Dell Security Management Server

Installation and Migration Guide v10.2.4

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam a melhorar a utilização do produto.

AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.

2019-05

Rev. A01

Contents

1

Introdução

Acerca do Security Management Server

O Security Management Server tem as seguintes funções:

- Gestão centralizada de dispositivos, utilizadores e política de segurança
- Relatórios e auditorias de conformidade centralizados
- Separação de deveres administrativos
- Criação e gestão de políticas de segurança baseadas em funções
- Distribui as políticas de segurança quando os clientes estabelecem ligação
- Recuperação de dispositivos assistida por administrador
- Caminhos fidedignos para comunicação entre componentes
- Geração de chaves de encriptação exclusivas e caução de chave de segurança automática

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo o seu Código de serviço ou Código de serviço expresso disponível quando nos contactar.

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

2

Requisitos e arquitetura

Esta secção especifica os requisitos de hardware e software e as recomendações de projeto de arquitetura para implementação do Dell Security Management Server.

Arquitetura do Security Management Server

As soluções Dell Encryption, Endpoint Security Suite Enterprise e Data Guardian são produtos altamente dimensionáveis, com base no número de pontos terminais pretendidos para encriptação na sua organização.

Componentes da arquitetura

Abaixo encontram-se sugestões de configurações de hardware que se adequam à maioria dos ambientes.

Security Management Server

- Sistema Operativo: Windows Server 2012 R2 (Standard, Datacenter de 64 bits), Windows Server 2016 (Standard, Datacenter de 64 bits), Windows Server 2019 (Standard, Datacenter)
- Máquina virtual/física
- CPU: 4 Core(s)
- RAM: 16 GB
- Unidade C: 30 GB de espaço disponível no disco rígido para registos e bases de dados da aplicação

> **NOTA: Podem ser consumidos até 10 GB para uma base de dados local guardada no PostgreSQL.**

Servidor Proxy

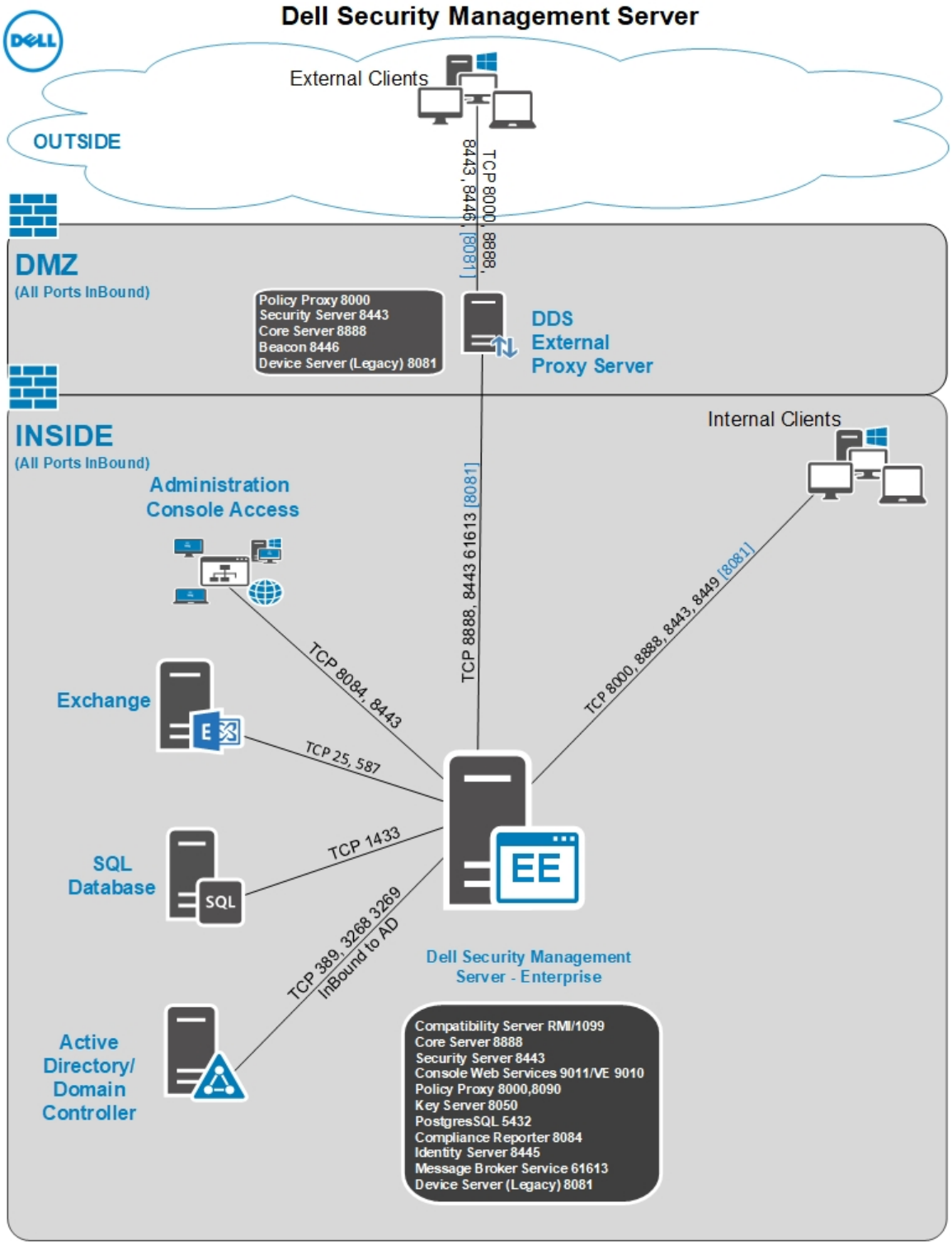
- Sistema Operativo: Windows Server 2012 R2 (Standard, Datacenter de 64 bits), Windows Server 2016 (Standard, Datacenter de 64 bits), Windows Server 2019 (Standard, Datacenter)
- Máquina virtual/física
- CPU: 2 Core(s)
- RAM: 8 GB
- Unidade C: 20 GB de espaço disponível no disco rígido para registos

Especificações do hardware do SQL Server

- CPU: 4 Core(s)
- RAM: 24 GB
- Unidade de dados: 100 -150 GB de espaço disponível no disco rígido (depende do ambiente)
- Unidade de registos: 50 GB de espaço disponível no disco rígido (depende do ambiente)

> **NOTA: A Dell recomenda seguir as Melhores práticas do SQL Server, mas as informações acima devem cobrir a maioria dos ambientes.**

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



NOTA: Se a organização tiver mais de 20 000 pontos terminais, contacte o Dell ProSupport para obter assistência.

Requisitos

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

Antes de iniciar a instalação, certifique-se que são realizadas todas as atualizações e aplicações de patches em todos os servidores utilizados na instalação.

Hardware

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

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

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

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

Virtualization

The Security Management Server can be installed in a virtual environment. Only the following environments are recommended.

Security Management Server v10.2.4 has been validated on the following platforms.

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

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

Security Management Server v10.2.4 has been validated with VMware ESXi 5.5, VMware ESXi 6.0, and VMware ESXi 6.5.

NOTE: When running VMware ESXi and Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019, VMXNET3 Ethernet Adapters are recommended.

- VMware ESXi 5.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-55/index.jsp for more information
- VMware ESXi 6.0
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-60/index.jsp for more information
- VMware ESXi 6.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - See http://www.vmware.com/resources/compatibility/search.php for a complete list of supported Host Operating Systems
  - Hardware must conform to minimum VMware requirements
  - 4 GB minimum RAM for dedicated image resource
  - See http://pubs.vmware.com/vsphere-65/index.jsp for more information

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

SQL Server

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

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

Software

A tabela seguinte descreve pormenorizadamente os requisitos de software para o Security Management Server e o servidor proxy.

NOTA: Devido à natureza sensível dos dados que o Security Management Server retém e para cumprir a regra de privilégios mínimos, a Dell recomenda a instalação do Security Management Server no seu próprio sistema operativo dedicado ou que faça parte de um servidor de aplicação com papéis e direitos limitados ativados para ajudar a assegurar um ambiente seguro. Isto inclui não instalar o Security Management Server em servidores de infraestrutura privilegiada. Consulte https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models para obter mais informações sobre como implementar a regra de privilégios mínimos.

NOTA: O Universal Account Control (UAC) tem de estar desativado durante a instalação num diretório protegido. Depois de desativar o UAC, o servidor tem de ser reiniciado para que esta alteração seja implementada.

NOTA: Localização dos registos do Policy Proxy (se instalado): HKLM\SOFTWARE\Wow6432Node\Dell

NOTA: Localização do registo dos servidores Windows: HKLM\SOFTWARE\Dell

Pré-requisitos

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

  Se não estiver instalado, o instalador irá fazê-lo por si.
- **Pacote Redistribuível do Visual C++ 2013**

  Se não estiver instalado, o instalador irá fazê-lo por si.
- **Pacote Redistribuível do Visual C++ 2015**

  Se não estiver instalado, o instalador irá fazê-lo por si.
- **.NET Framework Versão 3.5 SP1**
- **.NET Framework Versão 4.5**

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

  Se utilizar o SQL Server 2012 ou o SQL Server 2016.

  Se não estiver instalado, o instalador irá fazê-lo por si.

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

- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition
- **Windows Server 2016**

- Standard Edition

- Datacenter Edition

- **Windows Server 2019**

  - Standard Edition

  - Datacenter Edition

Repositório LDAP

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

Management Console e Compliance Reporter

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

NOTA: O browser tem de aceitar cookies.

Ambientes virtuais recomendados para os componentes do Security Management Server

O Security Management Server pode ser instalado num ambiente virtual.

A Dell atualmente suporta o alojamento do Dell Security Management Server ou do Dell Security Management Server Virtual num ambiente de infraestrutura como um serviço (IaaS) alojado na nuvem, como por exemplo, Amazon Web Services, Azure e vários outros fornecedores. O suporte para estes ambientes está limitado à funcionalidade do Security Management Server. A administração e a segurança destas máquinas virtuais são da responsabilidade do administrador da solução IaaS.

Requisitos adicionais de infraestrutura. Os requisitos adicionais de infraestrutura, tais como o Active Directory e o SQL Server, continuam a ser necessários para uma funcionalidade adequada.

NOTA: A base de dados do SQL Server que aloja o Security Management Server tem de ser executada num computador independente.

Base de dados

- **SQL Server 2008 R2 –** 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
- **SQL Server 2017 -** Standard Edition/Enterprise Edition

NOTA: Express Editions não são suportadas para ambientes de produção. Express Editions podem ser utilizadas apenas em POC e avaliações.

NOTA: Abaixo encontram-se os requisitos para permissões do SQL. O utilizador que está a executar a instalação e os serviços tem de ter direitos de administrador local. Além disso, são necessários direitos de administrador local para a conta de serviço que gere os serviços do Dell Security Management Server.

Tipo	Ação	Cenário	Privilégio do SQL necessário
Back-end	Atualizar	Por definição, as atualizações já têm DB e Início de sessão/ Utilizador estabelecidos	db_owner
Back-end	Restaurar instalação	Restaurar envolve um DB e início de sessão já existentes.	db_owner
Back-end	Nova instalação	Utilizar DB existente	db_owner
Back-end	Nova instalação	Criar novo DB	dbcreator, db_owner
Back-end	Nova instalação	Utilizar início de sessão existente	db_owner
Back-end	Nova instalação	Criar novo início de sessão	securityadmin
Back-end	Desinstalar	ND	ND
Proxy de front-end	Qualquer um	ND	ND

NOTA: Se o Controlo de Conta de Utilizador (UAC) estiver ativado, é necessário desativá-lo antes da instalação no Windows Server 2012 R2 quando instalar em C:\Program Files. O servidor tem de ser reiniciado para que esta alteração seja implementada.

Durante a instalação, são necessárias as credenciais de autenticação do Windows ou SQL para configurar a base de dados. Independentemente do tipo de credenciais utilizado, a conta tem de ter privilégios adequados para a ação a realizar. A tabela anterior descreve os privilégios necessários para cada tipo de instalação. Para além disso, a conta utilizada para criar e configurar a base de dados deve possuir um esquema predefinido configurado para dbo.

Estes privilégios são apenas necessários durante a instalação para configurar a base de dados. Assim que o Security Management Server estiver instalado, a conta utilizada para gerir o acesso a SQL pode ser restringida às funções db_owner e pública.

Se não tem a certeza sobre os privilégios ou conetividade à base de dados, peça ao seu administrador da base de dados para os confirmar antes de iniciar a instalação.

Suporte de idiomas da Management Console

A Management Console está em conformidade com a norma MUI (Multilingual User Interface - Interface do utilizador multilíngue) e suporta os seguintes idiomas:

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

3

Configuração de Pré-instalação

Antes de começar, leia o documento *Security Management Server Technical Advisories* (Avisos técnicos do Security Management Server) para ficar a conhecer soluções alternativas existentes ou problemas conhecidos relacionados com o Security Management Server.

A configuração de pré-instalação dos servidores onde pretende instalar o Security Management Server é muito importante. Preste especial atenção a esta secção para garantir a instalação correta do Security Management Server.

Configuração

1 Se ativada, desative a Configuração de segurança avançada do Internet Explorer (ESC). Adicione o URL do servidor Dell aos sites fidedignos nas opções de segurança do browser. Reinicie o servidor.

2 Abra as portas seguintes para cada componente:

Internas:

Comunicação por Active Directory: TCP/389

Comunicação por correio eletrónico (opcional): 25

Para front-end (se necessário):

Comunicação do Policy Proxy externo com o Message Broker: STOMP/61613

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

Comunicação para o Core Server de back-end: HTTPS/8888

Comunicação para portas RMI - 1099

Comunicação para o Device Server de back-end: HTTP(S)/8443 - Se a sua versão do Security Management Server for a v7.7 ou posterior. Se tiver uma versão anterior à v7.7 do Dell Server, HTTP(S)/8081.

Servidor de sinalizador: HTTP/8446 (se utilizar o Data Guardian)

Externas (se necessário):

Base de dados SQL: TCP/1433

Management Console: HTTPS/8443

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

Compatibility Server: TCP/1099

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

Identity Server: HTTPS/8445

Core Server: HTTPS/8888 (8888 é configurado automaticamente na instalação)

Device Server: HTTP(S)/8443 (Security Management Server v7.7 ou posterior) ou HTTP(S)/8081 (anterior à v7.7 do Dell Server)

Key Server: TCP/8050

Policy Proxy: TCP/8000

Security Server: HTTPS/8443

Autenticação do cliente: HTTPS/8449 (se utilizar Server Encryption)

Comunicação do cliente, se utilizar Advanced Threat Prevention: HTTPS/TCP/443

Criar base de dados Dell Server

3 Estas instruções são opcionais. O instalador cria uma base de dados por si, caso ainda não exista. Se preferir configurar uma base de dados antes de instalar o Security Management Server, siga as instruções abaixo para criar uma base de dados do SQL e utilizador do SQL no SQL Management Studio.

Ao instalar o Security Management Server, siga as instruções em Instalar servidor de back-end com a base de dados existente.

O Security Management Server suporta autenticação SQL e Windows. O método de autenticação predefinido é a autenticação SQL.

Após criar a base de dados, crie um utilizador de base de dados Dell com direitos de db_owner. O db_owner pode atribuir permissões, fazer cópias de segurança e restaurar a base de dados, criar e eliminar objetos e gerir contas de utilizador e funções sem qualquer limitação. Além disso, certifique-se de que este utilizador tem permissões/privilégios para executar procedimentos armazenados.

Quando utilizar uma instância não predefinida do SQL Server, após a instalação do Security Management Server, precisa de especificar a porta dinâmica da instância no separador Base de dados do Server Configuration Tool. Para mais informações, consulte a Server Configuration Tool. Como alternativa, ative o serviço SQL Server Browser e certifique-se de que a porta UDP 1434 está aberta. Para obter mais informações, consulte https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

O agrupamento não predefinido esperado e suportado pela sua base de dados SQL ou instância SQL é o agrupamento "SQL_Latin1_General_CP1_CI_AS".

Para criar a base de dados SQL e o utilizador SQL no SQL Management Studio, escolha um:

Instalar os pacotes redistribuíveis do Visual C++ 2010/2013/2015

4 *Se ainda não estiverem instalados*, instale os pacotes redistribuíveis do Microsoft Visual C++ 2010, 2013 e 2015. Se assim o desejar, pode permitir que o instalador do Security Management Server instale estes componentes.

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

Instalar o .NET Framework 4.5

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

Windows Server 2012 R2, Windows Server 2016 ou Windows Server 2019 - https://www.microsoft.com/en-us/download/details.aspx?id=30653

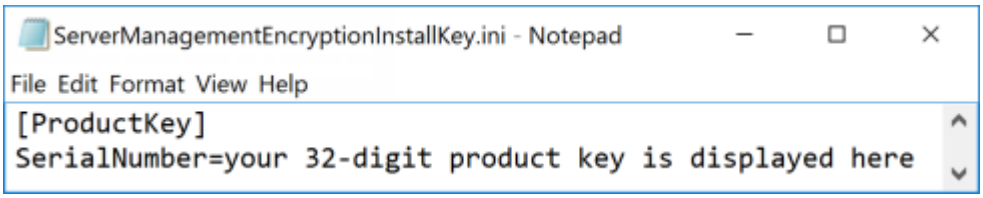
Instalar o SQL Native Client 2012

6 *Se estiver a utilizar o SQL Server 2012 ou o SQL Server 2016*, instale o SQL Native Client 2012. Se assim o desejar, pode permitir que o instalador do Security Management Server instale este componente.

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

Opcional

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



A configuração de pré-instalação do servidor está concluída. Continue para Instalar ou Atualizar/Migrar.

4

Instalar ou Atualizar/Migrar

O capítulo fornece instruções para o seguinte:

- Nova instalação - Para instalar um novo Security Management Server.
- Atualização/Migração - Para atualizar a partir de um Enterprise Server funcional, v9.2 ou posterior.
- Desinstalar o Security Management Server - Para remover a instalação atual, se necessário.

  Se for necessário que a sua instalação inclua mais do que um servidor principal (back-end), contacte o seu representante do Dell ProSupport.

Antes de iniciar a Instalação ou a Atualização/Migração

Antes de começar, certifique-se de que concluiu os passos da Configuração de Pré-instalação aplicáveis.

Leia o documento *Security Management Server Technical Advisories* (Avisos técnicos do Security Management Server) para ficar a conhecer quaisquer soluções alternativas existentes ou problemas conhecidos relacionados com a instalação do Security Management Server.

Para reduzir o tempo de instalação no Server 2016, adicione as exclusões a seguir para o Windows Defender:

- C:\Program Files\Dell\Enterprise Edition
- C:\Windows\Installer
- O caminho do ficheiro a partir do qual o instalador é executado

A Dell recomenda que sejam seguidas as melhores práticas de utilização de bases de dados para a base de dados do servidor da Dell e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

Se pretender implementar componentes Dell no DMZ, certifique-se de que estão devidamente protegidos contra ataques.

Para produção, a Dell recomenda vivamente que instale o SQL Server num servidor dedicado.

Instalar o servidor de back-end antes de instalar e configurar um servidor de front-end constitui uma boa prática.

Os ficheiros de registo de instalação estão localizados neste diretório: **C:\Users\<LoggedOnUser>\AppData\Local\Temp**

Nova instalação

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

- Instalar servidor de back-end e nova base de dados - Para instalar um novo Security Management Server e uma nova base de dados.
- Instalar servidor de back-end com a base de dados existente - Para instalar um novo Security Management Server e ligar-se a uma base de dados do SQL criada durante a Configuração de Pré-instalação ou a uma base de dados do SQL (v9.x ou posterior), quando a versão de esquema corresponde à versão do Security Management Server a ser instalada. Uma base de dados v9.2 ou posterior deve ser migrada para o esquema mais recente com a versão mais recente da ferramenta Server Configuration Tool. Para instruções sobre a migração da base de dados com a Server Configuration Tool, consulte Migrar a base de dados. Para obter a Server Configuration Tool mais recente ou para migrar uma base de dados anterior à v9.2, entre em contacto com o Dell ProSupport para obter assistência.

NOTA:
Se tem um Enterprise Server funcional, v9.2 ou posterior, consulte as instruções em **Atualizar/migrar servidores de back-end**.

Se instalar o servidor de front-end, realize esta instalação depois da instalação do servidor de back-end:

- Instalar um servidor de front-end - Para instalar um servidor de front-end para comunicar com um servidor de back-end.

Instalar servidor de back-end e nova base de dados

1 No suporte multimédia de instalação da Dell, aceda ao diretório Security Management Server. **Descomprima** (NÃO copie/cole nem arraste/largue) o Security Management Server-x64 para o diretório de raiz do servidor onde está a instalar o Security Management Server. ***As operações de copiar/colar ou arrastar/largar produzem erros e uma instalação malsucedida.***

2 Clique duas vezes no ficheiro **setup.exe**.

3 Selecione o idioma da instalação e, de seguida, clique em **OK**.

4 Se os pré-requisitos ainda não estiverem instalados, é apresentada uma mensagem a informar que pré-requisitos serão instalados. Clique em **Instalar**.

5 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

7 Se copiou, opcionalmente, o ficheiro **EnterpriseServerInstallKey.ini** para **C:\Windows** tal como explicado na Configuração de Pré-instalação, clique em **Seguinte**. Caso contrário, introduza a chave do produto de 32 caracteres e clique em **Seguinte**. A chave do produto encontra-se no ficheiro **EnterpriseServerInstallKey.ini**.

8 Selecione **Instalação de back end** e clique em **Seguinte**.

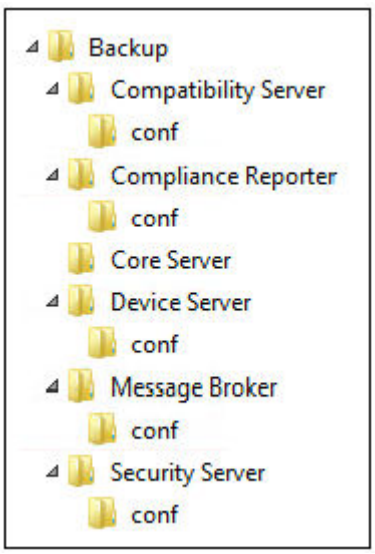
9 Para instalar o Security Management Server na localização predefinida **C:\Program Files\Dell** clique em **Seguinte**. Caso contrário, clique em **Alterar** para selecionar outra localização e clique em **Seguinte**.

10 Para selecionar uma localização para guardar os ficheiros de configuração da cópia de segurança, clique em **Alterar** e navegue até à pasta pretendida, em seguida, clique em **Seguinte**.

A Dell recomenda que selecione uma localização de rede remota ou uma unidade externa para a cópia de segurança.

Após a instalação, deve ser manualmente criada uma cópia de segurança com quaisquer alterações efetuadas nos ficheiros de configuração, incluindo alterações feitas com a Server Configuration Tool, nestas pastas. Os ficheiros de configuração são uma parte importante das informações totais utilizadas para restaurar manualmente o servidor Dell, se necessário.

NOTA: A estrutura de pastas criada pelo instalador durante esta etapa de instalação (exemplo apresentado abaixo) deve manter-se inalterada.



11 Tem à sua disposição vários tipos de certificados digitais que pode utilizar. **É altamente recomendável que utilize um certificado digital de uma autoridade de certificação fidedigna.**

Selecione a opção "a" ou "b" abaixo:

a Para utilizar um certificado existente comprado junto de uma autoridade de CA, selecione **Importar um certificado existente** e clique em **Seguinte**.

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

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exportar um Certificado para .PFX Utilizando a Consola de Gestão de Certificados.

Clique em **Seguinte**.

> **NOTA:**
> Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no “Certificate Export Wizard” (Assistente para Exportar Certificados):
>
> - Personal Information Exchange - PKCS#12 (.PFX)
> - Incluir todos os certificados no caminho de certificação, se possível
> - Exportar todas as propriedades expandidas

OU

b Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para a key store** e clique em **Seguinte**.

Na caixa de diálogo *Criar certificado autoassinado*, introduza as seguintes informações:

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

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Distrito (nome completo)

País: abreviatura de duas letras do país

Clique em **Seguinte**.

> **NOTA: A validade do certificado é de 10 anos, por predefinição.**

12 Para o Server Encryption, tem à sua disposição vários tipos de certificados digitais que pode utilizar. É altamente recomendável que utilize um certificado digital de uma autoridade de certificação fidedigna.

Selecione a opção "a" ou "b" abaixo:

a Para utilizar um certificado existente comprado junto de uma autoridade de CA, selecione **Importar um certificado existente** e clique em **Seguinte**.

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

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exportar um Certificado para .PFX Utilizando a Consola de Gestão de Certificados.

Clique em **Seguinte**.

NOTA:

Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no "Certificate Export Wizard" (Assistente para Exportar Certificados):

- Personal Information Exchange - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades expandidas

OU

b Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para a key store e clique em Seguinte.**

Na caixa de diálogo *Criar certificado autoassinado*, introduza as seguintes informações:

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

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Distrito (nome completo)

País: abreviatura de duas letras do país

Clique em **Seguinte**.

NOTA: A validade do certificado é de 10 anos, por predefinição.

13 A partir da caixa de diálogo *Configuração da instalação do servidor de back-end*, pode visualizar ou editar os nomes dos anfitriões e as portas.

- Para aceitar as portas e os nomes dos anfitriões predefinidos, na caixa de diálogo *Configuração da instalação do servidor de back-end*, clique em **Seguinte**.
- Se estiver a utilizar um servidor de front-end, selecione **Trabalha com o front-end para comunicar com clientes internamente na sua rede ou externamente no DMZ** e introduza o nome do anfitrião do Security Server de front-end (por exemplo: servidor.domínio.com).
- Para ver ou editar nomes de anfitriões, clique em **Editar nomes de anfitriões**. Edite os nomes dos anfitriões apenas se necessário. A Dell recomenda que utilize os nomes predefinidos.

NOTA: Um nome de anfitrião não pode conter um caráter de sublinhado ("_").

Quando terminar, clique em **OK**.

- Para ver ou editar portas, clique em **Editar Portas**. Edite as portas apenas se necessário. A Dell recomenda que utilize os nomes predefinidos. Quando terminar, clique em **OK**.

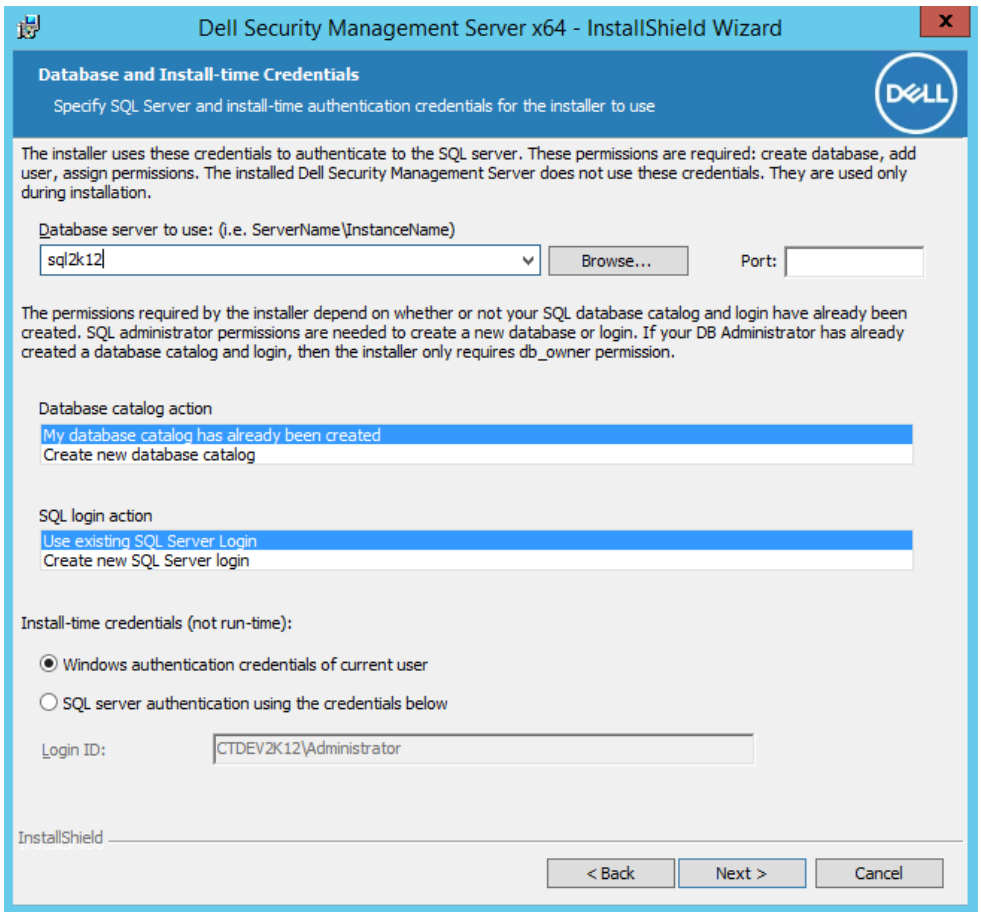
14 Para criar uma nova base de dados, siga estes passos:

a Clique em **Procurar** para selecionar o servidor onde pretende instalar a base de dados.

b Selecione o método de autenticação que o instalador deve utilizar para configurar a base de dados do Dell Server. Após a instalação, o produto instalado não utiliza as credenciais aqui especificadas.

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

  Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows são utilizadas para autenticação (o *Nome de utilizador* e *Palavra-passe* não são editáveis). Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server.



OU

- **Autenticação do SQL Server a utilizar as credenciais abaixo apresentadas**

  Se utilizar a autenticação do SQL, a conta SQL utilizada precisa ter direitos de administrador do sistema no SQL Server.

  O instalador precisa efetuar a autenticação no SQL Server com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões.

c Identifique o catálogo da base de dados:

Introduza o nome do novo catálogo da base de dados. Na caixa de diálogo seguinte é-lhe solicitado que crie um novo catálogo.

d Clique em **Seguinte**.

e Para confirmar que pretende que o instalador crie uma base de dados, clique em **Sim**. Para voltar ao ecrã anterior e fazer alterações, clique em **Não**.

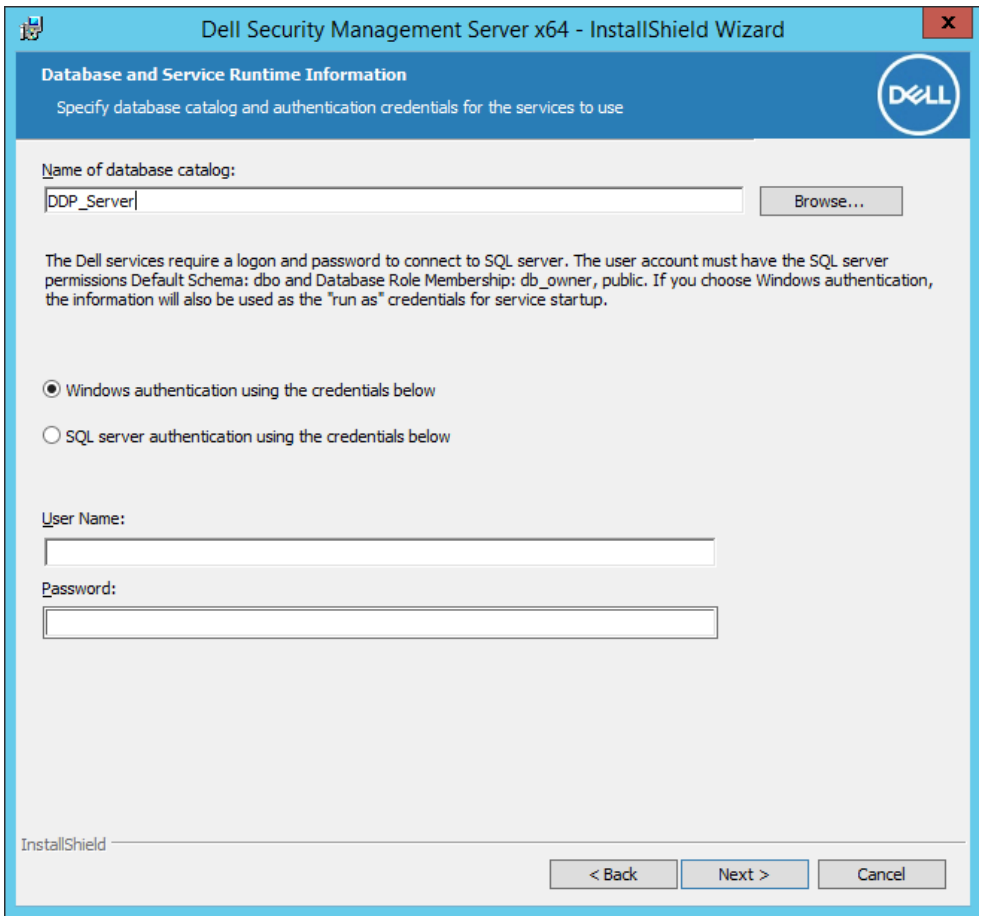
15 Selecione o método de autenticação que o produto deve utilizar. Esta etapa associa uma conta ao produto.

- **Autenticação do Windows**

  Selecione **Autenticação do Windows utilizando as credenciais, abaixo** introduza as credenciais do produto a utilizar e clique em **Seguinte**.

  Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

  Estas credenciais são também utilizadas por serviços Dell, uma vez que são compatíveis com o Security Management Server.



OU

- **Autenticação do SQL Server**

  Selecione **Autenticação do SQL Server utilizando as credenciais abaixo**, introduza as credenciais do SQL Server para os serviços Dell utilizarem enquanto se ligam ao Security Management Server e clique em **Seguinte.**

  A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

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

É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

17 Quando a instalação estiver concluída, clique em **Concluir**.

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

Os serviços Dell são reiniciados no final da instalação. Não é necessário reiniciar o Dell Server.

Instalar servidor de back-end com a base de dados existente

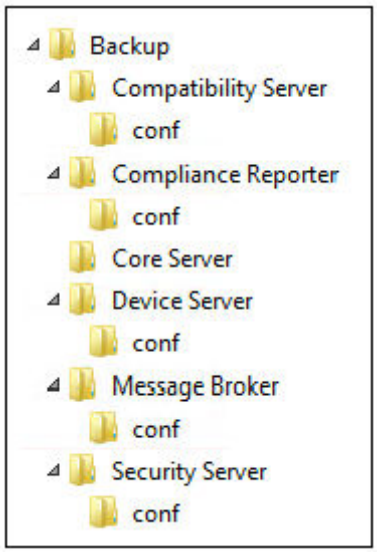
NOTA:

Se possui um Dell Server funcional, v9.2 ou posterior, consulte as instruções em Atualizar/migrar servidores de back-end.

Pode instalar um novo Security Management Server e ligar-se a uma base de dados do SQL criada durante a Configuração de pré-instalação ou a uma base de dados do SQL existente (v9.x ou posterior), quando a versão de esquema corresponde à versão do Security Management Server a ser instalada.

A conta de utilizador a partir da qual a instalação é realizada deve ter privilégios de proprietário de base de dados para a base de dados do SQL. Se não tem a certeza sobre os privilégios ou conetividade à base de dados, peça ao seu administrador da base de dados para os confirmar antes de iniciar a instalação.

Se a base de dados existente tiver sido anteriormente instalada com o Security Management Server, antes de iniciar a instalação, certifique-se de que efetua uma cópia de segurança da base de dados existente, dos ficheiros de configuração e da secretKeyStore e de que estes estão acessíveis a partir do servidor no qual está a instalar o Security Management Server. Se necessário, aceda a estes ficheiros para configurar o Security Management Server e a base de dados existente. A estrutura de pastas criada pelo instalador durante a instalação (exemplo apresentado abaixo) não pode ser alterada.



1 No suporte multimédia de instalação da Dell, aceda ao diretório Security Management Server. **Descomprima** (NÃO copie/cole nem arraste/largue) o Security Management Server-x64 para o diretório de raiz do servidor onde está a instalar o Security Management Server. ***As operações de copiar/colar ou arrastar/largar produzem erros e uma instalação malsucedida.***

2 Clique duas vezes no ficheiro **setup.exe**.

3 Selecione o idioma da instalação e, de seguida, clique em **OK**.

4 Se os pré-requisitos ainda não estiverem instalados, é apresentada uma mensagem a informar que pré-requisitos serão instalados. Clique em **Instalar**.

5 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

7 Se copiou, opcionalmente, o ficheiro **EnterpriseServerInstallKey.ini** para **C:\Windows** tal como explicado na Configuração de Pré-instalação, clique em **Seguinte**. Caso contrário, introduza a chave do produto de 32 caracteres e clique em **Seguinte**. A chave do produto encontra-se no ficheiro **EnterpriseServerInstallKey.ini**.

8 Selecione **Instalação de back-end** e **Instalação de recuperação**, em seguida clique em **Seguinte**.

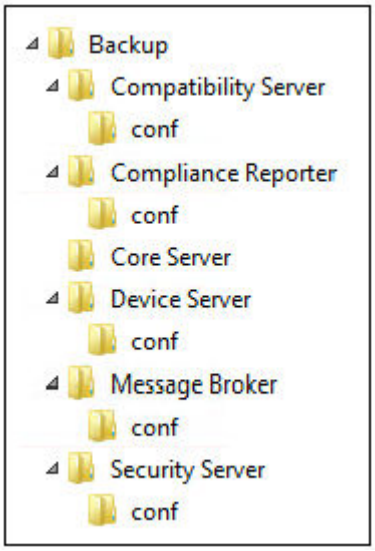
9 Para instalar o Security Management Server na localização predefinida **C:\Program Files\Dell** clique em **Seguinte**. Caso contrário, clique em **Alterar** para selecionar uma localização diferente e clique em **Seguinte**.

10 Para selecionar uma localização para guardar os ficheiros de recuperação e configuração da cópia de segurança, clique em **Alterar** e navegue até à pasta pretendida, em seguida, clique em **Seguinte**.

A Dell recomenda que selecione uma localização de rede remota ou uma unidade externa para a cópia de segurança.

Após a instalação, deve ser manualmente criada uma cópia de segurança com quaisquer alterações efetuadas nos ficheiros de configuração, incluindo alterações feitas com a Server Configuration Tool, nestas pastas. Os ficheiros de configuração são uma parte importante das informações totais utilizadas para restaurar manualmente o Dell Server.

NOTA: A estrutura de pastas criada pelo instalador durante a instalação (exemplo apresentado abaixo) não pode ser alterada.



11 Tem à sua disposição vários tipos de certificados digitais que pode utilizar. **É altamente recomendável que utilize um certificado digital de uma autoridade de certificação fidedigna.**

Selecione a opção "a" ou "b" abaixo:

a Para utilizar um certificado existente comprado junto de uma autoridade de CA, selecione **Importar um certificado existente** e clique em **Seguinte**.

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

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exportar um Certificado para .PFX Utilizando a Consola de Gestão de Certificados.

Clique em **Seguinte**.

> **NOTA:**
> Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no "Certificate Export Wizard" (Assistente para Exportar Certificados):
>
> - Personal Information Exchange - PKCS#12 (.PFX)
> - Incluir todos os certificados no caminho de certificação, se possível
> - Exportar todas as propriedades expandidas

OU

b Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para a key store e clique em Seguinte.**

Na caixa de diálogo *Criar certificado autoassinado*, introduza as seguintes informações:

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

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Distrito (nome completo)

País: abreviatura de duas letras do país

Clique em **Seguinte**.

NOTA: A validade do certificado é de 10 anos, por predefinição.

12 A partir da caixa de diálogo *Configuração da instalação do servidor de back-end*, pode visualizar ou editar os nomes dos anfitriões e as portas.

- Para aceitar as portas e os nomes dos anfitriões predefinidos, na caixa de diálogo *Configuração da instalação do servidor de back-end*, clique em **Seguinte**.
- Se estiver a utilizar um servidor de front-end, selecione **Trabalha com o front-end para comunicar com clientes internamente na sua rede ou externamente no DMZ** e introduza o nome do anfitrião do Security Server de front-end (por exemplo: servidor.domínio.com).
- Para ver ou editar nomes de anfitriões, clique em **Editar nomes de anfitriões**. Edite os nomes dos anfitriões apenas se necessário. A Dell recomenda que utilize os nomes predefinidos.

  NOTA: Um nome de anfitrião não pode conter um caráter de sublinhado ("_").

  Quando terminar, clique em **OK**.
- Para ver ou editar portas, clique em **Editar Portas**. Edite as portas apenas se necessário. A Dell recomenda que utilize os nomes predefinidos. Quando terminar, clique em **OK**.

13 Especifique o método de autenticação que o instalador deve utilizar.

a Clique em **Procurar** para selecionar o servidor onde se encontra a base de dados.

b Selecione o tipo de autenticação.

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

  Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows são utilizadas para autenticação (o *Nome de utilizador* e a *Palavra-passe* não são editáveis). Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server.

  OU

- **Autenticação do SQL Server a utilizar as credenciais abaixo apresentadas**

  Se utilizar a autenticação do SQL, a conta SQL utilizada precisa ter direitos de administrador do sistema no SQL Server.

  O instalador precisa efetuar a autenticação no SQL Server com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões.

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

d Clique em **Seguinte**.

14 Se for apresentada uma caixa de diálogo com a mensagem Erro na base de dados existente, selecione a opção apropriada.

Se o instalador detetar um problema na base de dados, é apresentada uma caixa de diálogo com a mensagem *Erro na base de dados existente*. As opções da caixa de diálogo dependem das circunstâncias:

- O esquema da base de dados é de uma versão anterior. (Consulte o passo a.)
- A base de dados já tem um esquema de base de dados que corresponde à versão que está atualmente a ser instalada. (Consulte o passo b.)

a Se o esquema da base de dados for de uma versão anterior, selecione **Sair do instalador para terminar esta instalação**. Em seguida, deve efetuar uma cópia de segurança da base de dados.

As opções seguintes apenas DEVEM ser utilizadas com a ajuda do Dell ProSupport:

- A opção **Migrar esta base de dados para o esquema atual** é utilizada para recuperar uma base de dados boa de uma implementação do servidor com falhas. Esta opção utiliza os ficheiros de recuperação da pasta \Backup para se ligar novamente à base de dados e, em seguida, executa a migração da base de dados para o esquema atual. Esta opção *apenas* deve ser utilizada após tentar reinstalar a versão correta do Security Management Server pela primeira vez e, em seguida, executar o instalador mais recente para atualizar a versão.
- A opção **Avançar sem migrar a base de dados** instala os ficheiros do Security Management Server sem configurar completamente a base de dados. A configuração da base de dados deve ser concluída mais tarde, manualmente, utilizando a Server Configuration Tool e requer alterações manuais adicionais.

b Se o esquema da base de dados já tiver o esquema da versão atual, mas não estiver ligado a um Security Management Server de back-end, é considerado uma *Recuperação*. Se a opção **Instalação de recuperação** não foi selecionada neste passo, é apresentada esta caixa de diálogo:

- Selecione **Modo de instalação de recuperação** para continuar a instalação com a base de dados selecionada.
- Selecione **Selecionar uma nova base de dados** para escolher uma base de dados diferente.
- Selecione **Sair do instalador para concluir esta instalação**.

c Clique em **Seguinte**.

15 Selecione o método de autenticação que o produto deve utilizar. Esta é a conta que o produto utiliza para trabalhar com a base de dados e os serviços Dell.

- **Para usar a autenticação do Windows**

  Selecione **Autenticação do Windows utilizando as credenciais, abaixo**, introduza as credenciais da conta que o produto pode utilizar e clique em **Seguinte**.

  Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

  OU

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

  Selecione **Autenticação do SQL Server utilizando as credenciais, abaixo**, introduza as credenciais do SQL Server e clique em **Seguinte**.

  A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

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

É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

Quando a instalação estiver concluída, clique em **Concluir**.

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

Os serviços Dell são reiniciados no final da instalação. Não é necessário reiniciar o servidor.

Instalar servidor de front-end

Instalação do servidor de front-endO fornece uma opção de front-end (modo DMZ) para utilização com o Security Management Server. Se pretender implementar componentes Dell no DMZ, certifique-se de que estão devidamente protegidos contra ataques.

NOTA: O serviço de Sinalizador é instalado como parte desta instalação para apoiar o sinalizador de chamada de retorno do Data Guardian, o qual insere um sinalizador de chamada de retorno em cada ficheiro protegido pelo Data Guardian ao permitir ou implementar os documentos protegidos do Office no ambiente. Isto permite a comunicação entre qualquer dispositivo em qualquer localização e o servidor de front-end. Certifique-se de que a segurança de rede necessária está configurada antes de usar o sinalizador de chamada de retorno.

Para efetuar esta instalação, irá necessitar do nome de anfitrião totalmente qualificado do servidor DMZ.

1 No suporte multimédia de instalação da Dell, aceda ao diretório Security Management Server. **Descomprima** (NÃO copie/cole nem arraste/largue) o Security Management Server-x64 para o diretório de raiz do servidor onde está a desinstalar o Security Management Server. ***As operações de copiar/colar ou arrastar/largar produzem erros e uma instalação malsucedida.***

2 Clique duas vezes no ficheiro **setup.exe**.

3 Selecione o idioma da instalação e, de seguida, clique em **OK**.

4 Se os pré-requisitos ainda não estiverem instalados, é apresentada uma mensagem a informar que pré-requisitos serão instalados. Clique em **Instalar**.

5 Clique em **Seguinte** na caixa de diálogo Bem-vindo.

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

7 Se copiou, opcionalmente, o ficheiro **EnterpriseServerInstallKey.ini** para **C:\Windows** tal como explicado na Configuração de Pré-instalação, clique em **Seguinte**. Caso contrário, introduza a chave do produto de 32 caracteres e clique em **Seguinte**. A chave do produto encontra-se no ficheiro **EnterpriseServerInstallKey.ini**.

8 Selecione **Instalação de front-end** e clique em **Seguinte**.

9 Para instalar o servidor de front-end na localização predefinida **C:\Program Files\Dell**, clique em **Seguinte**. Caso contrário, clique em **Alterar** para selecionar outra localização e clique em **Seguinte**.

10 Tem à sua disposição vários tipos de certificados digitais que pode utilizar.

NOTA: É altamente recomendável que utilize um certificado digital de uma autoridade de certificação fidedigna.

Selecione a opção "a" ou "b" abaixo:

a Para utilizar um certificado existente comprado junto de uma autoridade de CA, selecione **Importar um certificado existente** e clique em **Seguinte**.

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

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exportar um Certificado para .PFX Utilizando a Consola de Gestão de Certificados.

Clique em **Seguinte**.

NOTA:

Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no “Certificate Export Wizard” (Assistente para Exportar Certificados):

- Personal Information Exchange - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades expandidas

b Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para a key store e clique em Seguinte.**

Na caixa de diálogo *Criar certificado autoassinado*, introduza as seguintes informações:

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

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Distrito (nome completo)

País: abreviatura de duas letras do país

Clique em **Seguinte**.

NOTA: A validade do certificado é de 10 anos, por predefinição.

11 Na caixa de diálogo *Configuração do servidor de front-end*, introduza o nome de anfitrião totalmente qualificado ou o alias de DNS do servidor de back-end, selecione **Dell Security Management Server** e clique em **Seguinte**.

12 A partir da caixa de diálogo *Configuração da instalação do servidor de front-end*, pode visualizar ou editar os nomes dos anfitriões e as portas.

- Para aceitar as portas e os nomes dos anfitriões predefinidos, na caixa de diálogo *Configuração da instalação do servidor de front-end*, clique em **Seguinte**.
- Para ver ou editar os nomes dos anfitriões, na caixa de diálogo *Configuração do servidor de front-end*, clique em **Editar nomes dos anfitriões**. Edite os nomes dos anfitriões apenas se necessário. A Dell recomenda que utilize os nomes predefinidos.

  NOTA:
  Um nome de anfitrião não pode conter um caráter de sublinhado ("_").

  Desmarque um proxy apenas se tiver a certeza de que não o pretende configurar para instalação. Se desmarcar um proxy nesta caixa de diálogo, este não é instalado.

  Quando terminar, clique em **OK**.
- Para ver ou editar as portas, na caixa de diálogo *Configuração do servidor de front-end*, clique em **Editar portas externas** ou **Editar portas de ligação internas**. Edite as portas apenas se necessário. A Dell recomenda que utilize os nomes predefinidos.

  Se desmarcar um proxy na caixa de diálogo *Editar nomes de anfitriões de front-end*, a respetiva porta não é apresentada nas caixas de diálogo Portas externas ou Portas internas.

  Quando terminar, clique em **OK**.

13 Na caixa de diálogo *Preparado para instalar o programa*, clique em **Instalar**.
É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

14 Quando a instalação estiver concluída, clique em **Concluir**.
As tarefas de instalação do servidor de front-end estão completas.

Atualização/Migração

Pode atualizar o Enterprise Server v9.2 e posteriores para o Security Management Server v10.x. Se a versão do Dell Server for anterior à 9.2, primeiro tem de o atualizar para a v9.2 e, de seguida, atualizar para uma versão posterior.

Antes de iniciar uma Atualização/Migração

Antes de começar, certifique-se de que concluiu a Configuração de Pré-instalação.

Leia o documento *Security Management Server Technical Advisories* (Avisos técnicos do Security Management Server) para ficar a conhecer quaisquer soluções alternativas existentes ou problemas conhecidos relacionados com a instalação doSecurity Management Server.

A conta de utilizador a partir da qual a instalação é realizada deve ter privilégios de proprietário de base de dados para a base de dados do SQL. Se não tem a certeza sobre os privilégios ou conectividade à base de dados, peça ao seu administrador da base de dados para os confirmar antes de iniciar a instalação.

A Dell recomenda que sejam seguidas as melhores práticas de utilização de bases de dados para a base de dados do servidor da Dell e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

Se pretender implementar componentes Dell no DMZ, certifique-se de que estão devidamente protegidos contra ataques.

Para produção, a Dell recomenda que instale o SQL Server num servidor dedicado.

Para beneficiar das funcionalidades completas das políticas, a Dell recomenda que atualize o Security Management Server e os Clientes para as versões mais recentes.

Security Management Server v9.x suporta:

- Encryption Enterprise:
  - Clientes Windows v7.x/8.x
  - Clientes Mac v7.x/8.x
  - Clientes SED v8.x
  - Autenticação v8.x
  - BitLocker Manager v7.2x+ e v8.x
  - Data Guardian v1.x
- Endpoint Security Suite Pro v1.x
- Endpoint Security Suite Enterprisev1.x
- Atualização/Migração do Security Management Server versão v9.2 ou posterior. (Ao migrar do Security Management Server anterior à versão v9.2, contacte o Dell ProSupport para obter assistência.)

Ao atualizar/migrar o seu Security Management Server para uma versão que inclua novas políticas, consolide a política atualizada após a atualização/migração, de modo a garantir a implementação das suas preferências de políticas, para as novas políticas, em vez dos valores predefinidos.

Regra geral, o procedimento de atualização recomendado consiste em atualizar/migrar o Security Management Server e os seus componentes e, depois, instalar/atualizar o cliente.

Aplicar alterações de políticas

1 Como administrador Dell, inicie sessão na Management Console.

2 No menu esquerdo, clique em **Gestão** > **Consolidar**.

3 Em *Comentário*, introduza uma descrição da alteração.

4 Clique em **Consolidar políticas**.

5 Quando a consolidação estiver completa, termine sessão na Management Console.

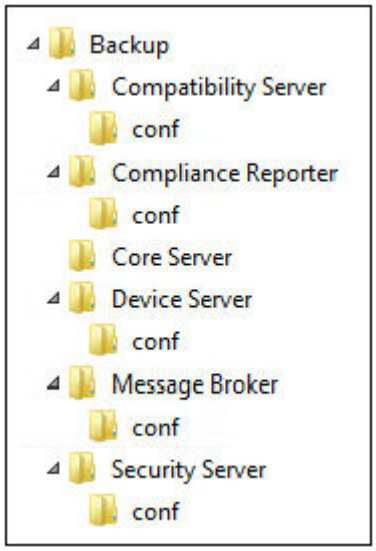
Certifique-se de que os serviços Dell estão a ser executados

6 No menu *Iniciar* do Windows, clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Fazer uma cópia de segurança da instalação existente

7 Faça uma cópia de segurança da totalidade da instalação existente e guarde-a num local alternativo. A cópia de segurança deve incluir a base de dados SQL, a secretKeyStore e os ficheiros de configuração. Serão necessários vários ficheiros da sua instalação existente quando o processo de atualização/migração estiver concluído.

> **NOTA:**
> A estrutura de pastas criada pelo instalador durante a instalação (exemplo abaixo apresentado) não pode ser alterada



Atualizar/migrar servidores de back-end

1 No suporte multimédia de instalação da Dell, aceda ao diretório Security Management Server. **Descomprima** (NÃO copie/cole nem arraste/largue) o Security Management Server-x64 para o diretório de raiz do servidor onde está a instalar o Security Management Server. ***As operações de copiar/colar ou arrastar/largar produzem erros e uma instalação malsucedida.***

2 Clique duas vezes no ficheiro **setup.exe**.

3 Selecione o idioma da instalação e, de seguida, clique em **OK**.

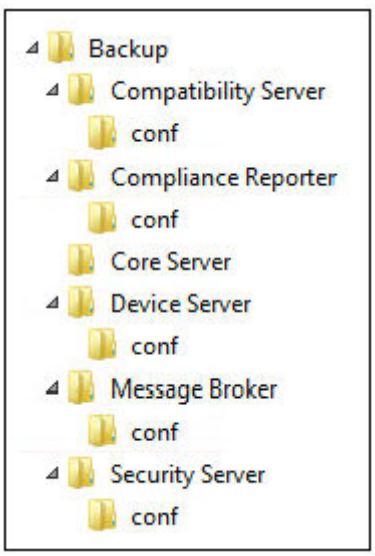
4 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

6 Para selecionar uma localização para guardar os ficheiros de configuração da cópia de segurança, clique em **Alterar** e navegue até à pasta pretendida, depois clique em **Seguinte**.

A Dell recomenda que selecione uma localização de rede remota ou uma unidade externa para a cópia de segurança.

A estrutura de pastas criada pelo instalador durante a instalação (exemplo apresentado abaixo) não pode ser alterada.



7 Quando o instalador localizar corretamente a base de dados existente, a caixa de diálogo é preenchida por si.

Para se ligar à base de dados existente, especifique o método de autenticação a utilizar. Após a instalação, o produto instalado não utiliza as credenciais aqui especificadas.

a Selecione o tipo de autenticação da base de dados:

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

  Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows são utilizadas para autenticação (o *Nome de utilizador* e *Palavra-passe* não são editáveis).

  Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

  OU

- **Autenticação do SQL Server a utilizar as credenciais abaixo apresentadas**

  Se utilizar a autenticação do SQL, a conta SQL utilizada precisa ter direitos de administrador do sistema no SQL Server.

  O instalador precisa efetuar a autenticação no SQL Server com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões.

b Clique em **Seguinte**.

8 Se a caixa de diálogo Informações da conta de tempo de execução do serviço não for pré-preenchida, especifique o método de autenticação que o produto irá utilizar após a instalação.

a Selecione o tipo de autenticação.

b Introduza o nome de utilizador e a palavra-passe da conta do serviço de domínio que os serviços Dell irão utilizar para aceder ao SQL Server e clique em **Seguinte**.

A conta de utilizador precisa estar no formato DOMAIN\Username e possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados dbo_owner, público.

9 Se não for feita uma cópia de segurança da base de dados, ***tem*** de fazer a cópia de segurança antes de prosseguir com a instalação. ***A atualização da base de dados não pode ser revertida.*** Apenas depois de efetuar a cópia de segurança da base de dados, selecione **Sim**, **foi efetuada a cópia de segurança da base de dados** e clique em **Seguinte**.

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

É apresentada uma caixa de diálogo de progresso durante todo o processo de atualização.

11 Quando a instalação estiver concluída, clique em **Concluir**.

Os serviços Dell são reiniciados no final da migração. Não é necessário reiniciar o Dell Server.

O instalador realiza as etapas 12-13 por si. A verificação destes valores para garantir que as alterações foram efetuadas corretamente é uma das melhores práticas.

12 Na cópia de segurança da sua instalação copie e cole: <Compatibility Server install dir>\conf\secretKeyStore para a nova instalação: <Compatibility Server install dir>\conf\secretKeyStore

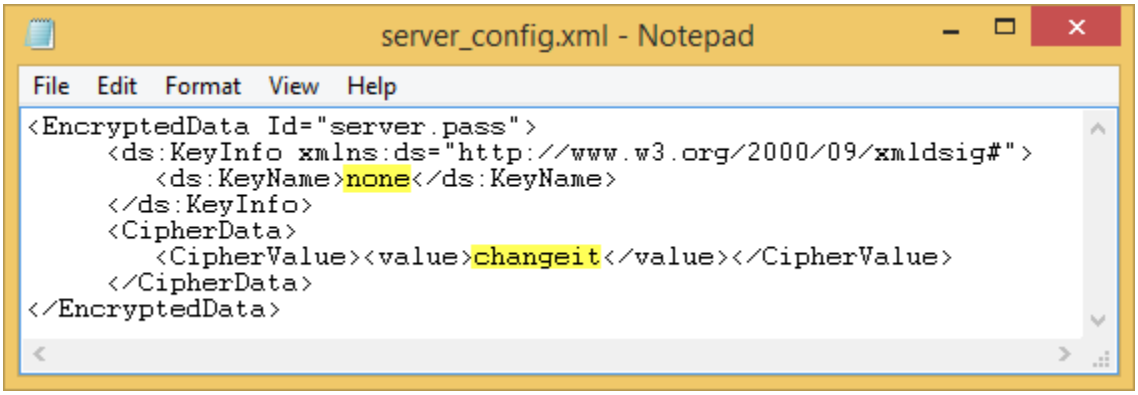
13 Na nova instalação, abra <Compatibility Server install dir>\conf\server_config.xml e substitua o valor **server.pass** pelo valor da cópia de segurança <Compatibility Server install dir>\conf\server_config.xml, conforme se segue:

Instruções para server.pass:

Se souber a palavra-passe, consulte o ficheiro de exemplo server_config.xml e faça as alterações seguintes:

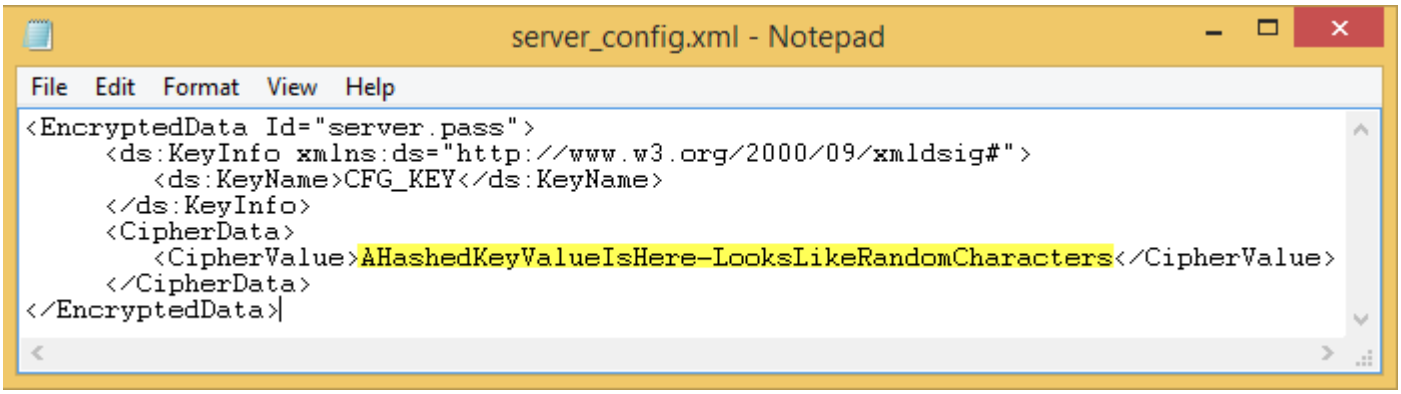
- Edite o *KeyName* de **CFG_KEY** para **nenhum**.
- Introduza a palavra-passe em texto simples e inclua-a entre *<value> </value>*, o que neste exemplo é **<value>changeit</value>**
- Quando o Security Management Server é iniciado, a palavra-passe em texto simples é convertida numa palavra-passe com hash e este valor com hash substitui o texto simples.

Palavra-passe conhecida



Se não souber a palavra-passe, corte e cole a secção semelhante à secção apresentada na Figura 4-2 do ficheiro de cópia de segurança <Compatibility Server install dir>\conf\server_config.xml para a secção correspondente do novo ficheiro *server_config.xml*.

Palavra-passe desconhecida



Guarde e feche o ficheiro.

NOTA:
Não tente mudar a palavra-passe do Security Management Server editando o valor server.pass em server_config.xml em nenhuma circunstância. Se alterar este valor, perde acesso à base de dados.

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

Atualizar/migrar servidores de front-end

NOTA: A partir da v9.5, o Serviço de Sinalizador é instalado como parte desta atualização, utilizando o nome do anfitrião predefinido e a porta 8446. O Serviço de Sinalizador apoia o sinalizador de chamada de retorno do Data Guardian, que insere um sinalizador de chamada de retorno em cada ficheiro protegido pelo Data Guardian ao permitir ou implementar os Protected Office Documents num ambiente. Isto permite a comunicação entre qualquer dispositivo em qualquer localização e o servidor de front-end. Certifique-se de que a segurança de rede necessária está configurada antes de usar o sinalizador de chamada de retorno.

1 No suporte multimédia de instalação da Dell, aceda ao diretório Security Management Server. **Descomprima** (NÃO copie/cole nem arraste/largue) o Security Management Server-x64 para o diretório de raiz do servidor onde está a instalar o Security Management Server. ***As operações de copiar/colar ou arrastar/largar produzem erros e uma instalação malsucedida.***

2 Clique duas vezes no ficheiro **setup.exe**.

3 Selecione o idioma da instalação e, de seguida, clique em **OK**.

4 Se os pré-requisitos ainda não estiverem instalados, é apresentada uma mensagem a informar que pré-requisitos serão instalados. Clique em **Instalar**.

5 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

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

É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

8 Quando a instalação estiver concluída, clique em **Concluir**.

9 Configure o servidor de back-end para comunicar com o servidor de front-end.

a No servidor back-end, aceda a <Security Server install dir>\conf\ e abra o ficheiro application.properties.

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

c Localize a publicdns.server.port e defina a porta (a predefinição é 8443).

Os serviços Dell são reiniciados no final da instalação. Não é necessário reiniciar o Dell Server enquanto as tarefas de configuração pós-instalação não forem concluídas.

Instalação no Modo Desligado

O modo desligado isola o Security Management Server da Internet e de uma LAN ou outra rede não segura. Após a instalação do Security Management Server em Modo Desligado, este permanece em Modo Desligado e não pode ser mudado para o Modo Ligado.

O Security Management Server é instalado no Modo Desligado na linha de comandos.

A tabela seguinte lista os comutadores disponíveis.

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

A tabela seguinte lista as opções de visualização disponíveis.

Opção	Significado
/q	Sem caixa de diálogo de Progresso, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de progresso com botão **Cancelar**
/qn	Sem interface de utilizador

A tabela seguinte descreve os parâmetros disponíveis para a instalação. Estes parâmetros podem ser especificados na linha de comandos ou utilizados a partir de um ficheiro, através da propriedade:

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

Parâmetros
AGREE_TO_LICENSE=Yes - este valor deve ser "Yes."
PRODUCT_SN=xxxxx - opcional se tiver a informação de licença na localização normal; caso contrário, introduza-a aqui.
INSTALLDIR=<path> - opcional.
BACKUPDIR=<path> - onde os ficheiros de recuperação são armazenados.

NOTA: A estrutura de pastas criada pelo instalador durante esta etapa de instalação (exemplo apresentado abaixo) deve manter-se inalterada.

AIRGAP=1 - este valor tem de ser "1" para instalar o Security Management Server em Modo Desligado.

Parâmetros

SSL_TYPE=n - sendo n igual a 1 para importar um certificado existente adquirido de uma autoridade certificadora e 2 para criar um certificado autoassinado. O valor SSL_TYPE determina as propriedades de SSL obrigatórias.

É necessário o seguinte com SSL_TYPE=1:

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

É necessário o seguinte com SSL_TYPE=2:

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY - opcional, predefinição = "US"

SSL_STATENAME

SSOS_TYPE=n - sendo n igual a 1 para importar um certificado existente adquirido de uma autoridade certificadora e 2 para criar um certificado autoassinado. O valor SSOS_TYPE determina as propriedades SSOS obrigatórias.

É necessário o seguinte com SSOS_TYPE=1:

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

É necessário o seguinte com SSOS_TYPE=2:

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY - opcional, predefinição = "US"

SSOS_STATENAME

DISPLAY_SQLSERVER - este valor será interpretado para obter a informação de instância e porta do SQL Server.

Exemplo:

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE - opcional. O valor predefinido é FALSE, o que significa que a base de dados não é criada. A base de dados deve já existir no servidor.

Para criar uma nova base de dados, defina este valor como TRUE.

IS_SQLSERVER_AUTHENTICATION=0 - opcional. O valor predefinido é 0, que especifica que as credenciais de autenticação do Windows do utilizador com sessão iniciada atual são utilizadas para autenticar o SQL Server. Para utilizar autenticação SQL, defina este valor como 1.

Parâmetros

NOTA: O instalador necessita efetuar a autenticação no servidor SQL com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões. As credenciais são credenciais de tempo de instalação e não credenciais de tempo de execução.

Se for utilizada a autenticação SQL, é necessário o seguinte:

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION - obrigatória. Especifique o método de autenticação que o produto deve utilizar. Esta etapa associa uma conta ao produto. Estas credenciais são também utilizadas por serviços Dell, uma vez que permitem ligar ao Security Management Server. Para utilizar autenticação do Windows, defina este valor como 0. Para utilizar autenticação SQL, defina o valor como 1.

NOTA: Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador deve ter o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

SQL_EE_USERNAME - obrigatório. Com autenticação Windows, utilize este formato: DOMÍNIO\nome de utilizador. Com autenticação SQL, especifique o nome de utilizador.

SQL_EE_PASSWORD - obrigatório. Especifique a palavra-passe associada ao nome de utilizador Windows ou SQL.

Se for utilizada a autenticação SQL (EE_SQLSERVER_AUTHENTICATION=1), é necessário o seguinte:

RUNAS_KEYSERVER_USER - defina o Key Server para "executar como" nome de utilizador Windows com o seguinte formato: Domínio \utilizador. Deve tratar-se de uma conta de utilizador Windows.

RUNAS_KEYSERVER_PSWD - defina o Key Server para "executar como" a palavra-passe associada à conta de utilizador Windows.

SQL_ADD_LOGIN=T - opcional. A predefinição é zero (estes dados de início de sessão não são adicionados). Quando o valor está definido como T, se SQL_EE_USERNAME não for o início de sessão ou o utilizador da base de dados, o programa de instalação tenta adicionar as credenciais de autenticação SQL do utilizador e definir os privilégios para permitir que as credenciais sejam utilizadas pelo produto.

Seguem-se os parâmetros de nome do anfitrião. Edite os nomes dos anfitriões apenas se necessário. A Dell recomenda que utilize os nomes predefinidos. O formato deve ser `server.domain.com`.

NOTA: Um nome de anfitrião não pode conter um caráter de sublinhado ("_").

CORESERVERHOST - opcional. Nome do anfitrião do Core Server.

RMIHOST - opcional. Nome do anfitrião do Compatibility Server.

REPORTERHOST - opcional. Nome do anfitrião do Compliance Reporter.

DEVICEHOST - opcional. Nome do anfitrião do Device Server.

KEYSERVERHOST - opcional. Nome do anfitrião do Key Server.

TIGAHOST - opcional. Nome do anfitrião do Security Server.

SMTP_HOST - opcional. Nome do anfitrião do SMTP.

ACTIVEMQHOST - opcional. Nome do anfitrião do Message Broker.

Seguem-se os parâmetros de porta. Edite as portas apenas se necessário. A Dell recomenda que utilize as predefinições

SERVERPORT_CLIENTAUTH - opcional.

Parâmetros
REPORTERPORT - opcional.
DEVICEPORT - opcional.
KEYSERVERPORT - opcional.
GKPORT - opcional.
TIGAPORT - opcional.
SMTP_PORT - opcional.
ACTIVEMQ_TCP - opcional.
ACTIVEMQ_STOMP - opcional.

Instalar o Security Management Server em modo desligado

O exemplo seguinte instala o Security Management Server no modo silencioso, com uma caixa de diálogo de progresso, utilizando os parâmetros de instalação listados no ficheiro, `C:\mysetups\eeoptions.txt\" "`

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

Desinstalar o Security Management Server

1. No suporte multimédia de instalação da Dell, aceda ao diretório Security Management Server. **Descomprima** (NÃO copie/cole nem arraste/largue) o Security Management Server-x64 para o diretório de raiz do servidor onde está a desinstalar o Security Management Server. ***As operações de copiar/colar ou arrastar/largar produzem erros e uma instalação malsucedida.***
2. Clique duas vezes no ficheiro **setup.exe**.
3. Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.
4. Na caixa de diálogo *Remover o programa*, clique em **Remover**.
   É apresentada uma caixa de diálogo de progresso durante todo o processo de desinstalação.
5. Quando a desinstalação estiver concluída, clique em **Concluir**.

5

Configuração de Pós-instalação

Leia o documento *Security Management Server Technical Advisories* (Avisos Técnicos do Security Management Server) para ficar a conhecer quaisquer soluções alternativas existentes ou problemas conhecidos relacionados com a configuração do Security Management Server.

Quer esteja a instalar o Security Management Server pela primeira vez ou a atualizar uma instalação existente, alguns componentes do seu ambiente têm de ser configurados.

Depois de instalar o Security Management Server, devem ser alteradas as seguintes predefinições:

- Altere a palavra-passe do servidor de back-end na seguinte localização:

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

- Altere a palavra-passe para cada servidor de front-end no seu ambiente na seguinte localização:

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

A palavra-passe é apresentada da seguinte forma: `proxy-server.password=ENC(<texthere>)`

Para alterar a palavra-passe:

1 Selecione: `ENC(<texthere>)`

2 Altere o texto selecionado para: `CLR(<newpasswordhere>)`

Depois de reiniciar o serviço, a linha modificada é alterada para `ENC` de `CLR` e a palavra-passe é encriptada.

NOTA: é possível modificar o nome de utilizador do servidor proxy. No entanto, este deve corresponder ao ficheiro de propriedades da aplicação Message Broker e a todos os servidores de front-end ativos.

Configuração do Modo DMZ

Se o Security Server for implementado numa DMZ e numa rede privada, e se apenas o servidor da DMZ tiver um certificado de domínio de uma autoridade de certificação (AC) fidedigna, é necessário realizar alguns passos manualmente para adicionar o certificado fidedigno à keystore Java do Security Server da rede privada.

Se for utilizado um certificado fidedigno, ignore esta secção.

NOTA: A Dell recomenda vivamente que utilize certificados de domínio de autoridades de certificação fidedignas tanto para servidores de rede privada como DMZ.

Para obter informações sobre a atualização do certificado da Dell Encryption com um certificado existente na keystore da Microsoft, consulte http://www.dell.com/support/article/us/en/19/sln297240/.

Server Configuration Tool

Se for necessário configurar o seu ambiente depois de ter completado a instalação, utilize a Server Configuration Tool para fazer essas alterações.

A Server Configuration Tool permite-lhe:

- Adicionar certificados novos ou atualizados
- Importar Certificado do Dell Manager
- Importar Certificado de Identidade
- Configurar as definições de Certificado do Servidor SSL
- Configurar definições de SMTP para Data Guardian ou serviços de email
- Alterar o nome da base de dados, a localização ou as credenciais
- Migrar a base de dados

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

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

A Server Configuration Tool guarda os registos em **C:\Program Files\Dell\Enterprise Edition\Server Configuration Tool\Logs.**

Adicionar certificados novos ou atualizados

Pode escolher que tipo de certificados pretende utilizar - autoassinados ou assinados:

- Os certificados **autoassinados** são assinados pelo próprio criador. Os certificados autoassinados são adequados para pilotos, POCs, etc. Para um ambiente de produção, a Dell recomenda a utilização de certificados assinados por uma AC pública ou assinados por domínio.
- Os certificados **assinados** (assinados por uma AC pública ou assinados por domínio) são assinados por uma AC pública ou por um domínio. No caso de certificados assinados por uma autoridade de certificação (AC) pública, o certificado da autoridade assinante normalmente já existe no arquivo de certificados da Microsoft e, como tal, a cadeia de certificação é automaticamente estabelecida. No caso dos certificados de uma AC de domínio, se a estação de trabalho tiver sido anexada ao domínio, o certificado da AC assinante de domínio terá sido adicionado ao arquivo de certificados da Microsoft da estação de trabalho, criando também uma cadeia de certificação.

Os componentes afetados pela configuração de certificados são:

- Serviços Java (por exemplo, Device Server, etc.)
- Aplicações .NET (Core Server)
- Validação de smart cards utilizados para a Autenticação de pré-arranque (Security Server)
- Importação de chaves de encriptação privadas para serem utilizadas na assinatura de pacotes de política a enviar ao Dell Manager. O Dell Manager efetua a validação SSL para clientes de encriptação geridos com unidades de encriptação automática ou com o BitLocker Manager.
- Estações de trabalho cliente:
  - Estações de trabalho que executam o BitLocker Manager
  - Estações de trabalho que executam o Encryption Enterprise (Windows)
  - Estações de trabalho que executam o Endpoint Security Suite Enterprise

Informação acerca do tipo de certificados a utilizar:

A autenticação de pré-arranque utilizando smart cards requer a validação SSL com o Security Server. O Dell Manager efetua a validação SSL ao ligar-se ao Dell Core Server. Para este tipo de ligações, a AC assinante terá de estar na keystore (seja na keystore da Java ou na

keystore da Microsoft, dependendo do componente do Dell Server em causa). Se forem selecionados certificados autoassinados, estão disponíveis as seguintes opções:

- Validação de smart cards utilizados para a autenticação de pré-arranque:
  - Importe o certificado de assinatura da "Agência raiz" e a cadeia de certificação completa para a keystore Java do Security Server. Tem de ser importada a cadeia de certificação completa.

Dell Manager:

- Insira o certificado de assinatura da "Agência raiz", a partir do certificado autoassinado que foi gerado, em "Autoridades de Certificação de Raiz Fidedigna" (para o "computador local") da estação de trabalho na keystore da Microsoft.
- Modificar o comportamento da validação SSL do lado do servidor. Para desativar a validação de confiança SSL do lado do servidor, selecione **Desativar verificação da cadeia de certificação** no separador Definições.

Existem dois métodos para criar um certificado — o *Expresso* e o *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, POC, etc. Para um ambiente de produção, a Dell recomenda a utilização de certificados assinados por uma autoridade de certificação (AC) pública ou assinados por domínio.
- Avançado - Escolha este método para configurar cada componente separadamente.

Expresso

1 A partir do menu superior, selecione **Ações** > **Configurar certificados**.

2 Quando o assistente de configuração for iniciado, selecione **Expresso** e clique em **Seguinte**. São utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Security Management Server, se disponíveis.

3 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

A configuração do certificado foi concluída. O resto da presente secção descreve pormenorizadamente o método avançado de criação de um certificado.

Avançado

Existem duas formas de criar um certificado - *Gerar um certificado autoassinado* e *Utilizar as definições atuais*. Escolha **uma** das formas:

- Caminhio1 - Gerar certificado autoassinado
- Caminho 2 - Utilizar definições atuais

Caminhio1 - Gerar certificado autoassinado

1 A partir do menu superior, selecione **Ações** > **Configurar certificados**.

2 Quando o assistente de configuração for iniciado, selecione **Avançado** e clique em **Seguinte**.

3 Selecione **Gerar certificado autoassinado** e clique em **Seguinte**. São utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Security Management Server, se disponíveis.

4 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

A configuração do certificado foi concluída. O resto da presente secção descreve pormenorizadamente o outro método de criação de um certificado.

Caminho 2 - Utilizar definições atuais

1 A partir do menu superior, selecione **Ações** > **Configurar certificados**.

2 Quando o assistente de configuração for iniciado, selecione **Avançado** e clique em **Seguinte**.

3 Selecione **Utilizar as definições atuais** e clique em **Seguinte**.

4 Na janela *Certificado SSL do Compatibility Server*, selecione **Gerar certificado autoassinado** e clique em **Seguinte**. São utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Security Management Server, se disponíveis.

Clique em **Seguinte**.

5 Na janela *Certificado SSL do Core Server*, selecione uma das seguintes opções:

- *Selecionar certificado* - Selecione esta opção para utilizar um certificado existente. Clique em **Seguinte**.

  Navegue até à localização do certificado existente, introduza a palavra-passe associada ao certificado existente e clique em **Seguinte**.

  Clique em **Concluir** quando tiver terminado.
- *Gerar certificado autoassinado* – São utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Security Management Server, se disponíveis. Se selecionar esta opção, a janela Certificado de segurança da mensagem não é apresentada (a janela é apresentada se selecionar a opção *Utilizar definições atuais* e é utilizado o certificado criado para o Dell Compatibility Server.

  Verifique se o nome do computador completamente qualificado está correto. Clique em **Seguinte**.

  É apresentada uma mensagem de aviso indicando que já existe um certificado com o mesmo nome. Quando lhe for perguntado se o pretende utilizar, clique em **Sim**.

  Clique em **Concluir** quando tiver terminado.
- *Utilizar definições atuais* - Selecione esta opção para alterar uma definição num certificado a qualquer altura após a configuração inicial do Security Management Server. Se selecionar esta opção, o seu certificado já configurado é guardado no devido lugar. Ao selecionar esta opção, avança até à janela Certificado de segurança da mensagem.

  Na janela Certificado de segurança da mensagem, selecione **uma** das seguintes opções:

  – *Selecionar certificado* - Selecione esta opção para utilizar um certificado existente. Clique em **Seguinte**.

    Navegue até à localização do certificado existente, introduza a palavra-passe associada ao certificado existente e clique em **Seguinte**.

    Clique em **Concluir** quando tiver terminado.
  – *Gerar certificado autoassinado* – São utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Security Management Server, se disponíveis.

    Clique em **Seguinte**.

    Clique em **Concluir** quando tiver terminado.

A configuração do certificado está concluída.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Importar Certificado do Dell Manager

Se a sua implementação incluir clientes Security Management Server geridos remotamente com Encryption Management Agents, tem de importar o seu certificado recentemente criado (ou existente). O certificado do Dell Manager é utilizado como um meio de proteger a chave privada utilizada para assinar os pacotes de políticas a enviar para os clientes Security Management Server geridos remotamente e para o

Encryption Management Agent. Este certificado pode ser independente de qualquer um dos outros certificados. Adicionalmente, se a chave estiver comprometida, esta pode ser substituída por uma chave nova, e o Dell Manager irá pedir uma nova chave pública se não conseguir desencriptar os conjuntos de política.

1 Abra a Consola de Gestão da Microsoft (MMC - Microsoft Management Console).
2 Clique em **Ficheiro** > **Adicionar/Remover Snap-in**.
3 Clique em **Adicionar**.
4 Na janela *Adicionar Snap-in autónomo*, selecione **Certificados** e clique em **Adicionar**.
5 Selecione **Conta de computador** e clique em **Adicionar**.
6 Na janela *Selecionar computador*, selecione **Computador local (o computador onde esta consola é executada** e clique em **Concluir**.
7 Clique em **Fechar**.
8 Clique em **OK**.
9 Na pasta *Raiz da consola*, expanda *Certificados (computador local)*.
10 Aceda à pasta *Pessoal* e localize o certificado pretendido.
11 Realce o certificado pretendido, clique com o botão direito do rato em **Todas as tarefas** > **Exportar**.
12 Quando o assistente para exportar certificados abrir, clique em **Seguinte**.
13 Selecione **Sim, exportar a chave privada** e clique em **Seguinte**.
14 Selecione **Personal Information Exchange - PKCS #12 (.PFX)** e depois selecione as subopções **Incluir todos os certificados no caminho de certificação, se possível** e **Exportar todas as propriedades expandidas**. Clique em **Seguinte**.
15 Introduza e confirme uma palavra-passe. Esta pode ser qualquer palavra-passe da sua escolha. Escolha uma palavra-passe que seja fácil de recordar, mas difícil de outros adivinharem. Clique em **Seguinte**.
16 Clique em **Procurar** para navegar para o local onde gostaria de guardar o ficheiro.
17 No campo *Nome do ficheiro*, introduza um nome para guardar o ficheiro. Clique em **Guardar**.
18 Clique em **Seguinte**.
19 Clique em **Concluir**.
20 É apresentada uma mensagem indicando que a exportação foi realizada com êxito. Feche a MMC.
21 Volte para a Dell Server Configuration Tool.
22 A partir do menu superior, selecione **Ações** > **Importar certificado DM**.
23 Navegue até à localização onde o ficheiro exportado foi guardado. Selecione o ficheiro e clique em **Abrir**.
24 Introduza a palavra-passe associada a este ficheiro e clique em **OK**.

A importação do certificado do Dell Manager está agora concluída.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.
2 Feche a Dell Server Configuration Tool.
3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Importar certificado SSL/TLS BETA

Se a sua implementação incluir o Server Encryption, terá de importar o certificado recentemente criado (ou existente). O certificado SSL/TLS BETA protege a chave privada que é utilizada para assinar os pacotes de políticas enviados para os servidores de cliente.

1 A partir do menu superior, selecione **Ações** > **Importar SSL/TLS BETA**.
2 Procure para selecionar um certificado e clique em **Seguinte**.

3 No pedido de *Palavra-passe de certificado*, introduza a palavra-passe associada ao certificado existente.

4 Na Caixa de diálogo de conta do Windows, escolha uma opção:

   a Para alterar as credenciais associadas com o certificado de identidade, selecione **Utilizar credenciais de conta do Windows diferentes com o certificado de identidade**.

   b Para continuar e utilizar as credenciais da conta presentemente ativa, clique em **Seguinte**.

5 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

Configurar as definições de Certificado do Servidor SSL

Em Server Configuration Tool, clique no separador **Definições**.

Dell Manager:

Para desativar a validação de confiança SSL do lado do servidor do Dell Manager, selecione **Desativar verificação de cadeia de certificação**.

SCEP:

Se estiver a utilizar a Mobile Edition, introduza o URL do servidor anfitrião do SCEP.

NOTA: A partir da versão 9.8, a Mobile Edition já não é suportada.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Configurar as definições SMTP

Em Server Configuration Tool, clique no separador **SMTP**.

Este separador configura as definições SMTP para o Data Guardian, Boletins de produtos, notificações e mensagens de comunicação de ameaças do Advanced Threat Prevention.

Quando as alterações de configuração estiverem concluídas, reinicie o serviço de Security Server. O serviço de Security Server deve ser reiniciado para as configurações serem atualizadas.

Introduza a informação seguinte:

1 Em *Nome do anfitrião*, introduza o FQDN do seu servidor SMTP, por exemplo smtpservername.domain.com.

2 Em *Nome de utilizador*, introduza o nome de utilizador para iniciar sessão no servidor de e-mail. O formato pode ser DOMÍNIO\jsilva, jsilva ou o que for estabelecido pela sua organização.

3 Em *Palavra-passe*, introduza a palavra-passe associada a este nome de utilizador.

4 Em *Do endereço*, introduza o endereço de e-mail de onde será enviada a mensagem. Este pode ser o mesmo da conta do nome de utilizador (jsilva@domínio.com), mas também pode ser de outra conta a que o nome de utilizador especificado tenha acesso para enviar mensagens de correio eletrónico (RegistonaNuvem@domínio.com).

5 No campo *Porta*, introduza o número da porta (normalmente 25).

6 No menu *Autenticação*, selecione *Verdadeiro* ou *Falso*.

NOTA: O nome de utilizador e a palavra-passe devem ser deixados em branco se a autenticação for definida como falsa.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Alterar o nome da base de dados, a localização ou as credenciais

Em Server Configuration Tool, clique no separador **Base de dados**.

1 Em *Nome do servidor*, introduza o nome de domínio totalmente qualificado (no caso de existir um nome de instância, inclua-o) do servidor anfitrião da base de dados. Por exemplo, SQLTest.domain.com\DellDB.

A Dell recomenda a utilização de um nome de domínio totalmente qualificado, embora possa ser utilizado um endereço IP.

2 Em *Porta do servidor*, introduza o número da porta.

Quando utilizar uma instância não predefinida do SQL Server, tem de especificar a porta dinâmica da instância em *Porta:*. Como alternativa, ative o serviço SQL Server Browser e certifique-se de 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 Em *Base de dados*, introduza o nome da base de dados.

4 Em *Autenticação:*, selecione **Autenticação do Windows** ou **Autenticação de SQL Server**. Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows são utilizadas para autenticação (o *Nome de utilizador* e a *Palavra-passe* não são editáveis).

5 Em *Nome de utilizador:*, introduza o nome de utilizador associado a esta base de dados.

6 Em *Palavra-passe:*, introduza a palavra-passe associada ao nome de utilizador facultado no campo *Nome de utilizador*.

7 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

8 Para testar a configuração da base de dados, no menu superior, selecione **Ações** > **Testar Configuração da Base de Dados**. O Assistente de configuração é iniciado.

9 Na janela *Teste de Configuração*, leia a informação e depois clique em **Seguinte**.

10 No caso de escolher a Autenticação do Windows no separador *Base de dados*, poderá, opcionalmente, introduzir credenciais alternativas para utilizar as mesmas credenciais usadas para executar o Security Management Server. Clique em **Seguinte**.

11 Na janela de *Testar Configuração*, serão exibidos os resultados das definições de Testar Ligação, Teste de Compatibilidade e Teste Migrado de Base de Dados.

12 Clique em **Concluir**.

NOTA:

Se a base de dados do SQL ou instância do SQL está configurada com um agrupamento não predefinido, o agrupamento precisa ser sensível a maiúsculas e minúsculas. Para ver a lista de agrupamentos e de sensibilidade a maiúsculas e minúsculas, consulte https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Migrar a base de dados

Pode migrar uma base de dados v9.2 ou posterior para o esquema mais recente com a atualização mais recente do servidor.

Em Server Configuration Tool, clique no separador **Base de dados**.

1 Caso ainda não tenha realizado a cópia de segurança da sua atual base de dados do Dell Server, **faça-a agora**.

2 No menu superior, selecione **Ações** > **Migrar Base de Dados**. O Assistente de configuração é iniciado.

3 Será exibida uma mensagem de aviso na janela *Migrar Base de Dados Enterprise*. Confirme que realizou a cópia de segurança da totalidade da base de dados ou confirme que não é necessário realizar uma cópia de segurança da sua base de dados corrente. Clique em **Seguinte**.

   Na janela *A Migrar Base de Dados* serão exibidas mensagens informativas sobre o estado da migração.

   Ao terminar, verifique se ocorreram erros.

   NOTA: Uma mensagem de erro identificada por , indica que houve uma falha numa tarefa da base de dados e que é necessário tomar uma ação corretiva antes de poder migrar corretamente a base de dados. Clique em Concluir, corrija os erros da base de dados e repita o procedimento descrito nesta secção.

4 Clique em **Concluir**.

Uma vez concluída a migração:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

6

Tarefas administrativas

Atribuir o papel de administrador da Dell

1 Inicie sessão na Management Console como administrador do Security Management Server Virtual: https://server.domain.com:8443/webui/. As credenciais predefinidas são **superadmin/changeit**.
2 No painel esquerdo, clique em **Populações** > **Domínios**.
3 Clique num domínio para adicionar um utilizador.
4 Na página Detalhe do domínio, clique no separador **Membros**.
5 Clique em **Adicionar utilizador**.
6 Introduza um filtro para pesquisar o nome de utilizador por Nome comum, Nome principal universal ou sAMAccountName. O carácter universal é *.

   Tem de ser definido no servidor de diretório da empresa um Nome comum, Nome principal universal ou sAMAccountName para cada utilizador. Se um utilizador for membro de um Domínio ou Grupo mas não aparecer na lista de Membros do Domínio ou Grupo em Management Console, certifique-se de que os três nomes estão definidos de forma adequada para o utilizador no servidor de diretório da empresa.

   A consulta irá procurar automaticamente por nome comum, UPN e nome sAMAccount, por esta ordem, até ser encontrada uma correspondência.
7 Selecione os utilizadores na *Lista de utilizadores do diretório* para adicionar ao domínio. Utilize <Shift><click> ou <Ctrl><click> para selecionar múltiplos utilizadores.
8 Clique em **Adicionar**.
9 Na barra de menus, clique no separador **Detalhes e ações** do utilizador especificado.
10 Desloque-se na barra de menus e selecione o separador **Administração**.
11 Selecione os papéis do administrador a adicionar a este utilizador.
12 Clique em **Guardar**.

Iniciar uma sessão com o Papel de administrador da Dell

1 Termine sessão na Management Console.
2 Inicie sessão na Management Console e inicie sessão com as credenciais de utilizador do domínio.

Carregar licença de acesso de cliente

Deverá ter recebido as licenças de acesso de cliente separadamente dos ficheiros de instalação, com a compra inicial ou mais tarde se tiver adicionado mais licenças de acesso de cliente.

1 No painel da esquerda, clique em **Management** (Gestão).
2 Clique em **License Management** (Gestão de licenças).
3 Clique em **Choose File** (Escolher ficheiro) para localizar e selecionar o ficheiro de licença de cliente.

Consolidar políticas

Consolide políticas quando a instalação estiver concluída.

Para consolidar políticas após a instalação ou, posteriormente, após as modificações de políticas serem guardadas, siga estes passos:

1 No painel da esquerda, clique em **Gestão** > **Consolidar**.
2 Em *Comentário*, introduza uma descrição da alteração.
3 Clique em **Consolidar políticas**.

Configurar o Dell Compliance Reporter

1 No painel da esquerda, clique em **Compliance Reporter**.
2 Quando o Dell Compliance Reporter iniciar, inicie sessão com as credenciais predefinidas de *superadmin/changeit*.

Realizar Cópias de Segurança

Tendo em vista a recuperação de desastres, certifique-se de que são feitas semanalmente cópias de segurança das seguintes localizações, com diferenciais noturnos. Para obter mais informações sobre o planeamento para recuperação de desastres, consulte http://www.dell.com/support/article/us/en/04/sln292355/plan-for-disaster-recovery-and-high-availability-with-dell-security-management-server-dell-data-protection-server?lang=en. Para obter mais informações sobre como realizar uma cópia de segurança de dados do Compliance Reporter, consulte http://www.dell.com/support/article/de/en/debsdt1/sln289096/how-to-backup-and-import-custom-compliance-reports-in-dell-security-management-server-dell-data-protection-enterprise-edition-server?lang=en.

Cópias de segurança do Security Management Server

Realize regularmente cópias de segurança dos ficheiros que estão armazenados na localização que selecionou para a cópia de segurança do ficheiro de configuração durante a instalação (passo 10 na página 27 ou Atualização/Migração (passo 6 na página 68). É aceitável a realização de cópias de segurança semanais destes dados, uma vez que raramente são alterados e que podem ser reconfigurados manualmente, se necessário. Os ficheiros mais importantes contêm as informações necessárias para estabelecer ligação à base de dados:

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

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

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

Cópias de segurança do SQL Server

Realize cópias de segurança completas noturnas com registo transacional ativado e realize cópias de segurança da base de dados diferencial a cada 3-4 horas. Se estiver disponível uma cópia de segurança de base de dados, a recomendação seria que os registos transacionais e/ou tarefas de envio de registos sejam realizadas em intervalos de 15 minutos (ou intervalos menores, se possível). Como sempre, a Dell recomenda que sejam seguidas as melhores práticas de utilização de base de dados para a base de dados da Dell e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

Para mais informações sobre as melhores práticas do SQL Server, consulte a seguinte lista. As melhores práticas devem ser implementadas quando o Dell Security for instalado, caso ainda não esteja implementado.

Cópias de segurança do PostgreSQL Server

Os eventos de auditoria são armazenados no servidor PostgreSQL, que deve ser alvo de uma cópia de segurança regular. Para obter instruções sobre cópias de segurança, consulte https://www.postgresql.org/docs/9.5/static/backup.html.

A Dell recomenda que sejam seguidas as melhores práticas de utilização da base de dados para a base de dados PostgreSQL e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

7

Portas

A tabela seguinte descreve cada componente e a sua função.

Nome	Porta predefinida	Descrição
Compliance Reporter	HTTP(S)/ 8084	Oferece uma visão abrangente do ambiente, tendo em vista a elaboração de relatórios de auditoria e conformidade.
Management Console	HTTP(S)/ 8443	Consola de administração e centro de controlo para implementação na empresa inteira.
Core Server	HTTPS/ 8888	Gere o fluxo das políticas, as licenças e o registo para PBA (Preboot Authentication), SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa dados de inventário para utilização pelo Compliance Reporter e pela Management Console. Reúne e armazena os dados de autenticação. Controla o acesso baseado em funções.
Device Server	HTTPS/ 8081	Suporta ativações e recuperação de palavra-passe. Um componente do Security Management Server. Necessário para Encryption Enterprise (Windows e Mac)
Security Server	HTTPS/ 8443	Comunica com o Policy Proxy; gera obtenções de chaves forenses, ativações de clientes, Data Guardian, comunicação SED-PBA e Active Directory para autenticação ou reconciliação, incluindo validação de identidades para autenticação na Management Console. Requer o acesso à base de dados SQL.
Compatibility Server	TCP/ 1099	Um serviço para gerir a arquitetura empresarial. Reúne e armazena os dados de inventário iniciais durante a ativação e os dados de políticas durante as migrações. Processa os dados com base nos grupos de utilizadores.
Message Broker Service	TCP/ 61616 e STOMP/ 61613	Trata da comunicação entre serviços do Dell Server. Prepara as informações de políticas criadas pelo Compatibility Server para colocação em fila de Policy Proxy. Requer o acesso à base de dados SQL.
Key Server	TCP/ 8050	Negocia, autentica e encripta uma ligação de cliente utilizando APIs Kerberos. Requer o acesso à base de dados do SQL para extrair os dados de chave.

Nome	Porta predefinida	Descrição
Policy Proxy	TCP/ 8000	Oferece uma linha de comunicação com base na rede de forma a proporcionar atualizações de políticas de segurança e atualizações de inventário.
LDAP	TCP/ 389/636 (controlador de domínio local), 3268/3269 (catálogo global) TCP/ 135/ 49125+ (RPC)	Porta 389 - Esta porta é utilizada para o pedido de informações a partir do controlador de domínio local. Os pedidos de LDAP enviados à porta 389 podem ser utilizados para procurar objetos apenas dentro do domínio raiz do catálogo global. No entanto, a aplicação requerente pode obter todos os atributos para esses objetos. Por exemplo, um pedido na porta 389 poderia ser utilizado para obter um departamento de utilizador. Porta 3268 - Esta porta é utilizada para consultas especificamente direcionadas para o catálogo global. Os pedidos de LDAP enviados à porta 3268 podem ser utilizados para procurar objetos na floresta inteira. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, um departamento de utilizador não poderia ser devolvido utilizando a porta 3268 uma vez que este atributo não é replicado para o catálogo global.
Base de dados Microsoft SQL	TCP/ 1433	A porta do SQL Server predefinida é a 1433 e é atribuído um valor aleatório entre 1024 e 5000 às portas de cliente.
Client Authentication	HTTPS/ 8449	Permite aos servidores cliente autenticarem com o Dell Server. Necessário para Server Encryption.
Beacon de chamada de retorno	HTTP/TCP 8446	Permite que um beacon de chamada de retorno seja inserido em cada ficheiro protegido do Office ao executar o modo protegido do Office do Data Guardian.

8

Melhores práticas do SQL Server

A lista seguinte explica as melhores práticas do SQL Server, que devem ser aplicadas quando o Dell Security for instalado, se ainda não estiver implementado.

1 Certifique-se de que o tamanho do bloco NTFS onde se encontram o ficheiro de dados e o ficheiro de registo é de 64 KB. As extensões do SQL Server (unidade básica do armazenamento do SQL) são de 64 KB.

   Para obter mais informações, procure "Understanding Pages and Extents" (Compreender páginas e extensões" nos artigos TechNet da Microsoft).

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

2 Como orientação geral, defina a quantidade máxima da memória do SQL Server para 80% da memória instalada.

   Para obter mais informações, procure *Server Memory Server Configuration Options* (Opções de configuração do servidor de memória) nos artigos TechNet da Microsoft.

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

3 Defina -t1222 nas propriedades de arranque da instância para garantir que as informações de impasse são capturadas, se ocorrer um.

   Para obter mais informações, procure "Trace Flags (Transact-SQL)" [Sinalizadores de rastreio (Transact-SQL)] nos artigos TechNet da Microsoft.

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

4 Certifique-se de que todos os índices são abrangidos por um trabalho de manutenção semanal para reconstruir os índices.

9

Certificados

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

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

Para obter informações sobre os requisitos mínimos para solicitar certificados SSL/TLS a serem utilizados pelo servidor Dell Data Security, consulte http://www.dell.com/support/article/us/en/19/sln307037/dell-data-protection-enterprise-edition-and-virtual-edition-dell-security-management-sever-and-virtual-server-ssl-tls-certificate-minimum-requirements?lang=en.

Para obter informações sobre a atualização do certificado da Dell Encryption com um certificado existente na keystore da Microsoft, consulte http://www.dell.com/support/article/us/en/19/sln297240/.

Criar um certificado autoassinado e gerar um pedido de assinatura de certificado

Esta seção detalha os passos necessários para criar um certificado autoassinado para os componentes baseados em Java. Este processo **não pode** ser utilizado para criar um certificado autoassinado para componentes baseados em .NET.

A Dell recomenda a utilização de um certificado autoassinado *apenas* num ambiente de não produção.

Se a sua organização requerer um certificado de servidor SSL, ou se precisar de criar um certificado por outras razões, esta secção descreve o processo para criar uma keystore Java utilizando a aplicação Keytool.

Se a sua organização planear utilizar smart cards para autenticação, tem de utilizar a aplicação Keytool para importar a cadeia de certificação completa utilizada no certificado do utilizador do smart card.

A aplicação Keytool cria chaves privadas que são transmitidas no formato de Solicitação de Assinatura de Certificado (CSR) a uma Autoridade de Certificação (AC), como VeriSign® ou Entrust®. Com base nesta CSR, a AC irá então criar um certificado de servidor assinado. O certificado de servidor é depois transferido para um ficheiro, juntamente com o certificado da autoridade assinante. De seguida, os certificados são importados para o ficheiro cacerts.

Gerar um novo par de chaves e um certificado autoassinado

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

2 Faça uma cópia de segurança da base de dados de certificados predefinida:

Clique em **Iniciar** > **Executar** e escreva `move cacerts cacerts.old`.

3 Adicione a aplicação Keytool ao caminho do sistema. Escreva o seguinte comando numa janela de comandos:

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

4 Para gerar um certificado, execute a aplicação Keytool como indicado:

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

5 Introduza as informações seguintes à medida que forem solicitadas pela aplicação Keytool.

NOTA:
Faça uma cópia de segurança dos ficheiros de configuração antes de editá-los. Mude apenas os parâmetros especificados. Se mudar outros dados nestes ficheiros, incluindo as etiquetas, pode corromper o sistema e causar a sua falha. A Dell não pode garantir que os problemas resultantes de alterações não autorizadas a estes ficheiros possam ser resolvidos sem a reinstalação do Security Management Server.

- *Palavra-passe da Keystore*: introduza uma palavra-passe (os caracteres não suportados são <>;&" ') e defina a variável no ficheiro **conf** do componente com o mesmo valor, conforme se segue:

  <Compliance Reporter install dir>\conf\eserver.properties. Defina o valor eserver.keystore.password =

  <Device Server install dir>\conf\application.properties. Defina o valor keystore.password =

  <Security Server install dir>\conf\application.properties. Defina o valor keystore.password =
- *Nome completamente qualificado do servidor*: introduza o nome completamente qualificado do servidor onde está instalado o componente com o qual está a trabalhar. Este nome completamente qualificado inclui o nome do anfitrião e o nome do domínio (exemplo: server.domain.com).
- *Unidade organizacional*: introduza o valor adequado (por exemplo, Segurança).
- *Organização*: introduza o valor apropriado (por exemplo, Dell).
- *Cidade ou localização*:introduza o valor apropriado (por exemplo, Lisboa).
- *Estado ou região*: introduza o nome não abreviado do estado ou da região (por exemplo, Mondego).
- Código de país de duas letras.
- O utilitário solicita que confirme se a informação está correta. Se for o caso, escreva `yes` (sim).

  Caso contrário escreva `no` (não). A aplicação Keytool apresenta os valores introduzidos anteriormente. Clique em **Enter** para aceitar o valor ou altere o valor e clique em **Enter**.
- *Palavra-passe para alias*: se não introduzir outra palavra-passe aqui, esta palavra-passe é predefinida como a palavra-passe da Keystore.

Solicitar um certificado assinado de uma autoridade de certificação

Use este procedimento para gerar uma Solicitação de Assinatura de Certificado (CSR) para o certificado autoassinado criado em Generate a New Key Pair and a Self-Signed Certificate (Gerar um novo par de chaves e um certificado autoassinado).

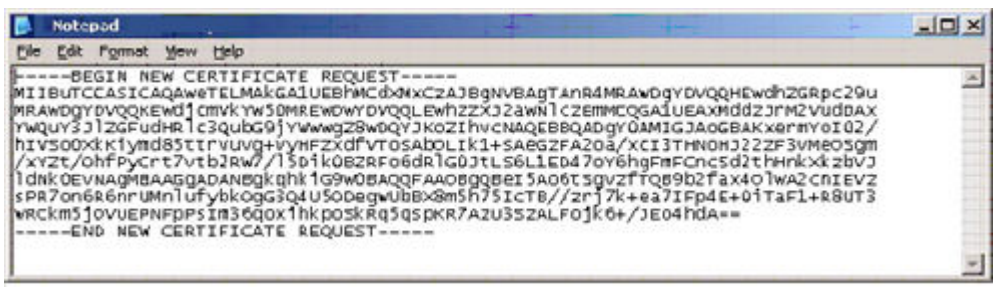
1 Substitua o mesmo valor utilizado anteriormente para <**certificatealias**>:

```
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 ficheiro .csr contém o par BEGIN/END que será utilizado durante a criação do certificado na AC.

Exemplo de um ficheiro .CSR



2 Siga o seu processo organizacional para adquirir um certificado do servidor SSL de uma Autoridade de certificação. Envie o conteúdo do <csr-filename> para assinatura.

> **NOTA:**
> Existem vários métodos para solicitar um certificado válido. É apresentado um exemplo de método em **Exemplo de método para solicitar um certificado**.

3 Quando receber o certificado assinado, guarde-o num ficheiro.

4 Como recomendação, faça uma cópia de segurança deste certificado para o caso de ocorrer algum erro durante o processo de importação. Esta cópia de segurança evita que tenha de recomeçar o processo.

Importar um certificado de raiz

Se a autoridade de certificação do certificado de raiz for o Verisign (mas não o teste de Verisign), ignore o procedimento seguinte e importe o certificado assinado.

O certificado de raiz da autoridade de certificação valida certificados assinados.

1 Realize **um** dos seguintes procedimentos:

- Transfira o certificado de raiz da autoridade de certificação e guarde-o num ficheiro.
- Obtenha o certificado de raiz do Enterprise Directory Server.

2 Realize **um** dos seguintes procedimentos:

- Se pretender ativar o SSL para o Compliance Reporter, Security Server ou Device Server, mude para o diretório **conf** do componente.
- Se pretender ativar o SSL entre o Security Management Server e o Enterprise Directory Server, mude para <**Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (a palavra-passe predefinida para JRE cacerts é **changeit**).

3 Execute a aplicação Keytool conforme descrito a seguir para instalar o certificado de 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`

Exemplo de método para solicitar um certificado

Um exemplo de método para solicitar um certificado é utilizar um browser para aceder ao Microsoft CA Server, que é configurado internamente pela sua organização.

1 Navegue até ao Microsoft CA Server. O endereço IP é fornecido pela sua organização.

2 Selecione **Solicitar certificado** e clique em **Seguinte**.

Serviços de certificados da Microsoft

3 Selecione **Solicitação avançada** e clique em **Seguinte**.

Escolher tipo de pedido

4 Selecione a opção para **Enviar uma solicitação de certificado utilizando um ficheiro PKCS #10 com codificação de base 64** e clique em **Seguinte**.

Pedido de certificado avançado

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

Submeter um pedido guardado

6 Guarde o certificado. Selecione **Codificação DER** e clique em **Transferir certificado AC**.

Transferir certificado AC

7 Guarde o certificado. Selecione **Codificação DER** e clique em **Transferir caminho da certificação AC**.

Transferir caminho da certificação AC

8 Importe o certificado da autoridade assinante convertido. Volte para a linha de comandos. Escreva:

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

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

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

Utilize o alias do certificado autoassinado para emparelhar a solicitação de CSR com o certificado do servidor.

10 A lista do ficheiro cacerts mostra que o certificado do servidor tem uma **cadeia de certificação com um comprimento** de **2**, o que indica que o certificado não é autoassinado. Escreva:

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

A impressão digital do segundo certificado na cadeia é o certificado da autoridade assinante importado (que também é mostrado na lista, abaixo do certificado de servidor).

Exportar um certificado para .PFX utilizando a consola de gestão de certificados

Quando tiver um certificado no formato de ficheiro .crt na MMC, tem de o converter para um ficheiro .pfx para poder utilizá-lo com a aplicação Keytool quando o Security Server é utilizado no modo DMZ *e* quando importa um certificado do Dell Manager para a Server Configuration Tool.

1 Abra a Consola de Gestão da Microsoft (MMC - Microsoft Management Console).
2 Clique em **Ficheiro** > **Adicionar/Remover Snap-in**.
3 Clique em **Adicionar**.
4 Na janela *Adicionar Snap-in autónomo*, selecione **Certificados** e clique em **Adicionar**.
5 Selecione **Conta de computador** e clique em **Adicionar**.
6 Na janela *Selecionar computador*, selecione **Computador local (o computador onde esta consola é executada** e clique em **Concluir**.
7 Clique em **Fechar**.
8 Clique em **OK**.
9 Na pasta *Raiz da consola*, expanda *Certificados (computador local)*.
10 Aceda à pasta *Pessoal* e localize o certificado pretendido.
11 Realce o certificado pretendido, clique com o botão direito do rato em **Todas as tarefas** > **Exportar**.
12 Quando o assistente para exportar certificados abrir, clique em **Seguinte**.
13 Selecione **Sim, exportar a chave privada** e clique em **Seguinte**.
14 Selecione **Personal Information Exchange - PKCS #12 (.PFX)** e depois selecione as subopções **Incluir todos os certificados no caminho de certificação, se possível** e **Exportar todas as propriedades expandidas**. Clique em **Seguinte**.
15 Introduza e confirme uma palavra-passe. Esta pode ser qualquer palavra-passe da sua escolha. Escolha uma palavra-passe que seja fácil de recordar, mas difícil de outros adivinharem. Clique em **Seguinte**.
16 Clique em **Procurar** para navegar para o local onde gostaria de guardar o ficheiro.

17 No campo *Nome do ficheiro*, introduza um nome para guardar o ficheiro. Clique em **Guardar**.

18 Clique em **Seguinte**.

19 Clique em **Concluir**.

É apresentada uma mensagem indicando que a exportação foi realizada com êxito. Feche a MMC.

Adicionar um certificado fidedigno de assinatura ao Security Server quando foi utilizado um certificado SSL não fidedigno

1 Pare o Security Server, se este estiver a ser executado.

2 Faça uma cópia de segurança do ficheiro cacerts em <Security Server install dir>\conf\.

Utilize a aplicação Keytool para completar o seguinte:

3 Exporte o PFX fidedigno para um ficheiro de texto e documente o alias:

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

4 Importe o PFX para o ficheiro cacerts em <Security Server install dir>\conf\.

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

5 Modifique o valor keystore.alias.signing em <Security Server install dir>\conf\application.properties.

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

Inicie o serviço Security Server.