# Dell Data Protection

## Guia de Instalação e Migração do Enterprise Server v9.7

## 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 perda de dados e ensina como evitar o problema.**

**ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.**



**Guia de Instalação e Migração do Enterprise Server**

2017 - 04

Rev. A01

# Índice

# Apresentação do Dell Enterprise Server

## Sobre o Dell Enterprise Server

O Enterprise Server é o componente de administração de segurança da solução da Dell. O Remote Management Console permite monitorar o estado de pontos finais, a aplicação de políticas e a proteção em toda a empresa.

O Enterprise Server tem os seguintes recursos:

- Gerenciamento centralizado de dispositivos
- Criação e gerenciamento de política de segurança baseada em função
- Recuperação de dispositivo auxiliado pelo administrador
- Separação de deveres administrativos
- Distribuição automática de políticas de segurança
- Caminhos confiáveis para comunicação entre os componentes
- Geração de chave de criptografia exclusiva e depósito de chave de segurança
- Auditoria e relatórios de compatibilidade centralizados

## 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 Data Protection.

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

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

Para obter os números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

2

# Requisitos e arquitetura do Dell Enterprise Server

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

## Requisitos do Dell Enterprise Server

Os componentes do Dell Enterprise Server têm requisitos de hardware e software além do software fornecido na mídia de instalação Dell. Verifique se o ambiente de instalação atende aos requisitos antes de continuar com as tarefas de instalação ou upgrade/migração.

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

## Pré-requisitos do Dell Enterprise Server

A tabela a seguir detalha o software que deve estar instalado antes da instalação do Dell Enterprise Server. Links e instruções para instalar esses pré-requisitos estão detalhados em Configuração de pré-instalação.

**Todo item de software aplicável precisa ser instalado antes de iniciar a instalação, a menos que seja indicado que o próprio instalador realiza sua instalação. Caso contrário, a instalação falhará.**

## Hardware do Dell Enterprise Server

**Pré-requisitos**

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

  Se não estiver instalado, o instalador realizará o processo para você.
- **Pacote redistribuível do Visual C++ 2013**

  Se não estiver instalado, o instalador realizará o processo para você.
- **Pacote redistribuível do Visual C++ 2015**

  Se não estiver instalado, o instalador realizará o processo para você.
- **.NET Framework versão 3.5 SP1**
- **.NET Framework versão 4.5**

  A Microsoft publicou as atualizações de segurança para o .NET Framework versão 4,5.
- **SQL Native Client 2012**

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

  Se não estiver instalado, o instalador realizará o processo para você.

A tabela a seguir detalha os requisitos mínimos de hardware do Dell Enterprise Server. Consulte Design de arquitetura do Dell Enterprise Server para obter informações adicionais sobre dimensionamento com base no porte da sua implementação.

### Requisitos de hardware

**Processador**

No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

CPU Quad-Core moderna (2 GHz+) para configuração de servidor único

**RAM**

mínimo de 8GB, dependendo da configuração

16 GB para configuração de servidor único

**Espaço livre em disco**

Cerca de 1,5 GB de espaço livre em disco (mais espaço de paginação virtual)

20 GB ou mais de espaço livre em disco (além do espaço de paginação virtual)

**Placa de rede**

Placa de interface de rede 10/100/1000

**Diversos**

TCP/IPv4 instalado e ativado

# Software do Dell Enterprise Server

A tabela a seguir detalha os requisitos de software do Dell Enterprise Server e Proxy Server.

**NOTA: O UAC deve ser desativado antes da instalação. O servidor precisa ser reiniciado para que essa alteração tenha efeito. No Windows Server 2012 R2 e no Windows Server 2016, o instalador desativa o UAC.**

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

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

**Dell Enterprise Server - Servidor de back-end e servidor de front-end Dell**

- **Windows Server 2008 R2 SP0-SP1 64 bits**

  - Standard Edition

  - Enterprise Edition
- **Windows Server 2008 SP2 64 bits**

  - Standard Edition

  - Enterprise Edition
- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition
- **Windows Server 2016**

  - Standard Edition

- Datacenter Edition

**Exchange ActiveSync Servers**

Se você quiser usar o Mobile Edition, os seguintes Exchange ActiveSync Servers são suportados. Este componente está instalado no seu Exchange Server front-end.

- Exchange ActiveSync 12.0 – um componente do Exchange Server 2007
- Exchange ActiveSync 12.1 – um componente do Exchange Server 2007 SP1
- Exchange ActiveSync 14.0 – um componente do Exchange Server 2010
- Exchange ActiveSync 14.1 – um componente do Exchange Server 2010 SP1

O **Microsoft Message Queuing (MSMQ)** precisa ser instalado/configurado no Exchange Server.

**Repositório do LDAP**

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

**Ambientes virtuais recomendados para Componentes do Dell Enterprise Server**

O Dell Enterprise Server pode opcionalmente ser instalado em um ambiente virtual. Apenas os ambientes a seguir são recomendados.

O Dell Enterprise Server v9.7 foi validado com o Hyper-V Server (instalação completa ou básica), e como uma função no Windows Server 2012 R2 ou Windows Server 2016.

- Hyper-V Server (instalação completa ou básica)
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - 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 Dell Enterprise Server v9.7 foi validado com o VMWare ESXi 5.5 e VMware ESXi 6.0. Certifique-se de que todos os patches e as atualizações sejam aplicados imediatamente ao VMware ESXi para solucionar possíveis vulnerabilidades.

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

- VMware ESXi 5.5
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - 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-55/index.jsp para obter mais informações
- VMware ESXi 6.0
  - CPU x86 de 64 bits necessária

- Computador host com no mínimo dois núcleos
- Mínimo de 8 GB de RAM recomendado
- Não é necessário ter um sistema operacional específico
- 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

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

**Banco de dados**

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

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

**Dell Data Protection Remote Management Console e Compliance Reporter**

- Internet Explorer 11.x ou posterior
- Mozilla Firefox 41.x ou posterior
- Google Chrome 46.x ou posterior

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

# Suporte de idiomas do Dell Enterprise Server

O Remote 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 | |

# Design da Arquitetura do Dell Enterprise Server

As soluções Dell Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise e Data Guardian são altamente dimensionáveis conforme o tamanho da sua organização e o número de endpoints que se deseja criptografar. Esta seção fornece um conjunto de diretrizes para dimensionar a arquitetura para 5.000 a 60.000 endpoints.

**NOTA: Se a organização tiver mais de 50.000 endpoints, entre em contato com o Dell ProSupport para obter assistência.**

**NOTA:**

**Cada um dos componentes apresentados em cada seção contém as especificações mínimas de hardware necessárias para garantir um ótimo desempenho na maioria dos ambientes. A falha em alocar recursos adequados a quaisquer desses componentes pode resultar em degradação do desempenho ou problemas funcionais com o aplicativo.**

### Até 5.000 endpoints

Essa arquitetura atende a maioria das empresas de pequeno a médio porte que possuem entre 1 e 5.000 endpoints. Todos os componentes do Dell Enterprise Server podem ser instalados em um único servidor. Como opção, um servidor de front-end pode ser instalado na DMZ para publicar políticas e/ou ativar endpoints na Internet.

#### Componentes da arquitetura

#### Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

#### Configuração de servidor único

16 GB; 20 GB ou mais de espaço livre em disco (além do espaço de paginação virtual); CPU Quad-Core moderna (2 GHz+)

#### Configuração de servidor quando usado com servidor front-end

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

#### Servidor Front-End Externo Dell

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

#### SQL Server

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

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

### 5.000 a 20.000 endpoints

Essa arquitetura atende a ambientes que possuem entre 5.000 e 20.000 endpoints. Um servidor front-end é adicionado para distribuir a carga adicional e é projetado para lidar com aproximadamente 15.000 a 20.000 endpoints. Como opção, um servidor de front-end pode ser instalado na DMZ para publicar políticas e/ou ativar endpoints na Internet.

#### Componentes da arquitetura

**Dell Enterprise Server**

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

**Servidor de front-end interno Dell (1) e Servidor de front-end externo Dell (1)**

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

**SQL Server**

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

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

**20.000 a 40.000 endpoints**

Essa arquitetura atende a ambientes que possuem entre 20.000 e 40.000 endpoints. Um servidor front-end adicional é adicionado para distribuir a carga adicional. Cada servidor front-end é projetado para lidar com aproximadamente 15.000 a 20.000 endpoints. Como opção, um servidor front-end pode ser instalado na DMZ para ativar endpoints e/ou publicar políticas para endpoints na Internet.

**Componentes da arquitetura**

**Dell Enterprise Server**

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

**Servidores de front-end interno Dell (2) e Servidor de front-end externo Dell (1)**

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

**SQL Server**

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

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

**40.000 a 60.000 endpoints**

Essa arquitetura atende a ambientes que possuem entre 40.000 e 60.000 endpoints. Um servidor front-end adicional é adicionado para distribuir a carga adicional. Cada servidor front-end é projetado para lidar com aproximadamente 15.000 a 20.000 endpoints. Como opção, um servidor front-end pode ser instalado na DMZ para ativar endpoints e/ou publicar políticas para endpoints na Internet.

**NOTA:**
Se a organização tiver mais de 50.000 endpoints, entre em contato com o Dell ProSupport para obter assistência.

**Componentes da arquitetura**

**Dell Enterprise Server**

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

**Servidores de front-end interno Dell (2) e Servidor de front-end externo Dell (1)**

Windows Server 2008 R2 SP0-SP1 64 bits/Windows Server 2008 SP2 64 bits - Standard ou Enterprise Edition

Windows Server 2012 R2 - Standard ou Datacenter Edition

Windows Server 2016 - Standard ou Datacenter Edition

Mínimo de 8 GB, dependendo da configuração; +-1,5 GB de espaço livre em disco (além do espaço de paginação virtual); No mínimo, CPU Dual-Core moderna (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente da AMD

**SQL Server**

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

SQL Server 2012 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2014 Standard Edition / Business Intelligence / Enterprise Edition

SQL Server 2016 Standard Edition / Enterprise Edition

**Considerações de alta disponibilidade**

Essa é uma arquitetura altamente disponível que suporta até 60.000 endpoints. Há dois Dell Enterprise Servers configurados em um modelo ativo/passivo. Para fazer o failover no segundo Dell Enterprise Server, interrompa os serviços no nó primário e aponte o alias do DNS (CNAME) para o segundo nó. Inicie os serviços no segundo nó e abra o Remote Management Console para garantir que o aplicativo esteja funcionando adequadamente. Os serviços no segundo nó (passivo) precisam ser configurados como “Manual”, a fim de evitar que sejam iniciados acidentalmente durante atividades regulares de manutenção e aplicação de patches.

Uma organização pode optar por ter também um servidor de banco de dados SQL Cluster. Nessa configuração, o Dell Enterprise Server precisa ser configurado para usar o IP ou o nome de host do cluster.

**NOTA:**
**A replicação de banco de dados não é suportada.**

O tráfego de clientes é distribuído para três servidores front-end internos. Como opção, vários servidores front-end podem ser instalados na DMZ para ativar endpoints e/ou publicar políticas para endpoints na Internet.

**Virtualização**

O Dell Enterprise Server pode opcionalmente ser instalado em um ambiente virtual. Apenas os ambientes a seguir são recomendados.

O Dell Enterprise Server v9.7 foi validado com o Hyper-V Server (instalação completa ou básica), e como uma função no Windows Server 2012 R2 ou Windows Server 2016.

- Hyper-V Server (instalação completa ou básica)
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - 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 Dell Enterprise Server v9.7 foi validado com o VMWare ESXi 5.5 e VMware ESXi 6.0. Certifique-se de que todos os patches e as atualizações sejam aplicados imediatamente ao VMware ESXi para solucionar possíveis vulnerabilidades.

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

- VMware ESXi 5.5
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - 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-55/index.jsp para obter mais informações
- VMware ESXi 6.0
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - 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

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

### 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 de todos os índices de bancos de dados e a coleta de estatísticas.

3

# Configuração de pré-instalação

Antes de começar, leia os relatórios técnicos do *Enterprise Server* de qualquer solução ou problema conhecido relacionado ao Dell Enterprise Server.

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

## Configuração

1 Se estiver ativado, desative a Configuração de segurança reforçada do Internet Explorer (ESC). Adicione a URL do servidor à lista de Sites Confiáveis nas opções de segurança do navegador. Reinicie o servidor.

2 Abra as portas a seguir para cada componente:

**Interno:**

Comunicação do Active Directory: TCP/389

Comunicação de e-mail (opcional): 25

**Para o servidor Front End (se necessário):**

Comunicação do Dell Policy Proxy externo para o Dell Message Broker: TCP/61616 e STOMP/61613

Comunicação para o servidor back-end Dell Security Server: HTTPS/8443

Comunicação para o servidor back-end Dell Security Core Server: HTTPS/8888 e 9000

Comunicação para portas RMI - 1099

Comunicação para o servidor back-end Dell Security Server: HTTP(S)/8443 - Se o seu Dell Enterprise Server for o v7.7 ou superior. Se o seu Dell Enterprise Server for o pre-v7.7, HTTP(S)/8081.

Servidor de sinalizador: HTTP/8446 (se estiver usando Data Guardian)

**Externo (se necessário):**

Banco de dados SQL: TCP/1433

Remote Management Console: HTTPS/8443

LDAP: TCP/389/636 (controlador de domínio local), TCP/3268/3269 (catálogo global), TCP/135/49125+ (RPC)

Dell Compatibility Server: TCP/1099

Dell Compliance Reporter: HTTP(S)/8084 (configurada automaticamente na instalação)

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 e 9000 (8888 é configurada automaticamente na instalação)

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

Dell Key Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell Security Server: HTTPS/8443

Autenticação de cliente: HTTPS/8449 (se estiver usando Server Encryption)

Comunicação do cliente, se estiver usando o Advanced Threat Prevention: HTTPS/TCP/443

**NOTA:**
Se os seus clientes Enterprise Edition forem ser habilitados de fábrica ou se você comprar licenças de fábrica, defina o GPO no controlador de domínio para ativar a habilitação (não pode ser o mesmo servidor que está executando o Enterprise Edition). Certifique-se de que a porta de saída 443 esteja disponível para se comunicar com o Servidor. Se a porta 443 estiver bloqueada por qualquer motivo, a funcionalidade de habilitação não funcionará. Para obter mais informações, consulte o Guia de Instalação Avançada do Enterprise Edition.

**Criar banco de dados Dell**

3 Se você ainda não tem um banco de dados SQL configurado para o Dell Enterprise Server, o instalador cria o banco de dados para você durante a instalação. Se você preferir configurar um banco de dados antes de instalar o Dell Enterprise Server, siga as instruções abaixo para criar o banco de dados SQL e o usuário SQL no SQL Management Studio. ***Essas instruções são opcionais, já que o instalador criará um banco de dados para você caso um já não exista.***

Ao instalar o Dell Enterprise Server, siga as instruções disponíveis Instalar um servidor de back-end com um banco de dados existente.

O Dell Enterprise Server é preparado para Autenticação SQL e do Windows. O método padrão de autenticação é a Autenticação SQL.

Após você criar o banco de dados, crie um usuário de banco de dados Dell com os direitos db_owner. O db_owner pode atribuir permissões, fazer backup e restauração do banco de dados, criar e apagar objetos e gerenciar contas de usuário e funções sem nenhuma restrição. Além disso, verifique se esse usuário tem permissões/privilégios para executar os procedimentos armazenados.

Ao usar uma instância do SQL Server que não seja a instância padrão, após a instalação do Dell Enterprise Server, você precisa especificar a porta dinâmica da instância na guia Banco de dados da Server Configuration Tool. Para obter mais informações, consulte Server Configuration Tool. 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.

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.

Para criar o banco de dados SQL e usuário SQL no SQL Management Studio, escolha uma das opções:

**Crie um novo banco de dados do Windows SQL Server usando a Autenticação do Windows:**

a Clique em **Iniciar** > **Todos os programas** > **Microsoft SQL Server** > **Management Studio**.

b Clique com o botão direito na pasta Bancos de dados e, em seguida, clique em Novo banco de dados. A caixa de diálogo Propriedades do banco de dados é exibida.

c Digite o Nome do banco de dados e clique em **OK**.

d Abra a pasta *Segurança* e clique com o botão direito em **Logons**.

e Clique em **Novo logon** para criar um proprietário para o novo banco de dados.

f Digite um nome de usuário no campo *Nome*.

g Selecione a opção de autenticação *Autenticação do Windows*.

h Selecione **Mapeamento de usuário** e realce o novo banco de dados.

i Selecione a função do banco de dados (db_owner) e clique em **OK**.

OU

**Crie um novo banco de dados do SQL Server usando a Autenticação do SQL Server:**

a Clique em **Iniciar** > **Todos os programas** > **Microsoft SQL Server** > **Management Studio**.

b Clique com o botão direito na pasta *Bancos de dados* e, em seguida, clique em **Novo banco de dados**. A caixa de diálogo *Propriedades do banco de dados* é exibida.

c Digite o Nome do banco de dados e clique em **OK**.

d Abra a pasta *Segurança* e clique com o botão direito em **Logons**.

e Clique em **Novo logon** para criar um proprietário para o novo banco de dados.

f Digite um nome de usuário no campo *Nome*.

g Selecione a opção de autenticação *Autenticação do SQL Server*. Digite e confirme a senha.

h Desmarque **Impor vencimento de senha**.

i Selecione **Mapeamento de usuário** e realce o novo banco de dados.

j Selecione a função do banco de dados (db_owner) e clique em **OK**.

**Instale os Pacotes redistribuíveis do Visual C++ 2010/2013/2015**

4 *Se ainda não estiver instalado,* instale os Pacotes redistribuíveis do Visual C++ 2010, 2013 e 2015. Se desejar, você pode permitir que o instalador do Dell Enterprise Server instale esses componentes.

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

**Instale o .NET Framework 4.5**

5 *Se ainda não estiver instalado*, instale o .NET Framework 4.5.

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

**Instale o SQL Native Client 2012**

6 *Se estiver usando SQL Server 2012 ou SQL Server 2016*, instale o SQL Native Client 2012. Se desejar, você pode permitir que o instalador do Dell Enterprise Server instale esse componente.

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

**Configure o Microsoft CA (MSCEP)**

**Esta etapa só precisa ser concluída em seu servidor com MSCEP se você deseja usar o iOS com o Mobile Edition.**

7 Configure o MSCEP.

O Windows Server 2008 R2 precisa ser a versão Enterprise Edition. ***A versão Standard Edition não permitirá que a função MSCEP seja instalada***.

a Abra o Gerenciador de Servidores. No menu à esquerda, selecione **Funções do Servidor** e marque a caixa **Serviços de certificados do Active Directory**. Clique em **Avançar**. O Assistente para adicionar funções o guiará pelas próximas etapas.

Em *AD CS > Serviços de função*, marque as caixas dos serviços de função **Autoridade de Certificação** e **Registro na Web de autoridade de certificação**. Selecione **Adicionar serviços de função necessários para o IIS do servidor Web** (se for solicitado). Clique em **Avançar**.

Em *AD CS > Tipo de instalação*, selecione **Autônoma**. Clique em **Avançar**.

Em *AD CS > Tipo de autoridade de certificação*, selecione **Autoridade de certificação subordinada**. Clique em **Avançar**.

Em *AD CS > Chave privada*, selecione **Criar uma nova chave privada**. Clique em **Avançar**.

Em *AD CS > Chave Privada > Criptografia*, mantenha os valores padrão de **RSA#Microsoft Software Key Storage Provider**, **2048** e **SHA1**. Clique em **Avançar**.

Em *AD CS > Chave privada > Nome da autoridade de certificação*, mantenha todos os valores padrão. Clique em **Avançar**.

Em *AD CS > Chave Privada > Solicitação de Certificado*., selecione **Enviar uma solicitação de certificado a uma CA pai**. Selecione **Procurar por: nome da CA**. Navegue e selecione **Parent CA** (CA pai). Clique em **Avançar**.

Em *AD CS > Banco de dados de certificados*, mantenha os valores padrão. Clique em **Avançar**.

Em *Servidor Web (IIS)*, clique em **Avançar**.

Em *Servidor Web (IIS) > Serviços de função*, mantenha os valores padrão. Clique em **Avançar**.

Em *Confirmação*, clique em **Instalar**.

Em *Resultados*, analise os resultados e clique em **Fechar**.

Em *Gerenciador de servidores > Funções*, selecione **Adicionar serviços de função** em *Serviços de certificados do Active Directory*.

Quando a janela *Selecionar serviços de funçãoRole Services* aparecer, marque a caixa **Serviço de inscrição do dispositivo de rede**. Clique em **Avançar**.

Adicione a conta do usuário que o *Serviço de inscrição do dispositivo de rede* deve usar ao autorizar solicitações de certificados ao Grupo de usuários de IIS_IUSRS do servidor local. O formato é domínio\nome de usuário. Clique em **OK**.

Na janela Especificar conta de usuário, selecione o usuário que acabou de ser adicionado ao grupo IIS_IUSRS. Clique em **Avançar**.

Na janela *Especificar informações da autoridade de registro*, mantenha os valores padrão de *Informações necessárias* e *Adicionar informações opcionais* conforme desejado. Clique em **Avançar**.

Na janela *Configurar criptografia para autoridade de registro*, mantenha os valores padrão. Clique em **Avançar**.

Na janela *Confirmar seleções de instalação*, clique em **Instalar**.

Na janela *Resultados da instalação*, analise os resultados e clique em **Fechar**.

Feche o Gerenciador de servidores.

b Modifique a Chave de registro da seguinte forma:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

c Abra o Gerenciador do IIS. Acesse **\<ServerName > \Sites\Default Web Site\CertSrv\mscep_admin**.

Abra *Autenticação* e habilite **Autenticação anônima**.

d Clique em **Iniciar** > **Executar**. Digite *certsrv.msc* e pressione **Enter**.

Quando a janela *certsrv* aparecer, clique com o botão direito no nome do servidor, selecione **Propriedades** e clique na guia **Módulo de diretivas**.

Clique em **Propriedades** e selecione **Siga as configurações do modelo de certificado, se aplicável. Caso contrário, emita o certificado automaticamente** Clique em **OK**.

e Feche o Gerenciador do IIS.

f Reinicie o servidor. Para confirmar, abra o Internet Explorer e, na barra de endereços, digite

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

Fim da instalação do MSCEP Windows Server 2008 R2.

**Windows Server 2012 R2 ou Windows Server 2016:**

a Siga instruções de configuração no artigo, Serviço de inscrição de dispositivo de rede (NDES) no Active Directory Certificate Services (AD CS)."

b Modifique a Chave de registro da seguinte forma:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

c Abra o Gerenciador do IIS. Acesse **\<ServerName\Sites\Default Web Site\CertSrv\mscep_admin**.

Abra *Autenticação* e habilite **Autenticação anônima**.

d Clique em **Iniciar** > **Executar**. Digite *certsrv.msc* e pressione **Enter**.

Quando a janela *certsrv* aparecer, clique com o botão direito no nome do servidor, selecione **Propriedades** e clique na guia **Módulo de diretivas**.

Clique em **Propriedades** e selecione **Siga as configurações do modelo de certificado, se aplicável. Caso contrário, emita o certificado automaticamente** Clique em **OK**.

e Feche o Gerenciador do IIS.

f Reinicie o servidor. Para confirmar, abra o Internet Explorer e, na barra de endereços, digite

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

Fim da instalação do MSCEP Windows Server 2012 R2/Windows Server 2016.

**Instalar/Configurar MSMQ (Microsoft Message Queuing)**

**Essa etapa só precisa ser concluída se você quiser usar o Mobile Edition.** Este é um pré-requisito para que o Gerenciador de Dispositivos do EAS e o Gerenciador de caixas de correio do EAS possam se comunicar.

8 No Windows Server 2008 ou Windows Server 2008 R2 (no servidor que hospeda o ambiente do Exchange): http://msdn.microsoft.com/en-us/library/aa967729.aspx

OU

No Windows Server 2012 R2:

a Abra o Gerenciador de Servidores.

b Navegue até **Gerenciar** > **Adicionar funções e recursos.**

c Na tela Antes de começar, clique em **Avançar**.

d Selecione **Instalação baseada em função ou recursos** e clique em **Avançar**.

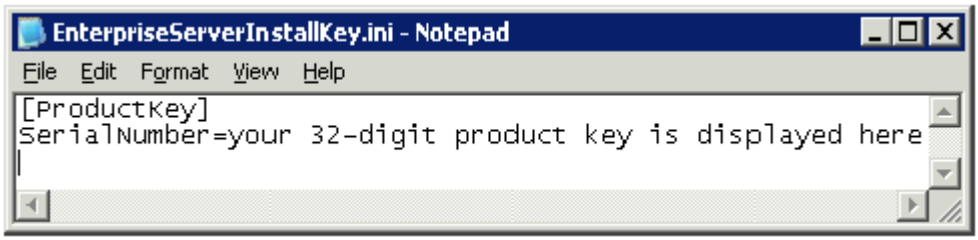
e Selecione o servidor no qual você deseja instalar o recurso e clique em **Avançar**.

f Não selecione nenhuma função de servidor. Clique em **Avançar**.

g Em Recursos, selecione **Fila de mensagens** e clique em **Instalar**.

**Opcional**

9 **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 Dell Enterprise Server.




A configuração pré-instalação do servidor está completa. Continue para Instalar ou Atualizar/migrar.

4

# Instalar ou fazer upgrade/migrar

O capítulo fornece instruções sobre o seguinte:

- Nova instalação - Instalar um novo Dell Enterprise Server.
- Atualização/migração - Fazer upgrade de um Dell Enterprise Server v8.0 ou posterior existente e funcional.
- Desinstalar o Dell Enterprise 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 atualização/migração

Antes de começar, certifique-se de que as etapas aplicáveis da Configuração de pré-instalação foram concluídas.

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

Se o Controle de conta de usuário (UAC - User Account Control) estiver ativado, você precisará desativá-lo. No Windows Server 2012 R2, o instalador desativa o UAC. 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. Se você selecionar a Autenticação do Windows, serão usadas as credenciais do usuário conectado. O usuário precisa ter direitos de administrador do sistema e direitos para criar e gerenciar o banco de dados SQL (criar banco de dados, adicionar usuário e atribuir permissões). Para Autenticação SQL, a conta usada precisa ter esses mesmos direitos. Essas credenciais são usadas somente durante a instalação. O produto instalado não usa essas credenciais.

Também durante a instalação, as credenciais de autenticação de tempo de execução do serviço a serem usadas pelos serviços Dell para acessar o SQL Server precisarão ser especificadas. A conta do usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Database Role Membership: dbo_owner, public.

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 da Dell e que o software da 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 de instalação estão localizados neste diretório: **C:\ProgramData\Dell\Dell Data Protection\Installer Logs**

# 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 Dell Enterprise Server e um novo banco de dados.

- Instalar um servidor de back-end com banco de dados existente - Para instalar um novo Dell Enterprise 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 Dell Enterprise Server a ser instalada. Um banco de dados 8.x ou mais recente 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 8.0, entre em contato com a Dell ProSupport para obter assistência.

**NOTA:**
Se você tiver um Dell Enterprise Server 8.x funcional ou mais recente, consulte as instruções em **Atualizar/Migrar os 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 Dell Enterprise Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Dell Enterprise Server-x64 no diretório raiz do servidor onde você está instalando o Enterprise Server. ***Copiar/colar ou arrastar/soltar produzirá erros e causará uma instalação malsucedida.***

2 Clique duas vezes em **setup.exe**.

3 Quando o *Assistente do InstallShield* aparecer, selecione o idioma da 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, concluiu, de forma opcional, a etapa 9 na 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**.

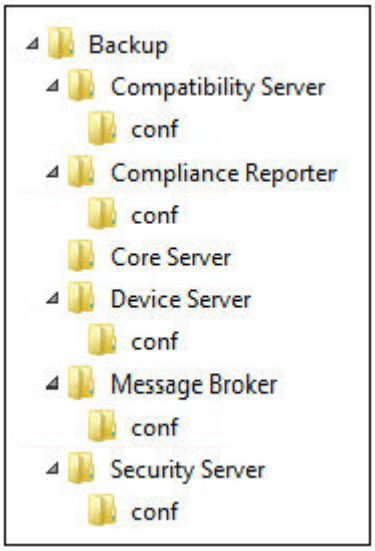
9 Para instalar o Dell Enterprise Server no local padrão **C:\Program Files\Dell**, clique em **Avançar**. Caso contrário, clique em **Alterar** para selecionar outro local e clique em **Avançar**.

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.

**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 ano.

12 Para a Criptografia do servidor (SE - 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 ano.

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**.

- 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:

a Clique em **Procurar** para selecionar o servidor no qual será instalado o banco de dados.

b Selecione o método de autenticação a ser usado pelo instalador para configurar o banco de dados do Dell Data Protection. 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 serão usadas para autenticação (os campos Nome de usuário e Senha não poderão 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 Dell Enterprise 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 operar com o Dell Enterprise 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 servidor.

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

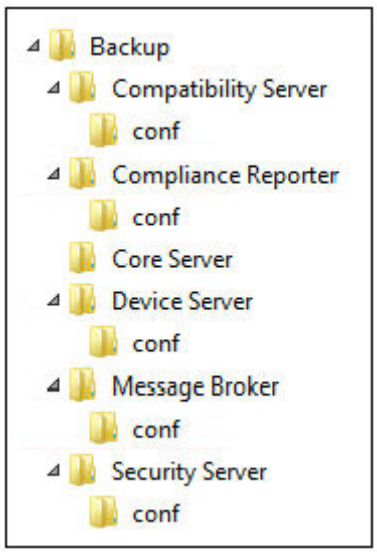
**NOTA:**
Se você tiver um Dell Enterprise Server 8.x funcional ou mais recente, consulte as instruções em Atualizar/Migrar os servidor(es) de back-end.

Você pode instalar um novo Dell Enterprise 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 Dell Enterprise Server a ser instalada.

Um banco de dados 8.x ou mais recente 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 8.0**, entre em contato com a Dell ProSupport para obter assistência**.**

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 Dell Enterprise 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 Dell Enterprise Server. O acesso a esses arquivos é necessário para configurar o Dell Enterprise 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 Dell Enterprise Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Dell Enterprise Server-x64 no diretório raiz do servidor onde você está instalando o Enterprise Server. ***Copiar/colar ou arrastar/soltar produzirá erros e causará uma instalação malsucedida.***

2 Clique duas vezes em **setup.exe**.

3 Quando o *Assistente do InstallShield* aparecer, selecione o idioma da 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, concluiu, de forma opcional, a etapa 9 na 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**.

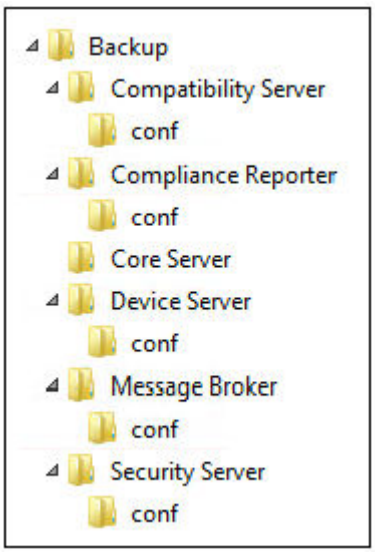
9 Para instalar o Dell Enterprise Server no local padrão **C:\Program Files\Dell**, clique em **Avançar**. Caso contrário, clique em **Alterar** para selecionar outro local e clique em **Avançar**.

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.

**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**.

**NOTA:**

**Por padrão, o certificado expira em um ano.**

12 Para a Criptografia do servidor (SE - 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

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 ano.**

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**.
- 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 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 login no Windows serão usadas para autenticação (os campos Nome de usuário e Senha não poderão 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**.

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.

  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 Enterprise 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 Enterprise 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 Dell Enterprise Server, isso é considerado uma *Recuperação.* Esta caixa de diálogo é mostrada:

- 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**.

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

**NOTA: O Serviço de sinalizador é instalado como parte desta instalação para suportar o sinalizador de retorno de chamada do Data Guardian, que insere um sinalizador de retorno de chamada em cada arquivo protegido pelo Data Guardian ao executar o modo Protected Office (Documentos protegidos do Office). Isso permite a comunicação entre qualquer dispositivo em qualquer local e o Servidor Front-End Dell. Verifique se a segurança da rede necessária está configurada antes de usar o sinalizador de retorno de chamada. A política Enable Callback Beacon (Ativar sinalizador de retorno de chamada) está ativada por padrão.**

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

1 Na mídia de instalação Dell, navegue até o diretório do Dell Enterprise Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Dell Enterprise Server-x64 no diretório raiz do servidor onde você está instalando o Enterprise Server. ***Copiar/colar ou arrastar/soltar produzirá erros e causará uma instalação malsucedida.***

2 Clique duas vezes em **setup.exe**.

3 Quando o *Assistente do InstallShield* aparecer, selecione o idioma da 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 Inserir a chave do produto.

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. **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

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 ano.**

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 **Enterprise Edition** 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 você tiver certeza de que não quer configurá-lo para instalação. Se você desmarcar um proxy nessa caixa de diálogo, ele não será instalado.

  Quando concluído, clique em **OK**.
- Para ver ou editar as portas, na caixa de diálogo *Configuração do servidor de front-end* clique em **Edit 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.

# Upgrade/Migração

Você pode fazer o upgrade do Dell Enterprise Server v8.0 ou posterior para o Dell Enterprise Server v9.x. Se a sua versão do servidor for anterior à v8.0, primeiramente você precisará fazer o upgrade para a v8.0 e, em seguida, para a v9.x.

## Antes de iniciar a atualização/migração

Antes de começar, certifique-se de que toda a Configuração de pré-instalação esteja concluída. Isso é de grande importância se você estiver implantando o Mobile Edition.

Leia os *relatórios técnicos do Enterprise Server* para conhecer qualquer solução atual ou problema conhecido relacionado à instalação do Dell Enterprise 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 da Dell e que o software da 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 de políticas, recomendamos atualizar para as versões mais recentes do Dell Enterprise Server e dos Clientes.

O Dell Enterprise Server v9.x suporta:

- Enterprise Edition:
  - Clientes do Windows v7.x/8.x
  - Clientes Mac v7.x/8.x
  - Clientes do SED v8.x
  - Authentication v8.x
  - BitLocker Manager v7.2x+ e v8.x
  - Data Guardian v1.x
- Endpoint Security Suite v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Atualização/migração do Dell Enterprise Server v8.x ou superior. Ao migrar de uma versão anterior para a versão 8.x do Dell Enterprise Server, entre em contato com o Dell ProSupport para obter assistência.

Ao fazer upgrade/migração do Dell Enterprise 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 Dell Enterprise Server e seus componentes, seguido da instalação/upgrade do cliente.

**Aplicar as alterações da política**

1 Como um administrador Dell, faça login no Remote Management Console.

2 No menu à esquerda, clique em **Gerenciamento** > **Confirmar**.

3 Digite uma descrição da alteração no campo Comentário.

4 Clique em **Confirmar políticas**.

5 Quando a confirmação for concluída, faça logoff do Remote Management Console.

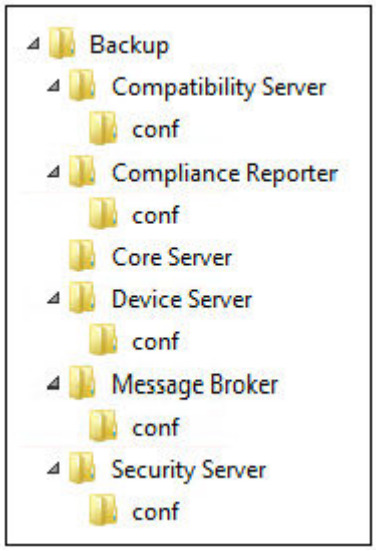
**Confirmar se os Serviços Dell estão funcionando**

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 serão 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 Dell Enterprise Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Dell Enterprise Server-x64 no diretório raiz do servidor onde você está instalando o Enterprise Server. ***Copiar/colar ou arrastar/soltar produzirá erros e causará uma instalação malsucedida.***

2 Clique duas vezes em **setup.exe**.

3 Quando o *Assistente do InstallShield* aparecer, selecione o idioma da instalação e clique em **OK**.

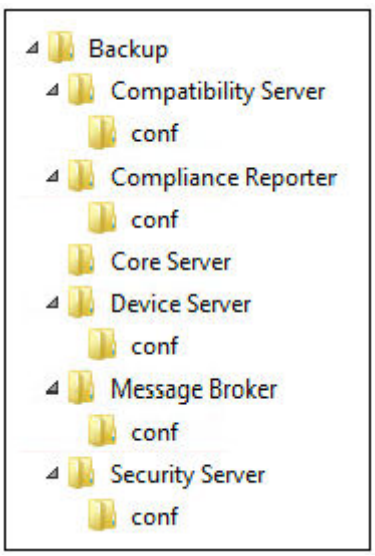
4 Na caixa de diálogo *Bem-vindo*, clique em **Avançar**.

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 serão usadas para autenticação (os campos Nome de usuário e Senha não poderão 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 servidor.

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

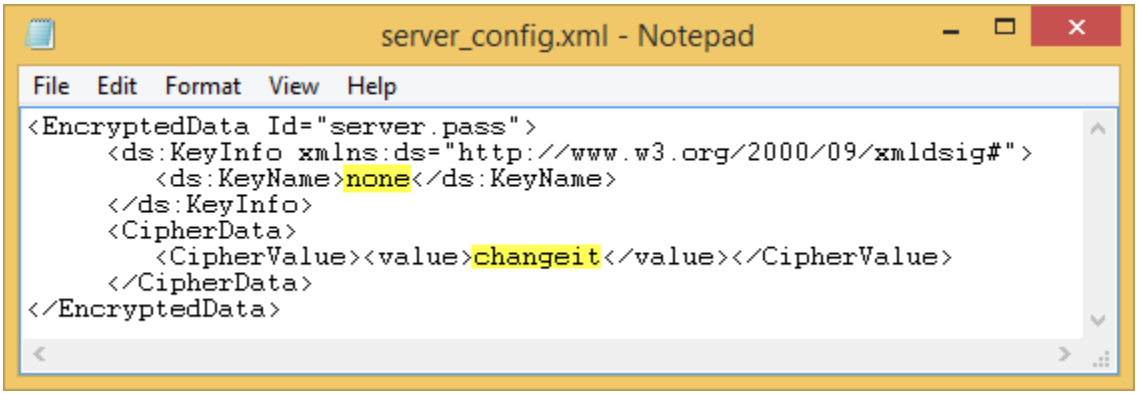
13 Na nova instalação, abra <diretório de instalação do Compatibility Server>\conf\server_config.xml e substitua o valor **server.pass** pelo valor do <diretório de instalação do Compatibility Server>\conf\server_config.xml, do qual foi feito backup, da seguinte forma:

**Instruções para server.pass:**

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

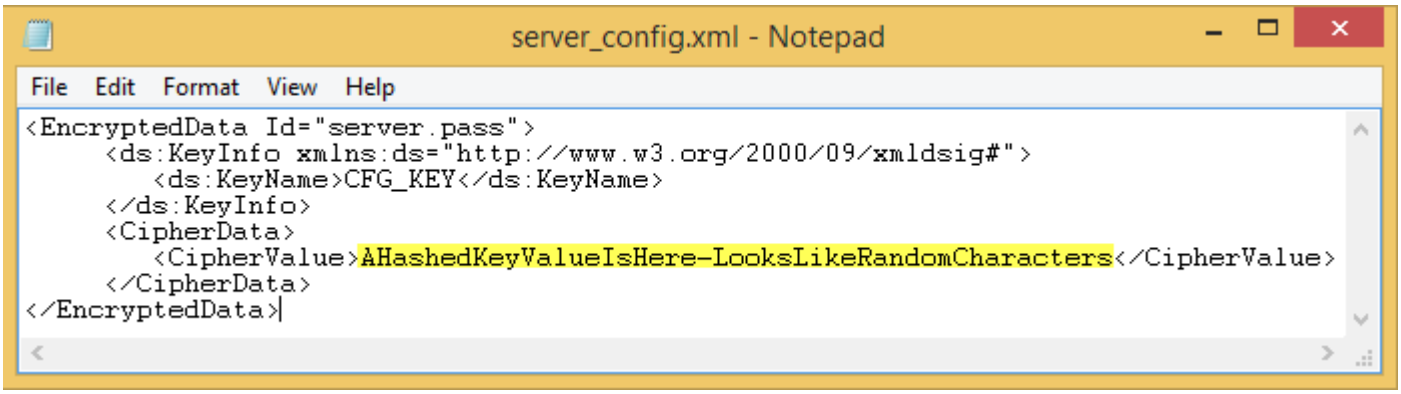
- Edite o *KeyName* do valor **CFG_KEY** para **none**.
- Digite a senha com texto sem formatação e coloque-a entre *<value> </value>*, que neste exemplo é **<value>changeit</value>**
- Quando o Dell Enterprise Server for iniciado, a senha com texto sem formatação terá hash, e o valor de hash substituirá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




Salve e feche o arquivo.

**NOTA:**
Não tente alterar a senha do **Dell** Enterprise 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.

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

**NOTA: Começando com a v9.5, o Serviço de sinalizador é instalado como parte desta atualização usando o nome de host padrão e a porta 8446. O Serviço de sinalizador suporta o sinalizador de retorno de chamada do Data Guardian, que insere um sinalizador de retorno de chamada em cada arquivo protegido pelo Data Guardian ao executar o modo Protected Office (Documentos protegidos do Office). Isso permite a comunicação entre qualquer dispositivo em qualquer local e o Servidor Front-End Dell. A política Enable Callback Beacon (Ativar sinalizador de retorno de chamada) está ativada por padrão. Verifique se a segurança da rede necessária está configurada antes de usar o sinalizador de retorno de chamada.**

1. Na mídia de instalação Dell, navegue até o diretório do Dell Enterprise Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Dell Enterprise Server-x64 no diretório raiz do servidor onde você está instalando o Enterprise Server. ***Copiar/colar ou arrastar/soltar produzirá erros e causará uma instalação malsucedida.***
2. Clique duas vezes em **setup.exe**.
3. Quando o *Assistente do InstallShield* aparecer, selecione o idioma da 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.

a No servidor de back-end, vá para <diretório de instalação do Security Server>\conf\ e abra o arquivo application.properties.

b Localize publicdns.server.host e defina o nome para um nome de host resolvido externamente.

c 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 servidor até que as tarefas de configuração pós-instalação sejam concluídas.

# Instalação em modo Desconectado

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

O Enterprise Server é instalado em modo Disconnected (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 **Cancel** (Cancelar) |
| /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 "Yes" (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 serão armazenados neste local. |

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

**Parâmetros**

AIRGAP=1 - Este valor deve ser "1" para instalar o Enterprise Server em modo Disconnected (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

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 - Esse valor será analisado para obter informações do servidor, da instância e da porta.

Exemplo:

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE - Opcional. O valor padrão é FALSE (falso), 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 (verdadeiro).

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.

**Parâmetros**

**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 também são usadas pelos serviços Dell, para operar com o Enterprise 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\nomedeusuário. 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 (nulo) (esse login não é adicionado). Quando o valor é definido como T, se o SQL_EE_USERNAME não for um login ou usuário do banco de dados, o instalador tentará adicionar as credenciais de autenticação SQL do usuário e definir privilégios para permitir que as credenciais sejam usadas pelo produto.

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 `servidor.domínio.com`.

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

CORESERVERHOST - Opcional. Nome de host do Core Server.

RMIHOST - Opcional. Nome de host do Compatibility Server.

REPORTERHOST - Opcional. Nome de host do Compliance Reporter.

DEVICEHOST - Opcional. Nome de host do Device Server.

KEYSERVERHOST - Opcional. Nome de host do Key Server.

TIGAHOST - Opcional. Nome de host do Security Server.

SMTP_HOST - Opcional. Nome de host SMTP.

ACTIVEMQHOST - Opcional. Nome de host 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.

| Parâmetros |
| --- |
| DEVICEPORT - Opcional. |
| KEYSERVERPORT - Opcional. |
| GKPORT - Opcional. |
| TIGAPORT - Opcional. |
| SMTP_PORT - Opcional. |
| ACTIVEMQ_TCP - Opcional. |
| ACTIVEMQ_STOMP - Opcional. |

# Instalar o Enterprise Server em modo Desconectado

O exemplo a seguir instala o Enterprise 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 Dell Enterprise Server

1. Na mídia de instalação Dell, navegue até o diretório do Dell Enterprise Server. **Descompacte** (NÃO copie/cole nem arraste/solte) o Dell Enterprise Server-x64 no diretório raiz do servidor de onde você está desinstalando o Enterprise Server. ***Copiar/colar ou arrastar/soltar produzirá erros e causará 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**.

5

# Configuração Pós-Instalação

Leia os *relatórios técnicos do Enterprise Server* para conhecer as soluções atuais ou os problemas conhecidos relacionados à instalação do Dell Enterprise Server.

Mesmo que você esteja instalando o Dell Enterprise Server pela primeira vez ou se estiver fazendo o upgrade de uma instalação existente, alguns componentes do seu ambiente precisam ser configurados.

## Instalação e Configuração do Gerenciamento do EAS

Esta seção precisa ser concluída se você quiser usar o Mobile Edition. Se não estiver, omita essa seção e continue para a Configuração do Dell Security Server no modo DMZ.

**Pré-requisitos**

- A conta de login do Serviço do Gerenciador de caixas de correio do EAS precisa ser uma conta com permissões para criar/modificar a política do Exchange ActiveSync, atribuir políticas às caixas postais dos usuários e consultar informações sobre os dispositivos do ActiveSync.
- O Utilitário de Configuração do EAS precisa ser executado com permissões de administrador para modificar arquivos e reiniciar Serviços.
- A conexão de rede com o Dell Policy Proxy é obrigatória.
- Tenha o FQDN do Dell Policy Proxy disponível.
- Tenha o número da porta do Dell Policy Proxy em mãos.
- O Microsoft Message Queuing (MSMQ) deve estar instalado/configurado no servidor que hospeda o ambiente do Exchange. Do contrário, consulte Instalar/Configurar MSMQ (Microsoft Message Queuing).

**Durante o processo de implantação**

Se você pretende usar o Exchange ActiveSync para gerenciar dispositivos móveis por meio do Mobile Edition, será necessário configurar o ambiente do Exchange Server.

## Instale o Gerenciador de dispositivos do EAS

1 Na mídia de instalação Dell, navegue até a pasta Gerenciamento do EAS. Na pasta Gerenciamento de EAS, copie o setup.exe para o(s) *Servidor(es) de Acesso de Clientes do Exchange*.

2 Clique duas vezes em **setup.exe** para iniciar a instalação. Se o seu ambiente inclui mais de um *Servidor de Acesso de Clientes do Exchange*, execute este instalador em cada um.

3 Selecione o idioma para a instalação e clique em **OK**.

4 Clique em **Avançar** quando a tela *Boas-vindas* for mostrada.

5 Leia o contrato de licença, concorde com os termos e clique em **Avançar**.

6 Clique em **Avançar** para instalar o Gerenciador de dispositivos do EAS no local padrão de **C:\Inetpub\wwwroot\Dell\EAS Device Manager**.

7 Clique em **Instalar** na tela *Pronto para começar a instalação*.

Uma janela de status mostra o andamento da instalação.

8 Se desejar, marque a caixa de seleção para mostrar o log do instalador do Windows e clique em **Concluir**.

# Instalar o Gerenciador de caixas de correio do EAS

1 Na mídia de instalação Dell, navegue até a pasta Gerenciamento do EAS. Na pasta Gerenciador de caixas de correio do EAS, copie o arquivo setup.exe para o(s) *Servidor(es) de caixas de correio do Exchange*.

2 Clique duas vezes em **setup.exe** para iniciar a instalação. Se o seu ambiente inclui mais de um Servidor de caixas de correio do Exchange, execute este instalador em cada um.

3 Selecione o idioma para a instalação e clique em **OK**.

4 Clique em **Avançar** quando a tela *Boas-vindas* for mostrada.

5 Leia o contrato de licença, concorde com os termos e clique em **Avançar**.

6 Clique em **Avançar** para instalar o Gerenciador de caixas de correio do EAS no local padrão de **C:\Program Files\EAS Mailbox Manager **.

7 Na tela Logon Information (Informações de login), digite as credenciais da conta do usuário que fará login para usar esse Serviço.

Nome de usuário: DOMÍNIO\Nome de usuário

Senha: a senha associada ao nome de usuário

Clique em **Avançar**.

8 Clique em **Instalar** na tela *Pronto para começar a instalação*.

Uma janela de status mostra o andamento da instalação.

9 Se desejar, marque a caixa de seleção para mostrar o log do instalador do Windows e clique em **Concluir**.

# Usar o Utilitário de configuração de EAS

1 No mesmo computador, acesse **Iniciar** > **Utilitário de configuração do EAS Dell** > > **Configuração do EAS** para executar o utilitário de configuração do EAS.

2 Clique em **Configurar** para definir as Configurações do Gerenciamento do EAS.

3 Insira as seguintes informações:

FQDN do Dell Policy Proxy

Porta do Dell Policy Proxy (a porta padrão é 8090)

Intervalo de Sondagem do Dell Policy Proxy (o padrão é 1 minuto)

Selecione a caixa para executar o EAS Device Manager no modo apenas relatório (recomendado durante a implementação)

> **NOTA:**
> O modo apenas de relatório permite que dispositivos/usuários desconhecidos tenham acesso ao Exchange ActiveSync, mas ainda informa o tráfego a você. Quando a sua implantação estiver ativa e funcionando, você poderá alterar essa configuração para reforçar a segurança.

Clique em **OK**.

4 Uma mensagem de êxito será exibida. Clique em **Sim** para reiniciar os Serviços do Gerenciador de caixas de correio do EAS e IIS.

5 Clique em **Sair** quando terminar.

# Definir as configurações de gerenciamento do EAS

Quando a sua implementação estiver ativa e funcionando e você estiver pronto para reforçar a segurança, siga as etapas abaixo.

1 Acesse **Iniciar** > **Dell** > **Utilitário de configuração de EAS** > **Configuração do EAS** para executar o Utilitário de configuração de EAS.
2 Clique em **Configurar** para definir as Configurações do Gerenciamento do EAS.
3 Insira as seguintes informações:
FQDN do Dell Policy Proxy

Porta do Dell Policy Proxy (a porta padrão é 8090)

Intervalo de Sondagem do Dell Policy Proxy (o padrão é 1 minuto)

Desmarque a caixa para executar o EAS Device Manager no modo apenas de relatório

Clique em **OK**.
4 Uma mensagem de êxito será exibida. Clique em **Sim** para reiniciar os Serviços do Gerenciador de caixas de correio do EAS e IIS.
5 Clique em **Sair** quando terminar.

# Dell Security Server na Configuração do Modo DMZ

Se o Dell 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 confiável, algumas etapas manuais serão necessárias para adicionar o certificado confiável ao armazenamento de chaves Java da rede privada do Dell Security Server.

Se um certificado confiável estiver sendo usado, omita esta seção e acesse Inscrição de APNs.

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

# Use o Keytool para importar o Certificado de Domínio de DMZ

**IMPORTANTE:**
Faça backup dos cacerts existentes do **Dell** Security Server antes de continuar com as instruções do Keytool. Se ocorrer um erro de configuração, não será possível reverter para o arquivo salvo.

**Suposições**

- O Dell Security Server foi instalado com um certificado não confiável.
- O Dell Security Server no Modo DMZ foi instalado usando um certificado assinado (Entrust, Verisign, etc.)
- Um arquivo de certificado .pfx está disponível. Se o seu certificado precisar ser convertido para .pfx, consulte Exportar um certificado para .PFX usando o Console de Gerenciamento de certificado.

**Processo**

1 Adicione Keytool ao caminho do sistema.

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

2 Use o Keytool para listar o conteúdo do certificado de domínio confiável que você deseja importar. Anote o Nome do Alias listado.

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

3 Use o Keytool para importar o conteúdo do certificado assinado para o arquivo cacert do Dell Security Server:

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

Para -srcalias, você terá que reunir estas informações do conteúdo exportado do certificado assinado.

Para -destalias, pode ser qualquer local que você escolha.

4 Faça backup e substitua o arquivo cacerts atual no diretório <Security Server install dir>\conf\ por este arquivo cacerts recém-criado no Dell Security Server.

# Modifique o arquivo application.properties

Modifique o arquivo application.properties para especificar o alias do certificado de assinatura.

1 Acesse o diretório <Security Server install dir>\conf\application.properties
2 Modifique as seguintes informações:
keystore.alias.signing=<Altere esse valor para aquele da etapa 3 acima para `-destalias>`
3 Reinicie o serviço do Dell Security Server.

# Inscrições de APNs

Se você deseja usar o Mobile Edition for Mobile Device Security com dispositivos iOS, o assistente de inscrição de APNs precisa ser usado para:

- Criar um CSR
- Criar um Apple Push Certificate
- Carregar um Push Certificate

Se você não deseja usar o Mobile Edition for Mobile Device Security com dispositivos iOS, omita esta seção e continue para a Server Configuration Tool.

O serviço Apple Push Notification (APNs) permite a comunicação segura com dispositivos do iOS sem fio. As APNs são usadas para enviar notificações a um dispositivo do iOS para fazer check in com o Dell Enterprise Server. As APNs apenas enviam notificações para o dispositivo, nenhum dado é enviado.

**Processo**

1 Abra um navegador e vá para https://<FQDN-of-security-server>:8443/csrweb.
2 No diálogo de login do Assistente de Inscrição de APNs, digite as credenciais do Dell Administrator e clique em **Login** (Fazer login).
3 Um diálogo é mostrado descrevendo as etapas que você terá que seguir. Clique em **Avançar**.

**Etapa I: Criar uma CSR**

4 Insira as seguintes informações:

Email: o endereço de e-mail pode ser qualquer UPN, mas recomendamos o uso de uma conta para o administrador que manterá o certificado de APNs.

Nome Comum: digite o Nome Comum associado a este endereço de email.

Clique em **Generate CSR** (Gerar CSR).

5 Após gerar um CSR, salve o arquivo em um local facilmente acessível.
6 Clique em **Avançar**.

**Etapa II: Criar um certificado Apple Push**

7 Clique no link do **Apple Push Certificate Portal**. Faça login com o ID Apple e senha.

8 Leia os Termos de Uso, indique a aceitação e clique em **Accept** (Aceitar).

9 Clique em **Browse** (Procurar) e, em seguida, faça **Upload** do CSR que você acabou de criar.

10 Na página *Certificates for Third-Party Servers* (Certificados para servidores de terceiros), clique em **Download** (Fazer download). Salve o arquivo em um local facilmente acessível.

11 Retorne o Assistente de Inscrição de APNs e clique em **Next** (Avançar).

**Etapa III: Carregar o certificado Push**

12 Digite as informações a seguir (use as mesmas credenciais que foram usadas na Etapa I: Criar CSR).

E-mail:

Nome comum:

Arquivo Push Cert: Clique em **Browse** (Procurar) para localizar o arquivo salvo na etapa 7. Clique em **Upload** (Fazer upload).

13 Uma mensagem de êxito será exibida. Clique em **Concluir**.

A inscrição do Certificado de APNs com o Dell Enterprise Server está concluída.

# Server Configuration Tool

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

O Dell Server Configuration Tool permite:

- Adicionar certificados novos ou atualizados
- Importar o Certificado do Dell Manager
- Importar certificado de identidade
- Definir as configurações certificado do SSL Server ou Mobile Edition
- Configurar parâmetros de SMTP para o Data Guardian ou serviços de e-mail
- Alterar o nome do banco de dados, o local ou as credenciais
- Migrar o banco de dados

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

Para iniciar o Dell Server Configuration Tool, acesse **Iniciar** > **Programas** > **Dell** > **Enterprise Edition** > **Server Configuration Tool** > **Executar Server Configuration Tool**.

Os logs da Dell Server Configuration Tool são salvos em **C:\Program Files\Dell\Enterprise Edition\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. Os certificados autoassinados são adequados para pilotos, POCs, etc. Para um ambiente de produção, a Dell recomenda certificados assinados por CA pública e assinados por domínio.
- **Assinados** (assinados por CA pública ou assinados por domínio) são assinados por uma CA pública ou um domínio. No caso de certificados que são assinados por uma autoridade de certificação (autoridade de certificação) pública, o certificado da autoridade de certificação 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, Dell Device Server e assim por diante)
- Aplicativos .NET (Dell Core Server)
- Validação de cartões inteligentes usados para Autenticação de Pré-Inicialização (Dell 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 clientes Enterprise Edition remotamente gerenciados com unidades de autocriptografia ou BitLocker Manager.
- Estações de trabalho clientes:
    - Estações de trabalho que executam BitLocker Manager
    - Estações de trabalho que executam o Enterprise Edition (clientes Windows)
    - Estações de trabalho que executam o Endpoint Security Suite
    - 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 cartões inteligentes exige validação de SSL com o Dell 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 precisa 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 Dell Security Server. Para obter mais informações, consulte Crie um Certificado autoassinado e gere uma Solicitação de assinatura de certificado. 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.
- 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, etc. 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 Enterprise Server serão usadas, se estiverem disponíveis.

3 No menu superior, selecione **Configuração** > **Salvar**. Se solicitado, confirme o salvamento.

A configuração do certificado foi 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 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 Enterprise Server serão usadas, se estiverem disponíveis.

4 No menu superior, selecione **Configuração** > **Salvar**. Se solicitado, confirme o salvamento.

A configuração do certificado foi 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 Enterprise Server serão 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 autoasssinado que foi criado durante a instalação do Enterprise Server serão 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 Dell Enterprise 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 autoasssinado que foi criado durante a instalação do Enterprise Server serão usadas, se estiverem disponíveis.

    Clique em **Avançar**.

    Clique em **Concluir** quando terminar.

A configuração do certificado foi 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 o Certificado do Dell Manager

Se sua implementação contém clientes Enterprise Edition remotamente gerenciados com unidades de autocriptografia ou BitLocker Manager, 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 sendo enviados aos clientes remotamente gerenciados do Enterprise Edition e ao BitLocker Manager. 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 o arquivo a ser salvo. 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 (Ferramenta de configuração do Dell Server).

22 No menu superior, selecione **Ações** > **Importar certificado do gerenciador**.

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 *Services* (Serviços) abrir, navegue até cada Serviço da Dell e clique em **Start the service** (Iniciar o serviço).

# Importar certificado de identidade

Se a sua implementação inclui o Server Encryption, você precisará importar seu certificado recém-criado (ou existente). O certificado de identidade protege a chave privada usada para assinar os pacotes de políticas enviados aos servidores clientes. Esse certificado pode ser independente de qualquer outro certificado.

1 No menu superior, selecione **Ações** > **Importar certificado de identidade**.

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 certificado do SSL Server ou Mobile Edition

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, marque a opção **Desativar a verificação da cadeia de confiança**.

**SCEP:**

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

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**.

# Configurar parâmetros de SMTP para o Data Guardian ou serviços de e-mail

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

Esta guia configura os parâmetros de SMTP para o Data Guardian. Se as configurações de SMTP tiverem de ser definidas para outras finalidades fora do Data Guardian, consulte o tópico AdminHelp "Ativar servidor SMTP para notificações de e-mail de licença".

Insira as seguintes informações:

1 No campo Nome de host:, digite o FQDN do seu servidor SMTP, como nomedoservidorsmtp.domínio.com.

2 No campo Nome de usuário:, digite o nome de usuário que fará login no servidor de email. O formato pode ser DOMÍNIO\joao, joao, ou o formato que sua organização exigir.

3 No campo Senha:, digite a senha asociada a este nome de usuário.

4 No campo Endereço de origem:, digite o endereço de email de origem. Pode ser igual ao da conta do nome de usuário (joao@domínio.com), mas também pode ser de outra conta que o nome de usuário epecificado tem acesso para enviar email (CloudRegistration@domínio.com).

5 No campo Porta:, digite o número da porta (normalmente 25).

6 No menu Autenticação:, selecione Verdadeiro ou Falso.

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 o nome do banco de dados, o local ou as credenciais

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

1 No campo `Server Name:` (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 No campo `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.

3 No campo *`Banco de dados:`*, digite o nome do banco de dados.

4 No campo *Autenticação*, selecione **Autenticação do Windows** ou **Autenticação do servidor SQL**. Se você escolher Autenticação do Windows, as mesmas credenciais usadas para fazer login no Windows serão usadas para autenticação (os campos Nome de usuário e Senha não poderão ser editados).

5 No campo `User Name:` (Nome do usuário:), digite o nome de usuário apropriado associado a este banco de dados.

6 No campo `Password:` (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 *Configuration Test* (Teste de configuração), leia as informações de teste e clique em **Next** (Avançar).

10 Se você escolher Windows Authentication (Autenticação do Windows) na guia *Database* (Banco de dados), poderá digitar credenciais alternativas para permitir o uso das mesmas credenciais que serão usadas para executar o Dell Enterprise Server. Clique em **Avançar**.

11 Na janela *Test Configuration* (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.

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 *Services* (Serviços) abrir, navegue até cada Serviço da Dell e clique em **Start the service** (Iniciar o serviço).

# Migrar o banco de dados

Você pode migrar um banco de dados da versão 8.x para o esquema mais recente com a versão mais recente da Server Configuration Tool. Para obter a Server Configuration Tool mais recente ou para migrar um banco de dados de versão anterior para a versão 8.0, entre em contato com a Dell ProSupport para obter assistência.

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

1 Se você ainda não tiver feito backup do banco de dados da Dell existente, **faça-o agora**.

2 No menu superior, selecione **Actions** > **Initialize Database** (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 *Migrating Database* (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 Finish (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 *Services* (Serviços) abrir, navegue até cada Serviço da Dell e clique em **Start the service** (Iniciar o serviço).

# 6

# Tarefas administrativas

## Atribuir Função de Dell Administrator

1 Como um Dell Administrator, faça login no Remote Management Console neste endereço: 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 em que você deseja 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 aparecer 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**.

## Fazer login com a Função de Dell Administrator

1 Faça logout do Remote Management ConsoleEnterprise Server.
2 Faça login no Remote Management ConsoleEnterprise Server e faça login com as credenciais de usuário de 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 após as modificações nas políticas forem salvas, siga as seguintes instruções:

1 No painel à esquerda, clique em **Gerenciamento > Confirmar**.
2 Digite uma descrição da alteração no campo Comentário.
3 Clique em **Confirmar políticas**.

# Configurar 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.
3 Dois métodos de autenticação diferentes são suportados. Para configurar, selecione:

- Configurar a autenticação do SQL com o Compliance Reporter
- Configurar a autenticação do Windows com o Compliance Reporter

# Configurar a autenticação do SQL com o Compliance Reporter

A partir da versão 8.1, a Origem de Dados é pré-configurada automaticamente. Não é necessário executar nenhuma configuração. Use as etapas abaixo para alterar a Origem de Dados, se for necessário.

1 Para definir a Origem de Dados, no menu superior, clique em **Settings** (Configurações). No menu à esquerda, clique em **Data Source** (Origem de Dados).
2 Digite o nome de usuário para fazer o login no banco de dados Dell.
3 Digite a senha para fazer o login no banco de dados Dell.
4 Digite o nome de host para fazer o login no banco de dados Dell.
5 Digite o nome do banco de dados para fazer o login no banco de dados Dell.
6 Digite o número máximo de conexões ociosas permitido. O padrão é 2.
7 Digite o número máximo de conexões (ativas) permitido. O padrão é 10.
8 Digite o tempo máximo de espera (número máximo de milissegundos para aguardar uma conexão). O valor -1 significa uma configuração indefinidamente.
9 Para verificar o URL do banco de dados e testar a conectividade entre o Dell Compliance Reporter e o banco de dados Dell, clique em **Test Connection** (Testar Conexão).
10 Clique em **Atualizar**. Para descartar as informações, clique em Cancelar.

As tarefas administrativas estão completas. O resto deste capítulo discute a Autenticação do Windows e pode ser ignorado caso a Autenticação SQL seja usada para o Dell Compliance Reporter.

**Se necessário**, continue para Criar um certificado auto-assinado e gerar uma solicitação de assinatura de certificado ou Exportar um certificado para .PFX usando o Console de gerenciamento de certificado.

# Configurar a autenticação do Windows com o Compliance Reporter

A partir da versão 8.1, a Origem de Dados é pré-configurada automaticamente. Não é necessário executar nenhuma configuração. Use as etapas abaixo para alterar a Origem de Dados, se for necessário.

1 Digite o nome de usuário para fazer o login no banco de dados Dell.
2 Deixe a senha em branco. Quando o usuário do domínio fizer o login, a senha será transmitida ao banco de dados.
3 Digite o nome de host para fazer o login no banco de dados Dell.
4 Digite o nome do banco de dados para fazer o login no banco de dados Dell.
5 Digite o número máximo de conexões ociosas permitido. O padrão é 2.
6 Digite o número máximo de conexões (ativas) permitido. O padrão é 10.

7 Digite o tempo máximo de espera (número máximo de milissegundos para aguardar uma conexão). O valor -1 significa uma configuração indefinidamente.

8 Para verificar o URL do banco de dados e testar a conectividade entre o Dell Compliance Reporter e o banco de dados Dell, clique em **Test Connection** (Testar Conexão).

9 Clique em **Atualizar**. Para descartar as informações, clique em Cancelar.

As tarefas administrativas estão completas. **Se necessário**, continue para Criar um certificado auto-assinado e gerar uma solicitação de assinatura de certificado ou Exportar um certificado para .PFX usando o Console de gerenciamento de certificado.

# Fazer backups

Para fins de recuperação de desastres, certifique-se de que os seguintes locais tenham um backup efetuado semanalmente, com diferenciais noturnos.

## Backups do Enterprise 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\gkresource.xml

## Backups do SQL Server

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, recomendamos que as boas práticas de bancos de dados sejam usadas para o banco de dados da Dell 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 explica as boas práticas do SQL Server que precisam ser implementadas quando o Dell Data Protection é instalado (caso ainda não tenham sido implementadas).

## Backups do PostgreSQL Server

Eventos de auditoria são armazenados no servidor PostgreSQL, cujo backup deve ser realizado regularmente. Para obter instruções de backup, consulte https://www.postgresql.org/docs/9.5/static/backup.html.

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.

# Descrições de componentes Dell

A tabela a seguir descreve cada componente e sua função.

| Nome | Descrição | Necessário para |
|---|---|---|
| Compliance Reporter | Fornece uma visão completa do ambiente para auditoria e geração de relatórios de conformidade.<br><br>Um componente do Dell Enterprise Server. | Geração de relatórios |
| Key Server | Negocia, autentica e criptografa uma conexão do cliente usando APIs Kerberos.<br><br>Precisa de acesso ao banco de dados SQL para obter os dados de chave.<br><br>Um componente do Dell Enterprise Server. | Utilitários de administrador Dell |
| Server Configuration Tool | Configura a comunicação do banco de dados com o Core Server e o Compatibility Server/ Security Server. Usado para inicializar o banco de dados na instalação ou para migrar o banco de dados para um esquema mais recente. Usado para controlar o Dell Services.<br><br>Um componente do Dell Enterprise Server. | Todos |
| Remote Management Console Enterprise Server Console | A central de controles e o console de administração da implantação de toda a empresa.<br><br>Um componente do Dell Enterprise Server. | Todos |
| Core Server | Gerencia o fluxo de política, as licenças, o registro para Preboot Authentication, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection. Processa os dados de inventário para uso pelo Compliance Reporter e pelo Remote Management Console. Coleta e armazena os dados de autenticação. Controla o acesso baseado em função.<br><br>Um componente do Dell Enterprise Server. | Todos |
| Security Server | Comunica-se com o Policy Proxy; gerencia as recuperações de chave forense, ativações dos clientes, produtos Data Guardian, comunicação SED-PBA e Active Directory para autenticação ou reconciliação, incluindo validação da identidade para a autenticação no Remote Management Console. Precisa de acesso ao banco de dados SQL. | Todos |

| Nome | Descrição | Necessário para |
|---|---|---|
| | Um componente do Dell Enterprise Server. | |
| Compatibility Server | 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 neste serviço.<br><br>Um componente do Dell Enterprise Server. | Todos |
| Message Broker Service | Lida com a comunicação entre os serviços do Enterprise Server. Armazena as informações de políticas criadas pelo Compatibility Server para o enfileiramento do Policy Proxy<br><br>Precisa de acesso ao banco de dados SQL.<br><br>Um componente do Dell Enterprise Server. | Todos |
| Device Server | Suporta ativações e a recuperação de senha.<br><br>Um componente do Dell Enterprise Server. | Enterprise Edition para Mac<br><br>Enterprise Edition para Windows<br><br>Proteções de assistentes digitais pessoais<br><br>CREDActivate |
| Plug-ins do Device Server | Fornece suporte para vários componentes.<br><br>Um componente do Dell Enterprise Server. | Todos |
| Identity Server | Processa as solicitações de autenticação de domínio.<br><br>Exige uma conta do Active Directory.<br><br>Precisa ser a conta usada para acessar o SQL quando a Autenticação do Windows é usada.<br><br>Um componente do Dell Enterprise Server. | Todos |
| Policy Proxy | Fornece um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário.<br><br>Um componente do Dell Enterprise Server. | Enterprise Edition para Mac<br><br>Enterprise Edition para Windows<br><br>Mobile Edition for Mobile Device Security |
| Security Token Services (STS) | Usado para ajudar a criar um canal de autenticação seguro entre a interface de usuários do Dell Enterprise Server e os serviços de back-end Dell. | Todos |
| EAS Device Manager | Ativa a funcionalidade sem fio. Instalado no Servidor de Acesso do Cliente Exchange. | Gerenciamento do Exchange ActiveSync de dispositivos móveis. |
| Gerenciador de caixas de correio do EAS | O agente de correio instalado no Servidor de caixa de correio do Exchange. | Gerenciamento do Exchange ActiveSync de dispositivos móveis. |

# 8

# Práticas recomendadas do SQL Server

A lista a seguir explica as boas práticas do SQL Server que precisam ser implementadas quando o Dell Data Protection é 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.

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

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

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

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

# Crie um Certificado autoassinado e gere 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.

Recomendamos 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 cartões inteligentes para autenticação, você precisará x'usar Keytool para importar a cadeia confiável de certificados completa que é usada no certificado do usuário de cartões inteligentes.

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 autoassinado

1 Navegue até o diretório **conf** do Dell Compliance Reporter, Dell Security Server ou Dell Device Server.

2 Faça o backup do banco de dados de certificado padrão:

Clique em **Start** (Iniciar) > **Run** (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 **Dell** Enterprise 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\eserver.properties. Defina o valor eserver.keystore.password =

<diretório de instalação do Security Server>\conf\eserver.properties. Defina o valor eserver.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. Esse nome totalmente qualificado inclui o nome do host e o nome do domínio (exemplo, server.domain.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.

# Solicite um certificado assinado de uma autoridade de certificado

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.

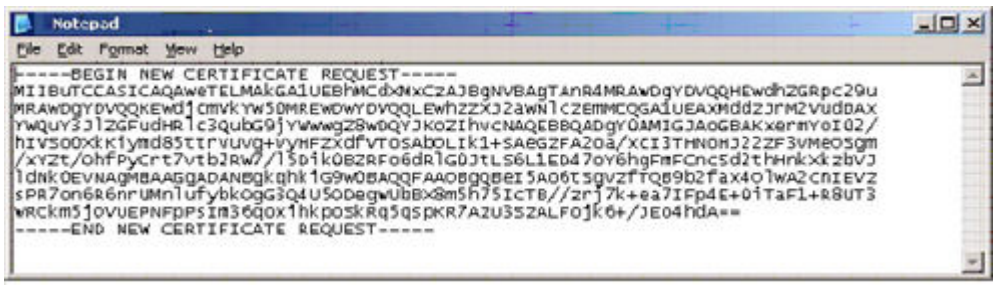
1 Substitua o mesmo valor usado anteriormente por <**certificatealias**>:

```
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 conterá um par BEGIN/END que será 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.

> **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 o 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 Dell Compliance Reporter, Dell Security Server ou Dell Device Server, altere o diretório **conf** do componente.
- Se você estiver ativando o SSL entre o Dell Enterprise 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, o que será configurado internamente pela sua organização.

1 Acesse o Microsoft CA Server. O endereço IP será 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. Volte à janela do DOS. 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 mostrará 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 Dell Security Server for usado no Modo DMZ *e* ao importar um certificado do Dell Manager para a Dell 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 o arquivo a ser salvo. 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 tiver sido usado para o 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.