DDP Enterprise Server - Virtual Edition

Quick Start Guide and Installation Guide v9.6

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

VE Quick Start Guide and Installation Guide

2017 - 02

Rev. A01

Contents

Virtual Edition Quick Start Guide

This Quick Start Guide is for more experienced users, to get DDP Enterprise Server - VE up and running fast. As a general rule, Dell recommends installing the DDP Enterprise Server - VE first, followed by installation of clients.

For more detailed instructions, see the Virtual Edition Installation Guide.

For information about VE prerequisites, see DDP Enterprise Server - VE Prerequisites, VE Remote Management Console Prerequisites, and Proxy Mode Prerequisites.

For information on how to update an existing DDP Enterprise Server - VE, see Update DDP Enterprise Server - VE.

Install DDP Enterprise Server - VE

1 Browse to the directory where the Dell Data Protection files are stored and double-click to import into VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**.
2 Power on DDP Enterprise Server - VE.
3 Follow the on-screen instructions.

Configure VE

Before you activate users, you must complete the following Configuration tasks at the DDP Enterprise Server - VE Terminal:

- Set or Change the Database Password
- Configure SMTP Settings
- Import an Existing Certificate or Enroll a New Server Certificate
- Update DDP Enterprise Server - VE
- Install an FTP client that supports SFTP on port 22, and Set up File Transfer (FTP) Users.

  If your organization has external facing devices, see Install and Configure Proxy Mode.

> **NOTE: If your Enterprise Edition clients will be entitled from the factory or you purchase licenses from the factory, set the GPO on the domain controller to enable entitlements (this may not be the same server running Virtual Edition). Ensure that outbound port 443 is available to communicate with the Server. If port 443 is blocked (for any reason), the entitlement functionality will not work.**

Open VE Remote Management Console

Open the VE Remote Management Console at this address:

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

The default credentials are **superadmin/changeit**.

For a list of supported web browsers, see VE Remote Management Console Prerequisites.

Administrative Tasks

If you have not launched the VE Remote Management Console, do so now. The default credentials are **superadmin/changeit**.

Dell recommends that you assign administrator roles as soon as it is convenient. To complete this task now, see Assign Dell Administrator Role.

Click "?" in the upper right corner of the VE Remote Management Console to launch *Dell Data Protection AdminHelp*. The *Get Started* page displays. Click **Add Domains**.

Baseline polices have been set for your organization but may need to be modified depending on your specific needs, as follows (licensing and entitlements guide all activations):

- Windows computers will be encrypted
- Computers with self-encrypting drives will be encrypted
- BitLocker Management is not enabled
- Advanced Threat Protection is not enabled
- Threat Protection is enabled
- External media will not be encrypted
- Devices connected to ports will not be encrypted
- Secure Lifecycle is enabled
- Mobile Edition is not enabled

See the AdminHelp topic *Manage Policies* to navigate to Technology Groups and policy descriptions.

Quick Start tasks are complete.

Virtual Edition Installation Guide

This Installation Guide is for less experienced users, to install and configure DDP Enterprise Server - VE. As a general rule, Dell recommends installing the DDP Enterprise Server - VE first, followed by installation of clients.

For information on how to update an existing DDP Enterprise Server - VE, see Update DDP Enterprise Server - VE.

About DDP Enterprise Server - VE

The DDP Enterprise Server - VE is the security administration piece of Dell's solution. The VE Remote Management Console allows administrators to monitor the state of endpoints, policy enforcement, and protection across the enterprise. Proxy Mode provides a front-end DMZ Mode option for use with DDP Enterprise Server - VE.

DDP Enterprise Server - VE has the following features:

- Centralized management of up to 3,500 devices
- Role-based security policy creation and management
- Administrator-assisted device recovery
- Separation of administrative duties
- Automatic distribution of security policies
- Trusted paths for communication between components
- Unique encryption key generation and automatic secure key escrow
- Centralized compliance auditing and reporting
- Auto-generation of self-signed certificates

Contact Dell ProSupport

Call 877-459-7304, extension 4310039 for 24x7 phone support for your Dell Data Protection product.

Additionally, online support for Dell Data Protection products is available at dell.com/support. Online support includes drivers, manuals, technical advisories, FAQs, and emerging issues.

Be sure to help us quickly connect you to the right technical expert by having your Service Code available when you call.

For phone numbers outside of the United States, check Dell ProSupport International Phone Numbers.

Requirements

DDP Enterprise Server - VE Prerequisites

Hardware

The recommended disk space for DDP Enterprise Server - VE is 80 GB.

Virtualized Environment

DDP Enterprise Server - VE v9.6 has been validated with the following virtualized environments.

Virtualized Environments

- VMware Workstation 12.5
  - 64-bit CPU required
  - 4 GB RAM recommended
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 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/workstation-11/index.jsp for more information
- VMware Workstation 11
  - 64-bit CPU required
  - 4 GB RAM recommended
  - See http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 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/workstation-11/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
  - An Operating System is not required
  - 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 5.5
  - 64-bit x86 CPU required
  - Host computer with at least two cores
  - 8 GB RAM minimum recommended
  - An Operating System is not required
  - 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

VE Remote Management Console Prerequisites

Internet Browsers

NOTE:

Your browser must accept cookies.

The following table details supported Internet browsers.

Internet Browsers
• Internet Explorer 11.x or later • Mozilla Firefox 41.x or later • Google Chrome 46.x or later

Proxy Mode Prerequisites

Hardware

The following table details the *minimum* hardware requirements for Proxy Mode.

Processor

2 GHz Core 2 Duo or better

RAM

+-2 GB minimum dedicated RAM / 4 GB dedicated RAM recommended

Free Disk Space

+-1.5 GB free disk space (plus virtual paging space)

Network Card

10/100/1000 network interface card

Miscellaneous

TCP/IP installed and activated

Software

The following table details the software that must be in place before installing Proxy Mode.

Prerequisites
• **Windows Installer 4.0 or later** Windows Installer 4.0 or later must be installed on the server where the installation is taking place. • **Microsoft Visual C++ 2010 Redistributable Package** If not installed, the installer will install it for you. • **Microsoft .NET Framework Version 4.5** Microsoft has published security updates for .NET Framework Version 4.5

The following table details the software requirements for the Proxy Mode server.

NOTE:

Always disable UAC when using Windows Server 2008. After disabling UAC, the server must be rebooted for this change to take effect.

Registry location for Windows Servers: HKLM\SOFTWARE\Dell.

Operating System

- **Windows Server 2008 R2 SP0-SP1 64-bit**
  - Standard Edition
  - Enterprise Edition
- **Windows Server 2008 SP2 64-bit**
  - Standard Edition
  - Enterprise Edition
- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2016**
  - Standard Edition
  - Datacenter Edition

Download DDP Enterprise Server - VE

At initial installation, DDP Enterprise Server - VE is delivered as an OVA file, an Open Virtual Application used to deliver software that runs on a virtual machine. The DDP Enterprise Server - VE OVA file is available at www.dell.com/support, on the Product Support pages for the following Dell Data Protection products:

Dell Data Protection | Encryption

Dell Data Protection | Endpoint Security Suite

Dell Data Protection | Endpoint Security Suite Enterprise

Dell Data Protection | Secure Lifecycle

To download the OVA file:

1. Navigate to the Product Support page for Dell Data Protection | Encryption, Dell Data Protection | Endpoint Security Suite, Dell Data Protection | Endpoint Security Suite Enterprise, or Dell Data Protection | Secure Lifecycle.
2. Click **Drivers & downloads**.
3. Next to "View all available updates for <OS version>," click **Change OS**, and select one of the following: **VMware ESXi 6.0, VMware ESXi 5.5,** or **VMware ESXi 5.1**.
4. Under "View by:" select **Show All**.
5. Under Dell Data Protection, select **Download**.

Install DDP Enterprise Server - VE

Before you begin, ensure that all system and virtual environment Requirements are met.

1 Locate the Dell Data Protection files in the installation media and double-click to import into VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**.

2 Power on DDP Enterprise Server - VE.

3 Select the language for the license agreement, and select **Display EULA**.

4 Read the agreement, and select **Accept EULA**.

5 If an update is available, select **Accept**.

6 Select **Default Mode** or **Disconnected Mode**.

> **NOTE:**
> If you select **Disconnected Mode**, VE can never be changed to Default Mode.
>
> Disconnected mode isolates VE from the Internet and an unsecured LAN or other network. All updates must be performed manually. For more information about Disconnected Mode functionality and policies, refer to *AdminHelp*.

7 At the default password change prompt, select **Yes**.

8 In the *Set ddpuser Password* screen, enter the current (default) password, **ddpuser**, then enter a unique password, re-enter the unique password, and select **OK**.

Passwords must include the following:

- At least 8 characters
- At least 1 uppercase letter
- At least 1 digit
- At least 1 special character

9 In the *Configure Hostname* dialog, use the Backspace key to remove the default hostname. Enter a unique hostname and select **OK**.

10 In the *Configure Network Settings* dialog, choose either option below, then select **OK**.

- (Default) Use DHCP.
- (Recommended) In the Use DHCP field, press the Spacebar to remove the X and manually enter these addresses, as applicable: Static IP Network Mask Default Gateway DNS Server 1 DNS Server 2 DNS Server 3

> **NOTE: When using a static IP, you must also create a host entry in the DNS server.**

11 In the *Time Zone* screen, use the arrow keys to highlight your time zone and select **Enter**.

12 At the time zone confirmation prompt, select **OK**.

13 When the message displays to indicate that initial configuration is completed, select **OK**.

14 Set or Change the Database Password.

15 Configure SMTP Settings.

16 Import an Existing Certificate or Enroll a New Server Certificate.

17 Update DDP Enterprise Server - VE.

18 Install an FTP client that supports SFTP on port 22, and Set up File Transfer (FTP) Users.

DDP Enterprise Server - VE installation tasks are complete.

Open VE Remote Management Console

Open the VE Remote Management Console at this address:

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

The default credentials are **superadmin/changeit**.

For a list of supported web browsers, see VE Remote Management Console Prerequisites.

Install and Configure Proxy Mode

Proxy Mode provides a front-end (DMZ Mode) option for use with DDP Enterprise Server - VE. If you intend to deploy Dell components in the DMZ, ensure that they are properly protected against attacks.

NOTE: The Beacon Service is installed as part of this installation to support Secure Lifecycle callback beacon, which inserts a callback beacon into every file protected by Secure Lifecycle when running Protected Office mode. This allows communication between any device in any location and the Dell Front End Server. Ensure that necessary network security is configured before using the callback beacon. The Enable Callback Beacon policy is enabled by default.

To perform this installation, you will need the fully-qualified hostname of the DMZ server.

1 In the Dell installation media, navigate to the Dell Enterprise Server directory. **Unzip** (DO NOT copy/paste or drag/drop) Dell Enterprise Server-x64 to the root directory of the server where you are installing VE. ***Copying/pasting or dragging/dropping will produce errors and an unsuccessful installation.***

2 Double-click **setup.exe**.

3 In the *InstallShield Wizard* dialog, select the language for installation, then click **OK**.

4 If prerequisites are not already installed, a message displays to inform you of which prerequisites will be installed. Click **Install**.

5 In the *Welcome* dialog, click **Next**.

6 Read the license agreement, accept the terms, then click **Next**.

7 Enter the Product Key.

8 Select **Front End Install** and click **Next**.

9 To install the Front End Server to the default location of **C:\Program Files\Dell**, click **Next**. Otherwise, click **Change** to select a different location, then click **Next**.

10 You have a choice of digital certificate types to use. **It is highly recommended that you use a digital certificate from a trusted certificate authority.**

Select option "a" or "b" below:

a To use an existing certificate that was purchased from a CA authority, select **Import an existing certificate** and click **Next**.

Click **Browse** to enter the path to the certificate.

Enter the password associated with this certificate. The key store file must be .p12 or pfx.

Click **Next**.

NOTE:

To use this setting, the exported CA certificate being imported must have the full trust chain. If unsure, re-export the CA certificate and ensure that the following options are selected in the "Certificate Export Wizard":

- Personal Information Exchange - PKCS#12 (.PFX)
- Include all certificates in the certification path if possible
- Export all extended properties

b To create a self-signed certificate, select **Create a self signed certificate and import it to key store and click Next.**

At the *Create Self-Signed Certificate* dialog, enter the following information:

Fully qualified computer name (example: computername.domain.com)

Organization

Organizational Unit (example: Security)

City

State (full name)

Country: Two-letter country abbreviation

Click **Next**.

> **NOTE:**
> **The certificate expires in one year, by default.**

11 In the *Front End Server Setup* dialog, enter the fully qualified hostname or DNS alias of the Back End Server, select **Enterprise Edition**, and click **Next**.

12 From the *Front End Server Install Setup* dialog, you can view or edit hostnames and ports.

- To accept the default hostnames and ports, in the *Front End Server Install Setup* dialog, click **Next**.
- To view or edit hostnames, in the *Front End Server Setup* dialog, click **Edit Hostnames**. Edit hostnames only if necessary. Dell recommends using the defaults.

  > **NOTE:**
  > **A hostname cannot contain an underscore character ("_").**

  Deselect a proxy only if you are certain that you do not want to configure it for installation. If you deselect a proxy in this dialog, it will not be installed.

  When finished, click **OK**.
- To view or edit Ports, in the *Front End Server Setup* dialog, click either **Edit External Facing Ports** or **Edit Internal Connecting Ports**. Edit ports only if necessary. Dell recommends using the defaults.

  If you deselect a proxy in the *Edit Front End Host Names* dialog, its port does not display in the External Ports or Internal Ports dialogs.

  When finished, click **OK**.

13 In the *Ready to Install the Program* dialog, click **Install**.

14 When the installation is completed, click **Finish**.

VE Terminal - Basic Configuration Tasks

Basic configuration tasks are accessed from the Main Menu.

Change Hostname

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Basic Configuration* menu, select **Hostname**.

2 Use the Backspace key to remove the existing DDP Enterprise Server - VE hostname then replace it with a new hostname and select **OK**.

Change Network Settings

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Basic Configuration* menu, select **Network Settings**.
2 In the *Configure Network Settings* screen, choose either option below then select **OK**.
   - (Default) Use DHCP.
   - (Recommended) In the Use DHCP field, press the Spacebar to remove the X and manually enter these addresses, as applicable:

     Static IP

     Network Mask

     Default Gateway

     DNS Server 1

     DNS Server 2

     DNS Server 3

     NOTE: When using a static IP, you must create a host entry in the DNS server.

Set DMZ Hostname

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Basic Configuration* menu, select **DMZ Hostname**.
2 Enter the fully qualified domain name of the DMZ server and select **OK**.

NOTE: To use Proxy Mode (DMZ Mode), you must Install and Configure Proxy Mode.

Change Time Zone

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Basic Configuration* menu, select **Time Zone**.
2 In the *Time Zone* screen, use the arrow keys to highlight your time zone and select **Enter**.
3 At the time zone confirmation prompt, select **OK**.

Update DDP Enterprise Server - VE

For information about a specific update, see VE Technical Advisories, located on the Dell Support website at http://www.dell.com/support. To see the version and installation date of an update that is already applied, from the **Basic Configuration** menu, select **Update DDP Enterprise Server - VE** > **Last successful update applied**.

To receive email notifications when VE updates are available, see Configure SMTP Settings.

NOTE: In Default Mode, an update should be performed after initial installation of DDP Enterprise Server - VE and also before clients are activated.

If policy changes have been made but not committed in the Remote Management Console, apply policy changes before updating VE:

1 As a Dell Administrator, log in to the Remote Management Console.
2 In the left menu, click **Management** > **Commit**.
3 Enter a description of the change in the Comment field.
4 Click **Commit Policies**.
5 When the commit is complete, log off the Remote Management Console.

Update VE (Default Mode)

1 Dell recommends performing a regular backup. Before updating, ensure that the backup process has been functioning properly. See Backup and Restore.
2 From the **Basic Configuration** menu, select **Update DDP Enterprise Server - VE**.
3 Select the desired action:
   - Set Update Server - Select this option to set or change the server location of DDP Enterprise Server - VE update packages. In the *Set Update Server* screen, use the Backspace key to remove the existing Server Hostname or IP address. Enter the new fully qualified domain name or IP address and select **OK**.

     The default update server is **act.credant.com**.
   - Set Proxy Settings - Select this option to set the Proxy Settings for downloading updates.

     In the *Configure Proxy Settings* screen, press the Spacebar to enter an **X** in the Use Proxy field. Enter the HTTPS, HTTP, and FTP Proxy addresses. If firewall authentication is required, press the Spacebar to enter an **X** in the Authentication Required field. Enter the username and password, and press **OK**.

     NOTE: To update from an FTP site, enter the FTP user name and password, followed by the URL.
   - Check for Update - Select this option to check the Update Server for a DDP Enterprise Server - VE update package.
   - Download Update - Select this option to download an update after it is discovered by Check for Update.
   - Apply Update - Select this option if you want to apply a DDP Enterprise Server - VE update package that you have downloaded. In the *Select an Update (.deb) File* screen, select the update package you want to install and press **Enter**.
   - Last successful update applied - Select this option to see the version and installation date of the current VE version.

Update VE (Disconnected Mode)

1 Dell recommends performing a regular backup. Before updating, ensure that the backup process has been functioning properly. See Backup and Restore.
2 Obtain the .deb file that contains the latest VE update from the Dell Support website.
   VE downloads are located in the **Drivers & downloads** folder at

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

   or

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

   or

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

or

www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-secure-lifecycle/research

3 Store the .deb file in the /updates folder on the secure FTP server of the VE.

Ensure that the FTP client supports SFTP on port 22, and an FTP user is set up. See Set up File Transfer (FTP) Users.

4 From the **Basic Configuration** menu, select **Update DDP Enterprise Server - VE**.

5 Select **Apply Update** and press **Enter**.

If the .deb file does not display, ensure that the .deb file is stored in the proper location.

6 Select the .deb update file you want to install and press **Enter**.

Change User Passwords

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

You can change passwords for these users:

- ddpuser (DDP Enterprise Server - VE Terminal Administrator) - This user has access to the VE Terminal and its menus.
- ddpconsole (DDP Enterprise Server - VE shell access) - This user has VE shell access. Shell access is available for a network administrator to check and troubleshoot network connectivity.
- ddpsupport (Dell ProSupport Administrator) - This user exists for Dell ProSupport use only. For security purposes, you control the password for this account.

1 From the *Basic Configuration* menu, select **Change User Passwords**.

2 In the *Change User Passwords* screen, select user password to change and select **Enter.**

3 In the *Set Password* screen, enter the current password, enter the new password, re-enter the new password, and select **OK**.

Passwords must include the following:

- At least 8 characters
- At least 1 uppercase letter
- At least 1 digit
- At least 1 special character

Set up File Transfer (FTP) Users

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

You can give up to three users access to the secure FTP server of the DDP Enterprise Server - VE for backup and restore tasks. The VE FTP server can also be used to store or upload updates to DDP Enterprise Server - VE.

1 From the *Basic Configuration* menu, select **File Transfer (FTP) Users**.

2 In the *Configure FTP Users* screen, to enable an FTP User, press the Spacebar to enter an **X** in the Status field for the user. To disable an FTP User, press the Spacebar to remove the **X** in the Status field for the user.

3 Enter a user name and password for the SFTP User.

Passwords must include the following:

- At least 8 characters
- At least 1 uppercase letter
- At least 1 digit
- At least 1 special character

4 When you are finished entering SFTP users, select **OK**.

Enable SSH

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

You can enable SSH for the Support Administrator login, DDP Enterprise Server - VE shell access, and the VE Terminal command-line interface.

1 From the *Basic Configuration* menu, select **SSH Settings**.
2 Highlight the user for which you want to enable SSH, press the Spacebar to enter an **X** in its field, and select **OK**.

Start or Stop VE Services

Perform this task only if needed. It is a best practice to restart the services any time a settings change is made.

1 To simultaneously start or stop all VE Services, from the *Basic Configuration* menu, select either **Start Application** or **Stop Application**.
2 At the confirmation prompt, select **Yes**.

NOTE: Server state changes may require up to two minutes to complete.

Reboot VE

Perform this task only if needed.

1 From the *Basic Configuration* menu, select **Reboot Appliance**.
2 At the confirmation prompt, select **Yes**.
3 After restart, log in to DDP Enterprise Server - VE.

Shut down VE

Perform this task only if needed.

1 From the *Basic Configuration* menu, scroll down and select **Shutdown Appliance**.
2 At the confirmation prompt, select **Yes**.
3 After restart, log in to DDP Enterprise Server - VE.

VE Terminal - Advanced Configuration Tasks

Advanced configuration tasks are accessed from the Main Menu.

Set or Change the Database Password

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Advanced Configuration* menu, select **Database Password**.
2 Enter a password to access the database and select **OK**.

Passwords must include the following:

- At least 8 characters
- At least 1 uppercase letter
- At least 1 digit
- At least 1 special character

NOTE: Dell recommends that you back up passwords after installation is completed.

Configure SMTP Settings

To receive DDP Enterprise Server - VE email notifications **or** to use Secure Lifecycle, follow the steps in this section to configure SMTP settings. DDP Enterprise Server - VE email notifications inform recipients of DDP Enterprise Server - VE server status error states, password updates, availability of DDP Enterprise Server - VE updates, and client license issues.

It is a best practice to restart the services any time a settings change is made.

To configure SMTP settings, follow these steps:

1 From the *Advanced Configuration* menu, select **Email Notifications**.
2 In the *Set up Email Notifications* screen, to enable email alerts, press the Spacebar to enter an **X** in the Enable Email Alerts field.
3 Enter the SMTP Server fully qualified domain name.
4 Enter the SMTP Port.
5 In the From User field, enter the email account ID that will send email notifications.
6 In the Enter User field, enter an email account ID for access to change configured email notifications.
7 In the Password field, enter a password for access to change configured email notifications.
8 In the Mail IDs fields for VE Status, Password Updates, and Updates Availability, enter lists of recipients for each notification type. Follow these conventions when listing recipients:
   - Email address format is recipient@dell.com.
   - Recipients are separated with commas or semicolons.
9 In the Service alert reminder field, to enable reminders, press the Spacebar to enter an **X** in the field then set the reminder interval in minutes. A Service alert reminder is triggered when the reminder interval has passed after a notification is sent about a system health issue and the host or service remains in the same state.
10 In the Summary Report field, to enable reports of notifications, select the desired interval (Daily, Weekly, or Monthly) and then press the Spacebar to enter an **X** in the field.
11 Select **OK**.

Import an Existing Certificate or Enroll a New Server Certificate

Certificates must be in place before you can activate users against DDP Enterprise Server - VE.

You can import an existing certificate or create a certificate request through the DDP Enterprise Server - VE.

It is a best practice to restart the services any time a settings change is made.

Import an Existing Server Certificate

1 Export the existing certificate and its full chain of trust from its keystore.

NOTE: Keep the export password because you will enter it when you import the certificate into DDP Enterprise Server - VE.

2 On the FTP Server of the DDP Enterprise Server - VE, store the certificate to **/opt/dell/vsftpd/files/certificates**.

3 From the DDP Enterprise Server - VE *Advanced Configuration* menu, select **Server Certificates**.

4 Select **Import Existing Certificate**.

5 Select a certificate file to be installed on DDP Enterprise Server - VE.

6 When prompted, enter the certificate export password and select **OK**.

7 When the import is complete, select **OK**.

Enroll a New Server Certificate

1 From the *Advanced Configuration* menu, select **Server Certificates**.

2 Select **New Server Certificate**.

3 Select **Create Certificate Request.**

4 Complete the fields in the *Generate Certificate Request* screen:

- Country Name: Two-letter country code.
- *State/Province*: Enter the unabbreviated state or province name (example, Texas).
- *Locality Name/City.* Enter the appropriate value (example, Dallas).
- *Organization*: Enter the appropriate value (example, Dell).
- *Organizational Unit*: Enter the appropriate value (example, Security).
- *Common Name:* Enter the fully qualified domain name of the server where DDP Enterprise Server - VE is installed. This fully qualified name includes the hostname and the domain name (example, server.domain.com).
- *Email ID:* Enter the email address to which your CSR will be sent.

5 Follow your organizational process for acquiring an SSL server certificate from a Certificate Authority. Send the contents of the CSR file for signing.

6 When you receive the signed certificate, export the certificate as a .p7b file, and download the full chain of trust in .der format.

7 Make backup copies of the certificate and chain of trust.

8 Upload the certificate file and its full chain of trust to the FTP Server of the DDP Enterprise Server - VE.

9 From the *Advanced Configuration* menu, select **Server Certificates**.

10 Select **New Server Certificate**.

11 Select `Complete Certificate Enrollment`.

12 Select the certificate file to be installed on DDP Enterprise Server - VE.

13 If prompted, enter the Certificate Password: **changeit**.

To enable trust validation on Windows-based Encryption clients, see Enable Manager Trust Chain Check.

Create and Install a Self-signed Certificate

1 From the DDP Enterprise Server - VE *Advanced Configuration* menu, select **Server Certificates**.

2 Select **Create and Install Self-signed Certificate**.

3 To confirm that you want to replace the pre-installed certificate with a new certificate, click **Yes**.

4 Enter the Certificate Password: **changeit**.

5 After the new certificate is installed, select **OK** and wait for services to restart.

VE services automatically restart.

Configure Log Rotation

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

Daily log rotation is enabled by default. To change the default log rotation, from the *Advanced Configuration* menu, select **Logrotate Configuration**.

To disable log rotation, use the Spacebar to enter an **X** in the No rotation field and select **OK**.

To enable log rotation, follow these steps:

1 To enable daily, weekly, or monthly rotation, use the Spacebar to enter an **X** in the appropriate field. For weekly or monthly rotation, enter the appropriate day of the week or month as a numeral, where Monday=1.
2 Enter a time for rotation in the Logrotate Time field.
3 Select **OK**.

Backup and Restore

Backups can be configured or performed at any time and are not required to begin using DDP Enterprise Server - VE. Dell recommends that you configure a regular backup process.

Backups can be stored to an external secure FTP server (recommended) or to the DDP Enterprise Server - VE. If stored on the VE Server, when the disk is at 90 percent capacity, no new backups are stored. You will receive an email notification that disk allocation space is low.

NOTE:
To preserve disk partition space and prevent automatic deletion of backups, remove unnecessary backups from DDP Enterprise Server - VE.

Backups are run daily, by default. Dell recommends storing backups to an external secure FTP server at a frequency that meets requirements of the organization for backups and appropriate use of storage space.

To configure a backup schedule, from the *Advanced Configuration* menu, select **Backup and Restore > Configuration** and follow these steps:

1 To enable daily, weekly, or monthly backups, use the Spacebar to enter an **X** in the appropriate field. For weekly or monthly backups, enter the appropriate day of the week or month as a numeral, where Monday=1. To disable backups, use the Spacebar to enter an **X** in the No backups field and select **OK**.
2 Enter a time for backup in the Backup Time field.
3 Select **OK**.

To perform an immediate backup, from the *Advanced Configuration* menu, select **Backup and Restore > Backup now.** When the backup confirmation displays, select **OK**.

NOTE:
Before beginning a Restore operation, all VE Server services must be Running. **Check Server Status**. If all services are not Running, restart services. For more information, see **Start or Stop VE Services**. Begin to Restore ***only*** when ***all*** services are Running.

To restore from a backup, from the *Advanced Configuration* menu, select **Backup and Restore > Restore** and select the backup file to be restored. At the confirmation screen select **Yes**.

VE reboots, and the backup is restored.

Store backups to a secure FTP server

To store backups to an FTP server, the FTP client must support SFTP on port 22.

According to backup requirements of the organization, backups can be downloaded in the following ways:

- Manually

- Through automated script
- Through the organization's approved backup solution

To download backups using the organization's backup solution, obtain detailed instructions from your backup solution vendor.

NOTE:
Virtual Edition is based on Linux Debian Ubuntu x64.

Log on to VE as ddpsupport, and use the sudo command to configure your backup solution:

`sudo` <instructions from backup solution vendor>

Back up contents of the following folders:

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

/opt/dell/vsftpd/files/certificates (strongly recommended)

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

When the sudo process is complete, type **exit** and press **Enter** until the login prompt displays.

Enable Database Remote Access

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

NOTE: Dell recommends that you enable database remote access only if necessary.

1 From the *Advanced Configuration* menu, select **Database Remote Access**.
2 Use the Spacebar to enter an **X** in the Enable Database Remote Access field and select **OK**. If the database password has not yet been configured, a prompt for the database password displays.
3 Enter the database password.
4 Re-enter the database password.
DDP application components stop automatically.

Enable DMZ Server Support

This task can be completed at any time. It is not required to begin using DDP Enterprise Server - VE. It is a best practice to restart the services any time a settings change is made.

1 From the *Advanced Configuration* menu, select **Enable DMZ Server Support**.
2 Use the Spacebar to enter an **X** in the Enable DMZ Server Support field and select **OK**.

NOTE: To use Proxy Mode (DMZ Mode), you must Install and Configure Proxy Mode.

DDP Enterprise Server - VE Administrator Tasks

Set or Change DDP Enterprise Server - VE Terminal Language

It is a best practice to restart the services any time a settings change is made.

1 In the Main Menu, select **Set Language**.
2 Use the arrow keys to select the preferred language.

Check Server Status

To check the status of DDP Enterprise Server - VE Services, in the Main Menu, select **Server Status**.

The following table describes each Service and its function.

Name	Description
Dell Message Broker	Enterprise Server Bus
Dell Identity Server	Handles domain authentication requests.
Dell Compatibility Server	A service for managing the enterprise architecture.
Dell Security Server	Provides the mechanism for controlling commands and communication with Active Directory. Used to communicate with the Dell Policy Proxy.
Dell Compliance Reporter	Provides an extensive view of the environment for auditing and compliance reporting.
Dell Core Server	A service for managing the enterprise architecture.
Dell Core Server HA (High Availability)	A high-availability service that allows for increased security and performance of HTTPS connections when managing the enterprise architecture.
Dell Inventory Server	Processes the inventory queue.
Dell Forensic Server	Provides web services for Forensic API.
Dell Policy Proxy	Provides a network-based communication path to deliver security policy updates and inventory updates.

DDP Enterprise Server - VE monitors and restarts its services, if necessary.

NOTE: If the databasecustomizer process fails, servers move to the Execution Failed state. To check the Databasecustomizer log, in the Main Menu, select View Logs.

View Logs

To check the following logs, in the Main Menu, select **View Logs**.

Syslog Log Mail Log Auth Log (SSH) Postgres Log Monitor Log

- System Logs

  Syslog Log

  Mail Log

  Auth Log (SSH)

  Postgres Log

  Monitor Log
- Server Logs

  Compatibility Server

  Security Server

  Message Broker

  Core Server

  Core Server HA

  Compliance Reporter

  Identity Server

  Inventory Server

  Forensic Server

  Policy Proxy
- Databasecustomizer Log

Open the Command-line Interface

To open the command-line interface, in the Main Menu, select **Launch Shell**.

To exit the command-line interface, type **exit** and press **Enter**.

Generate a System Snapshot Log

To generate a System Snapshot Log for Dell ProSupport, in the Main Menu, select **Support Tools.**

1 From the *Support Tools* menu, select **Generate System Snapshot Log**.
2 At the indication that the file is created, select **OK**.
If the ddpsupport user is activated, Dell ProSupport can retrieve the log from the DDP Enterprise Server - VE SFTP server. If the ddpsupport user is not activated, contact Dell ProSupport. For more information, see Contact Dell ProSupport.

4

DDP Enterprise Server - VE Maintenance

You must remove unnecessary DDP Enterprise Server - VE backups.

Only the ten most recent backups are retained. If disk partition space is at ten percent or less, no more backups are stored. If this condition occurs, you will receive an email notification that disk allocation space is low.

5

DDP Enterprise Server - VE Troubleshooting

If an error occurs, and you have configured email notifications, you will receive an email notification. Based on the information in the email notification, follow these steps:

1 Check applicable log files.
2 Restart services, as needed. It is a best practice to restart the services any time a settings change is made.
3 Generate a System Snapshot Log.
4 Contact Dell ProSupport. For more information, see Contact Dell ProSupport.

6

Post-Installation Configuration Tasks

After installation, some components of your environment may need to be configured, based on the Dell Data Protection solution used by your organization.

Configure VE for Secure Lifecycle

To configure VE to support Secure Lifecycle, in the VE Remote Management Console, set the Cloud Encryption policy to On. To enable Secure Lifecycle Protected Office Documents mode, set the Protected Office Documents policy to On.

For instructions to install the Secure Lifecycle client, refer to the *Enterprise Edition Advanced installation Guide*, *Enterprise Edition Basic installation Guide*, or *Secure Lifecycle User Guide*.

Install and Configure EAS Management for Mobile Edition

To use Mobile Edition, you must install and configure EAS Management. If you do not intend to use Mobile Edition, skip this section.

Prerequisites

- The logon account for the EAS Mailbox Manager Service must be an account with permissions to create/modify Exchange ActiveSync policy, assign policies to user mailboxes, and query information about ActiveSync devices.
- The EAS Configuration Utility must be run with Administrator permissions to modify files and restart Services.
- Network connection to the DDP Enterprise Server - VE is required.
- Have the hostname or IP address of the DDP Enterprise Server - VE available.
- Microsoft Message Queuing (MSMQ) must already be installed/configured on the server hosting the Exchange environment. If not, install MSMQ 4.0 on Windows Server 2008 or Windows Server 2008 R2 (on the server hosting the Exchange environment) - http://msdn.microsoft.com/en-us/library/aa967729.aspx

During the Deployment Process

If you intend to use Exchange ActiveSync to manage mobile devices through Mobile Edition, your Exchange Server environment must be configured.

Install EAS Device Manager

1. In the Mobile Edition installation media, navigate to the EAS Management folder. In the EAS Device Manager folder, copy setup.exe to your *Exchange Client Access Server(s)*.
2. Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Client Access Server*, run this installer on each one.
3. Select the language for installation, then click **OK**.
4. Click **Next** when the *Welcome* screen displays.
5. Read the license agreement, agree to the terms, and click **Next**.
6. Click **Next** to install EAS Device Manager in the default location of **C:\Inetpub\wwwroot\Dell\EAS Device Manager\.**
7. Click **Install** at the *Ready to Begin Installation* screen.

A status window displays the installation progress.

8 If desired, check the box to show the Windows Installer log and click **Finish**.

Install EAS Mailbox Manager

1 In the Mobile Edition installation media, navigate to the EAS Management folder. In the EAS Mailbox Manager folder, copy setup.exe to your *Exchange Mailbox Server(s)*.

2 Double-click **setup.exe** to begin the installation. If your environment includes more than one *Exchange Mailbox Server*, run this installer on each one.

3 Select the language for installation, then click **OK**.

4 Click **Next** when the *Welcome* screen displays.

5 Read the license agreement, agree to the terms, and click **Next**.

6 Click **Next** to install EAS Mailbox Manager in the default location of C:\Program Files\Dell\EAS Mailbox Manager\.

7 At the *Logon Information* screen, enter the credentials of the user account that will log on to use this Service.

User Name: DOMAIN\Username

Password: password associated with this user name

Click **Next**.

8 Click **Install** at the *Ready to Begin Installation* screen.

A status window displays the installation progress.

9 If desired, check the box to show the Windows Installer log and click **Finish**.

Use the EAS Configuration Utility

1 On the same computer, go to **Start** > **Dell** > **EAS Configuration Utility** > **EAS Configuration** to run the EAS Configuration Utility.

2 Click **Setup** to configure EAS Management Settings.

3 Enter the following information:

DDP Enterprise Server - VE hostname

Dell Policy Proxy Polling Interval (the default is 1 minute)

Select the box to run EAS Device Manager in report-only mode (recommended during deployment).

> **NOTE:**
> The Report-only mode allows unknown devices/users to have access to Exchange ActiveSync but still reports the traffic to you. Once your deployment is up and running, you can change this setting to tighten security.

Click **OK**.

4 A success message displays. Click **Yes** to re-start IIS and EAS Mailbox Manager Services.

5 Click **Quit** when finished.

After the Deployment Process

Once your deployment is up and running, and you are ready to tighten security, follow the steps below.

On your Exchange Mailbox Server(s)

1 Go to **Start** > **Dell** > **EAS Configuration Utility** > **EAS Configuration** to run the EAS Configuration Utility.

2 Click **Setup** to configure EAS Management Settings.

3 Enter the following information:

DDP Enterprise Server - VE hostname

Dell Policy Proxy Polling Interval (the default is 1 minute)

Clear the box to run EAS Device Manager in report-only mode

Click **OK**.

4 A success message displays. Click **Yes** to restart IIS and EAS Mailbox Manager Services.

5 Click **Quit** when finished.

Enable Manager Trust Chain Check

If a self-signed certificate is used on VE Server for SED or BitLocker Manager, SSL/TLS trust validation must remain ***disabled*** on the client computer. Before enabling SSL/TLS trust validation on the client computer, the following requirements must be met:

- A certificate signed by a root authority (for example, Entrust or Verisign) must be imported into VE Server. See Import an Existing Certificate or Enroll a New Server Certificate.
- The full chain of trust of the certificate must be stored in the Microsoft keystore on the client computer.

To enable SSL/TLS trust validation, on the client computer, change the value of the following registry entry to 0:

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

DisableSSLCertTrust=REG_DWORD (32-bit):0

VE Remote Management Console Administrator Tasks

Assign Dell Administrator Role

1 As a Dell Administrator, log in to the Remote Management Console at this address: https://server.domain.com:8443/webui/ The default credentials are **superadmin/changeit**.

2 In the left pane, click **Populations** > **Domains**.

3 Click a domain that you want to add a user to.

4 On the Domain Detail page, click the **Members** tab.

5 Click **Add User**.

6 Enter a filter to search the User Name by Common Name, Universal Principal Name, or sAMAccountName. The wild card character is *.

A Common Name, Universal Principal Name, and sAMAccountName must be defined in the enterprise directory server for every user. If a user is a member of a Domain or Group but does not appear in the Domain or Group Members list in the Management, ensure that all three names are properly defined for the user in the enterprise directory server.

The query will automatically search by common name, then UPN, and then sAMAccount name until a match is found.

7 Select users from the *Directory User List* to add to the Domain. Use <Shift><click> or <Ctrl><click> to select multiple users.

8 Click **Add**.

9 From the menu bar, click the **Details & Actions** tab of the specified user.

10 Scroll across the menu bar, and select the **Admin** tab.

11 Select the administrator roles to add to this user.

12 Click **Save**.

Log in with Dell Administrator Role

1 Log out of the Remote Management ConsoleEnterprise Server.

2 Log in to the Remote Management ConsoleEnterprise Server and login with Domain user credentials.

Click "?" in the upper right corner of the Remote Management Console to launch *Dell Data Protection AdminHelp*. The *Get Started* page displays. Click **Add Domains**.

Baseline polices have been set for your organization but may need to be modified depending on your specific needs, as follows (licensing and entitlements guide all activations):

- Windows computers will be encrypted
- Computers with self-encrypting drives will be encrypted
- Windows computers with Hardware Crypto Accelerators will be encrypted
- BitLocker Management is not enabled
- Advanced Threat Protection is not enabled
- Threat Protection is enabled
- External media will not be encrypted
- Devices connected to ports will not be encrypted

- Secure Lifecycle is enabled
- Mobile Edition is not enabled

See the AdminHelp topic *Manage Policies* to navigate to Technology Groups and policy descriptions.

Commit Policies

Commit policies when installation is completed.

To commit polices after installation or, later, after policy modifications are saved, follow these steps:

1 In the left pane, click **Management** > **Commit**.
2 Enter a description of the change in the Comment field.
3 Click **Commit Policies**.

8

Solution ports

The following table describes each component and its function.

Name	Default Port	Description	Required For
Compliance Reporter	HTTP(S)/8084	Provides an extensive view of the environment for auditing and compliance reporting. A component of the DDP Enterprise Server - VE.	Reporting
Remote Management Console	HTTPS/8443	Administration console and control center for the entire enterprise deployment. A component of the DDP Enterprise Server - VE.	All
Core Server	HTTPS/8888	Manages policy flow, licenses, and registration for Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Protection. Processes inventory data for use by Compliance Reporter and the Remote Management Console. Collects and stores authentication data. Controls role-based access. A component of the DDP Enterprise Server - VE.	All
Core Server HA (High Availability)	HTTPS/8888	A high-availability service that allows for increased security and performance of HTTPS connections with the Remote Management Console, Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, and Advanced Threat Protection. A component of the DDP Enterprise Server - VE.	All
Security Server	HTTPS/8443	Communicates with Policy Proxy; manages forensic key retrievals, activations of clients, Secure Lifecycle products, and SED-PBA communication. A component of the DDP Enterprise Server - VE.	All
Compatibility Server	TCP/1099 (closed)	A service for managing the enterprise architecture. Collects and stores initial inventory data during activation and policy data during migrations. Processes data based on user groups in this service. A component of the DDP Enterprise Server - VE.	All
Message Broker Service	TCP/61616 and STOMP/61613 (closed or, if configured for	Handles communication between services of the DDP Enterprise Server - VE. Stages policy information created by the Compatibility Server for policy proxy queuing. A component of the DDP Enterprise Server - VE.	All

Name	Default Port	Description	Required For
	DMZ, 61613 is open)		
Identity Server	HTTPS/8445	Handles domain authentication requests, including authentication of the SED Manager. Requires an Active Directory account. A component of the DDP Enterprise Server - VE.	All
Forensic Server	HTTPS/8448	Allows administrators that have appropriate privileges to get encryption keys from the Remote Management Console, for use in data unlocks or decryption tasks. A component of the DDP Enterprise Server - VE.	Forensic API
Inventory Server	8887	Processes the inventory queue. A component of the DDP Enterprise Server - VE.	All
Policy Proxy	TCP/ 8000/8090	Provides a network-based communication path to deliver security policy updates and inventory updates. A component of the DDP Enterprise Server - VE.	Enterprise Edition for Mac Enterprise Edition for Windows Mobile Edition
LDAP	389/636, 3268/3269 RPC - 135, 49125+	**Port 3268** - This port is used for queries specifically targeted for the global catalog. LDAP requests sent to port 3268 can be used to search for objects in the entire forest. However, only the attributes marked for replication to the global catalog can be returned. For example, a user's department could not be returned using port 3268 since this attribute is not replicated to the global catalog. **Port 389** - This port is used for requesting information from the local domain controller. LDAP requests sent to port 389 can be used to search for objects only within the global catalog's home domain. However, the requesting application can obtain all of the attributes for those objects. For example, a request to port 389 could be used to obtain a user's department.	All
Client Authentication	HTTPS/8449	Allows client servers to authenticate against DDP Enterprise Server - VE.	Server Encryption
Callback beacon	HTTP/8446	Allows a callback beacon to be inserted into each protected Office file, when running Secure Lifecycle Protected Office mode.	Secure Lifecycle
EAS Device Manager	N/A	Enables over-the-air functionality. Installed on the Exchange Client Access Server.	Exchange ActiveSync Management of mobile devices.
EAS Mailbox Manager	N/A	The mailbox agent that is installed on the Exchange Mailbox Server.	Exchange ActiveSync Management of mobile devices.

NTP Time Synchronization: TCP and UDP/123 (For more information, refer to https://help.ubuntu.com/lts/serverguide/NTP.html.)