cada valor inserido anteriormente. Pressione **Enter** para aceitar o valor ou alterar o valor e pressione **Enter**.

- *Senha da chave do alias*: se você não digitar outra senha, essa será definida como a senha padrão do armazenamento de chaves.

## Solicitar um certificado assinado em uma Autoridade de Certificação

Use este procedimento para gerar uma solicitação de assinatura de certificado (CSR) para o certificado auto-assinado criado na etapa [Gerar um novo par de chaves e um certificado auto-assinado](#).

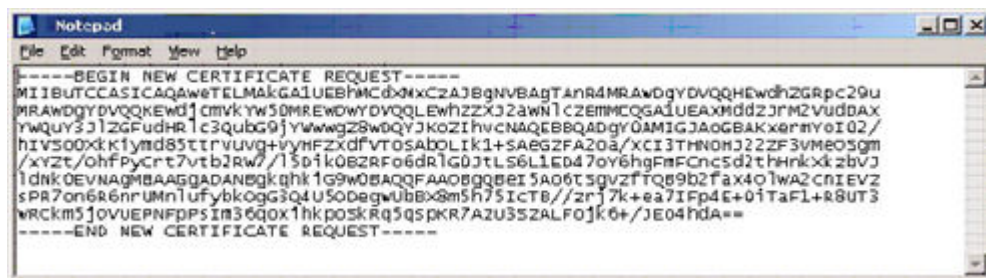
1. Substitua o mesmo valor usado anteriormente por **<certificatalias>**:

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

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

O arquivo .csr contém um par BEGIN/END a ser usado durante a criação do certificado na CA.

### Exemplo de arquivo .CSR



2. Siga o processo da sua organização para adquirir um certificado de servidor SSL de uma Autoridade de Certificado. Envie o conteúdo de <csr-filename> para assinatura.

#### **i** **NOTA:**

Há vários métodos para solicitar um certificado válido. Um método de exemplo é mostrado em **Método de exemplo para solicitar um certificado**.

3. Quando o certificado assinado é recebido, armazene-o em um arquivo.
4. Como prática recomendada, faça o backup deste certificado para a eventualidade de ocorrer um erro no processo de importação. Com este backup, você não precisará iniciar o processo de novo.

## Importar um certificado raiz

Se a Autoridade de Certificação do certificado raiz for a Verisign (não a Verisign Test), ignore o próximo procedimento e importe o certificado assinado.

O certificado raiz da Autoridade de Certificação valida certificado assinados.

1. Execute **uma** das seguintes ações:
  - Faça o download do certificado raiz da Autoridade de Certificação e armazene-o em um arquivo.
  - Obtenha o certificado raiz do servidor do diretório corporativo.
2. Execute **uma** das seguintes ações:
  - Se você estiver ativando SSL para o Compliance Reporter, Security Server ou Device Server, altere o diretório **conf** do componente.
  - Se você estiver ativando o SSL entre o Security Management Server e o servidor do diretório do enterprise, altere para <diretório de instalação Dell>\Java Runtimes\jre1.x.x\_xx\lib\security (a senha padrão de JRE cacerts é **changeit**).
3. Execute o Keytool conforme mostrado a seguir para instalar o certificado raiz:

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

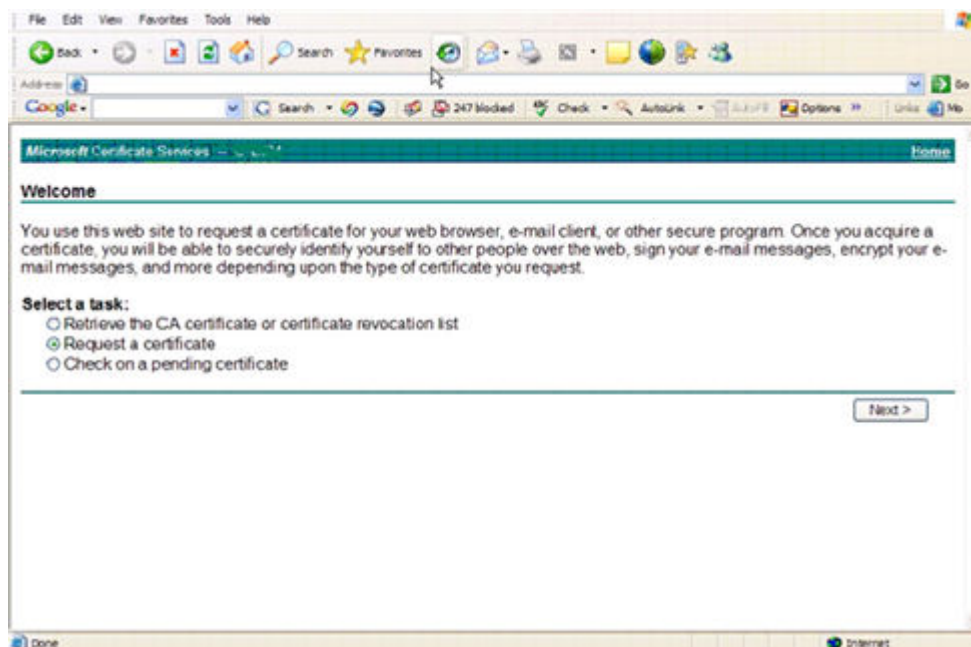
Por exemplo, `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

## Método de exemplo para solicitar um certificado

Um exemplo de método para solicitar um certificado é usar um navegador da Web para acessar o Microsoft CA Server, que é configurado internamente pela sua organização.

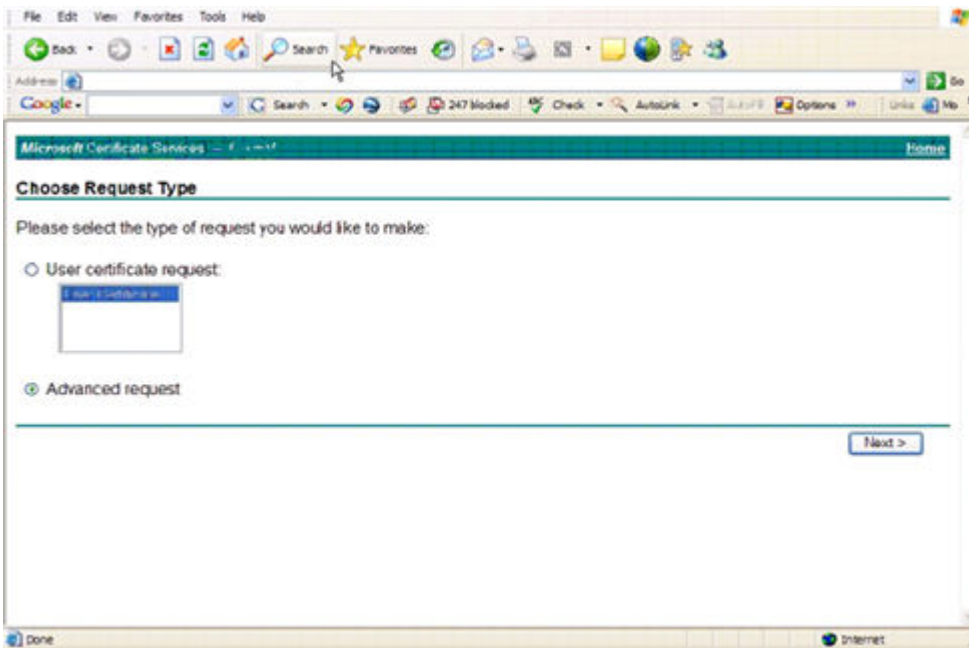
1. Acesse o Microsoft CA Server. O endereço IP é fornecido pela sua organização.
2. Selecione **Solicitar um certificado** e clique em **Avançar**.

### Serviços de Certificados da Microsoft



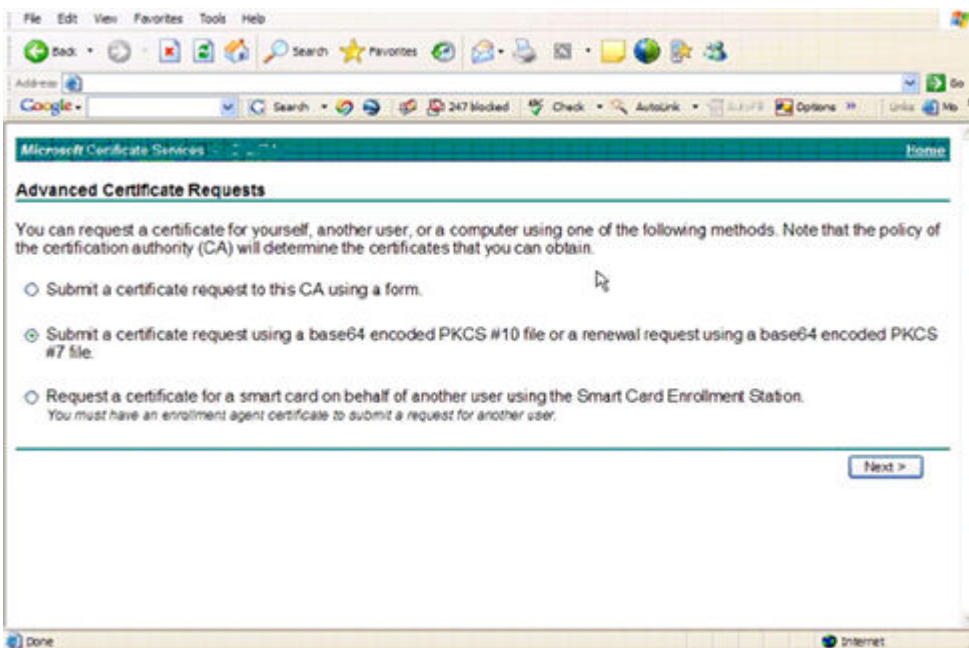
3. Selecione **Solicitação Avançada** e clique em **Avançar**.

### Escolha o tipo de solicitação

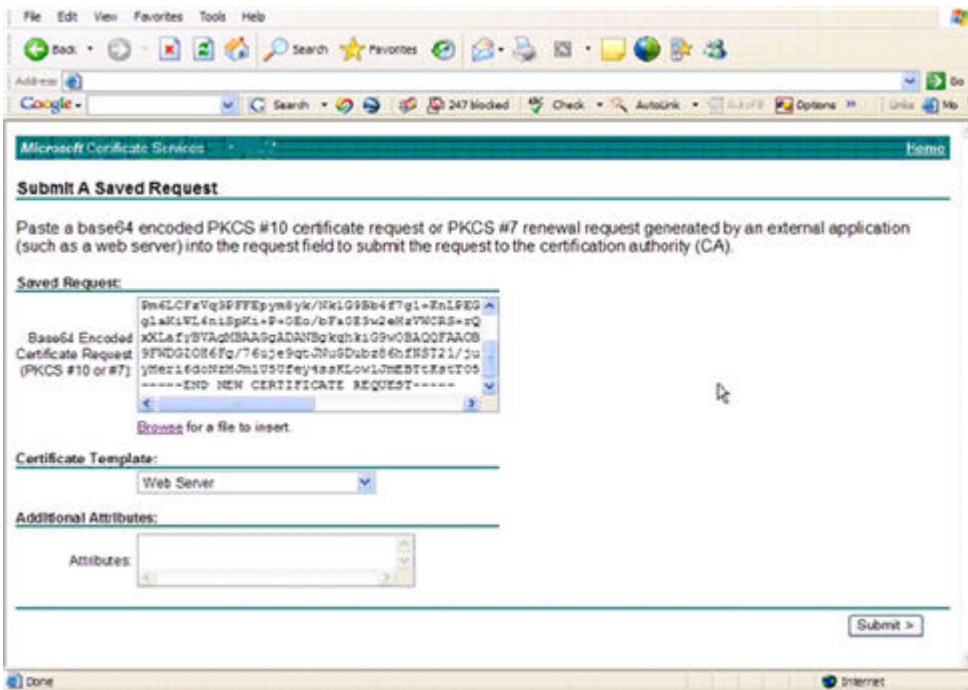


4. Selecione a opção para **Enviar uma solicitação de certificado usando um arquivo PKCS #10 de codificação de base 64** e clique em **Avançar**.

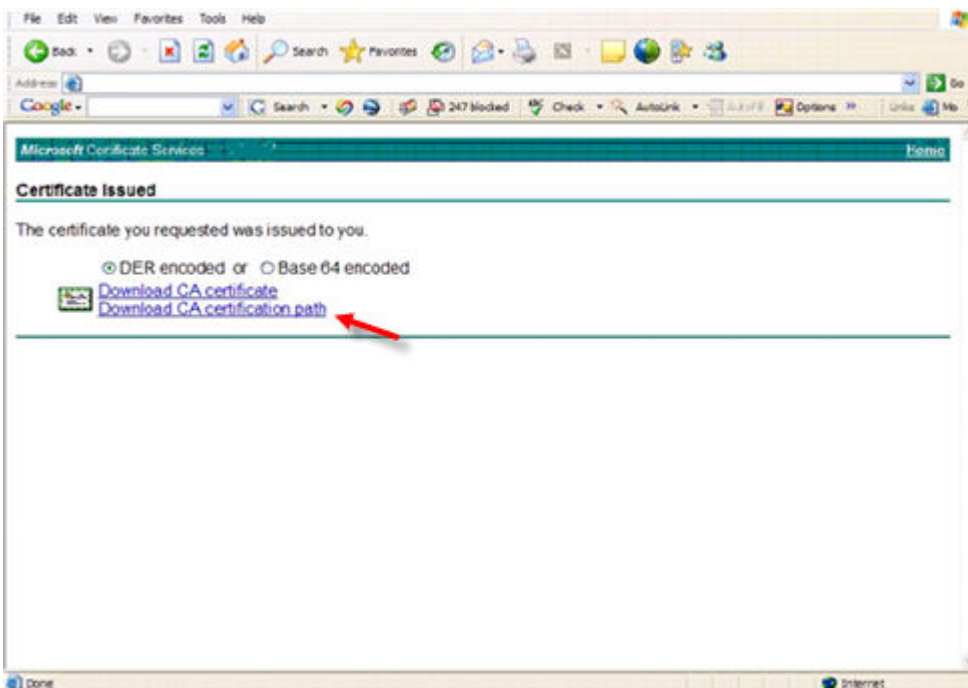
#### Solicitação Avançada de Certificado



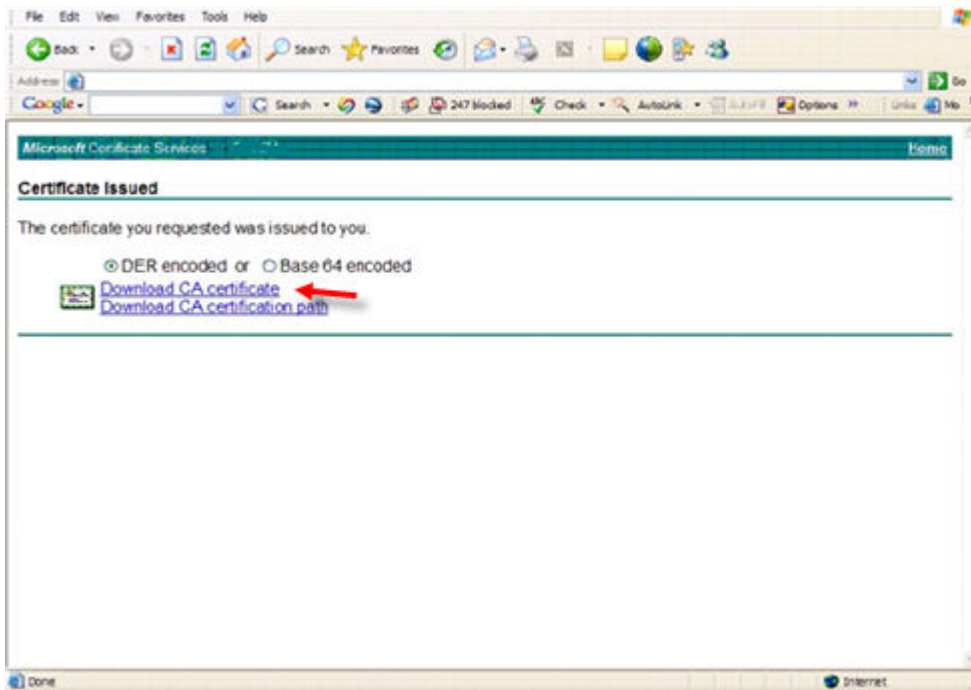
5. Cole o conteúdo da solicitação CSR na caixa de texto. Selecione um modelo de certificado do **Servidor Web** e clique em **Enviar**.  
**Enviar uma solicitação salva**



6. Salve o certificado. Selecione **Codificado por DER** e clique em **Fazer download de certificação CA**.  
**Fazer download do certificado de autoridade de certificação**



7. Salve o certificado. Selecione **Codificado por DER** e clique em **Fazer download do caminho de certificação CA**.  
**Fazer download do caminho de certificação de autoridade de certificação**



8. Importe o certificado da autoridade de assinatura convertido. Retorne ao prompt de comando. Digite:

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

9. Agora que o certificado de autoridade de assinatura foi importado, o certificado do servidor pode ser importado (a cadeia de confiança pode ser estabelecida). Digite:

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

Use o alias do certificado autoassinado para emparelhar a solicitação da CSR com o certificado do servidor.

10. Uma listagem do arquivo cacerts mostra que o certificado do servidor tem um **comprimento da cadeia de certificados** de **2**, o que indica que o certificado não é autoassinado. Digite:

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

A identificação do segundo certificado na cadeia é o certificado de autoridade de assinatura (que também é listado abaixo do certificado do servidor na listagem).

## Exportar um certificado para o formato .PFX usando o Console de gerenciamento do certificado

Depois de ter um certificado no formato de um arquivo .crt no MMC, ele precisa ser convertido para um arquivo .pfx para usar com o Keytool quando o Security Server for usado no Modo DMZ e ao importar um certificado do Dell Manager para a Server Configuration Tool.

1. Abra o Console de Gerenciamento Microsoft.
2. Clique em **Arquivo > Adicionar/remover snap-in**.
3. Clique em **Adicionar**.
4. Na janela *Adicionar snap-in autônomo*, selecione **Certificados** e clique em **Adicionar**.
5. Selecione **Conta de computador** e clique em **Avançar**.
6. Na janela *Selecionar computador*, selecione **Computador local (o computador no qual o console está sendo executado)** e clique em **Concluir**.
7. Clique em **Fechar**.
8. Clique em **OK**.
9. Na pasta *Raiz do console* expanda *Certificados (computador local)*.

10. Acesse a pasta *Pessoal* e encontre o certificado desejado.
11. Selecione o certificado desejado, clique com o botão direito em **Todas as tarefas > Exportar**.
12. Quando o Assistente para Exportação de Certificados abrir, clique em **Avançar**.
13. Selecione **Sim, exportar a chave privada** e clique em **Avançar**.
14. Selecione **Troca de Informações Pessoais - PKCS #12 (.PFX)** e selecione as subopções **Incluir todos os certificados no caminho de certificação, se possível** e **Exportar todas as propriedades estendidas**. Clique em **Avançar**.
15. Digite e confirme uma senha. Você pode escolher qualquer senha. Escolha uma senha fácil de lembrar, mas difícil de ser descoberta por outras pessoas. Clique em **Avançar**.
16. Clique em **Procurar** para ir até o local onde deseja salvar o arquivo.
17. No campo *Nome do arquivo*, digite um nome para salvar o arquivo. Clique em **Salvar**.
18. Clique em **Avançar**.
19. Clique em **Concluir**.

Será mostrada uma mensagem informando que a exportação foi bem-sucedida. Feche o Console de Gerenciamento Microsoft.

## Adicionar um Certificado de assinatura confiável ao Security Server quando um certificado não confiável foi usado para SSL

1. Pare o Security Server Service, se estiver em execução.
  2. Faça backup do arquivo cacerts no diretório <Security Server install dir>\conf\.
- Use o Keytool para concluir o seguinte:

3. Exporte o PFX confiável para um arquivo de texto e documente o Alias:

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

4. Importe o PFX para o arquivo cacerts no <Security Server install dir>\conf\.

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

5. Modifique o valor keystore.alias.signing no diretório <Security Server install dir>\conf\application.properties.

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

Inicie o Security Server Service.