DDP Enterprise Server - Virtual Edition

Guia de instalação e de início rápido v9.7

Notas, avisos e advertências

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

CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

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

Guia de instalação e de início rápido do VE

2017 - 04

Rev. A01

Índice

Guia de início rápido do Virtual Edition

Este Guia de início rápido destina-se a usuários mais experientes com o objetivo de colocar o DDP Enterprise Server - VE em uso o mais rápido possível. Como regra geral, a Dell recomenda instalar o DDP Enterprise Server - VE primeiro, seguido pela instalação dos clientes.

Para obter instruções mais detalhadas, consulte o Guia de instalação do Virtual Edition.

Para obter informações sobre pré-requisitos do VE, consulte Pré-requisitos do DDP Enterprise Server - VE, Pré-requisitos do VE Remote Management Console e Pré-requisitos do modo Proxy.

Para obter informações sobre como atualizar o DDP Enterprise Server - VE existente, consulte Atualizar o DDP Enterprise Server - VE.

Instalar o DDP Enterprise Server - VE

1 Navegue até o diretório no qual os arquivos do Dell Data Protection estão armazenados e clique duas vezes para importá-los para o VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**.
2 Ligue o DDP Enterprise Server - VE.
3 Siga as instruções na tela.

Configure o VE

Antes de ativar os usuários, é necessário concluir as seguintes tarefas de configuração no Terminal DDP Enterprise Server - VE:

- Definir ou alterar a senha de banco de dados
- Definir as configurações do SMTP
- Importar um certificado existente ou inscrever um novo certificado de servidor
- Atualizar o DDP Enterprise Server - VE
- Instale um cliente FTP que ofereça suporte para o protocolo SFTP na porta 22 e configure os usuários de FTP.

  Se sua organização tiver dispositivos voltados para a área externa, consulte Instalar e configurar o modo proxy.

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

Abrir o VE Remote Management Console

Abra o VE Remote Management Console neste endereço:

https://server.domain.com:8443/webui/

As credenciais padrão são **superadmin/changeit**.

Para obter uma lista de navegadores da Web compatíveis, consulte Pré-requisitos do VE Remote Management Console.

Tarefas administrativas

Se você não tiver iniciado o VE Remote Management Console, faça-o agora. As credenciais padrão são **superadmin/changeit**.

A Dell recomenda que você atribua funções de administrador o quanto antes. Para concluir essa tarefa agora, consulte Atribuir Função de Dell Administrator.

Clique em "?" no canto superior do VE Remote Management Console para iniciar a *AdminHelp do Dell Data Protection.* A página *Introdução* é mostrada. Clique em **Adicionar domínio**.

As políticas de linha de base foram definidas para a sua organização, mas estas podem precisar ser modificadas de acordo com as suas necessidades específicas, da seguinte maneira (o licenciamento e os direitos guiam todas as ativações):

- Computadores Windows serão criptografados
- Computadores com unidades de criptografia automática serão criptografados
- O BitLocker Management não é ativado
- O Advanced Threat Protection não é ativado
- O Threat Protection é ativado
- A mídia externa não será criptografada
- Os dispositivos conectados às portas não serão criptografados
- O Dell Data Guardian é ativado
- O Mobile Edition não é ativado

Veja o tópico *Gerenciar políticas* da AdminHelp para navegar para os grupos de tecnologia e obter as descrições das políticas.

As tarefas de início rápido estão concluídas.

Guia de Instalação do Virtual Edition

Este Guia de Instalação tem como objetivo ajudar usuários menos experientes com a instalação e configuração do DDP Enterprise Server - VE. Como regra geral, a Dell recomenda instalar o DDP Enterprise Server - VE primeiro, seguido pela instalação dos clientes.

Para obter informações sobre como atualizar o DDP Enterprise Server - VE existente, consulte Atualizar o DDP Enterprise Server - VE.

Sobre o DDP Enterprise Server - VE

O DDP Enterprise Server - VE é o componente de administração de segurança da solução da Dell. O VE Remote Management Console permite que os administradores monitorem o estado de pontos de extremidade, a aplicação de política e a proteção na empresa. O modo Proxy oferece uma opção de modo DMZ de front-end para uso com o DDP Enterprise Server - VE.

O DDP Enterprise Server - VE tem os seguintes recursos:

- Gerenciamento centralizado de até 3.500 dispositivos
- Criação e gerenciamento de política de segurança baseada em função
- Recuperação de dispositivo auxiliado pelo administrador
- Separação de deveres administrativos
- Distribuição automática de políticas de segurança
- Caminhos confiáveis para comunicação entre os componentes
- Geração de chave de criptografia exclusiva e depósito de chave de segurança
- Auditoria e relatórios de compatibilidade centralizados
- Autogeração de certificados autoassinados

Entre em contato com o Dell ProSupport

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

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

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

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

Requisitos

Pré-requisitos do DDP Enterprise Server - VE

Hardware

O espaço em disco recomendado para o DDP Enterprise Server - VE é de 80 GB.

Ambiente virtualizado

O DDP Enterprise Server - VE v9.6 foi validado com os seguintes ambientes virtualizados.

Ambientes virtualizados

- VMware Workstation 12.5
  - CPU de 64 bits necessária
  - 4 GB de RAM recomendado
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte http://pubs.vmware.com/workstation-11/index.jsp para obter mais informações.

- VMware Workstation 11
  - CPU de 64 bits necessária
  - 4 GB de RAM recomendado
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte http://pubs.vmware.com/workstation-11/index.jsp para obter mais informações.

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

- VMware ESXi 5.5
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado
  - Não é necessário ter um sistema operacional específico
  - Consulte a página http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operacionais host compatíveis
  - O hardware precisa estar em conformidade com os requisitos mínimos do VMware
  - Mínimo de 4 GB de RAM para recurso dedicado de imagem
  - Consulte http://pubs.vmware.com/vsphere-55/index.jsp para obter mais informações

- Hyper-V Server (instalação básica ou completa)
  - CPU x86 de 64 bits necessária
  - Computador host com no mínimo dois núcleos
  - Mínimo de 8 GB de RAM recomendado

Ambientes virtualizados

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

Pré-requisitos do VE Remote Management Console

Navegadores de Internet

NOTA:
Seu navegador precisa aceitar cookies.

A tabela a seguir detalha os navegadores de Internet suportados.

Navegadores de Internet

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

Pré-requisitos do modo Proxy

Hardware

A tabela a seguir detalha os requisitos *mínimos* de hardware para o modo Proxy.

Processador

Core 2 Duo de 2 GHz ou superior

RAM

No mínimo 2 GB dedicados de RAM/4 GB dedicados de RAM recomendados

Espaço livre em disco

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

Placa de rede

Placa de interface de rede 10/100/1000

Diversos

TCP/IP instalado e ativado

Software

A tabela a seguir detalha o software que já precisará estar instalado antes da instalação do modo Proxy.

Pré-requisitos

- **Windows Installer 4.0 ou posterior**

  O Windows Installer 4.0 ou posterior deve ser instalado no servidor no qual a instalação está sendo feita.

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

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

- **Microsoft .NET Framework versão 4.5**

  A Microsoft publicou as atualizações de segurança para o .NET Framework versão 4,5.

A tabela a seguir detalha os requisitos de software para o servidor do modo Proxy.

NOTA:
Sempre desative o UAC ao usar o Windows Server 2008. Após desativar o UAC, o servidor precisa ser reiniciado para que essa alteração tenha efeito.

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

Sistema operacional

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

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2008 SP2 64 bits**

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition

- **Windows Server 2016**

  - Standard Edition

  - Datacenter Edition

Fazer download do DDP Enterprise Server - VE

Na instalação inicial, o DDP Enterprise Server - VE é fornecido como um arquivo OVA (Open Virtual Application), um aplicativo virtual aberto usado para oferecer softwares que são executados em uma máquina virtual. O arquivo OVA do DDP Enterprise Server - VE está disponível em www.dell.com/support, nas páginas de Suporte a produtos para os seguintes produtos do Dell Data Protection:

Criptografia

ou

Endpoint Security Suite

ou

Endpoint Security Suite Enterprise

ou

Data Guardian

Para fazer download do arquivo OVA:

1 Navegue até a página de suporte do produto para o Encryption, o Endpoint Security Suite, o Endpoint Security Suite Enterprise ou o Data Guardian.
2 Clique em **Drivers e downloads**.
3 Ao lado de "Ver todas as atualizações disponíveis para <versão do SO>," clique em **Alterar SO** e selecione uma das opções a seguir: **VMware ESXi 6.0, VMware ESXi 5.5** ou **VMware ESXi 5.1**.
4 Em "Ver por:", selecione **Exibir todos**.
5 Em Dell Data Protection, selecione **Download**.

Instalar o DDP Enterprise Server - VE

Antes de começar, verifique se todos os requisitos de ambiente virtual e do sistema são atendidos.

1 Localize os arquivos do Dell Data Protection na mídia de instalação e clique duas vezes para importá-los para o VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**.
2 Ligue o DDP Enterprise Server - VE.
3 Selecione o idioma para o contrato de licença e selecione **Mostrar EULA**.
4 Leia o contrato e selecione **Aceitar EULA**.
5 Se houver uma atualização disponível, selecione **Aceitar**.
6 Selecione **Modo padrão** ou **Modo desconectado**.

> **NOTA:**
> Se você selecionar **Modo desconectado**, o VE nunca poderá ser alterado para Modo padrão.
>
> O modo desconectado isola o VE da Internet e de uma LAN não protegida ou outra rede. Todas as atualizações devem ser realizadas manualmente. Para obter mais informações sobre as políticas e a funcionalidade do Modo desconectado, consulte o tópico *AdminHelp*.

7 No prompt de alteração de senha padrão, selecione **Sim**.
8 Na tela *Definir senha do ddpuser*, digite a senha (padrão) atual, **ddpuser**, em seguida insira uma senha única, digite novamente a senha única e selecione **OK**.

   As senhas precisam conter o seguinte:

   - Pelo menos 8 caracteres
   - Pelo menos 1 letra maiúscula
   - Pelo menos 1 número
   - Pelo menos 1 caractere especial

9 Na caixa de diálogo *Configurar nome de host*, use a tecla Backspace para remover o nome de host padrão. Digite um nome de host único e selecione **OK**.
10 Na diálogo *Definir configurações da rede*, selecione qualquer uma das opções abaixo e selecione **OK**.

   - (Padrão) Usar o DHCP.
   - (Recomendado) No campo Usar DHCP, pressione a barra de espaço para remover o X e inserir manualmente esses endereços, conforme aplicável: IP estático, Máscara de rede, Gateway padrão, Servidor de DNS 1, Servidor de DNS 2, Servidor de DNS 3.

NOTA: Quando um IP estático é usado, é necessário também criar uma entrada de host no servidor DNS.

11 Na tela *Fuso horário*, use as teclas de seta para selecionar o fuso horário e, em seguida, selecione **Entrar**.

12 No prompt de confirmação do fuso horário, selecione **OK**.

13 Quando a mensagem for mostrada para indicar que a configuração inicial foi concluída, selecione **OK**.

14 Definir ou alterar a senha de banco de dados.

15 Definir as configurações do SMTP.

16 Importar um certificado existente ou inscrever um novo certificado de servidor.

17 Atualizar o DDP Enterprise Server - VE.

18 Instale um cliente FTP que ofereça suporte para o protocolo SFTP na porta 22 e configure os usuários de FTP.

As tarefas de instalação do DDP Enterprise Server - VE estão concluídas.

Abrir o VE Remote Management Console

Abra o VE Remote Management Console neste endereço:

https://server.domain.com:8443/webui/

As credenciais padrão são **superadmin/changeit**.

Para obter uma lista de navegadores da Web compatíveis, consulte Pré-requisitos do VE Remote Management Console.

Instalar e configurar o modo Proxy

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

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

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

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

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

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

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

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

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

7 Inserir a chave do produto.

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

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

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

Selecione a opção “a” ou “b” abaixo:

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

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

Digite a senha associada a esse certificado. O arquivo de armazenamento de chaves deve ser .p12 ou pfx.

Clique em **Avançar**.

> **NOTA:**
> Para usar essa configuração, o certificado CA exportado que está sendo importado precisa ter a cadeia de confiança completa. Se não tiver certeza, exporte novamente o certificado CA e verifique se as seguintes opções estão selecionadas no "Assistente para exportação de certificados":
>
> - Troca de informações pessoais - PKCS#12 (.PFX)
> - Incluir todos os certificados no caminho de certificação, se possível
> - Exportar todas as propriedades estendidas

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

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

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

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Estado (nome completo)

País: abreviação com duas letras

Clique em **Avançar**.

> **NOTA:**
> **Por padrão, o certificado expira em um ano.**

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

12 Na caixa de diálogo *Configuração de instalação do servidor de front-end*, você pode ver ou editar os nomes de host e as portas.

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

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

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

Quando concluído, clique em **OK**.

- Para ver ou editar as portas, na caixa de diálogo *Configuração do servidor de front-end* clique em **Edit Editar portas externas** ou **Editar portas de conexão internas**. Edite as portas apenas se necessário. A Dell recomenda usar as configurações padrão.

Se você desmarcar um proxy na caixa de diálogo *Editar nomes de host do front-end*, sua porta não será mostrada nas caixas de diálogo Portas externas ou Portas internas.

Quando concluído, clique em **OK**.

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

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

VE Terminal - Tarefas de configurações básicas

As tarefas de configuração básica são acessadas pelo menu principal.

Alterar nome de host

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu *Configuração básica*, selecione **Nome de host**.

2 Use a tecla Backspace para remover o nome de host existente do DDP Enterprise Server - VE e substitua-o por um novo nome; em seguida, selecione **OK**.

Alterar configurações de rede

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu *Configuração básica*, selecione **Configurações de rede**.

2 Na tela *Definir configurações da rede*, selecione qualquer uma das opções abaixo e selecione **OK**.

- (Padrão) Usar o DHCP.
- (Recomendado) No campo Usar DHCP, pressione a barra de espaço para remover o X e digite esses endereços manualmente, conforme necessário:

  IP estático

  Máscara de rede

  Gateway padrão

  Servidor DNS 1

  Servidor DNS 2

  Servidor DNS 3

  NOTA: Ao usar um IP estático, você precisa criar uma entrada de host no servidor DNS.

Definir nome de host do DMZ

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu *Configuração básica*, selecione **Nome de host do DMZ**.

2 Informe o nome de domínio totalmente qualificado do servidor DMZ e selecione **OK**.

NOTA: Para usar o Modo proxy (Modo DMZ), você precisará Instalar e configurar o modo proxy.

Alterar o fuso horário

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu *Configuração básica*, selecione **Fuso horário**.
2 Na tela *Fuso horário*, use as teclas de seta para selecionar o fuso horário e, em seguida, selecione **Entrar**.
3 No prompt de confirmação do fuso horário, selecione **OK**.

Atualizar o DDP Enterprise Server - VE

Para obter mais informações sobre uma atualização específica, consulte os avisos técnicos do VE, localizados no site de suporte da Dell em http://www.dell.com/support. Para ver a versão e a data de instalação de uma atualização que já foi aplicada, no menu **Configuração básica**, selecione **Atualizar o DDP Enterprise Server - VE** > **Última atualização bem-sucedida aplicada**.

Para receber notificações por e-mail quando atualizações do VE forem disponibilizadas, consulte Definir as configurações de SMTP.

NOTA: No modo padrão, uma atualização deverá ser realizada depois da instalação inicial do DDP Enterprise Server - VE e antes que clientes sejam ativados.

Se forem realizadas alterações na política, mas não confirmadas no Remote Management Console, aplique as alterações de política antes de atualizar o VE:

1 Como um administrador Dell, faça login no Remote Management Console.
2 No menu à esquerda, clique em **Gerenciamento** > **Confirmar**.
3 Digite uma descrição da alteração no campo Comentário.
4 Clique em **Confirmar políticas**.
5 Quando a confirmação for concluída, faça logoff do Remote Management Console.

Atualizar VE (Modo padrão)

1 A Dell recomenda a execução de um backup regular. Antes de atualizar, certifique-se de que o processo de backup esteve funcionando corretamente. Consulte Backup e restauração.
2 No menu **Configuração básica**, selecione **Atualizar o DDP Enterprise Server - VE**.
3 Selecione a ação desejada:
   - Definir servidor de atualização - Selecione essa opção para definir ou alterar o local do servidor dos pacotes de atualização do DDP Enterprise Server - VE. Na tela *Definir servidor de atualização*, use a tecla Backspace para remover o nome de host do servidor ou o endereço IP existente. Informe o nome do domínio totalmente qualificado ou o endereço IP e selecione **OK**.

     O servidor de atualização padrão é **act.credant.com**.
   - Definir as configurações de proxy – Selecione esta opção para definir as configurações de proxy para as atualizações sendo baixadas.

     Na tela *Definir as configurações de proxy*, pressione a barra de espaço para inserir um **X** no campo Usar proxy. Insira os endereços de Proxy do HTTPS, HTTP e FTP. Se for necessária a autenticação do firewall, pressione a barra de espaço para inserir um **X** no campo Autenticação necessária. Insira o nome de usuário e a senha e clique em **OK**.

     NOTA: Para atualizar a partir do site FTP, informe o nome de usuário e a senha do FTP, seguido pelo URL.
   - Verificar se há atualização - Selecione essa opção para verificar no Servidor de atualização se há um pacote de atualização do DDP Enterprise Server - VE.
   - Fazer download da atualização – Selecione essa opção para fazer download da atualização depois de verificar a existência de uma nova atualização por meio da opção Verificar se há atualização.

- Aplicar atualização - Selecione essa opção se você desejar aplicar um pacote de atualização do DDP Enterprise Server - VE baixado. Na tela *Selecionar um arquivo de atualização (.deb)*, selecione o pacote de atualização que deseja instalar e pressione **Entrar**.
- Última atualização bem-sucedida aplicada – Selecione essa opção para visualizar a versão e a data de instalação da versão atual do VE.

Atualizar VE (Modo desconectado)

1 A Dell recomenda a execução de um backup regular. Antes de atualizar, certifique-se de que o processo de backup esteve funcionando corretamente. Consulte Backup e restauração.

2 No site de suporte da Dell, obtenha o arquivo .deb que contém a atualização mais recente do VE.

Os downloads do VE estão localizados na pasta **Drivers e downloads** em:

www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

ou

www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

ou

www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

ou

www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

3 Armazene o arquivo .deb na pasta /updates no servidor FTP seguro do VE.

Certifique-se de que o cliente FTP ofereça suporte para o SFTP na porta 22 e que um usuário FTP esteja configurado. Consulte Configurar usuários de FTP.

4 No menu **Configuração básica**, selecione **Atualizar o DDP Enterprise Server - VE**.

5 Selecione **Aplicar atualização** e pressione a tecla **Enter**.

Se o arquivo .deb não for exibido, verifique se esse arquivo está armazenado no local correto.

6 Selecione o arquivo de atualização .deb que você deseja instalar e pressione a tecla **Enter**.

Alterar senhas de usuário

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

Você pode alterar senhas para esses usuários:

- ddpuser (Administrador de terminal do DDP Enterprise Server - VE) – Este usuário tem acesso ao VE Terminal e seus menus.
- ddpconsole (acesso ao shell do DDP Enterprise Server - VE) – Este usuário tem acesso ao shell do VE. O acesso ao shell está disponível para um administrador de rede a fim de verificar e solucionar problemas de conectividade de rede.
- ddpsupport (Administrador do Dell ProSupport) – Este usuário existe apenas para uso do Dell ProSupport. Para fins de segurança, você controla a senha para esta conta.

1 No menu *Configuração básica*, selecione **Alterar senhas de usuário**.

2 Na tela *Alterar senhas de usuário*, selecione a senha de usuário que será alterada e selecione **Entrar**.

3 Na tela *Definir senha*, insira a senha atual, insira a nova senha, insira a nova senha de novo e selecione **OK**.

As senhas precisam conter o seguinte:

- Pelo menos 8 caracteres
- Pelo menos 1 letra maiúscula

- Pelo menos 1 número
- Pelo menos 1 caractere especial

Configurar usuários de File Transfer (FTP)

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

Você pode conceder acesso a até três usuários ao servidor FTP seguro do DDP Enterprise Server - VE para tarefas de backup e restauração. O servidor FTP VE seguro também pode ser usado para armazenar ou carregar atualizações no DDP Enterprise Server - VE.

1 No menu *Configuração básica*, selecione **Usuários do File Transfer (FTP)**.
2 Na tela *Configurar usuários FTP*, para ativar um usuário FTP, pressione a barra de espaço para inserir um **X** no campo Status do usuário. Para desativar um usuário FTP, pressione a barra de espaço para remover o **X** no campo Status do usuário.
3 Informe um nome de usuário e uma senha para o usuário SFTP.
   As senhas precisam conter o seguinte:
   - Pelo menos 8 caracteres
   - Pelo menos 1 letra maiúscula
   - Pelo menos 1 número
   - Pelo menos 1 caractere especial
4 Quando terminar de inserir os usuários SFTP, selecione **OK**.

Habilitar o SSH

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

Você pode ativar o SSH para o login do Administrador de suporte, acesso ao shell do DDP Enterprise Server - VE e a interface de linha de comando do VE Terminal.

1 No menu *Configuração básica*, selecione **Configurações do SSH**.
2 Selecione o usuário para o qual deseja habilitar o SSH, pressione a barra de espaço para inserir um **X** no seu campo e selecione **OK**.

Iniciar ou parar serviços de VE

Execute esta tarefa somente se for necessário. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 Para iniciar ou parar simultaneamente todos os serviços de VE, no menu *Configuração básica*, selecione **Iniciar aplicativo** ou **Parar aplicativo**.
2 Na janela de confirmação, selecione Sim.

NOTA: As alterações no estado do servidor poderão levar até dois minutos para serem concluídas.

Reinicializar o VE

Execute esta tarefa somente se for necessário.

1 No menu *Configuração básica*, selecione **Reinicializar o dispositivo**.
2 Na janela de confirmação, selecione Sim.

3 Depois de reiniciar, faça login no DDP Enterprise Server - VE.

Encerrar o VE

Execute esta tarefa somente se for necessário.

1 No menu *Configuração básica*, desça e selecione **Encerrar dispositivo**.
2 Na janela de confirmação, selecione Sim.
3 Depois de reiniciar, faça login no DDP Enterprise Server - VE.

VE Terminal - Tarefas de configurações avançadas

As tarefas de configuração avançadas são acessadas no menu principal.

Definir ou alterar a senha de banco de dados

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu *Configuração avançada*, selecione **Senha de banco de dados**.
2 Informe a senha de acesso ao banco de dados e selecione **OK**.
As senhas precisam conter o seguinte:

- Pelo menos 8 caracteres
- Pelo menos 1 letra maiúscula
- Pelo menos 1 número
- Pelo menos 1 caractere especial

NOTA: A Dell recomenda que você faça backup das senhas depois de concluir a instalação.

Definir as configurações do SMTP

Para receber as notificações por email do DDP Enterprise Server - VE **ou** usar o Data Guardian, siga as etapas nesta seção para definir as configurações de SMTP. As notificações por email do DDP Enterprise Server - VE informam os destinatários dos estados de erro de status do servidor do DDP Enterprise Server - VE, atualizações de senhas, disponibilidade de atualizações do DDP Enterprise Server - VE e problemas com licenças de cliente.

É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

Para definir as configurações de SMTP, siga as seguintes etapas:

1 No menu *Configuração avançada*, selecione **Notificações por email**.
2 Na tela Configurar notificações por email, para ativar os alertas de e-mail, pressione a barra de espaço para inserir um *X* no campo Ativar alertas de e-mail.
3 Insira o nome do domínio totalmente qualificado do SMTP Server.
4 Informe a porta SMTP.
5 No campo Usuário de origem, insira o ID de conta de e-mail que enviará notificações por e-mail.
6 No campo Inserir usuário, insira um ID de conta de e-mail para acesso de alteração de notificações de e-mail configurado.
7 No campo Senha, insira uma senha para acesso de alteração de notificações de e-mail configurado.
8 Nos campos de IDs de e-mail, para o status do VE, as atualizações de senha e disponibilidade de atualizações, informe as listas de destinatários para cada tipo de notificação. Siga essas convenções ao listar os destinatários:

- O formato do endereço de e-mail é destinatário@dell.com.
- Os destinatários são separados por vírgula ou ponto-e-vírgula.

9 No campo de lembrete de Alerta de serviço, para ativar os lembretes, pressione a barra de espaço para inserir um **X** no campo e defina o intervalo do lembrete, em minutos. Um lembrete de Alerta de serviço será acionado quando o intervalo do lembrete passar após uma notificação ser enviada sobre um problema de saúde do sistema e o host ou o serviço permanecer no mesmo estado.

10 No campo Relatório de resumo, para ativar os relatórios ou notificações, selecione o intervalo desejado (diário, semanal ou mensal) e, em seguida, pressione a barra de espaço para inserir um **X** no campo.

11 Selecione **OK**.

Importar um certificado existente ou inscrever um novo certificado de servidor

Os certificados precisam ser instalados antes de ativar os usuários no DDP Enterprise Server - VE.

Você pode importar um certificado existente ou criar uma solicitação de certificado por meio do DDP Enterprise Server - VE.

É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

Importar um certificado de servidor existente

1 Exporte o certificado existente e sua cadeia completa de confiança do armazenamento de chaves.

> **NOTA: Mantenha a senha de exportação, pois você irá usá-la ao importar o certificado para o DDP Enterprise Server - VE.**

2 No servidor de FTP do DDP Enterprise Server - VE, armazene o certificado em **/opt/dell/vsftpd/files/certificates**.

3 No menu *Configuração avançada* do DDP Enterprise Server - VE, selecione **Certificados de servidor**.

4 Selecione **Importar certificado existente**.

5 Selecione um arquivo de certificado para ser instalado no DDP Enterprise Server - VE.

6 Quando solicitado, informe a senha de exportação do certificado e selecione **OK**.

7 Quando a importação estiver concluída, selecione **OK**.

Inscrever um novo certificado de servidor

1 No menu *Configuração avançada*, selecione **Certificados do servidor**.

2 Selecione **Novo certificado de servidor**.

3 Selecione **Criar solicitação de certificado**.

4 Preencha os campos na tela *Gerar solicitação de certificado*:

- Nome do país: código de duas letras de país.
- *Estado/província*: digite o nome do estado ou da província sem abreviação (por exemplo, Texas).
- *Nome do local/cidade.* Digite o valor adequado (por exemplo, Dallas).
- *Organização*: digite o valor apropriado (por exemplo, Dell).
- *Unidade organizacional*: digite o valor apropriado (por exemplo, Segurança).
- *Nome comum*: especifique o nome de domínio totalmente qualificado do servidor no qual o DDP Enterprise Server - VE está instalado. Este nome totalmente qualificado inclui o nome do host e o nome do domínio (por exemplo: domínio.com).
- *ID de e-mail*: informe o endereço de e-mail para o qual a sua CSR será enviada.

5 Siga o processo da sua organização para adquirir um certificado de servidor SSL de uma Autoridade de Certificado. Envie o conteúdo do arquivo da CSR para assinatura.

6 Ao receber o certificado assinado, exporte-o como um arquivo .p7b e baixe a cadeia completa de confiança no formato .der.

7 Faça cópias de backup do certificado e da cadeia de confiança.

8 Carregue o arquivo do certificado e sua cadeia completa de confiança no servidor FTP seguro do DDP Enterprise Server - VE.

9 No menu *Configuração avançada*, selecione **Certificados do servidor**.

10 Selecione **Novo certificado de servidor**.

11 Selecione `Concluir inscrição de certificado`.

12 Selecione o arquivo de certificado para ser instalado no DDP Enterprise Server - VE.

13 Se solicitado, digite a senha do certificado: **changeit**.

Para ativar a validação de confiança nos clientes do Encryption baseado no Windows, consulte Ativar a verificação de cadeia de confiança do gerenciador.

Criar e instalar um certificado autoassinado

1 No menu *Configuração avançada* do DDP Enterprise Server - VE, selecione **Certificados de servidor**.

2 Selecione **Criar e instalar um certificado autoassinado.**

3 Para confirmar que você quer substituir o certificado pré-instalado por um novo certificado, clique em **Sim**.

4 Digite a senha do certificado: **changeit**.

5 Após o novo certificado ser instalado, selecione **OK** e espere que os serviços sejam reiniciados.

Os serviços do VE são reiniciados automaticamente.

Configurar a rotação de log

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

A rotação de log diária é ativada por padrão. Para alterar a rotação de log padrão, no menu *Configuração avançada*, selecione **Configuração de rotação de log**.

Para desativar a rotação de log, use a barra de espaço para inserir um **X** no campo Sem rotação e selecione **OK**.

Para ativar a rotação de log, siga essas etapas:

1 Para ativar a rotação diária, semanal ou mensal, use a barra de espaço para inserir um **X** no campo adequado. Para rotação semanal ou mensal, informe o dia adequado da semana ou do mês em formato de numeral, onde segunda-feira=1.

2 Informe um horário para a rotação no campo Horário da rotação de log.

3 Selecione **OK**.

Backup e restauração

Os backups podem ser configurados ou executados a qualquer momento e não são necessários para começar a usar o DDP Enterprise Server - VE. A Dell recomenda que você configure um processo de backup regular.

Os backups podem ser armazenados em um servidor FTP seguro externo (recomendado) ou no DDP Enterprise Server - VE. Se forem armazenados no servidor VE, ao atingir 90% da capacidade do disco, nenhum backup novo será armazenado. Você receberá uma notificação por email informando que há pouco espaço de alocação em disco.

NOTA:
Para preservar o espaço em partição no disco e evitar o apagamento automático dos backups, remova os backups desnecessários do DDP Enterprise Server - VE.

Por padrão, os backups são executados diariamente. A Dell recomenda armazenar backups em um servidor FTP seguro externo em uma frequência que atenda às exigências da organização quanto aos backups e ao uso apropriado do espaço de armazenamento.

Para configurar uma programação de backup, no menu *Configuração avançada*, selecione **Backup e restauração > Configuração** e siga essas etapas:

1 Para ativar backups diários, semanais ou mensais, use a barra de espaço para inserir um **X** no campo adequado. Para ativar os backups semanalmente ou mensalmente, informe o dia adequado da semana ou o mês em formato de numeral, onde segunda=1. Para desativar os backups, use a barra de espaço para inserir um **X** no campo Sem backup e selecione **OK**.

2 Informe um horário para o backup no campo Horário do backup.

3 Selecione **OK**.

Para executar um backup imediato, no menu *Configuração avançada*, selecione **Backup e restauração > Fazer backup agora**. Quando a confirmação de backup for mostrada, selecione **OK**.

NOTA:
Antes de iniciar uma operação de Restauração, todos os serviços dos servidores do VE precisam estar em execução. **Verificar o status do servidor**. Se nem todos os serviços estiverem em execução, reinicie os serviços. Para obter mais informações, consulte **Iniciar ou parar os serviços VE**. Comece a restaurar ***apenas*** quando ***todos*** os serviços estiverem em execução.

Para fazer a restauração a partir de um backup, no menu *Configuração avançada*, selecione **Backup e restauração > Restaurar** e selecione o arquivo de backup a ser restaurado. Na tela de confirmação, selecione **Sim**.

O VE é reinicializado e o backup é restaurado.

Armazenar os backups em um servidor FTP seguro

Para armazenar os backups em um servidor FTP, o cliente FTP precisa suportar o SFTP na porta 22.

De acordo com os requisitos de backup da organização, os backups podem ser baixados das seguintes maneiras:

- Manualmente
- Através de script automatizado
- Através da solução de backup aprovada da organização

Para fazer download de backups usando a solução de backup da organização, obtenha instruções detalhadas por parte do seu fornecedor de soluções de backup.

NOTA:
A Virtual Edition é baseada no Linux Debian Ubuntu x64.

Faça login no VE como ddpsupport e use o comando sudo para configurar a solução de backup:

`sudo` <instruções do fornecedor de soluções de backup>

Faça backup dos conteúdos das seguintes pastas:

/opt/dell/vsftpd/files/backup (necessário)

/opt/dell/vsftpd/files/certificates (altamente recomendável)

/opt/dell/vsftpd/files/support (opcional)

Quando o processo sudo for concluído, digite **exit** (sair) e pressione **Enter** até o prompt de login ser exibido.

Ativar o acesso remoto ao banco de dados

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

NOTA: A Dell recomenda que você ative o acesso remoto ao banco de dados somente se necessário.

1 No menu *Configuração avançada*, selecione **Acesso remoto ao banco de dados**.
2 Use a barra de espaço para inserir um **X** no campo Ativar acesso remoto ao banco de dados e selecione **OK**. Se a senha do banco de dados ainda não tiver sido configurada, um prompt para essa senha será exibido.
3 Digite a senha de banco de dados.
4 Redigite a senha de banco de dados.

Os componentes de aplicativos de DDP se encerram automaticamente.

Ativar suporte do servidor DMZ

Essa tarefa pode ser executada a qualquer momento. Não é obrigatório começar usando o DDP Enterprise Server - VE. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu *Configuração avançada*, selecione **Ativar suporte do servidor DMZ**.
2 Use a barra de espaço para inserir um **X** no campo Ativar suporte do servidor DMZ e selecione **OK**.

NOTA: Para usar o Modo proxy (Modo DMZ), você precisará Instalar e configurar o modo proxy.

DDP Enterprise Server - Tarefas de administrador do VE

Definir ou alterar idioma do DDP Enterprise Server - VE Terminal

É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações

1 No menu principal, selecione **Definir idioma**.
2 Use as teclas de seta para selecionar o idioma preferencial.

Verificar o status do servidor

Para verificar o status dos serviços do DDP Enterprise Server - VE, no menu principal, selecione **Status do servidor**.

A tabela a seguir descreve cada Serviço e sua função.

Nome	Descrição
Dell Message Broker	Enterprise Server Bus
Dell Identity Server	Processa as solicitações de autenticação de domínio.
Dell Compatibility Server	Um serviço para gerenciar a arquitetura corporativa.
Dell Security Server	Fornece o mecanismo para controlar comandos e a comunicação com o Active Directory. Usado para a comunicação com o Dell Policy Proxy.
Dell Compliance Reporter	Fornece uma visão completa do ambiente para auditoria e geração de relatórios de conformidade.
Dell Core Server	Um serviço para gerenciar a arquitetura corporativa.
Dell Core Server HA (Alta disponibilidade)	Um serviço de alta disponibilidade que permite uma maior segurança e desempenho das conexões de HTTPS ao se gerenciar a arquitetura corporativa.
Dell Inventory Server	Processa a fila de inventário.
Dell Forensic Server	Oferece serviços web para a API forense.
Dell Policy Proxy	Fornece um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário.

O DDP Enterprise Server - VE monitora e reinicia seus serviços, se necessário.

NOTA: Se o processo do personalizador de banco de dados falhar, os servidores passarão para o estado Falha na execução. Para verificar o log do personalizador de banco de dados, no menu principal, selecione Ver logs.

Ver logs

Para verificar os seguintes logs, no menu principal, selecione **Ver logs**.

Log Syslog Log de e-mail Log de autenticação)SSH) Log Postgres Log de monitoramento

- Logs do sistema

  Log do Syslog

  Log de e-mail

  Log de autenticação do (SSH)

  Log do Postgres

  Log de monitoramento
- Logs de servidor

  Compatibility Server

  Security Server

  Message Broker

  Core Server

  Core Server HA

  Compliance Reporter

  Identity Server

  Inventory Server

  Forensic Server

  Policy Proxy
- Log do personalizador de banco de dados

Abrir a interface de linha de comando

Para abrir a interface de linha de comando, no menu principal, selecione **Iniciar shell**.

Para sair da interface de linha de comando, digite **exit** e pressione **Enter**.

Gerar um log de instantâneos do sistema

Para gerar um log de instantâneo do sistema para o Dell ProSupport, no menu principal, selecione **Ferramentas de suporte**.

1 No menu *Ferramentas de suporte*, selecione **Gerar log de instantâneo de sistema**.
2 Na indicação que o arquivo é criada, selecione **OK**.

Se o usuário ddpsupport estiver ativado, o Dell Pro Support poderá recuperar o log do servidor SFTP do DDP Enterprise Server - VE. Se o usuário ddpsupport não estiver ativado, entre em contato com o Dell ProSupport. Para obter mais informações, consulte Entrar em contato com o Dell ProSupport.

4

Manutenção do DDP Enterprise Server - VE

Você precisa remover backups desnecessários do DDP Enterprise Server - VE.

Somente os dez backups mais recentes são retidos. Se o espaço disponível na partição do disco estiver em dez por cento ou menos, não será armazenado mais nenhum backup. Se essa condição ocorrer, você receberá uma notificação por e-mail informando que há pouco espaço de alocação em disco.

5

Solução de problemas do DDP Enterprise Server - VE

Se ocorrer um erro e você tiver configurado as notificações de e-mail, você receberá uma notificação por e-mail. Com base nas informações fornecidas pela notificação por e-mail, siga essas etapas:

1 Verifique os arquivos de log aplicáveis.
2 Reinicie os serviços, conforme necessário. É uma boa prática reiniciar os serviços sempre que for realizada uma alteração nas configurações
3 Gerar um log de instantâneos do sistema.
4 Entre em contato com o Dell ProSupport. Para obter mais informações, consulte Entrar em contato com o Dell ProSupport.

6

Tarefas de configuração pós-instalação

Após a instalação, alguns componentes do seu ambiente poderão precisar ser configurados com base na solução Dell Data Protection usada pela sua organização.

Configurar o VE para o Data Guardian

Para configurar o VE para suportar o Data Guardian, no VE Remote Management Console, configure a política Criptografia da nuvem como Ativada. Para ativar o modo Documentos protegidos do Office do Data Guardian, configure a política Documentos protegidos do Office como Ativada.

Para obter instruções sobre como instalar o cliente do Data Guardian, consulte o *Guia de instalação avançada do Enterprise Edition*, o *Guia de instalação básica do Enterprise Edition* ou o *Guia do usuárioData Guardian*.

Instalar e configurar o Gerenciamento do EAS para o Mobile Edition

Para usar o Mobile Edition, é necessário instalar e configurar o Gerenciamento do EAS. Se você não pretende usar o Mobile Edition, ignore esta seção.

Pré-requisitos

- A conta de login do Serviço do Gerenciador de caixas de correio do EAS precisa ser uma conta com permissões para criar/modificar a política do Exchange ActiveSync, atribuir políticas às caixas postais dos usuários e consultar informações sobre os dispositivos do ActiveSync.
- O Utilitário de configuração de EAS deve ser executado com permissões de administrador para modificar arquivos e reiniciar os serviços.
- É necessária conexão de rede com o DDP Enterprise Server - VE.
- Tenha o nome de host ou o endereço IP do DDP Enterprise Server - VE disponível.
- O Microsoft Message Queuing (MSMQ) deve estar instalado/configurado no servidor que hospeda o ambiente do Exchange. Caso não esteja, instale o MSMQ 4.0 no Windows Server 2008 ou Windows Server 2008 R2 (no servidor que hospeda o ambiente) – http://msdn.microsoft.com/en-us/library/aa967729.aspx

Durante o processo de implantação

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

Instale o Gerenciador de dispositivos do EAS

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

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

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

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

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

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

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

Uma janela de status mostra o andamento da instalação.

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

Instalar o Gerenciador de caixas de correio do EAS

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

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

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

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

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

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

7 Na tela *Informações de login*, informe as credenciais da conta do usuário que fará login para usar este serviço.

Nome de usuário: DOMÍNIO\Nome de usuário

Senha: a senha associada ao nome de usuário

Clique em **Avançar**.

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

Uma janela de status mostra o andamento da instalação.

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

Usar o Utilitário de configuração de EAS

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

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

3 Insira as seguintes informações:

Nome de host do DDP Enterprise Server - VE

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

Marque a caixa para executar o Gerenciador de dispositivos do EAS no modo somente reportar (recomendado durante a implantação).

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

Clique em **OK**.

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

5 Clique em **Sair** quando terminar.

Após o processo de implementação

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

Nos seus servidores de caixas de correio do Exchange

1 Acesse **Iniciar** > **Dell** > **Utilitário de configuração de EAS** > **Configuração do EAS** para executar o Utilitário de configuração de EAS.

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

3 Insira as seguintes informações:

Nome de host do DDP Enterprise Server - VE

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

Desmarque a caixa para executar o Gerenciador de dispositivos do EAS no modo Somente reportar

Clique em **OK**.

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

5 Clique em **Sair** quando terminar.

Ativar verificação de cadeia de confiança do gerenciador

Se um certificado autoassinado for usado no VE Server para SED ou BitLocker Manager, a validação de confiança de SSL/TLS precisa permanecer ***desativada*** no computador cliente. Antes de ativar a validação de confiança de SSL/TLS no computador cliente, os seguintes requisitos precisam ser atendidos:

- Um certificado assinado por uma autoridade raiz (por exemplo, Entrust ou Verisign) precisa ser importado para o servidor do VE. Consulte Importar um certificado existente ou inscrever um novo certificado de servidor.
- A cadeia completa de confiança do certificado precisa ser armazenada no Microsoft keystore no computador do cliente.

Para ativar a validação de confiança de SSL/TLS no computador cliente, altere o valor da seguinte entrada no registro para 0:

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):0

7

Tarefas do administrador do VE Remote Management Console

Atribuir Função de Dell Administrator

1 Como um Dell Administrator, faça login no Remote Management Console neste endereço: https://server.domain.com:8443/webui/. As credenciais padrão são **superadmin/changeit**.

2 No painel à esquerda, clique em **Populações** > **Domínios**.

3 Clique em um domínio em que você deseja adicionar um usuário.

4 Na página Detalhes de domínios, clique na guia **Membros**.

5 Clique em **Adicionar usuário**.

6 Insira um filtro para pesquisar o nome de usuário por Nome comum, Nome principal universal ou sAMAccountName. O caractere curinga é *.

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

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

7 Selecione os usuários na *Lista de Usuários do Diretório* para adicionar ao Domínio. Use <Shift><clique> ou <Ctrl><clique> para selecionar múltiplos usuários.

8 Clique em **Adicionar**.

9 A partir da barra de menu, clique na guia **Detalhe e Ações** do usuário específico.

10 Role pela barra de menu e selecione a guia **Admin**.

11 Selecione as funções de administrador que serão adicionadas a este usuário.

12 Clique em **Salvar**.

Fazer login com a Função de Dell Administrator

1 Faça logout do Remote Management ConsoleEnterprise Server.

2 Faça login no Remote Management ConsoleEnterprise Server e faça login com as credenciais de usuário de domínio.

Clique em "?" no canto superior do Remote Management Console para iniciar a *AdminHelp do Dell Data Protection.* A página *Introdução* é mostrada. Clique em **Adicionar domínio**.

As políticas de linha de base foram definidas para a sua organização, mas estas podem precisar ser modificadas de acordo com as suas necessidades específicas, da seguinte maneira (o licenciamento e os direitos guiam todas as ativações):

- Computadores Windows serão criptografados
- Computadores com unidades de criptografia automática serão criptografados
- Computadores Windows com Hardware Crypto Accelerators serão criptografados
- O BitLocker Management não é ativado
- O Advanced Threat Protection não é ativado
- O Threat Protection é ativado
- A mídia externa não será criptografada

- Os dispositivos conectados às portas não serão criptografados
- O Data Guardian é ativado
- O Mobile Edition não é ativado

Veja o tópico *Gerenciar políticas* da AdminHelp para navegar para os grupos de tecnologia e obter as descrições das políticas.

Confirmar políticas

Confirme as políticas quando a instalação for concluída.

Para confirmar as políticas após a instalação ou após as modificações nas políticas forem salvas, siga as seguintes instruções:

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

8

Portas de solução

A tabela a seguir descreve cada componente e sua função.

Nome	Porta padrão	Descrição	Necessário para
Compliance Reporter	HTTP(S)/8084	Fornece uma visão completa do ambiente para auditoria e geração de relatórios de conformidade. Um componente do DDP Enterprise Server - VE.	Geração de relatórios
Remote Management Console	HTTPS/8443	A central de controles e o console de administração da implantação de toda a empresa. Um componente do DDP Enterprise Server - VE.	Todos
Core Server	HTTPS/8888	Gerencia o fluxo de política, as licenças, o registro para Preboot Authentication, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection. Processa os dados de inventário para uso pelo Compliance Reporter e pelo Remote Management Console. Coleta e armazena os dados de autenticação. Controla o acesso baseado em função. Um componente do DDP Enterprise Server - VE.	Todos
Core Server HA (Alta disponibilidade)	HTTPS/8888	Um serviço de alta disponibilidade que permite maior segurança e desempenho das conexões HTTPS com o Remote Management Console, Preboot Authentication, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection. Um componente do DDP Enterprise Server - VE.	Todos
Security Server	HTTPS/8443	Comunica-se com o Policy Proxy; gerencia as recuperações de chaves forense, ativações de clientes, produtos Data Guardian e comunicação SED-PBA. Um componente do DDP Enterprise Server - VE.	Todos
Compatibility Server	TCP/1099 (fechada)	Um serviço para gerenciar a arquitetura corporativa. Coleta e armazena os dados iniciais de inventário durante a ativação e os dados de política durante as migrações. Processa os dados baseados em grupos de usuário neste serviço. Um componente do DDP Enterprise Server - VE.	Todos
Message Broker Service	TCP/61616	Processa a comunicação entre os serviços do DDP Enterprise Server - VE. Armazena as informações de políticas criadas pelo	Todos

Nome	Porta padrão	Descrição	Necessário para
	e STOMP/61613 (fechada ou, caso configurado para DMZ, 61613 aberta)	Compatibility Server para o enfileiramento do Policy Proxy. Um componente do DDP Enterprise Server - VE.	
Identity Server	HTTPS/8445	Trata as solicitações de autenticação de domínio, incluindo autenticação do SED Manager. Exige uma conta do Active Directory. Um componente do DDP Enterprise Server - VE.	Todos
Forensic Server	HTTPS/8448	Permite aos administradores que têm privilégios adequados a obter chaves de criptografia a partir do Remote Management Console, para uso em bloqueios de dados e tarefas de descriptografia. Um componente do DDP Enterprise Server - VE.	API forense
Inventory Server	8887	Processa a fila de inventário. Um componente do DDP Enterprise Server - VE.	Todos
Policy Proxy	TCP/ 8000/8090	Fornece um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário. Um componente do DDP Enterprise Server - VE.	Enterprise Edition para Mac Enterprise Edition para Windows Mobile Edition
LDAP	389/636, 3268/3269 RPC - 135, 49125+	**Porta 3268** – Esta porta é usada para filas especificamente voltadas ao catálogo global. As solicitações de LDAP enviadas para a porta 3268 podem ser usadas para buscar objetos em toda a floresta. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, o departamento de um usuário poderia não ser devolvido usando a porta 3268 já que esse atributo não é replicado para o catálogo global. **Porta 389** – Esta porta é usada para solicitar informações a partir do controlador de domínio local. As solicitações de LDAP enviadas para a porta 389 podem ser usadas para buscar objetos apenas dentro do domínio doméstico do catálogo global. No entanto, o aplicativo de solicitação pode obter todos os atributos para esses objetos. Por exemplo, uma solicitação à porta 389 poderia ser usada para obter um departamento do usuário	Todos
Client Authentication	HTTPS/8449	Permite que os servidores clientes autentiquem com o DDP Enterprise Server - VE.	Criptografia do servidor
Sinalizador de retorno de chamada	HTTP/8446	Permite a inserção de um sinalizador de retorno de chamada em cada arquivo protegido do Office ao executar o modo Documentos protegidos do Office do Data Guardian.	Data Guardian

Nome	Porta padrão	Descrição	Necessário para
Prevenção avançada contra ameaças	HTTPS/TCP/443	Comunicação do cliente se estiver utilizando o Advanced Threat Prevention	Prevenção avançada contra ameaças
EAS Device Manager	N/A	Ativa a funcionalidade sem fio. Instalado no Servidor de Acesso do Cliente Exchange.	Gerenciamento do Exchange ActiveSync de dispositivos móveis.
Gerenciador de caixas de correio do EAS	N/A	O agente de correio instalado no Servidor de caixa de correio do Exchange.	Gerenciamento do Exchange ActiveSync de dispositivos móveis.

Sincronização de horário NTP: TCP e UDP/123 (para obter mais informações, consulte https://help.ubuntu.com/lts/serverguide/NTP.html.)