



# Dell Data Protection | Endpoint Security Suite Enterprise for VDI with VMware

Deployment and configuration runbook

Dell Engineering  
January 2017

## Revisions

Date	Description
August 2016	Initial release
January 2017	Added non-persistent VDI support

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Copyright © 2016-2017 Dell Inc. All rights reserved. Dell and the Dell logo are trademarks of Dell Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.



# Table of contents

Revisions.....	2
1 Introduction.....	5
1.1 Purpose.....	5
1.2 Scope.....	5
1.3 Configuration prerequisites.....	5
2 Solution architecture overview.....	6
2.1 Introduction.....	6
2.2 Endpoint Security Suite Enterprise overview.....	6
2.3 Dell Enterprise Server or VE Architecture.....	7
3 Hardware Components.....	9
3.1 Network.....	9
3.1.1 Dell Networking S4048 (10Gb ToR switch).....	9
3.2 Server.....	9
3.2.1 Dell PowerEdge R730.....	9
3.2.2 Architecture overview.....	9
4 Software components.....	12
4.1 Software inventory.....	12
4.1.1 Server OS.....	12
4.1.2 Horizon.....	13
4.1.3 Virtual Center.....	13
4.1.4 Horizon Administrator.....	13
4.1.5 Microsoft SQL Server.....	13
4.1.6 Endpoint Security Suite Enterprise.....	13
4.1.7 Virtual Edition.....	13
4.1.8 Dell Data Protection Suite.....	13
4.1.9 Certificates.....	14
4.2 Dell Enterprise Server installation.....	14
4.2.1 Installation.....	14
4.3 Virtual Edition.....	25
4.3.1 Installation.....	25
4.3.2 VE Configuration.....	29
5 Client Installation (Persistent or Non-Persistent).....	38



5.1	VMware View Agent .....	38
5.2	Advanced Threat Prevention (ATP) Install .....	43
5.3	Policy-Based Encryption (PBE) Install .....	43
5.4	System Data Encryption (SDE) .....	44
5.5	Removable Media Encryption (EMS) Install .....	44
5.6	Authentication .....	45
5.7	Endpoint Security Suite Enterprise Install .....	45
5.7.1	Client Install .....	45
5.7.2	Client manual and silent installation .....	50
5.7.3	Create registry entries for VDI awareness .....	51
5.7.4	Recomposing or updating VDI pools .....	52
6	Endpoint Security Suite Enterprise Management Console .....	53
6.1	Remote Management Console .....	53
6.1.1	Browser Language .....	53
6.1.2	Domain configuration .....	56
6.1.3	Licenses .....	58
6.2	Policy configuration .....	59
6.2.1	ATP policy configuration .....	59
6.2.2	ATP client verification .....	62
6.2.3	Policy-Based Encryption Configuration .....	63
6.2.4	Policy-Based Encryption Client Verification .....	65
6.2.5	EMS Policy Configuration .....	67
A	Appendix .....	72
A.1	List of features supported by Endpoint Security Suite Enterprise .....	72
A.2	Prevent Master Image Activation prior to deployment or pool update (Recompose) .....	72
A.3	Recommended VDI policies .....	74
A.4	DDP Resources .....	74



# 1 Introduction

## 1.1 Purpose

This document addresses the configuration and implementation considerations for the key components required to deliver Advanced Threat Prevention, Policy-Based Encryption and Removable Media Encryption in a VMware [persistent](#) or [non-persistent](#) Virtual Desktop Infrastructure (VDI) environment.

## 1.2 Scope

Relative to delivering the virtual desktop environment, the objectives of this document are to:

- Provide a configuration document for the setup of Endpoint Security Suite Enterprise in a VDI environment.
- Configuration of Advanced Threat Prevention.
- Configuration of Removable Media Encryption.
- Configuration of Policy-Based Encryption.

## 1.3 Configuration prerequisites

This lists the prerequisites needed:

- VMware Environment. See Section 4 for more details.
- Microsoft SQL Server available. See Section 4 for more details.
- Virtual Machine (VM) running Microsoft Server 2012 R2 for management.
- .Net Framework 3.5
- Endpoint Security Suite Enterprise and Dell Data Protection Server documentation located with the downloaded zip files.
- CALS – make sure that you have client access licenses for the Endpoint Security Suite Enterprise available. This does not cover VMware, Microsoft or application licenses requirements.

Note: For Endpoint Security Suite Enterprise CALS, contact Dell Sales Team or ProSupport for assistance.



## 2 Solution architecture overview

### 2.1 Introduction

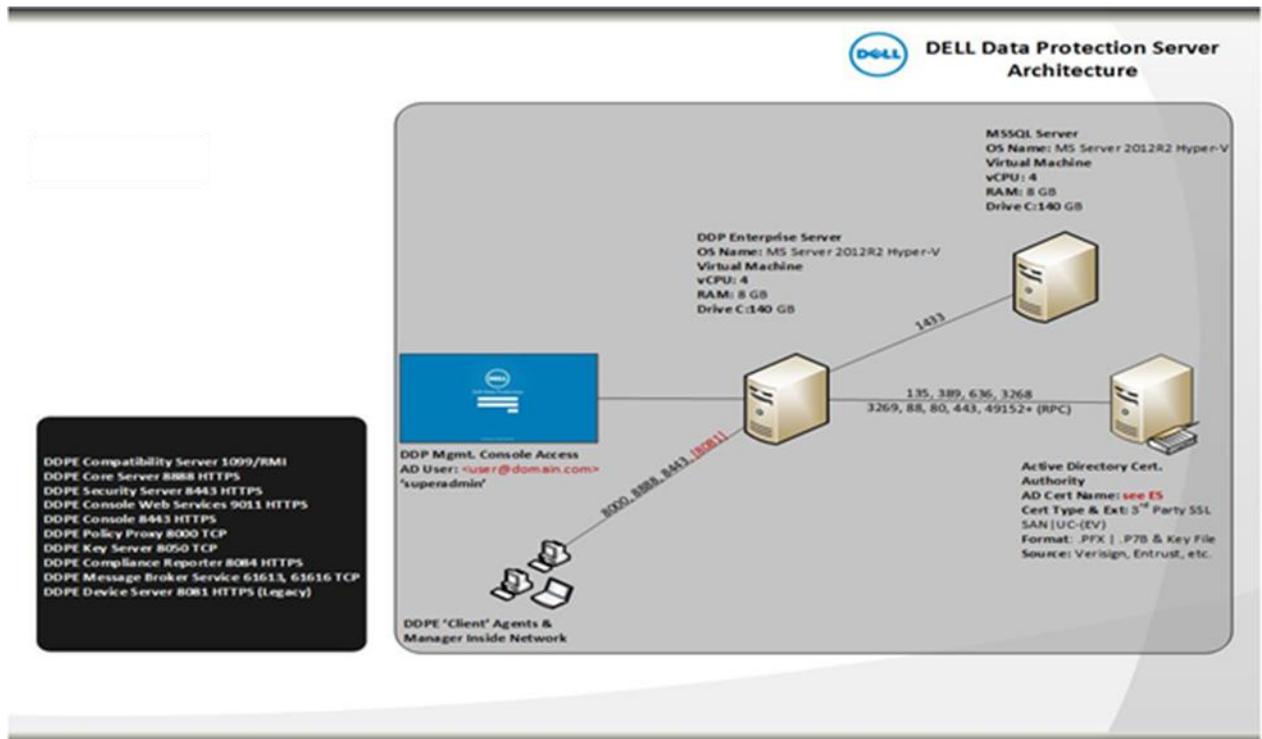
Endpoint Security Suite Enterprise and Dell Enterprise Server or Virtual Edition (VE) software delivers an out-of-the-box Advanced Threat Prevention (ATP), Policy-Based Encryption (PBE) and Removable Media Encryption (EMS) solution for virtual desktops that provide antivirus and encryption that other solution may not be able to offer. The Endpoint Security Suite Enterprise and Dell Server software is a turnkey solution that comes ready to integrate into your VMware VDI environment. The Endpoint Security Suite Enterprise and Dell Server unique architecture allows enterprises to protect their environment from endpoints to virtual desktops and physical machines with a simple path to enterprise protection.

### 2.2 Endpoint Security Suite Enterprise overview

Endpoint Security Suite Enterprise is to be configured in the VMware environment, which is outlined below. Dell Enterprise Server or VE includes the subcomponents shown below with a brief description of each.

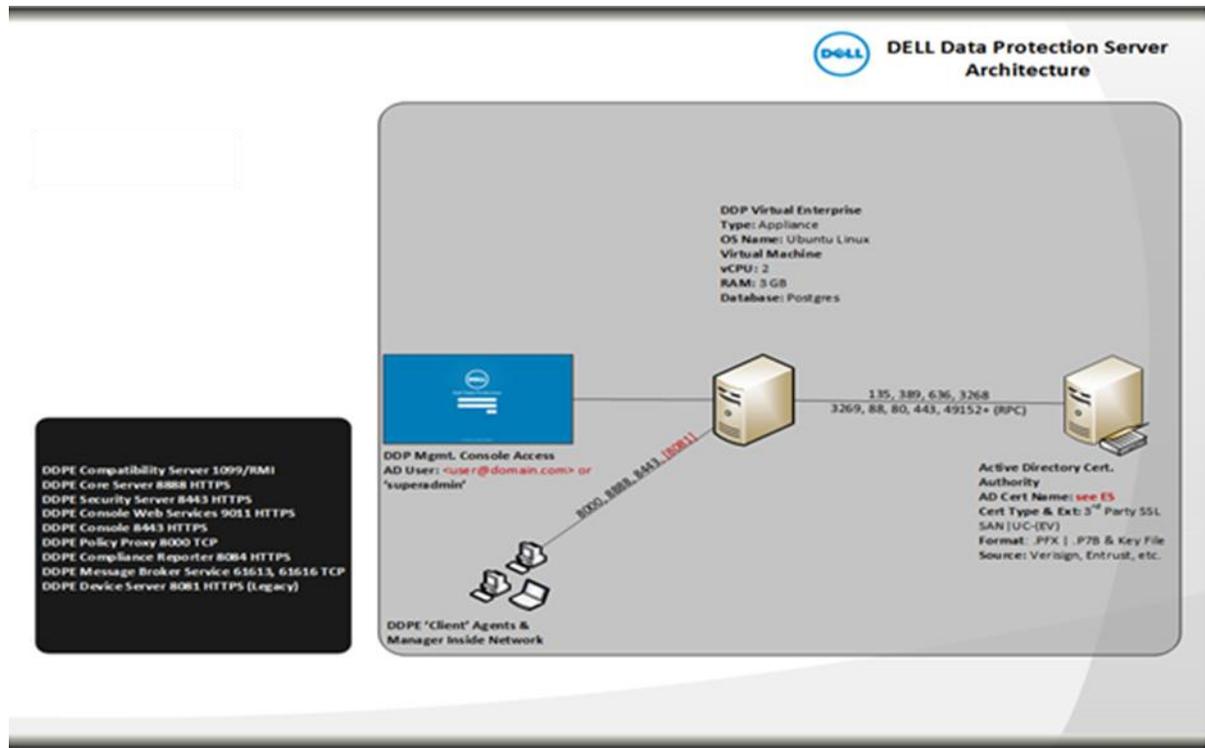
References to Endpoint Security Suite Enterprise includes Dell Enterprise Server or VE unless specifically called out in this document.

#### Dell Enterprise Server Architecture



- DDP Remote Management Console: This is where the administrator will configure security policies and domain settings for the environment.
- Dell Enterprise Server: Refer to section 2.3 for component breakdown of the DDP Server.
- Active Directory: Domain management.
- Microsoft SQL Server: Database used by Dell Enterprise Server.
- Certificate Authority: Handling of certificates in the domain environment.
- DDPE 'Client Agents: Encryption and Endpoint Security Suite Enterprise client software is installed in VDI environment providing the Encryption client and Advanced Threat Prevention agent.

## VE Server Architecture



- DDP Remote Management Console: This is where the administrator will configure security policies and domain settings for the environment.
- DDP Enterprise Server: Refer to section 2.3 for component breakdown of the DDP Server.
- Active Directory (AD): Domain management.
- Certificate Authority: Handling of certificates in the domain environment.
- DDPE Client Agents: Encryption and Endpoint Security Suite Enterprise client software is installed in VDI environment.

## 2.3 Dell Enterprise Server or VE Architecture

This is the actual back-end Dell Server installation. There are two types of server architectures for VMware environments: VE (virtual edition) which is an appliance solution or EE (enterprise edition) which is a Windows Server based solution. Both DDP servers are made up of the following components.



- Compliance Reporter - Provides an extensive view of the environment for auditing and compliance reporting.
- Core Server - Used for policy and license management as well as providing updates and registration.
- Key Server (Dell Enterprise Server only) - Service that negotiates, authenticates, and encrypts client connection using Kerberos API's. Requires SQL database to access the key data.
- Security Server - Communicates with Policy Proxy. Provides the mechanism for controlling commands and communication with Active Directory, which is used as an authentication source. Provides authentication, including identity validation for authentication into the Remote Management Console.
- Compatibility Server - 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.
- Device Server - Supports activations and password recovery.
- Message Broker - Handles communication between the services of the Dell Server. Stages policy information created by the Compatibility Server for policy proxy queuing.
- Policy Proxy - Provides a network based communication path to deliver DDP policy updates and inventory updates.
- Server Configuration Tool (Dell Enterprise Server only) - Configures database communication with the Core Server and Compatibility Server/ Security Server. Used to initialize the database upon installation or to migrate the database to a newer schema. Used to control Dell Services.



## 3 Hardware Components

### 3.1 Network

The following sections contain the core network components for Endpoint Security Suite Enterprise.

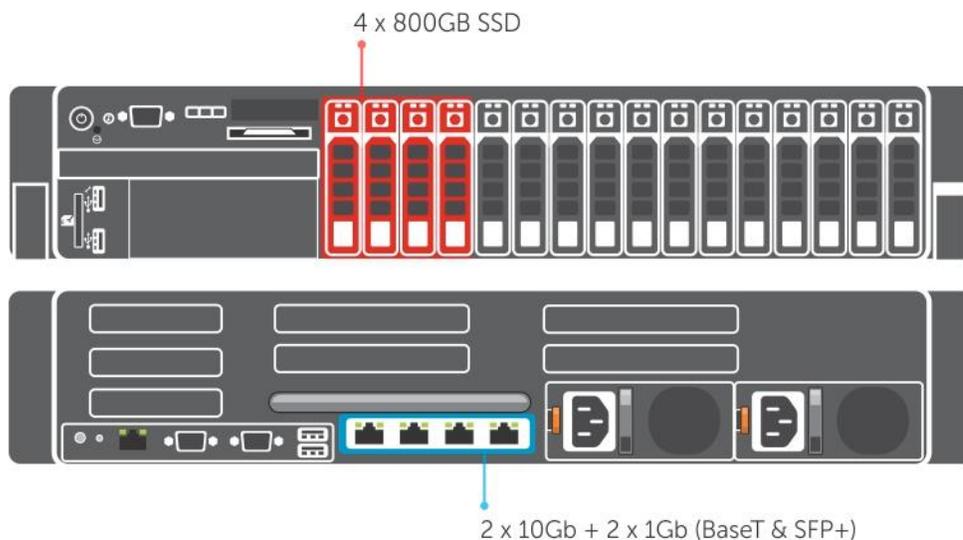
#### 3.1.1 Dell Networking S4048 (10Gb ToR switch)

Optimize your network for virtualization with a high-density, ultra-low-latency ToR switch that features 48 x 10GbE SFP+ and 6 x 40GbE ports (or 72 x 10GbE ports in breakout mode) and up to 720Gbps performance. The S4048-ON also supports ONIE for zero-touch installation of alternate network operating systems. For BaseT connectivity, the S4048T model is available.

### 3.2 Server

The following sections contain the core Dell Server components for Endpoint Security Suite Enterprise.

#### 3.2.1 Dell PowerEdge R730



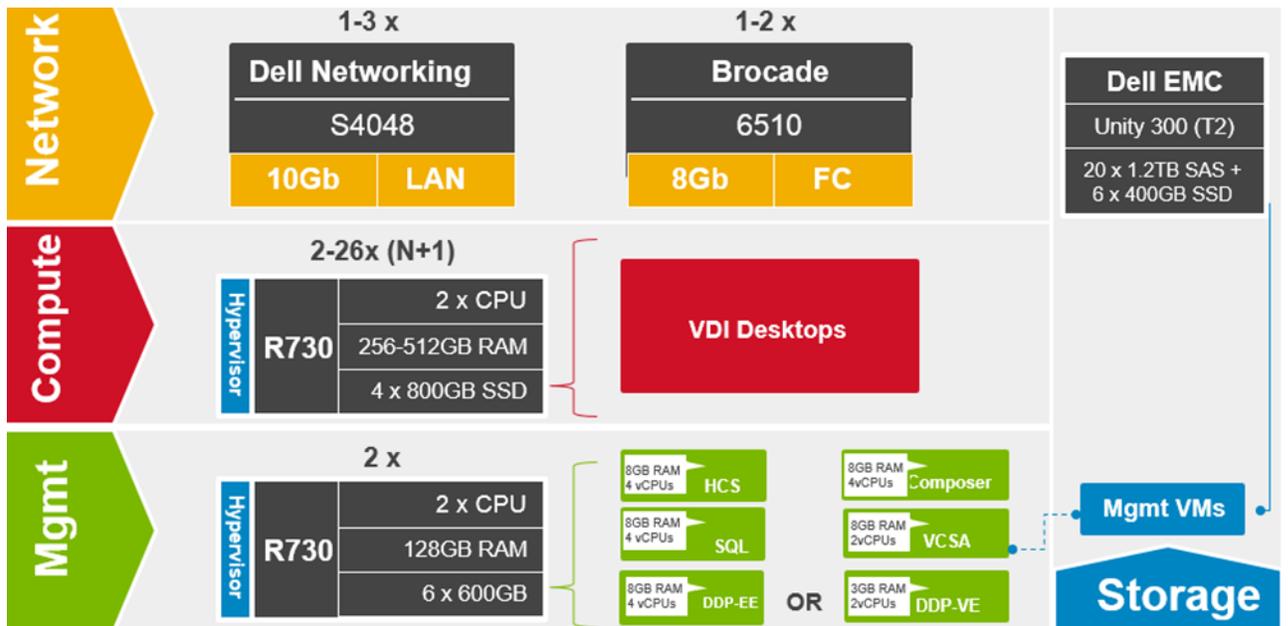
The Dell PowerEdge R730 is a 2U platform with a broad range of configuration options. The server comes equipped with dual CPUs, 10 to 20 cores, and up to 384GB of high-performance RAM by default. A minimum of four disks is required in the compute host, 4 x SSD for (Tier1). The PERC H730P is configured as a RAID 1+0 configuration connecting to the SSDs. Each platform can be outfitted with SFP+ or BaseT NICs. Refer to the next section for more specification on the architecture needed and break down of the server configurations.

#### 3.2.2 Architecture overview

This outlines the architecture overview of the Endpoint Security Suite Enterprise environment.



Separate Management and Compute Configuration.



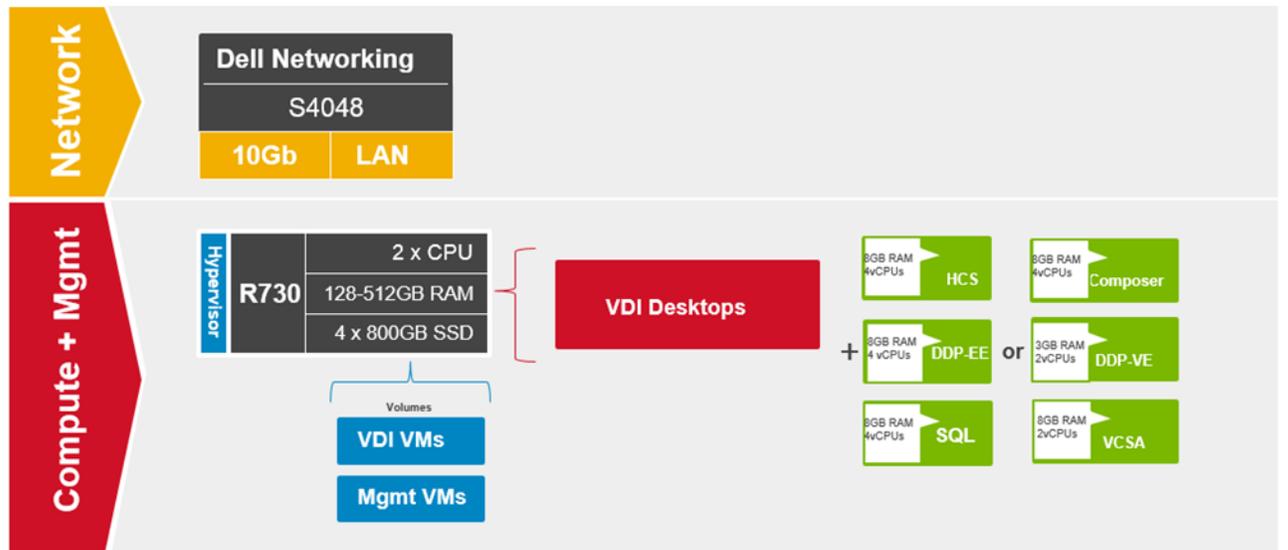
In this environment we have separate management and compute nodes configured.

Compute Node: Only has VDI desktops hosted on it.

Management Node: Only has management VMs hosted on it.

See the table below for the breakdown of the management VMs for the environment and their configurations, this covers both configurations outline here.

Combined management and compute.



All the management VMs are placed on a single node with the VDI desktops.

Management VMs configurations.

Role	vCPU	RAM (GB)	NIC	OS vDisk (GB)
Horizon	4	8	1	140
Virtual Center	2	8	1	146
Composer	4	8	1	140
MSSQL 2014	4	8	1	140
Dell Enterprise Server	4	8	1	140
VE	2	3	1	140
<b>TOTALS</b>	<b>20</b>	<b>43</b>	<b>6</b>	<b>846</b>

Note Dell does not recommend running both Dell Enterprise Server and VE together, either configure one or the other.

Note: VE and VCSA (VMware vCenter Server Appliance) are appliances and disk sizes are approximates.



## 4 Software components

### 4.1 Software inventory

This details the installation of the Endpoint Security Suite Enterprise software and dependencies in the environment. There are a number of components that make up the Endpoint Security Suite Enterprise software and these will be outlined below and their function.

Software	Description	Version
Server OS	VMware ESXi	6 update 2a
Horizon	VMware Horizon	7.0.1
Virtual Center	VMware Appliance (VCSA)	6.0.0
Composer	VMware Horizon Composer	7.0.1
MSSQL	Microsoft SQL Server	2014 Std. Ed.
Dell Enterprise Server	Enterprise Server	9.6
VE	Virtual Edition	9.6
Dell Data Protection Suite	Endpoint Security Suite Enterprise	1.3
Certificates	Certificates	OS supported.
Client OS	Windows 10 Enterprise	Win 10

Note: Client OS validation was done on the latest version of Windows operating system, Win 10. Please refer to Vendor documentation for supported OS level, and DDP documentation for supported Endpoint Security Suite Enterprise for supported versions of OS.

#### 4.1.1 Server OS

This is the operating system installed on the Host machines, which includes the installation of the Hypervisor, ESXi used for virtualization where applicable, i.e. on a physical host.



Note: Experience with the installation of VMware ESXi is assumed and therefore not covered in this document.

#### 4.1.2 Horizon

Horizon is used to provision VDI desktops, manage and give entitlements to users, who require these resources.

Note: Experience with the installation of Horizon is assumed and therefore not covered in this document.

#### 4.1.3 Virtual Center

This is the appliance version of VMware Virtual Center (VCSA), and is used to manage a VMWare environment.

Note: Experience with the installation of VMware Virtual Center is assumed and therefore not covered in this document.

#### 4.1.4 Horizon Administrator

This allows administrator to create pools, manage resources for VDI sessions.

Note: Experience with the installation of VMware Horizon Connection Server and Composer is assumed and therefore not covered in this document.

#### 4.1.5 Microsoft SQL Server

This is the database software that the Endpoint Security Suite Enterprise will use to update and query and track the Endpoint Security Suite Enterprise environment.

Note: Experience with the installation of Microsoft SQL Server is assumed and therefore not covered in this document.

#### 4.1.6 Endpoint Security Suite Enterprise

Endpoint Security Suite Enterprise is to be configured in the environment. See section 2.3 Endpoint Security Suite Enterprise Architecture for breakdown of the various components.

#### 4.1.7 Virtual Edition

This is the VE which is to be configured in the environment. See section 2.3 for breakdown of the various components.

#### 4.1.8 Dell Data Protection Suite

This is the Dell Data Protection Suite that is installed onto Clients (VDI VM's).



## 4.1.9 Certificates

Creation of signed certificates are beyond the scope of this document the only certificates implemented are self-signed certs.

Note: Experience with certificates is assumed and therefore not covered in this document.

## 4.2 Dell Enterprise Server installation

### 4.2.1 Installation

This section deals with the Server installation. Please refer to documentation in the extracted file location for further reference.

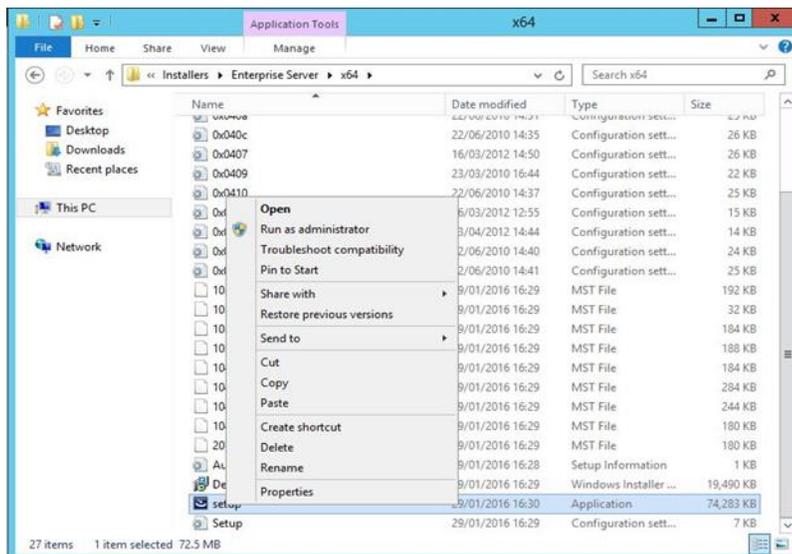
Copy **DDP-Enterprise-Server-9.6.0.xxx.zip** and extract to local system. This may take a while.

Copy the **extractedLocation\EnterpriseServerInstallKey.ini** file from the extracted file location to C:\Windows

Navigate to:

**extractedLocation\DDP-Enterprise-Server-9.6.xxx\Dell\EnterpriseServer\x64**

1. Install



Right click **Setup.exe**.

Select **Run as administrator** from menu.

2. Install Wizard



Select the language for installation.

Click **OK**.

### 3. Dependencies



Dependencies that are required will be listed for installation.

Click **Install**, wait for components to install this may take a while to run.

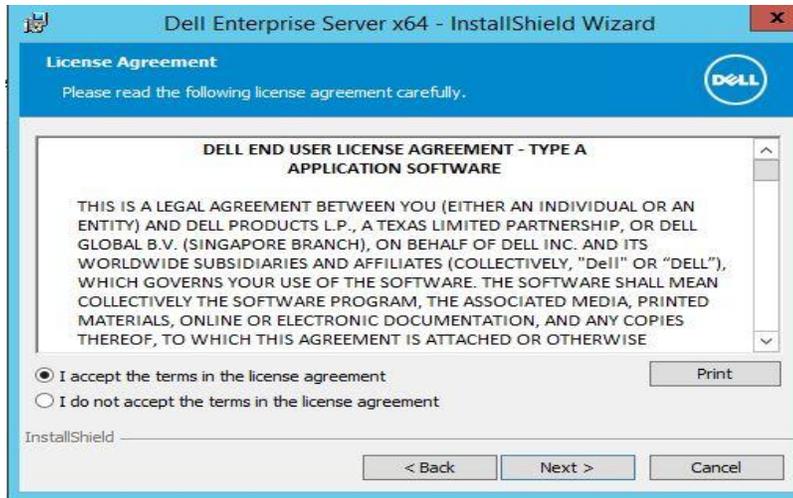
### 4. Welcome



Welcome wizard that will guide you through the installation process. Click **Next**.

### 5. License Agreement



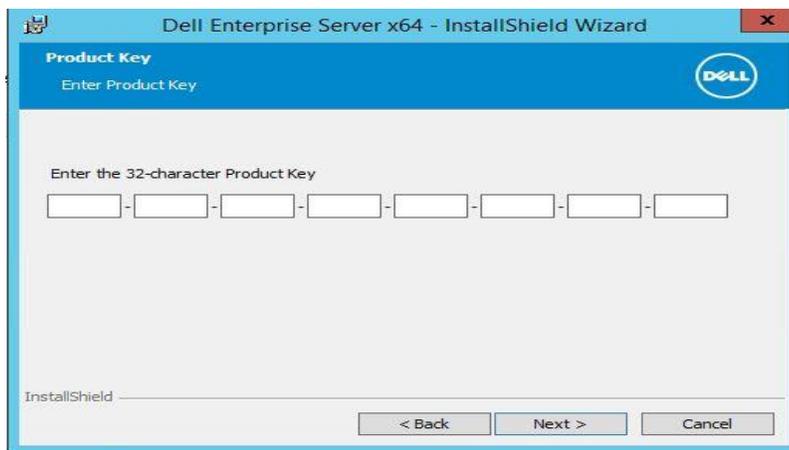


This is the license agreement review by using the scroll bar located on the right hand side or alternatively Click **Print** to print agreement.

Click **I accept the terms in the license agreement.**

Click **Next.**

#### 6. Product Key



Enter the Product Key, if you copied the EnterpriseServerInstallKey.ini as outlined in step 1, at start of this section in the install guide, this will auto populate the Product Key information. Otherwise open the EnterpriseServerInstallKey.ini and type in code manually.

Click **Next.**

#### 7. Installation Type



Select **Back End Install (Full Enterprise Server Installation)**

Click **Next**.

#### 8. Destination Folder



You may change to another install location by clicking the **Change...** button otherwise accept the default location to install into.

Click **Next**.

#### 9. Backup Location



You may change to another install location by clicking the **Change...** button otherwise accept the default location to install into.

Click **Next**.

#### 10. Certificate



You have the choice of selecting what type of digital certificate to import into the server.

Click **Create a self-signed certificate and import in to key store**.

Click **Next**.

#### 11. Create Self-Signed Certificate



Fill in Information as needed.

Click **Next**.

## 12. Install SSOS Certificate



Click "**Create a self-signed certificate and import it to key store,**"

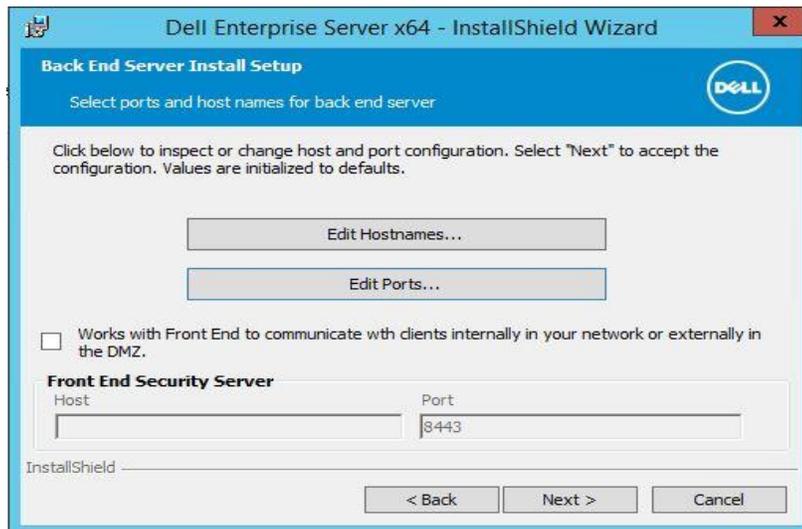
Click **Next**.

## 13. Create Self-Signed Certificate



You can elect to fill in additional information. But the required must be filled in.  
Click **Next**.

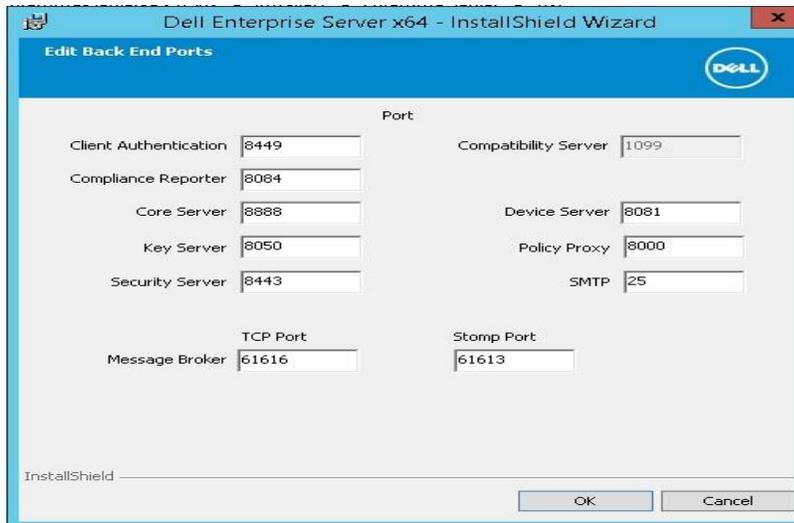
#### 14. Back End Server Install Setup



Check the ports being used.

Click **Edit Ports...**

#### 15. Edit Back End Ports

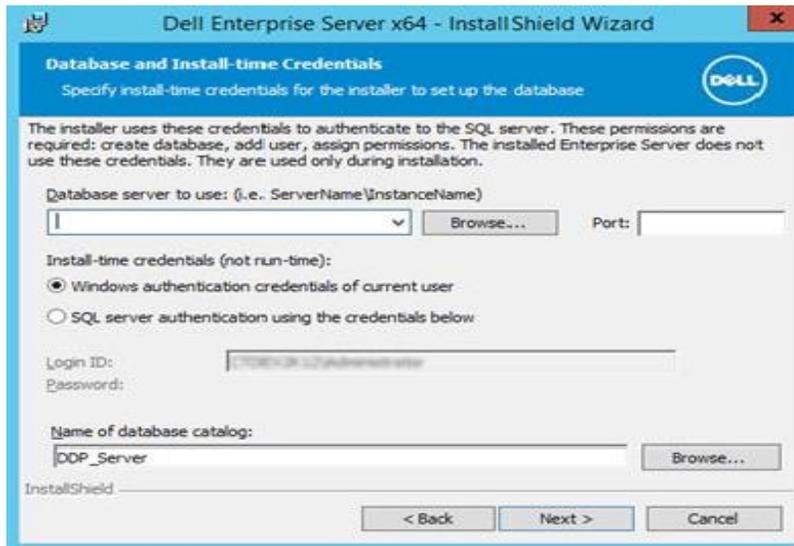


This lists the ports that are used for the Endpoint Security Suite Enterprise. Also refer to the Endpoint Security Suite Enterprise architecture diagram in Section 2.2 to make sure that the firewalls in your environment can accommodate the ports listed for Endpoint Security Suite Enterprise.

Click **OK**.

Click **Next**.

#### 16. Database Server



This is where you will configure the database connection for your environment to work.

Click **Browse** to select the server on which to install the database.

Server: **someSQLDBName**.

Port: 1433 –default port unless this has been changed in environment.

Select the authentication method for the installer to use to set up the Dell Data Protection database. After installation, the installed product does not use the credentials specified here.



Select connect using either Windows authentication or Server authentication.

Windows authentication credentials of current user - If you choose Windows Authentication, the same credentials that were used to log in to Windows will be used for authentication (User Name and Password fields will not be editable). Ensure that the account has system administrator rights and the ability to manage the SQL Server.

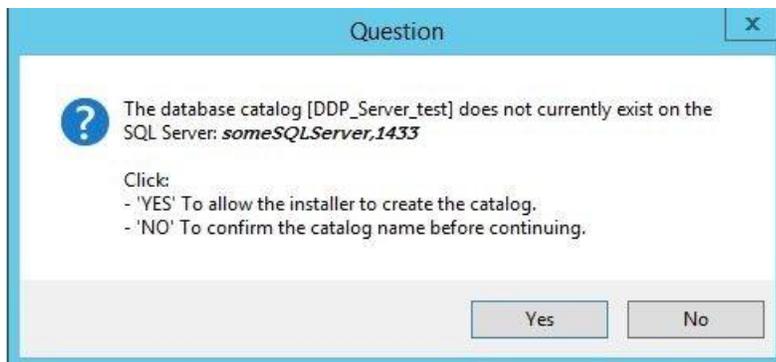
OR

SQL server authentication using the credentials below – If you use SQL authentication, the SQL account used must have system administrator rights on the SQL Server.

The installer must authenticate to the SQL Server with these permissions: create database, add user, assign permissions.

Name of catalog: database catalogue name, unless you wish to change it. Ours we changed to *DDP\_Server\_test*

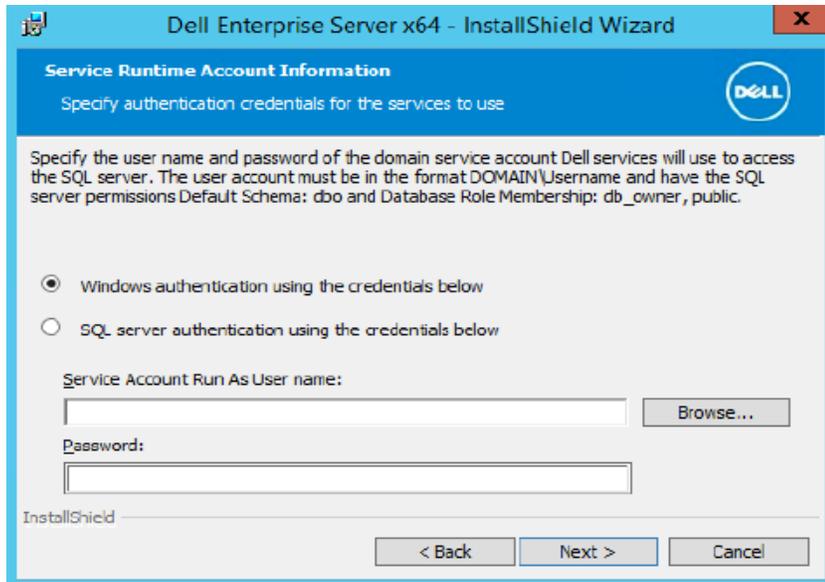
Click **Next**.



The Question relates to the fact that the database does not contain the catalog that has been specified. Shown above is an example table name we used.

Click **Yes**.

## 17. Service Startup Account Information



Select the authentication method for the product to use. This step connects an account to the product.

Windows authentication using the credentials below - Enter the credentials for the product to use, and click **Next**.

Ensure that the account has system administrator rights and the ability to manage the SQL Server. The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: db\_owner, public.

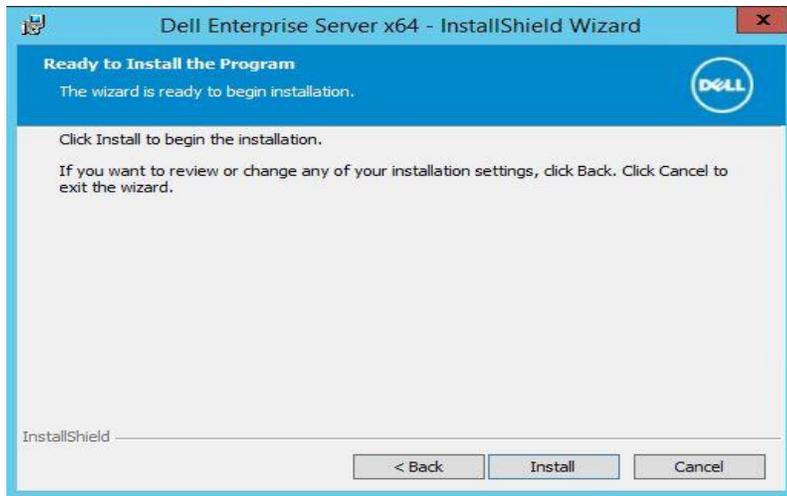
These credentials are also used by Dell services as they work with the Dell Enterprise Server.

OR

SQL server authentication using the credentials below – Enter the SQL Server credentials for the Dell services to use as they work with the Dell Enterprise Server, and click **Next**.

The user account must have the SQL Server permissions Default Schema: dbo and Database Role Membership: db\_owner, public.

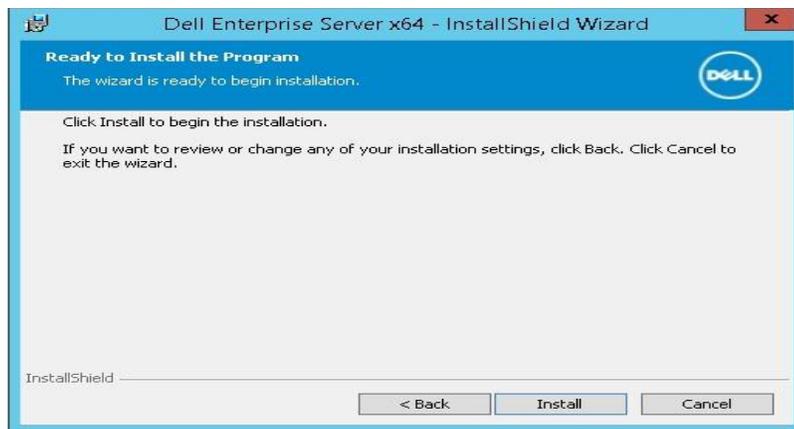
## 18. Ready to Install



This is where you will proceed with the installation of the software, at this point you can use the back button to step back through, to check if you need to change any settings.

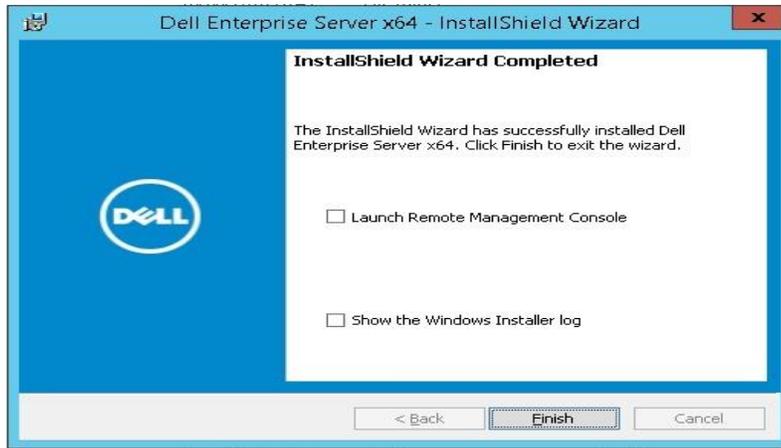
Click **Install**

#### 19. Ready to Install the Program



Click **Install.**

#### 20. InstallShield Wizard Completed



Checkbox **Launch Remote Management Console**.

Click **Finish**.

## 4.3 Virtual Edition

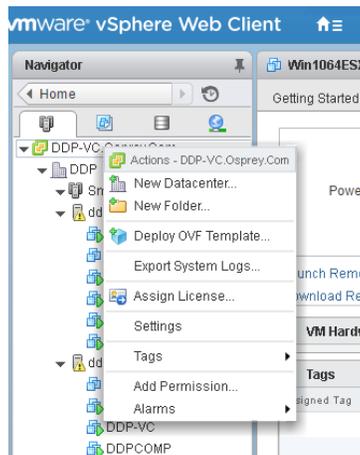
This section details the deployment and configuration of the DDP-VE appliance.

### 4.3.1 Installation

This section deals with the VE installation. Please refer to documentation in the extracted file location for further reference.

Copy the file DDP Enterprise Server - VE v9.x.x Build x.oVA. to the appropriate location.

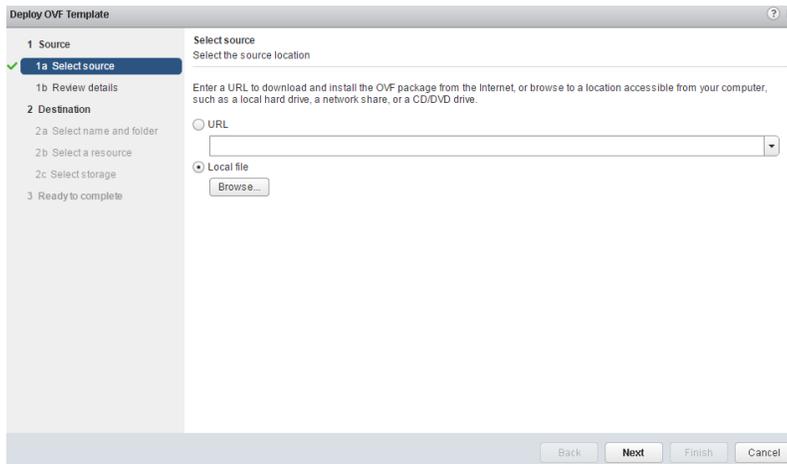
#### 1. Deploy OVF



On vSphere Web Client Right Click on top level Virtual Center location name for your infrastructure.

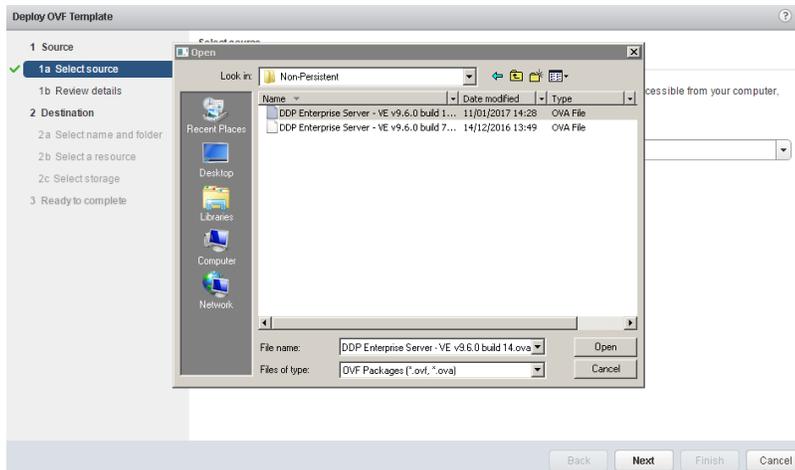
Select **Deploy OVF Template...**

## 2. Select Source.



Click **Local file**, Click **Browse...** button.

## 3. Select OVF.

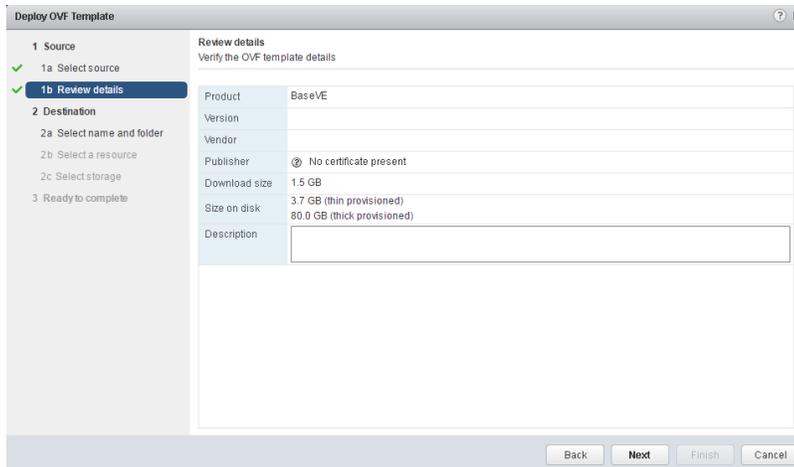


Navigate to the path where you extracted the DDP-Enterprise-Server-VE-9.6 zip file

Select the OVA file.

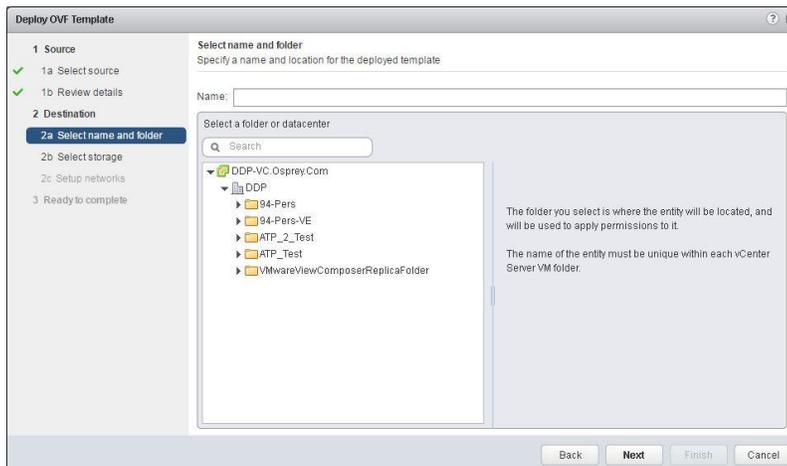
Click **Open**.

## 4. Review Details



Click **Next**.

## 5. Select Name and Folder

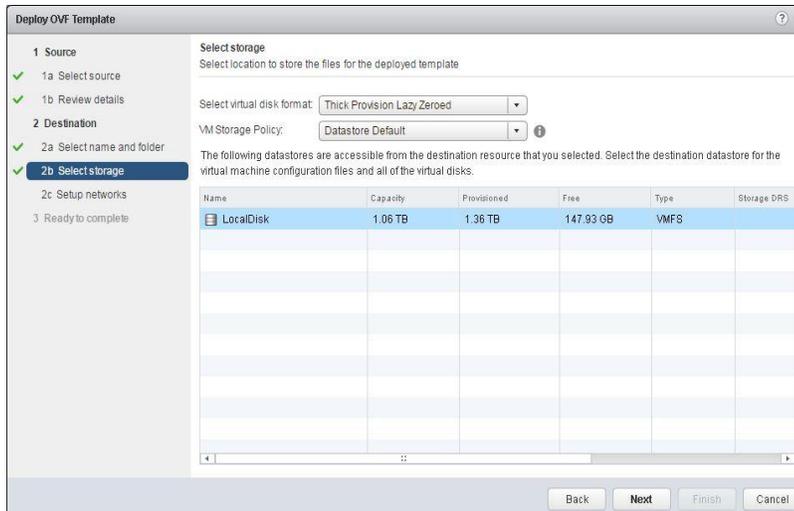


Name: **enterName** for VE,

Click **datacenter icon**

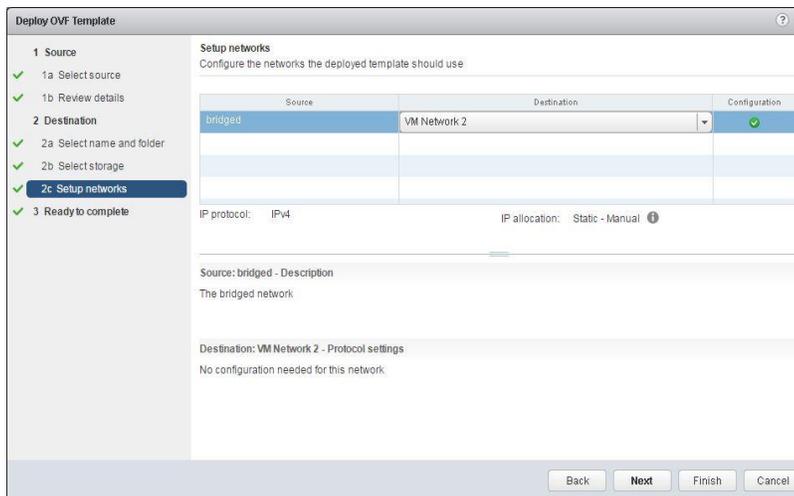
Click **Next**.

## 6. Select storage



Click **Next**.

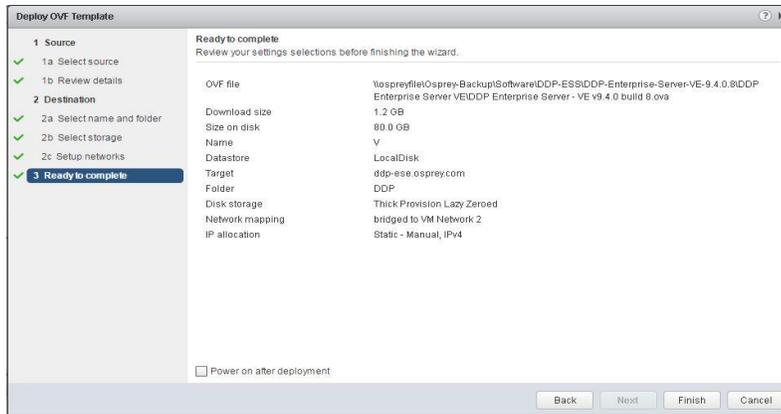
## 7. Setup networks



Change the networks if needed.

Click **Next**.

## 8. Ready to complete

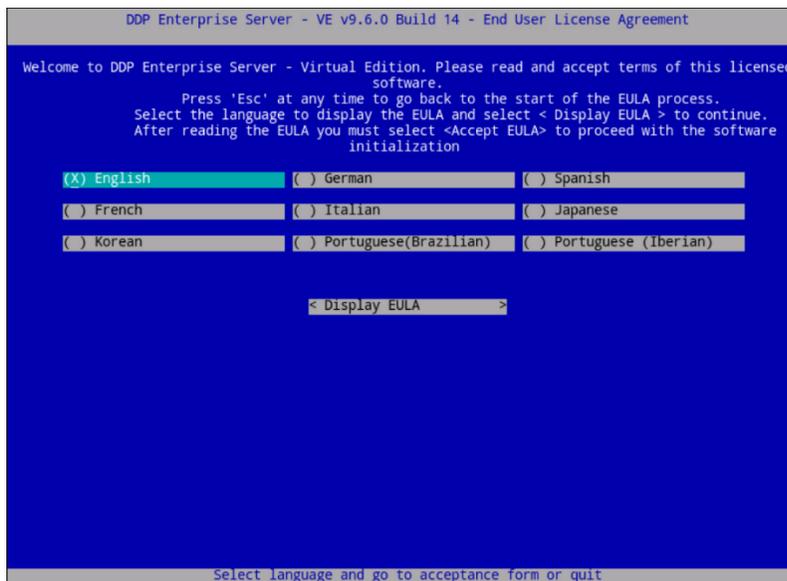


Click **Finish**.

**Note:** This may take some time to complete, this step must complete before continuing onto the appliance configuration.

## 4.3.2 VE Configuration

### 1. End User License Agreement



Press the **Enter Key** to select English, and

Use arrow key to navigate to **< Display EULA >**.

### 2. Display EULA

DELL END USER LICENSE AGREEMENT - TYPE A  
APPLICATION SOFTWARE

THIS IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR AN ENTITY) AND DELL PRODUCTS L.P., A TEXAS LIMITED PARTNERSHIP, OR DELL GLOBAL B.V. (SINGAPORE BRANCH), ON BEHALF OF DELL INC. AND ITS WORLDWIDE SUBSIDIARIES AND AFFILIATES (COLLECTIVELY, "DELL" OR "DELL"), WHICH GOVERNS YOUR USE OF THE SOFTWARE. THE SOFTWARE SHALL MEAN COLLECTIVELY THE SOFTWARE PROGRAM, THE ASSOCIATED MEDIA, PRINTED MATERIALS, ONLINE OR ELECTRONIC DOCUMENTATION, AND ANY COPIES THEREOF, TO WHICH THIS AGREEMENT IS ATTACHED OR OTHERWISE ASSOCIATED (the "Software" or "SOFTWARE"). PLEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY, INCLUDING, WITHOUT LIMITATION, ANY SUPPLEMENTAL TERMS AND CONDITIONS APPEARING OR REFERENCED BELOW, WHICH ARE HEREBY MADE PART OF THIS END USER LICENSE AGREEMENT (COLLECTIVELY, "EULA"), BEFORE DOWNLOADING, INSTALLING, ACTIVATING AND/OR OTHERWISE USING THE SOFTWARE. BY EXPRESSLY ACCEPTING THESE TERMS OR DOWNLOADING, INSTALLING, ACTIVATING AND/OR OTHERWISE USING THE SOFTWARE, YOU ARE AGREEING THAT YOU HAVE READ, AND THAT YOU AGREE TO COMPLY WITH AND TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS EULA AND ALL APPLICABLE LAWS AND REGULATIONS IN THEIR ENTIRETY WITHOUT LIMITATION OR QUALIFICATION. IF YOU DO NOT AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS EULA, THEN YOU MAY NOT DOWNLOAD, INSTALL, ACTIVATE OR OTHERWISE USE ANY OF THE SOFTWARE AND YOU MUST PROMPTLY RETURN THE SOFTWARE AND ANY HARDWARE TO WHICH IT IS ATTACHED, AS DIRECTED BY DELL OR ITS RESELLER (IF APPLICABLE) FOR A FULL REFUND. IF YOU ARE AN INDIVIDUAL REPRESENTING AN ENTITY, YOU ACKNOWLEDGE THAT YOU HAVE THE APPROPRIATE AUTHORITY TO ACCEPT THESE TERMS AND CONDITIONS ON BEHALF OF SUCH ENTITY.

## 1. License.

Provided that Dell receives timely payment for the Software and you comply with the terms, conditions and restrictions of this EULA (as a condition to the grant below), Dell hereby grants you a limited, personal, nonexclusive, nontransferable, non-assignable license, without rights to sublicense, to install or have installed, display and use the Software (in object code only) solely for internal business purposes, only on as many computers, devices and/or in such configurations as expressly permitted by Dell (e.g., as set forth

Use Arrow keys or Pg-Up/Dwn to move in text

Use Arrow Keys or Pg-Up/Down to move in text.

## 24. Entire Agreement.

Unless you have entered into another written agreement with respect to the Software which has been signed by you and an authorized representative of Dell and which conflicts with the terms of this EULA, you agree that this EULA supersedes all prior written or oral agreements, warranties or representations, including any and all other click-wrap, shrink-wrap or similar licenses or agreements, with respect to use of the Software. No amendment to or modification of this EULA, in whole or in part, will be valid or binding unless it is in writing and executed by authorized representatives of both parties. If any term (or part thereof) of this EULA is found to be invalid or unenforceable, the remaining provisions (including other valid parts within the effected term) will remain effective. You agree that any principle of construction or rule of law that provides that an agreement shall be construed against the drafter shall not apply to the terms and conditions of this EULA. No rights may arise by implication or estoppel, other than those expressly granted herein.

## 25. Notices.

Notice to Dell under this EULA must be in writing and sent to the address below or to such other address (including facsimile or e-mail) as specified in writing, and will be effective upon receipt.

Dell Inc., Attn: Dell Legal  
One Dell Way, Round Rock, Texas 78682  
Last rev. 072712

Supplemental Terms and Conditions:

END OF DOCUMENT

Dell Global EULA Type A- Revision Date 7-27-12

< Accept EULA > < Decline >

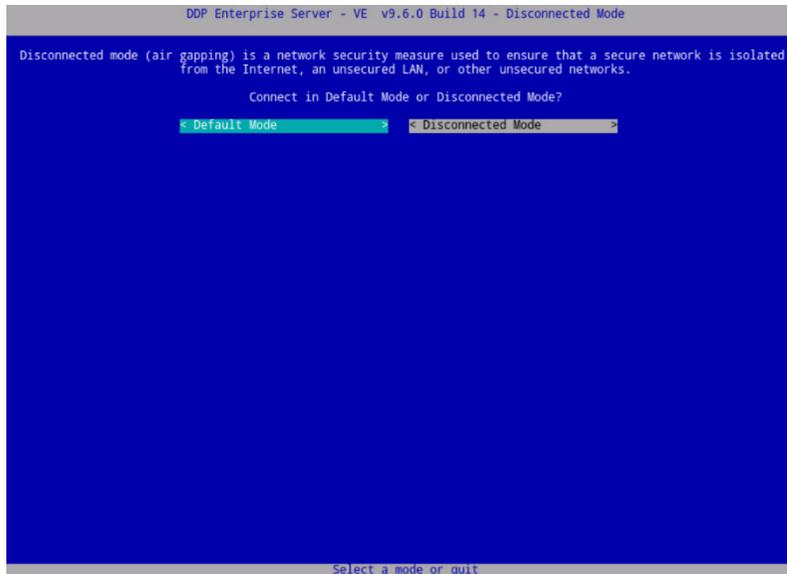
Use Arrow keys or Pg-Up/Dwn to move in text

Use arrow key to select < **Accept EULA** >.

Press the **Enter Key**.

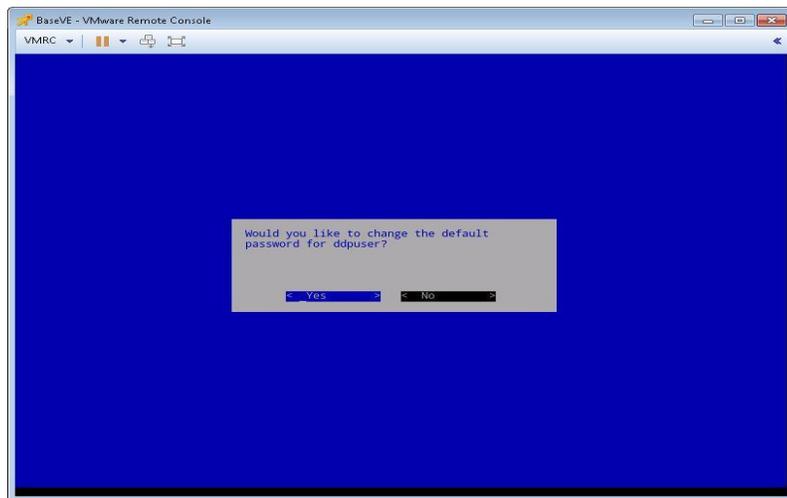
3. Select Default Mode.





Press the **Enter Key**.

4. Change ddpuser password



Select < **Yes** >.

Press the **Enter Key**.

5. Password

The New Password shown below is an example, enter a password that meets your organization's and the following requirements:

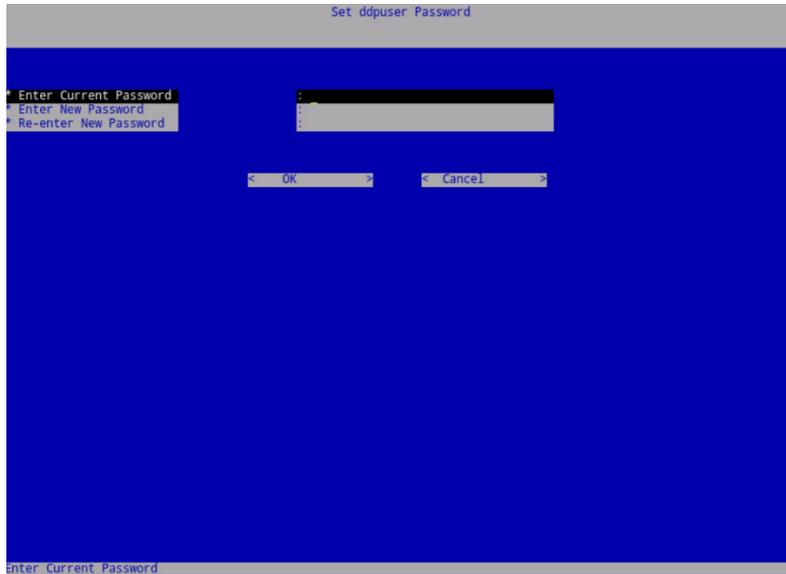
At least 8 characters•



At least 1 uppercase letter•

At least 1 digit•

At least 1 special character

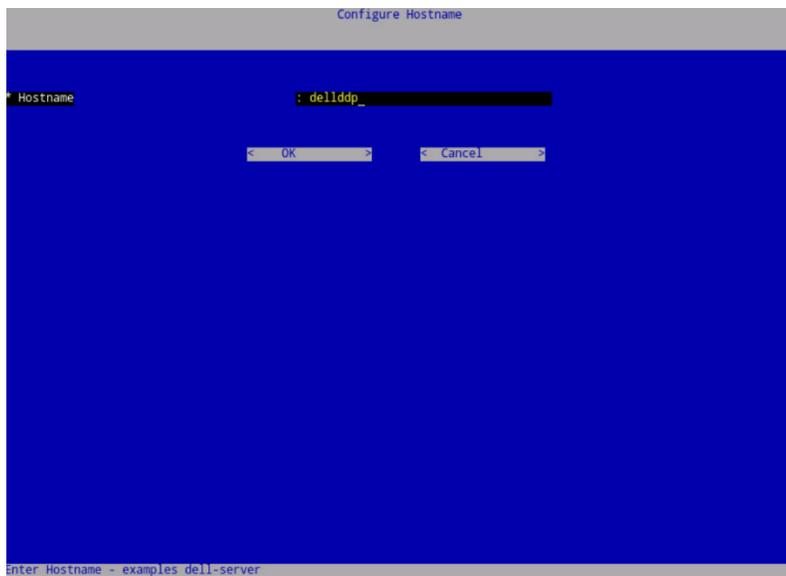


Enter Current (Default) Password: **ddpuser**

Enter New Password: **typeNewPassword**

Re-Enter New Password: **typeNewPassword**

## 6. Configure Hostname

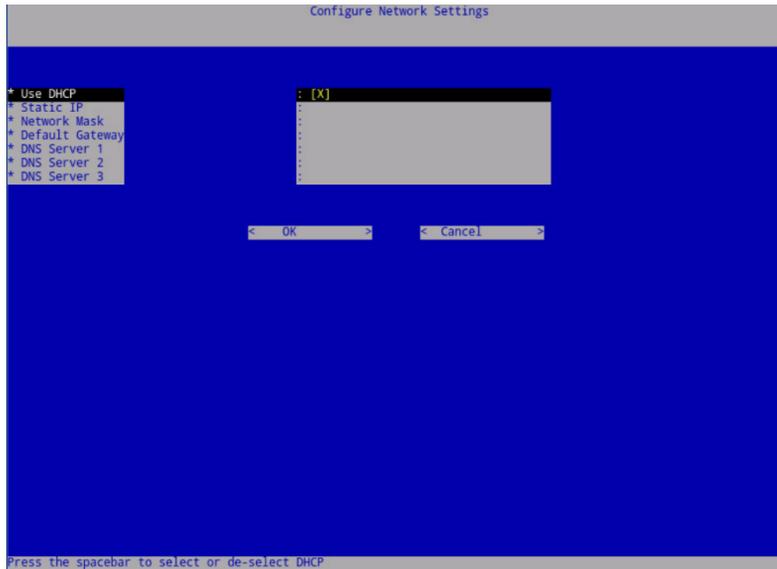


Hostname: **changeThis**

Select < **OK** >.

Press the **Enter Key**.

## 7. Configure Network Settings

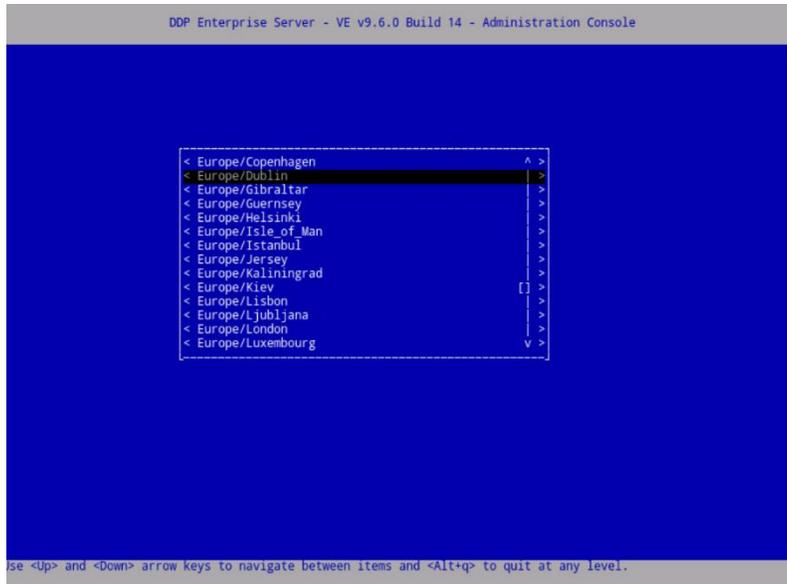


You can elect to change network setting here or finish the wizard and change afterwards.

Select < **OK** >.

Press the **Enter Key**.

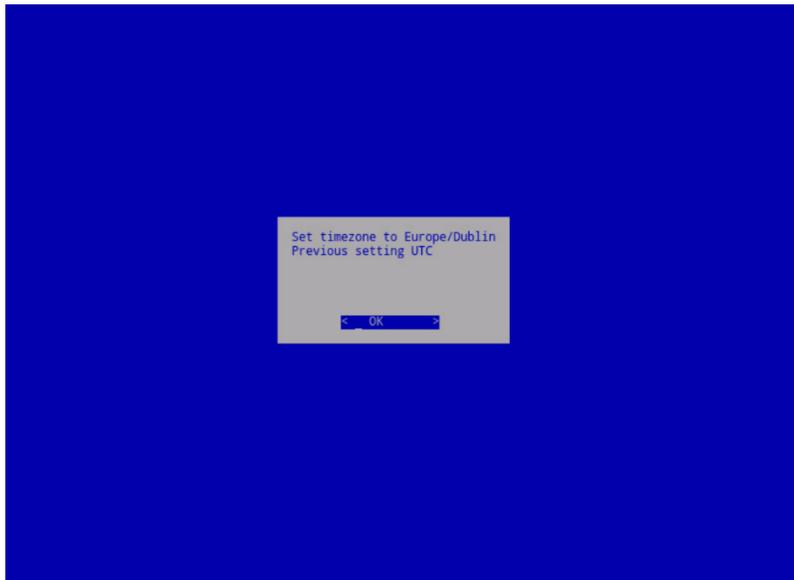
## 8. Time Zone



Select time zone from list.

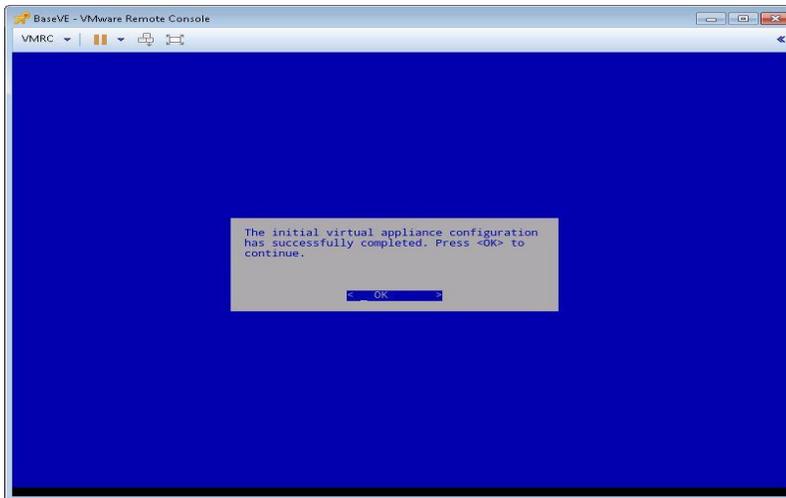
We selected Europe / Dublin as an example.

#### 9. Select TimeZone



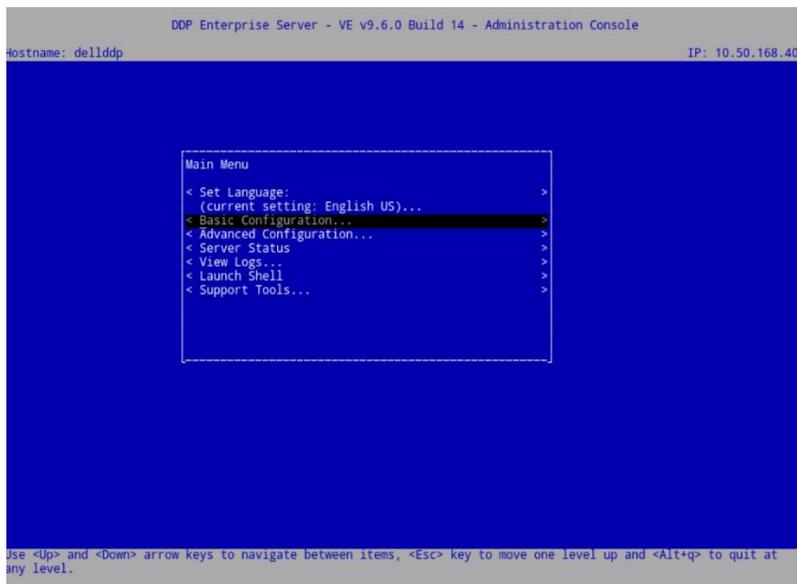
Press the **Enter Key**.

#### 10. Complete Installation



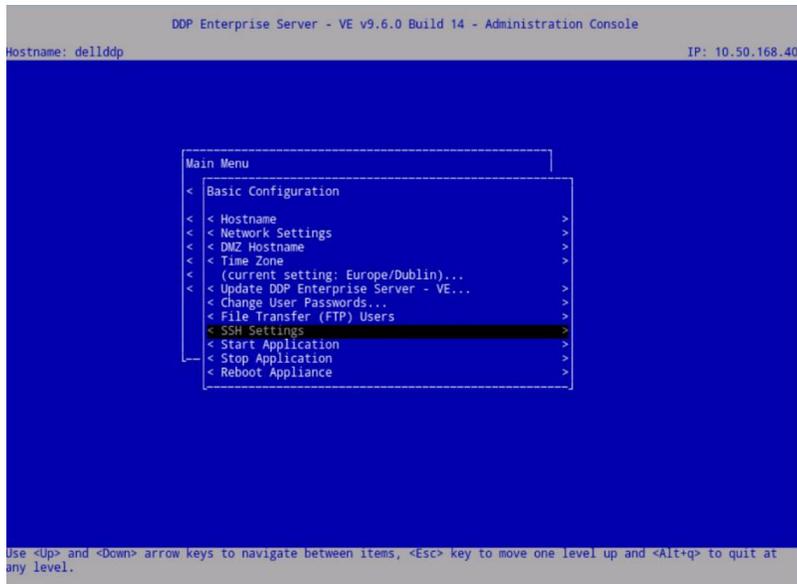
Press the **Enter Key**.

## 11. Secure Shell



Move down arrow key to **Basic Configuration...**

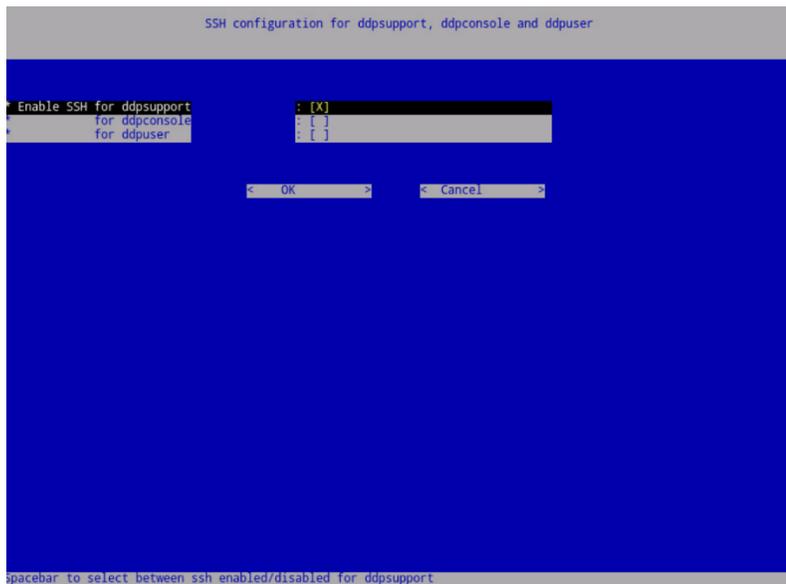
Press the **Enter Key**.



Select SSH Setting from menu.

Press the **Enter Key**.

## 12. SSH Configuration for users

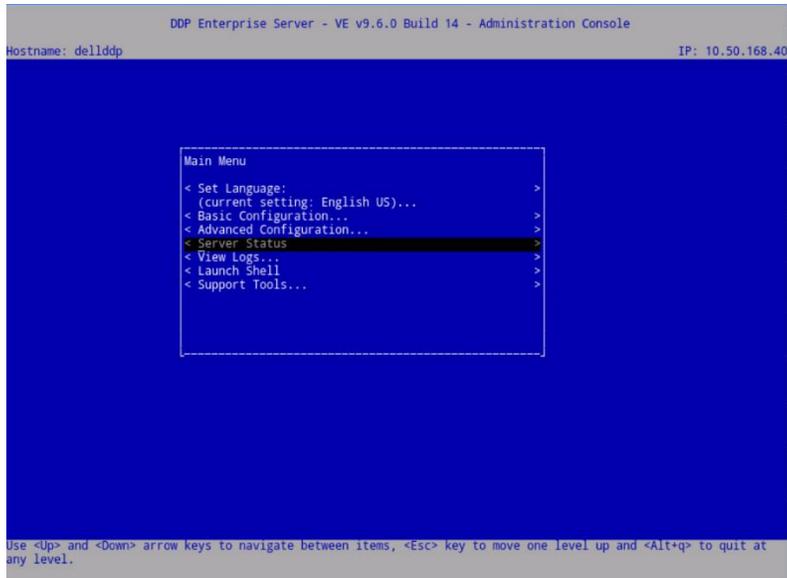


Enable for user in list by pressing **Space Bar** and using the cursor keys.

Highlight **< OK >**.

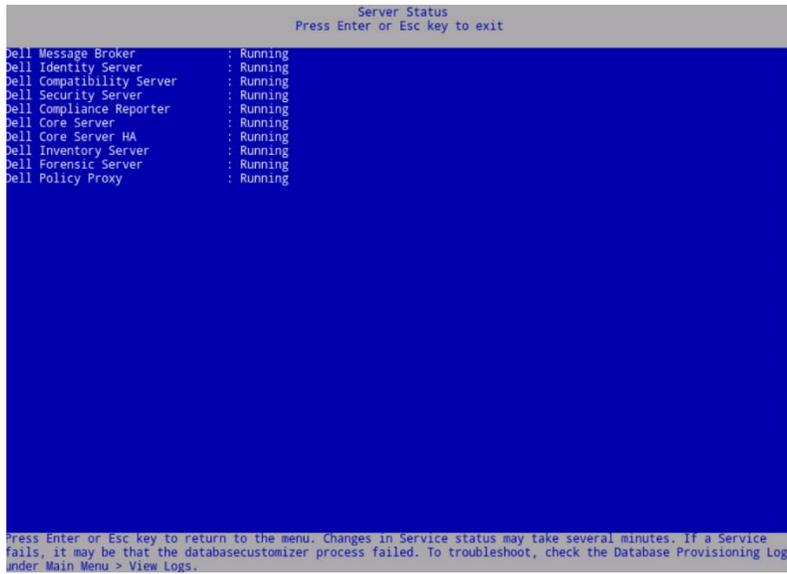
Press the **Enter key**.

## 13. Server Status



Select **Server Status** from Main Menu.

Press **Enter** key.



Check that **Running** is next to each service. Wait for all services to start before continuing.

Press the **Enter Key** or **Esc Key** to go back to the Main Menu.



## 5 Client Installation (Persistent or Non-Persistent)

Endpoint Security Suite Enterprise client installation is performed on the master image for both [persistent](#) and [non-persistent](#) VDI solutions.

### 5.1 VMware View Agent

This section details the Horizon Agent install.

**Note:** The VMware View Agent is only installed into the Master virtual machine.

#### 1. Run installer

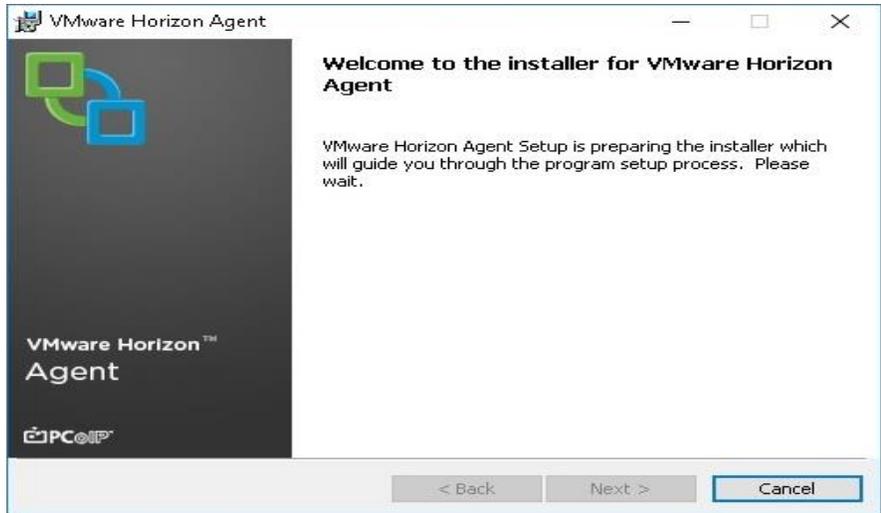


Right **Click** on **VMWare-Viewagent-x86\_64-7.0.1-XXXX**

Select **Run as administrator**.

**Note:** This may take a while to open.

#### 2. Welcome to the installer for VMware Horizon Agent.



Click **Next**

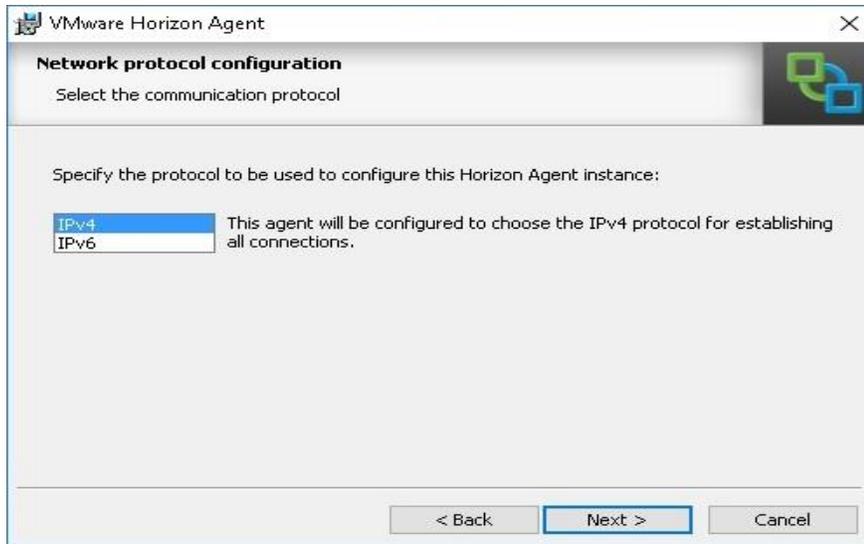
### 3. License Agreement



Select **I accept the terms in the license agreement.**

Click **Next**

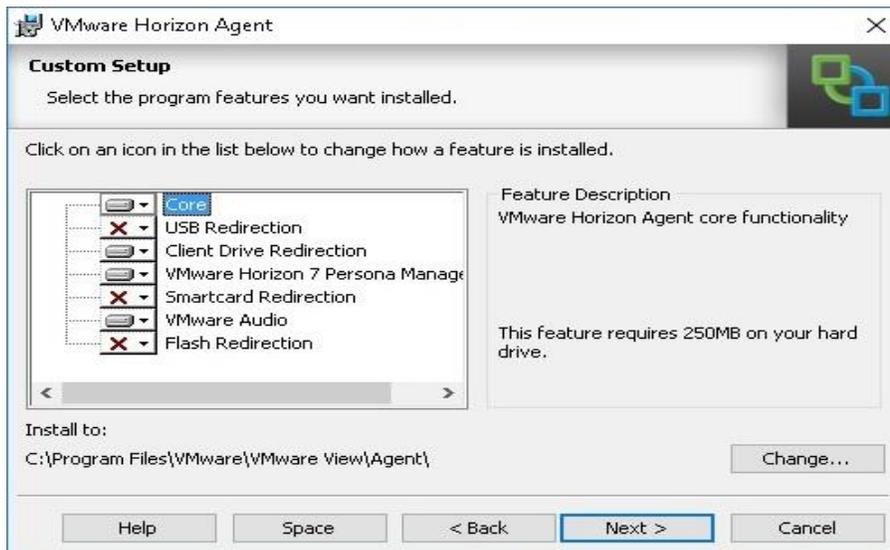
### 4. Network protocol configuration



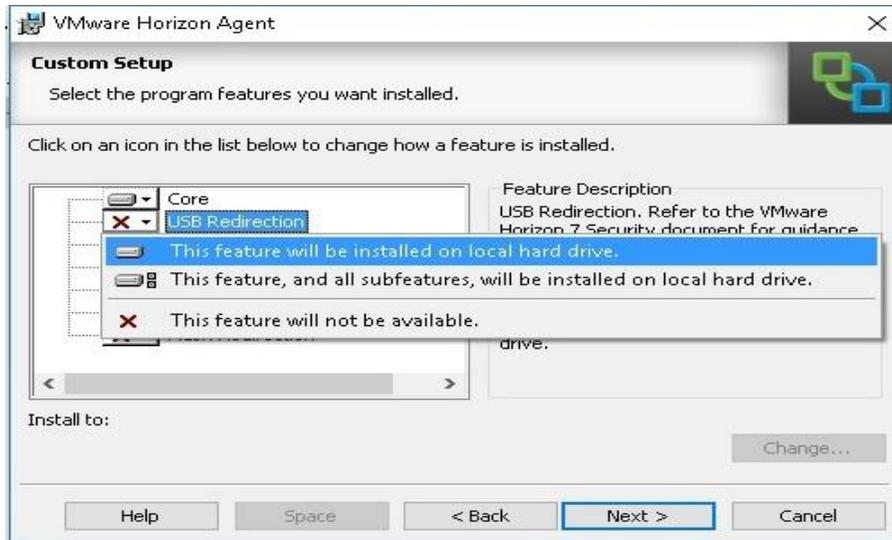
In our example we used IPv4.

Click **Next**

## 5. Custom Setup

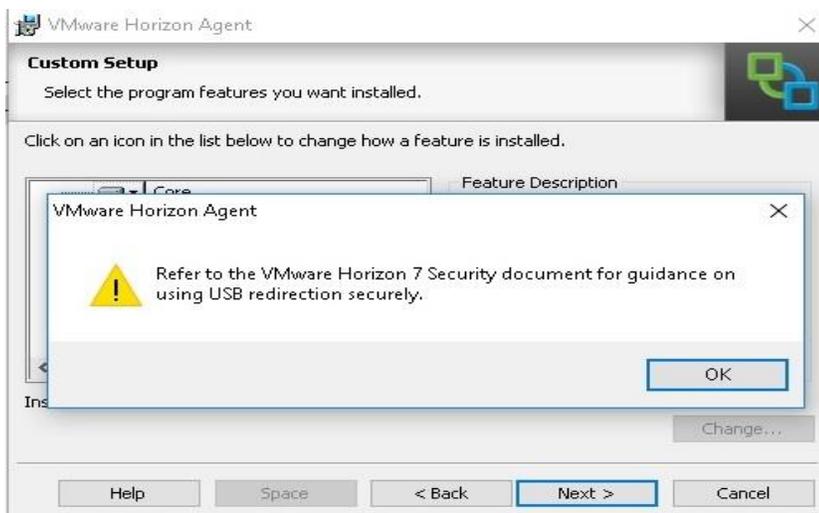


Select **USB Redirection**.



Select **This feature will be installed on local hard drive.**

## 6. VMware Horizon Agent



Click **OK**

Click **Next**

## 7. Register with Horizon 7 Connection Server

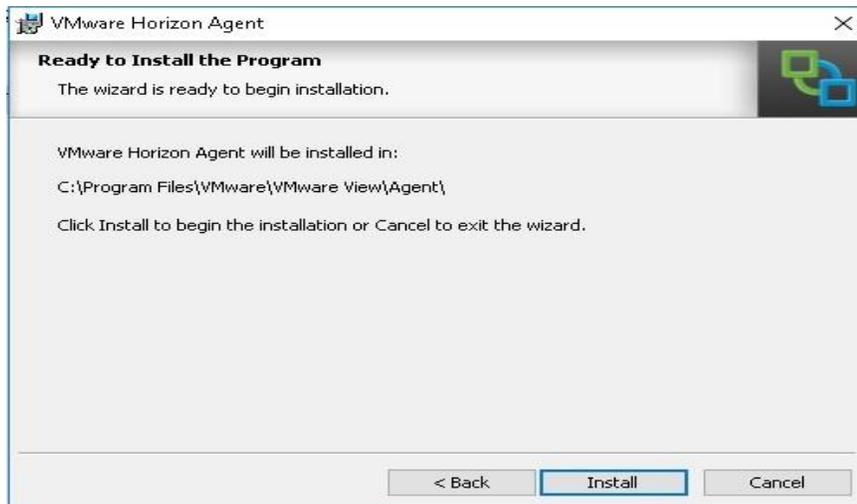


Enter **View Connection Server IP address or hostname**

Authentication: **Specify account or continue with currently logged on user**

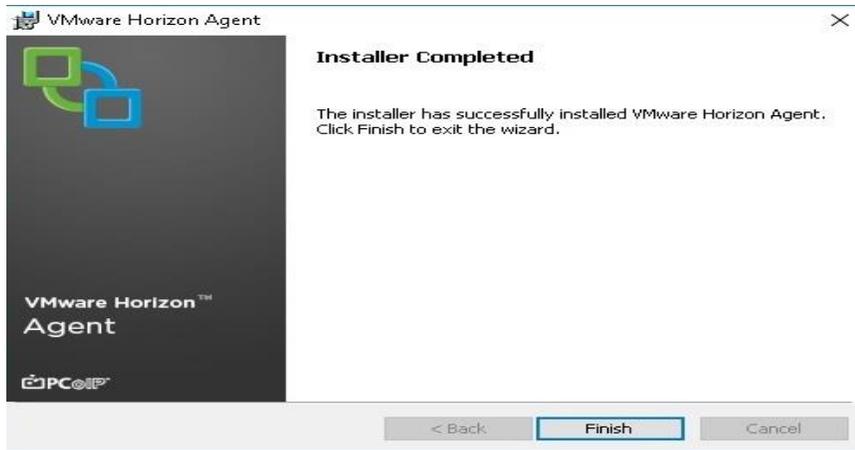
Click **Next**

#### 8. Ready to Install the Program



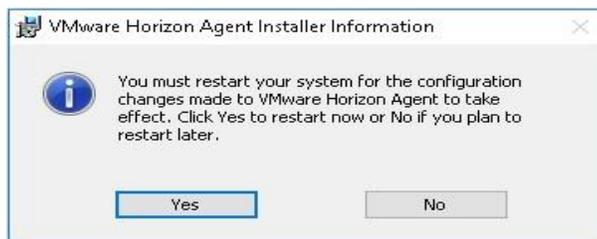
Click **Install**

#### 9. Installer Completed



Click **Finish**

#### 10. VMware Horizon Agent Installer Information



Click **Yes**

This will reboot the master VM.

## 5.2 Advanced Threat Prevention (ATP) Install

Note: ATP can be installed on persistent or non-persistent desktops

1. Create Master VM and install applications user will need. Install the Endpoint Security Suite Enterprise client at this point as described later in this document.
2. Create Desktop pool of either persistent or non-persistent desktops on Horizon administration console.

Refer to section 6.2.1 section below for ATP policy configuration.

## 5.3 Policy-Based Encryption (PBE) Install

Note: Policy-Based Encryption will not encrypt network drives by design. It can be installed on persistent or non-persistent desktops.

1. Create Master VM and install applications user will need. Install the Endpoint Security Suite Enterprise client at this point as described in section 5.7.1 and 5.7.3 following.
2. Refer to Endpoint Security Suite Enterprise documentation for scripted or System Center Configuration Manager (SCCM) deployment methods.

Note: Step 2 is beyond the scope of this document.

## 5.4 System Data Encryption (SDE)

Note: DO NOT enable SDE in a VDI environment or Encrypt Windows Page File. This configuration is not supported. If this feature is turned on the host will experience high disk IO and CPU utilization due to a file encryption sweep occurring that will affect the VM's that are assigned this policy. Contact Dell Support for assistance if this policy needs to be configured in the environment.

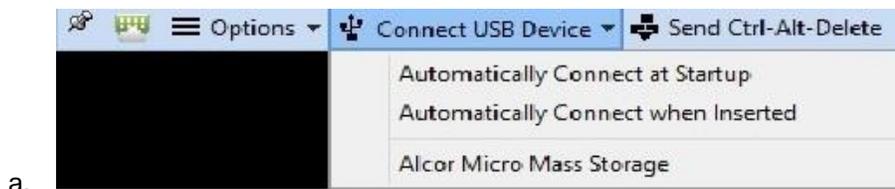
## 5.5 Removable Media Encryption (EMS) Install

Note: If you wish to install the EMS piece only and not ATP at the same time, Create desktops using the steps listed below. It can be installed on persistent or non-persistent desktops

1. Create Master VM and install applications user will need. Install the Endpoint Security Suite Enterprise client at this point as described in section 5.7.1 and 5.7.3 following.
2. When the Endpoint Security Suite Enterprise client is installed shutdown the machine but do not restart it.
3. Create Desktop pool of either persistent or non-persistent desktops on Horizon administration console.
4. Verify USB redirection in user's session.
  - a. From VMWare pull down menu located at top of VDI session, the following Icons should be visible.
  - b. 
  - c. **If the devices marked above do not appear in session menu then USB redirection is not enabled or session needs to be updated.**

**Note:** Refer to the VMware Horizon 7 security document for guidance on using USB redirection securely.

5. Insert Removable media



- b. Click **Devices**, in our example the USB device is an Alcor Micro Mass Storage.
- c. Click **Alcor Micro Mass Storage**.
- d. Refer to section 6.2.5 section below for EMS policy configuration.

## 5.6 Authentication

Note: The authentication features in Endpoint Security Suite Enterprise is not supported for virtual desktops at this time. It is only supported on physical PCs: please refer to vendor documentation

## 5.7 Endpoint Security Suite Enterprise Install

This section details the Endpoint Security Suite Enterprise client installation on client sessions. For all VDI installations for persistent or non-persistent desktops, follow the client install directions on the master image and make the registry changes documented below to differentiate between persistent and non-persistent desktops.

### 5.7.1 Client Install

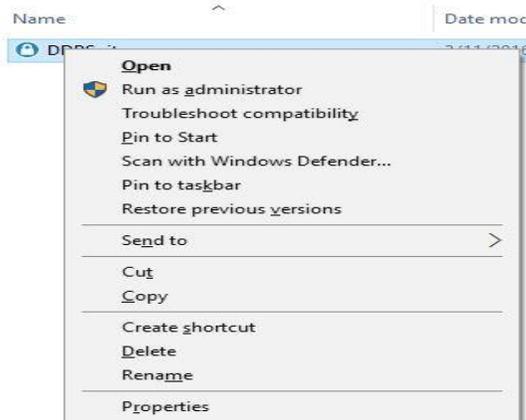
For VDI installations, the Endpoint Security Suite Enterprise client install installs the Encryption client and Advanced Threat Prevention agent. All other software including any VDI agents must already be installed. The Endpoint Security Suite Enterprise client install and setup of registry entries must be the last task performed on the master image before deployment. The master image should not be restarted before deployment.

In order to prevent the master image performing an activation before deployment with the Dell Server set the following for the correct Endpoint group (Non-Persistent/Persistent VDI Endpoint group) on the Dell Server

- Turn off Policy Based Encryption
- Turn off Advanced Threat Protection

See the appendix section for instructions

#### 1. File Extraction



Locate the **DDPSuite.exe** file, which should be where you copied or downloaded the software.

Right Click, select **Run as administrator** from menu.

## 2. Extraction



Install will continue to the Welcome screen.

## 3. Welcome



On the Welcome screen, click **Next**.

## 4. License Agreement



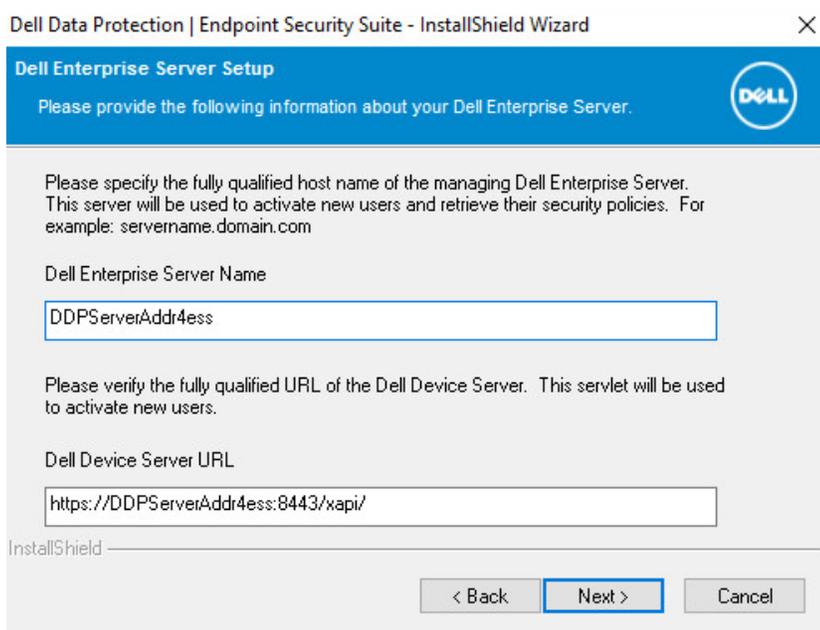
Review the license agreement by using the scroll bar located on the right hand side.

Click **Print** to print agreement.

Click **I accept the terms of the license agreement**.

Click **Next**.

#### 5. Dell Enterprise Server or VE Setup



This is where you will point the client to the Dell Server you have installed in the previous section.

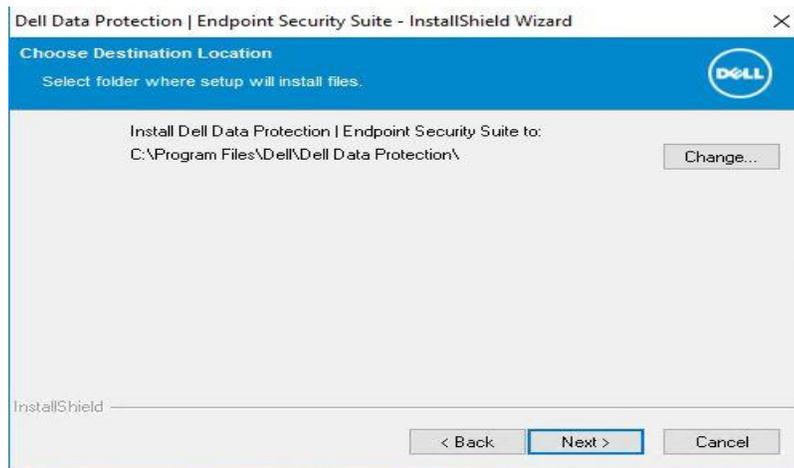
Dell Server Name: **enterDDPEEServerNameFQDN**

The Dell Device Server URL will auto-populate.

Click **Next**.



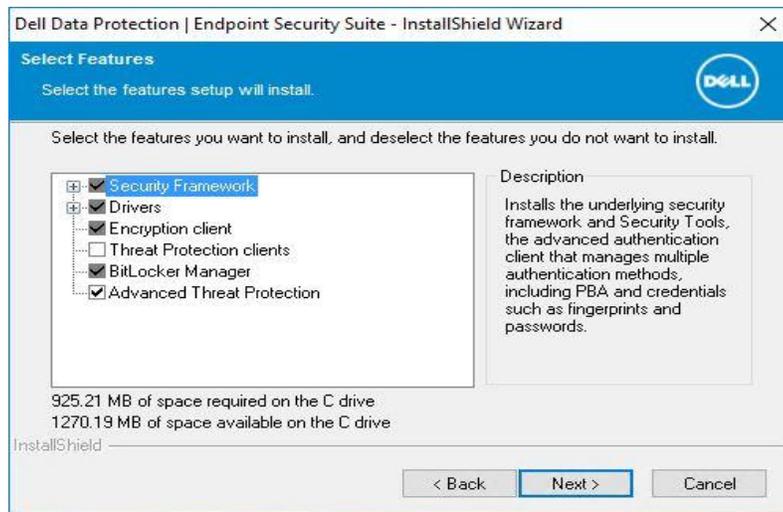
## 6. Choose Destination Location



You can change the destination location by clicking **Change...**, we proceeded with the Default destination.

Click **Next**.

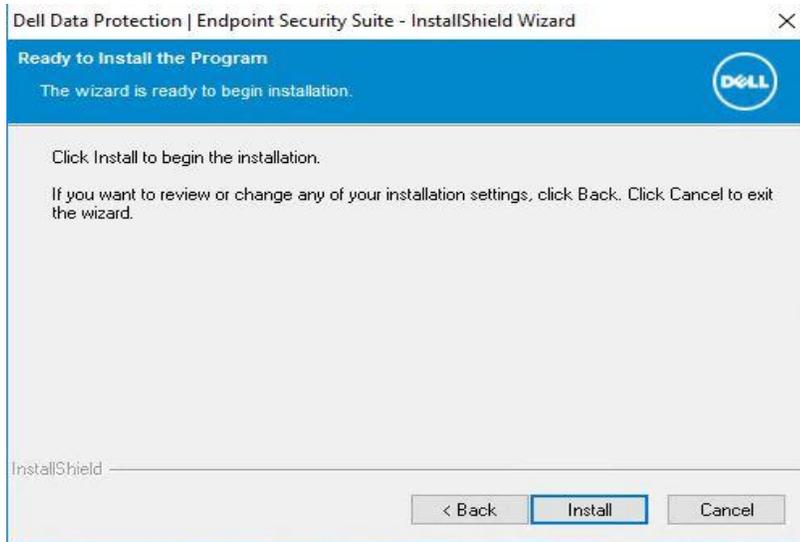
## 7. Select Features



Select **Advanced Threat Protection**.

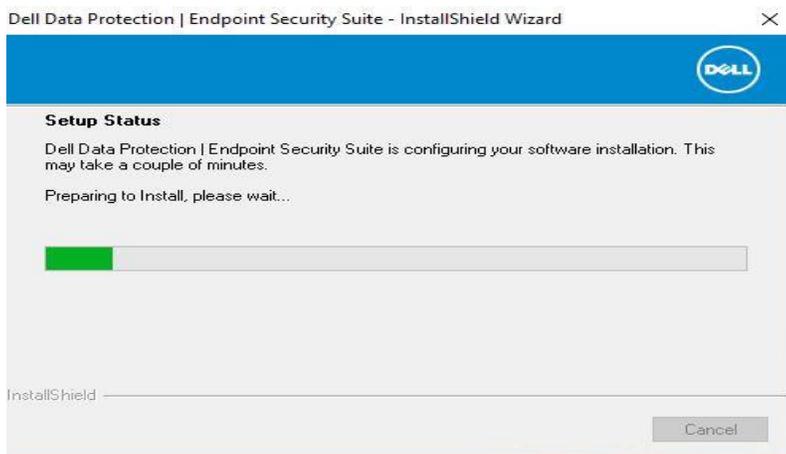
Click **Next**.

## 8. Ready to Install the Program



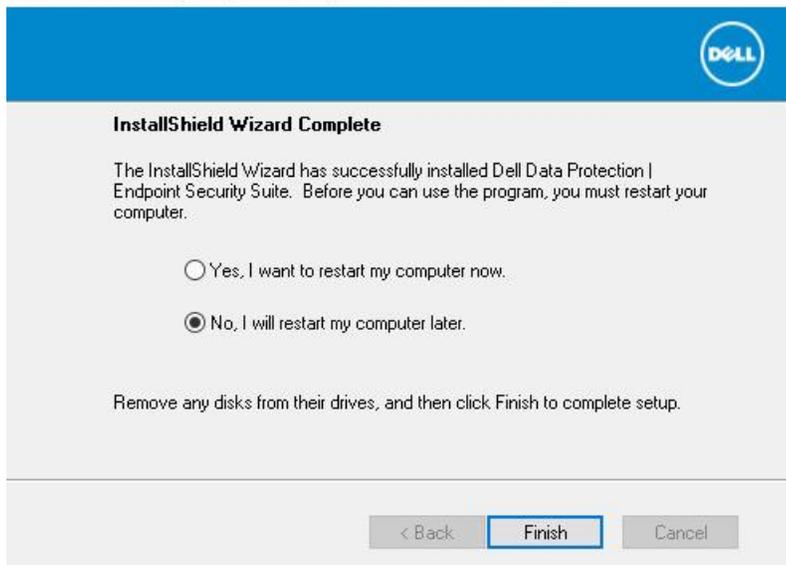
You can use the back button to check or change setting before proceeding.

Click **Install**.



The installation will take some time to complete.

## 9. Installation Wizard Complete



Default action is: **Yes, I want to restart my computer now,**

Select **No, I will restart my computer later.**

Click **Finish.**

Do not restart or shut down the VM at this stage. It is necessary to insert the registry entries that indicate that the client is running in a VDI environment.

## 5.7.2 Client manual and silent installation

This details the manual process to extract and install the components as needed, this covers in particular the ATP install.

1. Use the following command to extract the DDP Suite installer into its individual components:
  - a. From a command prompt do not run from PowerShell:
  - b. `DDPSuite.exe -y -gm2 /s /z "\"EXTRACT_INSTALLERS=C:\extracted\""`

Note: the /s option can be left out as this is the silent option, and the path can be changed to whatever suits your environment. This operation may take some time to complete.

2. Do the following to install ATP: Where the extracted installers are navigate to `extracted\AdvancedThreatProtection\Win64R`
3. At a command prompt, enter the following commands:
  - a. The following example installs the basic Dell Client Security Framework component, without the SED Management client or BitLocker Manager (silent installation, no reboot, installed in the default location of `C:\Program Files\Dell\Dell Data Protection`).`EMAgent_XXbit_setup.exe /s /v"FEATURE=BASIC CM_EDITION=1 SERVERHOST=server.organization.com SERVERPORT=8888 SECURITYSERVERHOST=server.organization.com SECURITYSERVERPORT=8443 /norestart /qn"`

- b. The following example installs Advanced Threat Prevention (silent installation, no reboot, installation log file and installation folder in the specified locations)
- c. `MSIEXEC.EXE /I "AdvancedThreatProtectionCSFPlugins_x64.msi" /qn REBOOT=ReallySuppress APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection\Plugins" /!v "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtectionPlugins.msi.log"`

and

- d. `AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection" /I "C:\ProgramData\Dell\Dell Data Protection\Installer Logs\AdvancedThreatProtection.log"`NOTE: These components must be installed by command line only. Double-clicking to install this component installs a non-Dell, non-managed version of the product, which is not supported. If this is accidentally done, simply go to Add/Remove Programs and uninstall that version.
- e. To check successful installation open Programs and Features in Control Panel and check for Cylance.

The following step will perform a completely silent install of DDP Suite.

1. From a command prompt that is started with administrative privileges run the following command:
  - a. `DDPSuite.exe -y -gm2 /S /z "\"SERVER=<server fqdn>\""`

### 5.7.3 Create registry entries for VDI awareness

In order to operate correctly in a VDI environment (Citrix or VMware) the master image must be prepared by inserting one of the following entries in the registry.

Note: Changes to the Windows registry are immediate and can have system wide consequences. There is no automatic backup taken of the registry. Ensure that you are confident to make these changes before proceeding.

#### Persistent VDI

For master images that will be used for persistent VDI solutions, add the following entry to the registry on the VM immediately after installing the Endpoint Security Suite Enterprise client. Shut down the master image once the registry change has been made.

*Windows Registry Editor Version 5.00*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment]*

*"Dell\_isVDI"=dword:1*

*"Dell\_VDI"=dword:102*

#### Non-Persistent VDI



For master images that will be used for non-persistent VDI solutions, add the following entry to the registry on the VM immediately after installing the Endpoint Security Suite Enterprise client. Shut down the master image once the registry change has been made.

*Windows Registry Editor Version 5.00*

*[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment]*

*"Dell\_isVDI"=dword:1*

*"Dell\_VDI"=dword:101*

Prior to deploying the VDI pools, ensure that Policy Based Encryption and Advanced Threat Prevention have been turned on at the DDP Server on the correct Endpoint group.

## 5.7.4 [Recomposing or updating VDI pools](#)

Any updates to the master image require that the master image is started before changes can be made. If the master image starts it will attempt to activate which will cause conflicts in the DDP Server.

In order to prevent the master image performing an activation before an update or recompose with the DDP server set the following for the correct Endpoint group (Non-Persistent/Persistent VDI Endpoint group) on the DDP server.

- Turn off Policy Based Encryption
- Turn off Advanced Threat Prevention

See appendix Section for instructions

## 6 Endpoint Security Suite Enterprise Management Console

### 6.1 Remote Management Console

The Remote Management Console is where you will configure licenses, enable and configure policies, and manage the environment.

You must first configure the Domain and Licenses before configuring the policies. The domain only needs to be configured once. Licenses can be added as needed for your environment.

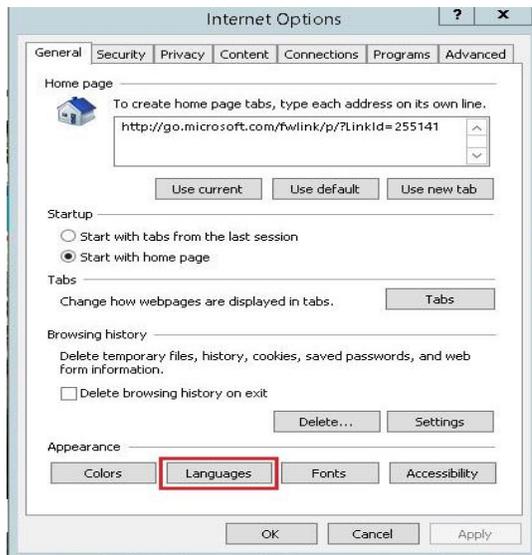
Note: This applies to both Endpoint Security Suite Enterprise and VE.

#### 6.1.1 Browser Language

The language settings must be changed to match the locale that the endpoints are set to. This is needed as endpoints will not update their policies correctly if this change is not made.

Note: The browser language changes being made are in Internet Explorer 11. If you are using a different web browser, refer to product documentation to change the language settings.

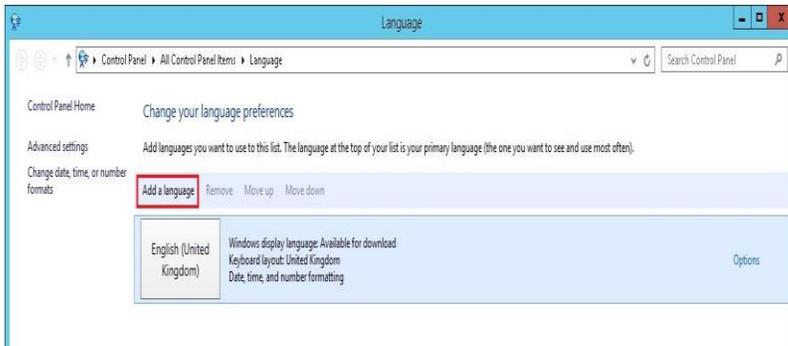
1. Launch Internet Explorer
2. Go To Tools, Internet Options



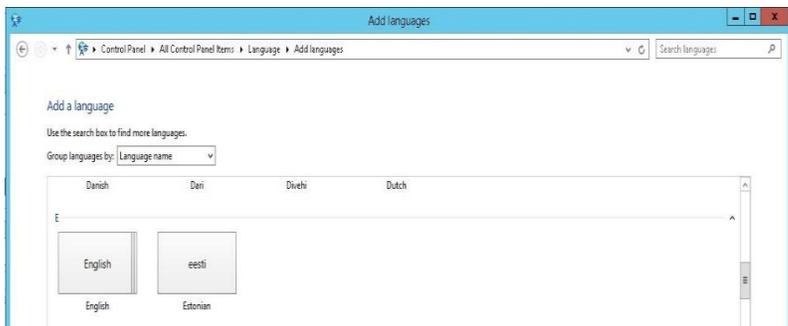
- 3.
4. Click **Languages**.
5. Language Preference



- 6.
7. Click **Set Language Preferences** button.
8. Change your language preferences



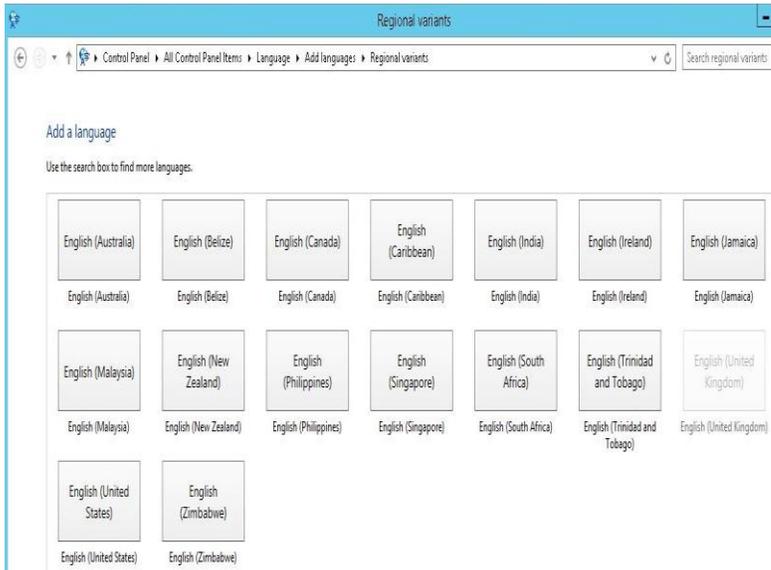
- 9.
10. Click **Add a language**
11. Add a Language



- 12.
13. Click **English**.



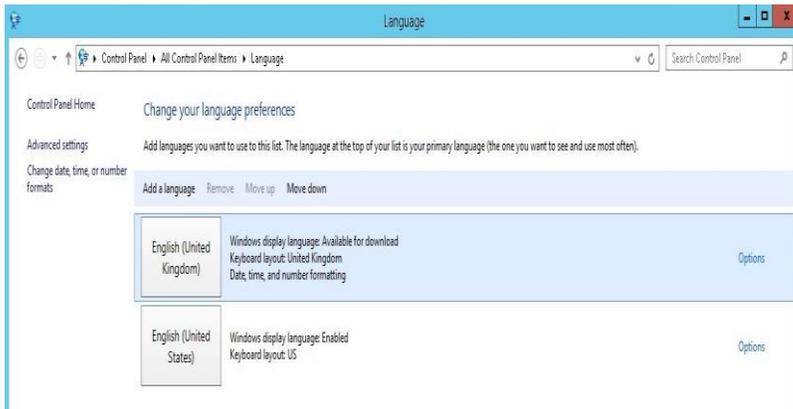
## 14. English



15.

16. Click **English (United States)**.

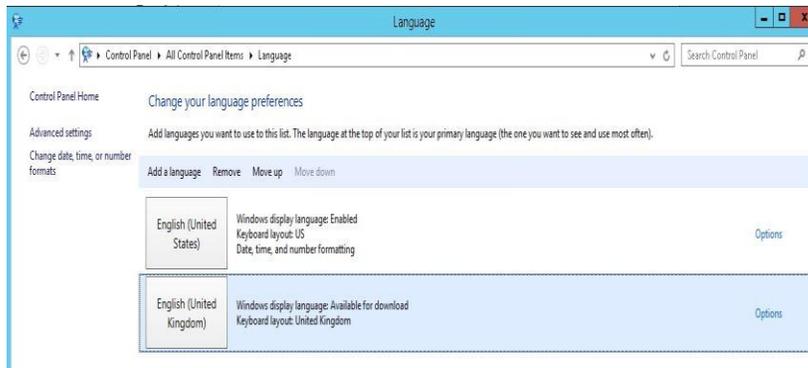
17. Change language preference



18.

19. Click first language

20. Select **Move Down** from menu bar so that English (United States) is first in the list.



21.

22. Close the Languages window.

## 6.1.2 Domain configuration

**Note:** If using Endpoint Security Suite Enterprise follow steps below, if using VE follow these steps in section 6.1.3

On the server where Dell Server or VE is installed, login and open a web browser.

1. Enter <https://serverNameFQDN:8443/webui/Login>



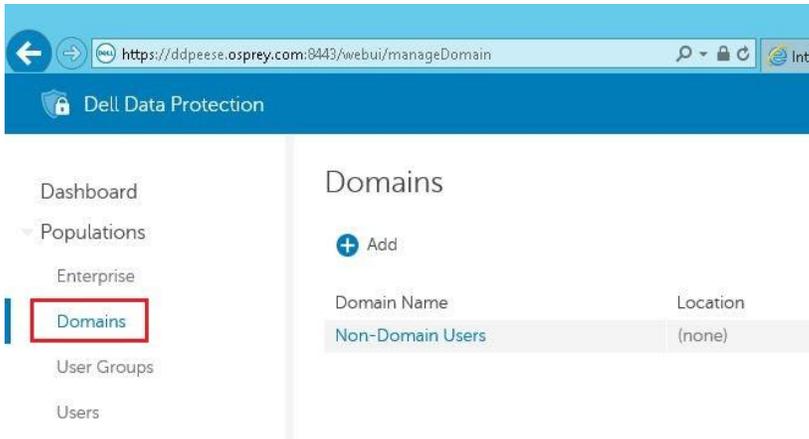
Use the following default username and password to access the management site.

**Username:** superadmin

**Password:** changeit

**Note:** Dell advises you to change the password at the earliest convenience.

2. Domain



This is where you will configure the Domain information.

Select **Domain** from the left pane, and click **Add**.

### 3. Add Domain

Host Name: **domainName**

Port: **389 or 3268**

Distinguished Name: will auto populate

User Name: account to read AD – must be UPN format **account@domain**

Password: **passwordForAccount**

Alias: **domainName** – Click Add

Click **Add Domain**

### 4. Domain Details

Domain Detail for: **someDomain**

Security Policies | **Details & Actions** | Members | Settings | Key Server

Details

Domain Name: someDomain

Location: someLocation

LDAP Url: someLDAPUrl

Status: **Good**

Once the domain is configured, check the status before continuing.

Make sure that Status is **Good**. If not, investigate immediately.

## 6.1.3 Licenses

### 1. Licenses

Dashboard

- Populations
  - Enterprise
  - Domains
  - User Groups
  - Users
  - Endpoint Groups
  - Endpoints
  - Administrators
- Compliance Reporter
- Management
  - Commit
  - Log Analyzer
  - Recover Data
  - Recover Endpoint
  - License Management**
  - Dropbox Management
  - Services Management
  - Alerts Management

License Management

Upload Licenses

**Choose File**

Client Licenses Owned

Alert	Type	Valid From	Valid To	Count	Status	
	Mobile Edition	1/1/1753 12:00 AM	12/31/9999 11:59 PM	30	None	Delete
	Shield for Server	1/1/1753 12:00 AM	12/31/9999 11:59 PM	4	None	Delete
	Enterprise Edition	1/1/1753 12:00 AM	12/31/9999 11:59 PM	30	None	Delete
	Cloud Edition	1/1/1753 12:00 AM	12/31/9999 11:59 PM	30	None	Delete
	External Media Edition	1/1/1753 12:00 AM	12/31/9999 11:59 PM	30	None	Delete

Client License Usage

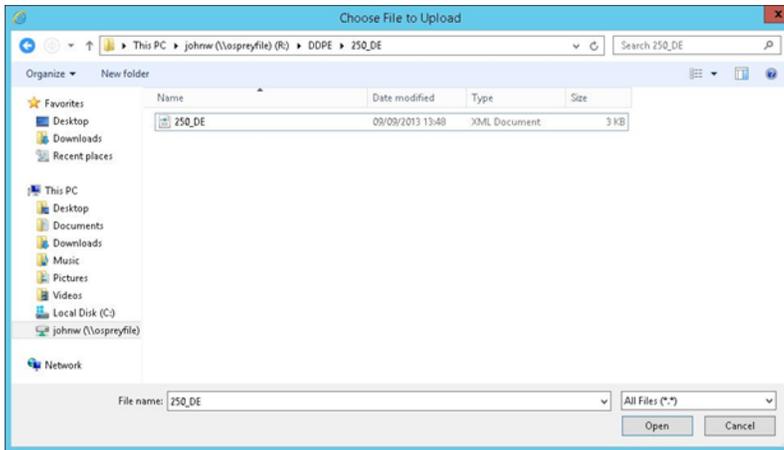
Alert	Type	Total	Used
	Enterprise Edition	10	0
	Cloud Edition	10	0
	External Media Edition	20	0
	Mobile Edition	10	0
	BitLocker Manager	20	0
	Threat Protection	10	0
	Shield for Server	4	0

You will need to add licenses to use in your environment.

Note: License details are beyond the scope of this document. Contact your Dell Sales Representative or ProSupport for assistance.

Click **Choose File**.

### 2. Choose File to Upload



Highlight the license file, and click **Open**.

### 3. Upload License



If license upload is successful, you will get the above dialog box.

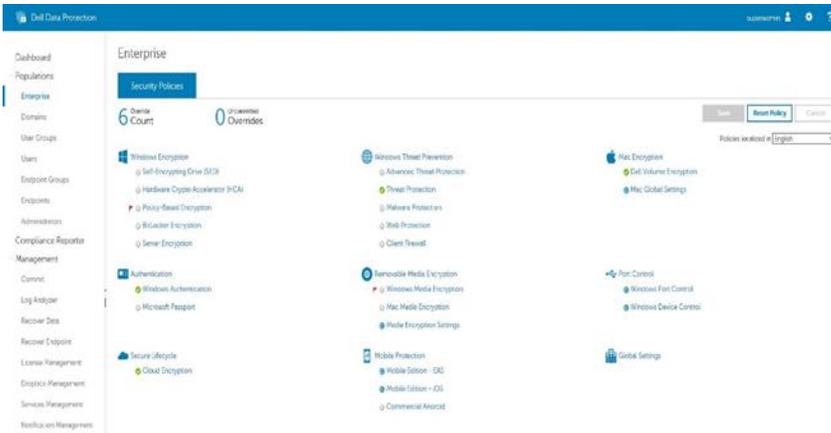
Click **OK**.

## 6.2 Policy configuration

This section details the policy configuration on the management console as well as verification on the client side.

### 6.2.1 ATP policy configuration

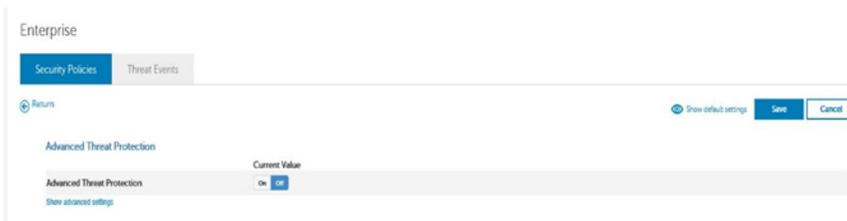
#### 1. ATP Policy Configuration



Click **Enterprise** in the left pane.

Under Windows Threat Protection, select **Advanced Threat Protection**.

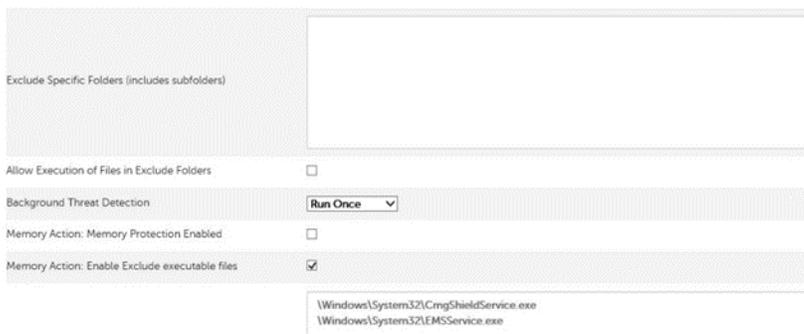
## 2. Security Policies



Go to advanced settings to configure additional settings.

Click **Show Advanced Settings**.

## 3. Settings

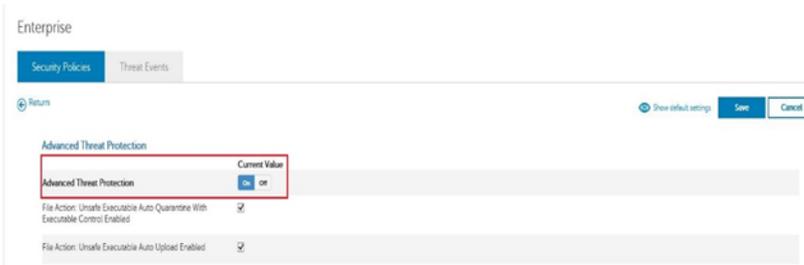


Check Memory Action: **Memory Protection Enabled**.

Add files to Exclude Specific Folders (includes subfolders).

Example may be C:\DDPE

Note: This document does not cover what Files, Folders need to be protected or excluded.

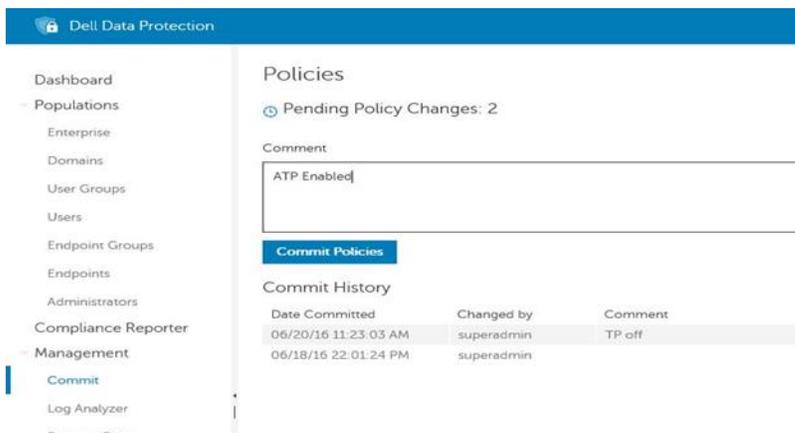


Refer to Endpoint Security Suite Enterprise Support for VDI for policy settings for persistent and non-persistent VDI clients.

Click On to enable protection.

Click Save.

#### 4. Commit



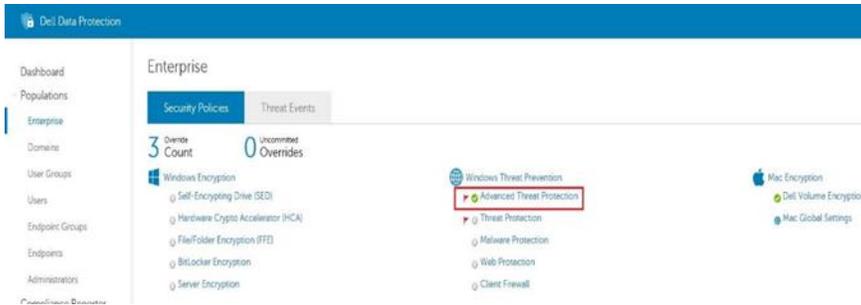
Note: If single or multiple changes are made, you will need to save these changes for each policy and then commit these changes for them to be updated.

Click **Commit** in the left pane.

Dell recommends that you add a comment about policies you have changed and reasons for the changes.

Click **Commit Policies**.

#### 5. Verify ATP is Enabled.



After policy changes are committed, Advanced Threat Protection should show a **Red flag** and **Green Check Mark**.

## 6.2.2 ATP client verification

1. Client verification on client desktop.



Log on to client desktop and look for the above icon.

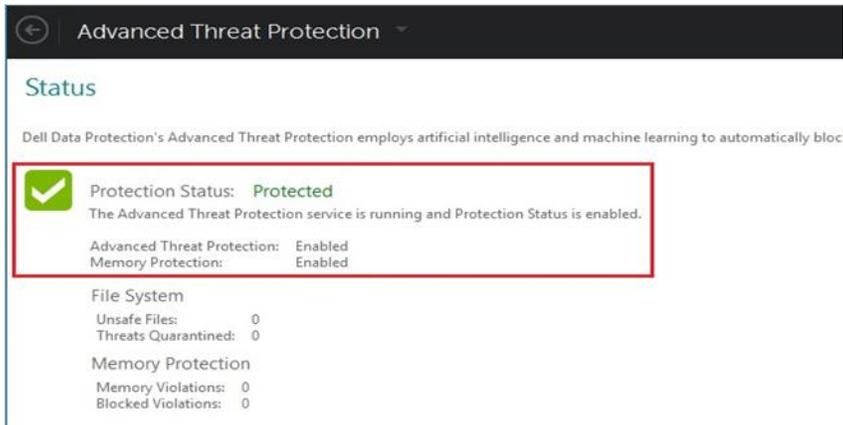
Double-click the **DDP Console** icon.

2. ATP Client



Click the Advanced Threat Protection tile as highlighted above.

3. Status



To check that Advanced Threat Prevention enabled for client.

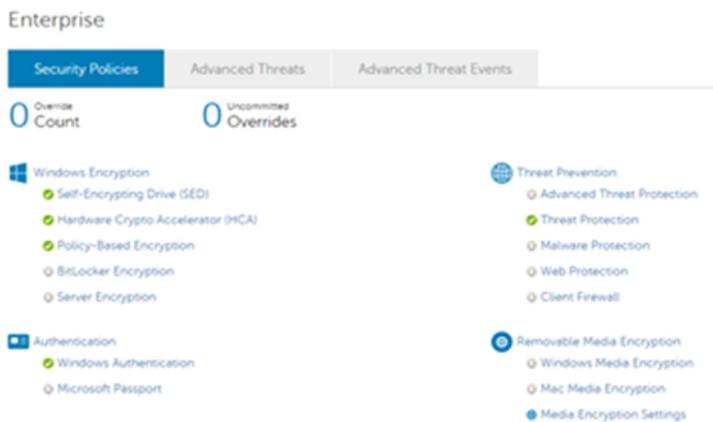
Protection Status: Protected

Advanced Threat Protection: Enabled

Memory Protection: Enabled

## 6.2.3 Policy-Based Encryption Configuration

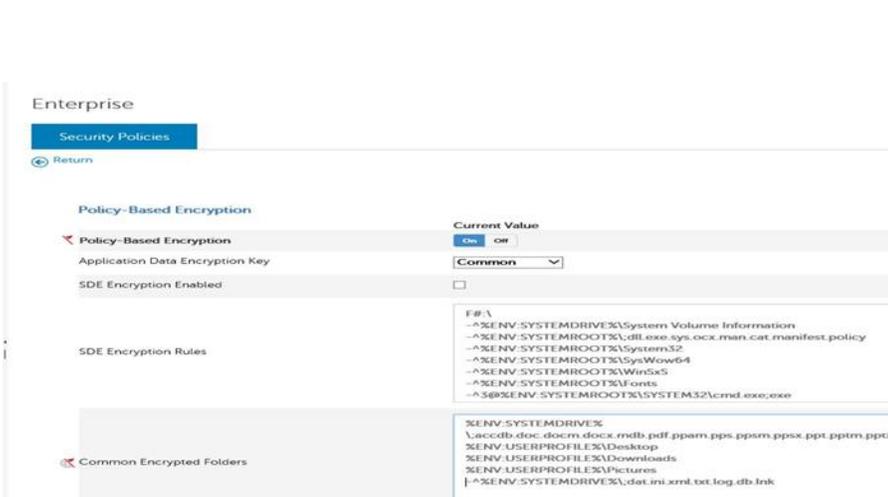
### 1. Policy-Based Encryption Configuration



Click **Enterprise** in the left pane.

Under Windows Encryption, select **Policy-Based Encryption**.

### 2. Enable Policy-Based Encryption



Refer to *Endpoint Security Suite Enterprise Support for VDI* for policy settings for persistent and non-persistent VDI clients.

Set Policy-Based Encryption to **On**.

Click **Save**.

### 3. Commit Policy



Click **Commit** in the left pane.

Dell recommends that you to add a comment about policies you have changed and reasons for the changes.

Click **Commit Policies**.

### 4. Verify policy is active

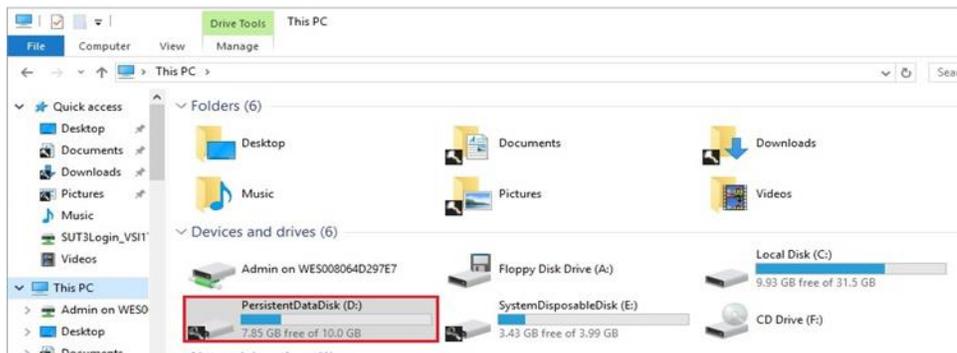




After policy changes are committed, Policy-Based Encryption should show a **Red flag** and **Green Check Mark**.

## 6.2.4 Policy-Based Encryption Client Verification

1. Verify Policy-Based Encryption on Client

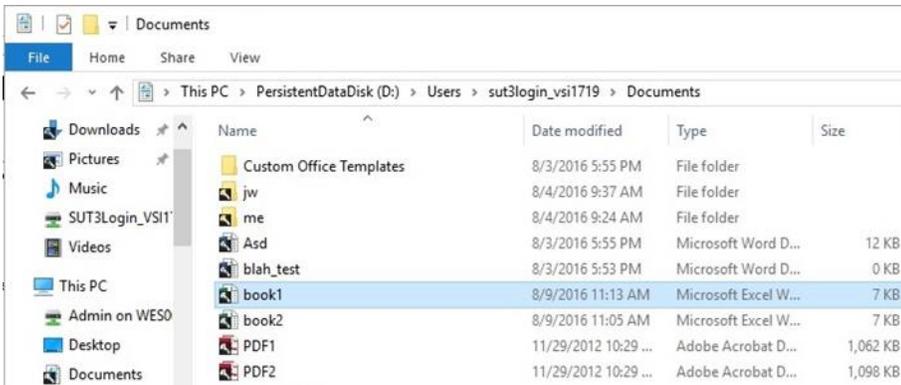


Open File Explorer and navigate to the user's home directories.

Note: The VMware (D:) is the Persistent Data Disk for persistent virtual machines, drive letter may change in customers environment.

Double-click on drive "**PersistentDataDisk (D:)**"

2. Encrypted files



Note: Key icons show that the files are encrypted.

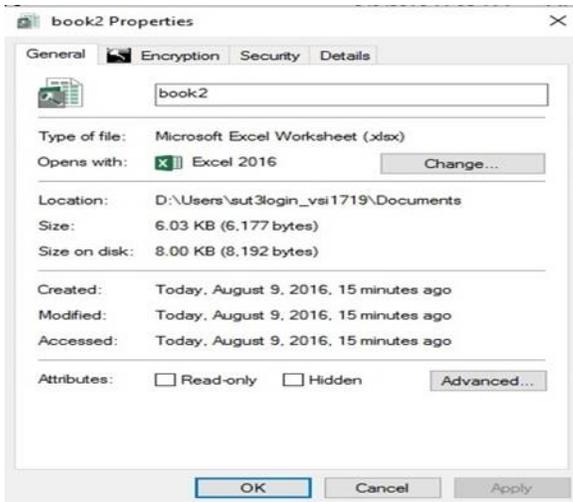
### 3. Properties



Right click any file that shows the encryption icon in the user's documents.

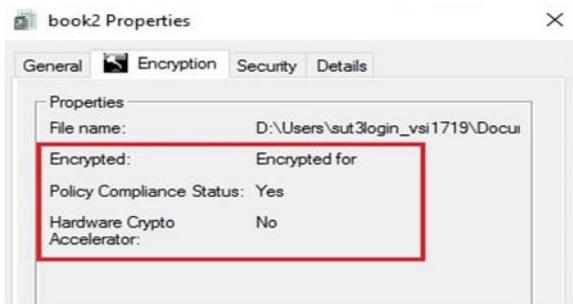
Click **Properties**.

### 4. Encryption Properties.



Select the Encryption tab.

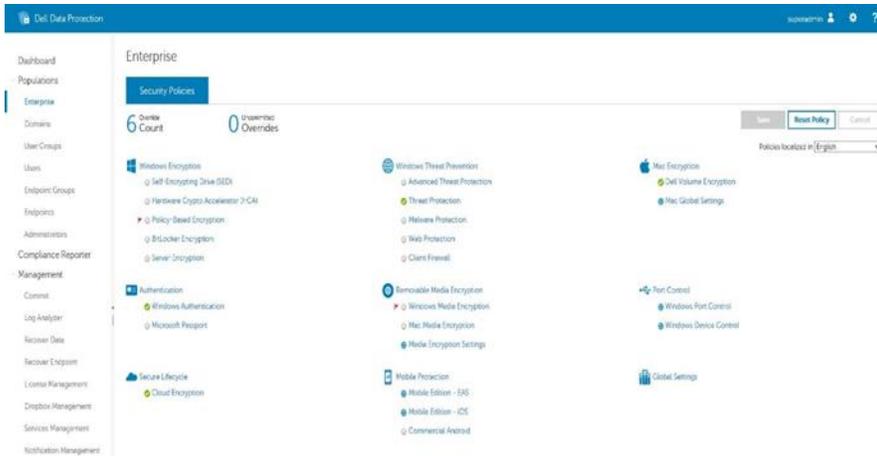
#### 5. File Encrypted properties



This indicates that the file is encrypted.

## 6.2.5 EMS Policy Configuration

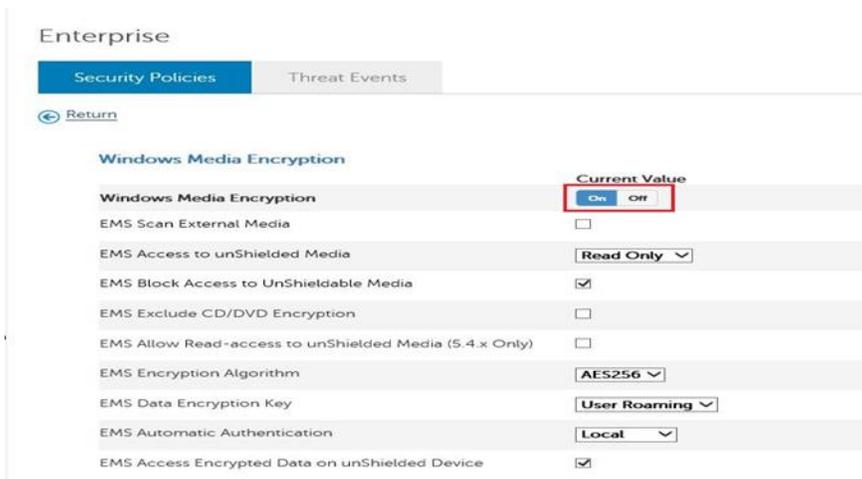
### 1. Removable Media Policy Configuration



Click **Enterprise** in the left pane.

Select **Removable Media Encryption**.

2. Windows Media Encryption



Refer to *Endpoint Security Suite Enterprise Support for VDI* for policy settings for persistent and non-persistent VDI clients.

Set Windows Media Encryption to **On**.

Click **Save**.

3. Commit



Date Committed	Changed by	Comment
06/20/16 11:45:56 AM	superadmin	ATP Enabled
06/20/16 11:23:03 AM	superadmin	TP off
06/18/16 22:01:24 PM	superadmin	

Click **Commit** in the left pane.

Dell recommends that you to add a comment about policies you have changed and reasons for the changes.

Click **Commit Policies**.

#### 4. Verify Removable Media

- Windows Encryption
  - Self-Encrypting Drive (SED)
  - Hardware Crypto Accelerator (HCA)
  - Policy-Based Encryption
  - BitLocker Encryption
  - Server Encryption
- Authentication
  - Windows Authentication
  - Microsoft Passport
- Secure Lifecycle
  - Cloud Encryption
- Windows Threat Prevention
  - Advanced Threat Protection
  - Threat Protection
  - Malware Protection
  - Web Protection
  - Client Firewall
- Removable Media Encryption
  - Windows Media Encryption
  - Mac Media Encryption
  - Media Encryption Settings
- Mobile Protection
  - Mobile Edition - EAS
  - Mobile Edition - iOS
  - Commercial Android

After policy changes are committed, Windows Media Encryption should show a **Red flag** and **Green Check Mark**.

#### 5. Unprotected Media Found





Click **Yes**. This will create a vault on the removable media.

If you select **No**, you will be able to access the removable media but will not be able to add any files or folders to the media.

6. Enter New Password



New Password: *thisIsYourPassword*

Retype Password: *thisIsYourPassword*

Click **OK**.

7. Shielding External Device



Note: Files already on the device will not be encrypted. Only new files that are added to the media will be encrypted. Wait for the process to complete before continuing. This may take a while.

#### 8. External Media Device Protected



Click **OK**.

At this point, you can proceed to copy file to external media, and the files will automatically be encrypted.

#### 9. Reading media on another computer

If you move the removable media to another computer, you will be prompted to enter the password for the vault on the media before you can read the encrypted files.

Note: Recovering lost passwords and encrypting files that were on the media before creating the vault is beyond the scope of this document.

Endpoint Security Suite Enterprise installation and configuration are complete.

## A Appendix

### A.1 List of features supported by Endpoint Security Suite Enterprise

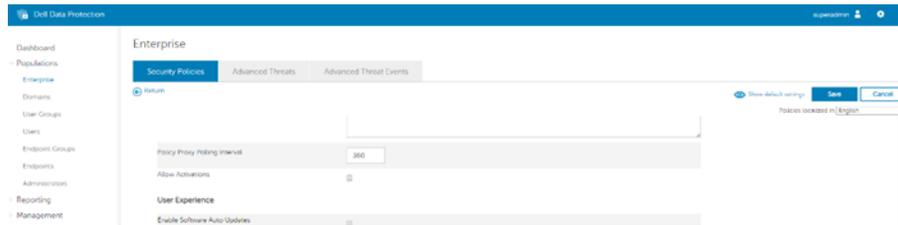
Feature	Persistent/Non-Persistent VDI	Physical PC
System Data Encryption	Not supported	Supported
Policy-Based Encryption	Supported	Supported
Removable Media Encryption	Supported	Supported
Self-Encrypted Disk	Not supported	Supported If hardware is available.
BitLocker Encryption	Not supported	Supported
Advanced Threat Prevention Execution Control	Supported	Supported
Advanced Threat Prevention Memory Protection	Supported	Supported
Advanced Threat Prevention Script Control	Supported	Supported
Authentication Refer to section 5.5	Not Supported	Supported

### A.2 Prevent Master Image Activation prior to deployment or pool update (Recompose)

The following actions will prevent the master image from activating if the master image is restarted or updated before a recompose. This also will prevent conflicts on the Dell Server.



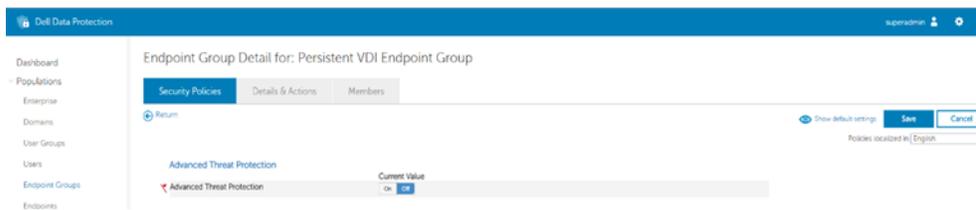
Turn off Encryption client activation by choosing **Policy-Based Encryption** on the Enterprise Menu. Choose **Show advanced settings**, clear the “Allow Activations” check box, and click **Save**.



Turn off the Advanced Threat Prevention by selecting the correct Endpoint group (e.g. Persistent VDI Endpoint Group).



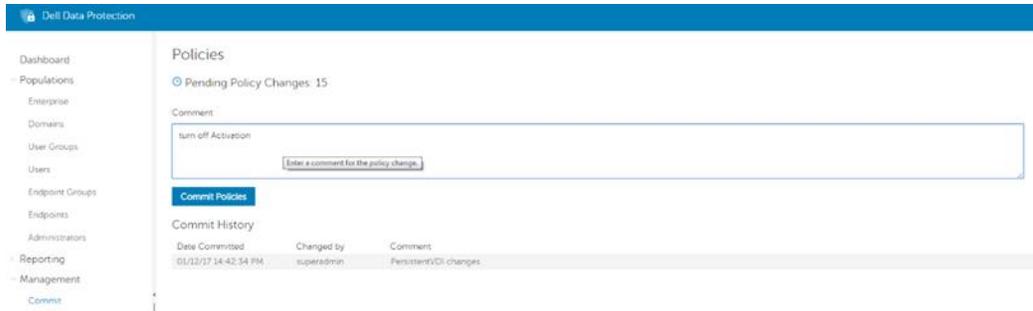
Select **Advanced Threat Protection** and set Advanced Threat Protection and click **Save**.



Click **Commit** in the left pane.

Dell recommends that you to add a comment about policies you have changed and reasons for the changes.

Click **Commit Policies**.



## A.3 Recommended VDI policies

Please see the following location for Dell Data Protection | Endpoint Security Suite Enterprise addendum.  
<http://www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals?rvps=y>

## A.4 DDP Resources

The following resources contain technical information about the Dell Data Protection product

The following page contains links to client and server manuals and also an Architectural overview

[Getting Started with Dell Data Protection](#)

Support site for Encryption is located at <http://www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research>

This site contains links to manuals, support articles and drivers. The following manuals can be found on the manuals page

[Endpoint Security Suite Enterprise Support for VDI](#)

[Endpoint Security Suite Enterprise Advanced Installation Guide](#)

[Enterprise Edition Advanced Installation Guide](#)

[Virtual Edition Quick Start Guide and Installation Guide](#)

[Enterprise Server Admin Help](#)