

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

Dell Engineering February 2017

## Revisions

Date	Description
August 2016	Initial release
January 2017	Non-Persistent VDI support

THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, HARDWARE SELECTIONS CONTAINED WITHIN ARE FROM THE BASIS OF BEST WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Copyright © 2017 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the Dell logo, and the Dell badge are trademarks of Dell Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries. VMWare is a registered trademark of VMWare, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

## Contents

1	Introd	duction	5
	1.1	Purpose	5
	1.2	Scope	5
	1.3	Configuration Prerequisites	5
2	Soluti	tion Architecture Overview	6
	2.1	Introduction	6
	2.2	Endpoint Security Suite Enterprise Overview	6
	2.3	Dell Enterprise Server or VE Architecture	9
3	Hardv	ware Components	10
	3.1	Network	10
	3.1.1	Dell Networking S4048 (10Gb ToR Switch)	10
	3.2	Dell Server	10
	3.2.1	Dell R730 Server	10
	3.2.2	Architecture Overview	11
4	Softw	vare Components	13
	4.1	Software Inventory	13
	4.1.1	Server OS	14
	4.1.2	Horizon	14
	4.1.3	Virtual Center	14
	4.1.4	Horizon Administrator	14
	4.1.5	Microsoft SQL Server	14
	4.1.6	Endpoint Security Suite Enterprise	14
	4.1.7	Virtual Edition	14
	4.1.8	Dell Data Protection Suite	15
	4.1.9	Certificates	15
	4.2	Dell Enterprise Server Installation	15
	4.2.1	Installation	15
	4.3	Virtual Edition	26
	4.3.1	Installation	26
	4.3.2	VE Configuration	

5	Clien	t Installation (Persistent or Non-Persistent)	
	5.1	VMware View Agent	
	5.2	Advanced Threat Prevention (ATP) Install	44
	5.3	Policy-Based Encryption (PBE) Install	44
	5.4	System Data Encryption (SDE)	45
	5.5	Removable Media Encryption (EMS) Install	45
	5.6	Authentication	46
	5.7	Endpoint Security Suite Enterprise Install	46
	5.7.1	Client Install	46
	5.7.2	2 Client Manual and Silent Install	
	5.7.3	Create Registry entries for VDI awareness	52
	5.7.4	Recomposing or updating VDI pools	53
6	Endp	point Security Suite Enterprise Management Console	54
	6.1	Remote Management Console	54
	6.1.1	Browser Language	54
	6.1.2	2 Domain Configuration	57
	6.1.3	Licenses	59
	6.2	Policy Configuration	60
	6.2.1	ATP Policy Configuration	60
	6.2.2	2 ATP Client Verification	63
	6.2.3	Policy-Based Encryption Configuration	64
	6.2.4	Policy-Based Encryption Client Verification	66
	6.2.5	EMS Policy Configuration	69
7	Арре	endix	73
	7.1	List of features supported by Endpoint Security Suite Enterprise	73
	7.2	Prevent Master Image Activation prior to deployment or pool update (Recompose)	74
	7.3	Recommended VDI Policies	75
	7.4	DDP Resources	75

## 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 <u>persistent</u> or <u>non-persistent</u> 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

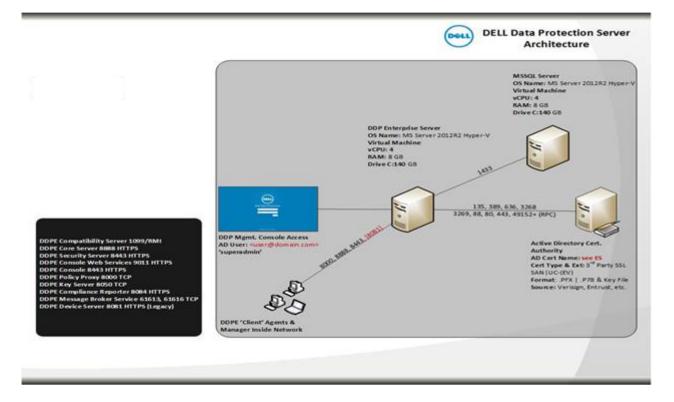
Endpoint Security Suite Enterprise and Dell Enterprise Server or Virtual Edition (VE) software delivers an outof-the-box Advanced Threat Prevention (ATP), Policy-Based Encryption (PBE) and Removable Media Encryption (EMS) solution for virtual desktops that provide antivirus and encryption that other 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.

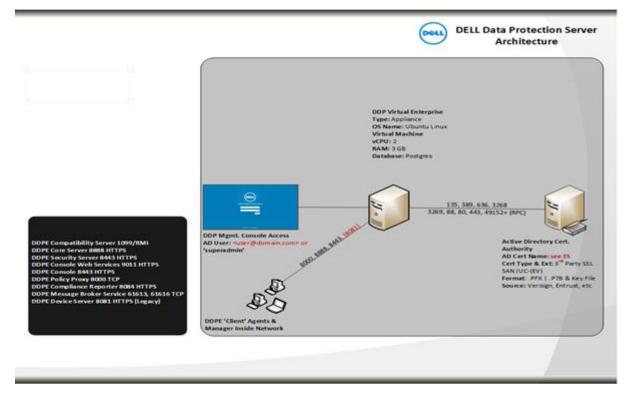
References to Endpoint Security Suite Enterprise includes Dell Enterprise Server or VE unless specifically called out in this document.

#### **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.

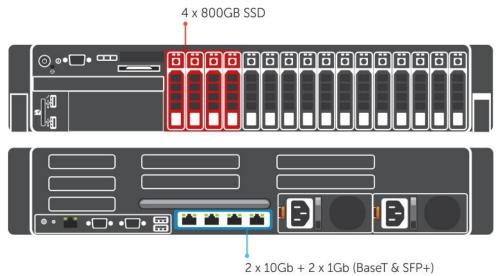
## 3.1.1 Dell Networking S4048 (10Gb ToR Switch)

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 Dell Server

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

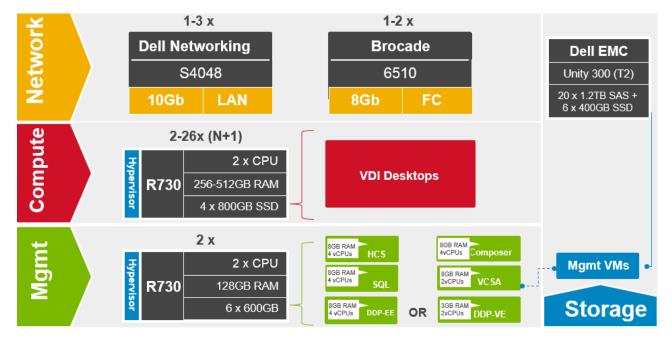
## 3.2.1 Dell R730 Server



The Dell 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.

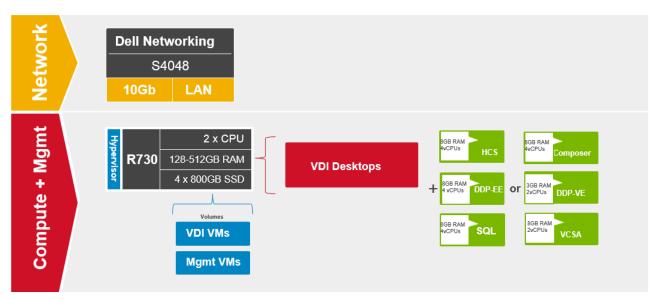
In this environment we have separate management and compute nodes configured.

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 place on a single node with the VDI desktops.

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
TOTALS	20	43	6	846

Management VMs configurations.

**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

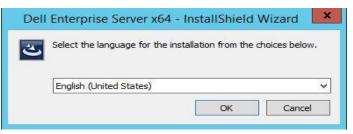
1. Install

File Home Shar	re View	Manage				~
🕣 🕤 🝷 🍈 🕣	Installers 🕨 Ente	erprise Server 🕨 x64 🕨	~ C	Search x64		Q
🔆 Favorites	Name	*	Date modified	Type Comigaration sect	Size	
E Desktop	0x040c		22/06/2010 14:35	Configuration sett	26 KB	
📕 Downloads	0x0407		16/03/2012 14:50	Configuration sett	26 KB	
强 Recent places	0x0409		23/03/2010 16:44	Configuration sett	22 KB	
	0x0410		22/06/2010 14:37	Configuration sett	25 KB	
👰 This PC	Dx0	Open	6/03/2012 12:55	Configuration sett	15 KB	
	🚳 0xt 🚱	Run as administrator	B/04/2012 14:44	Configuration sett	14 KB	
👊 Network	Dx0	Troubleshoot compatibility	2/06/2010 14:40	Configuration sett	24 KB	
	Oxt	Pin to Start	2/06/2010 14:41	Configuration sett	25 KB	
	10	Share with	9/01/2016 16:29	MST File	192 KB	
	10	Restore previous versions	9/01/2016 16:29	MST File	32 KB	
	10	Send to	9/01/2016 16:29	MST File	184 KB	
	10		9/01/2016 16:29	MST File	188 KB	
	10	Cut	9/01/2016 16:29	MST File	184 KB	
	10	Сору	9/01/2016 16:29	MST File	284 KB	
	10	Paste	9/01/2016 16:29	MST File	244 KB	
	10	Create shortcut	9/01/2016 16:29	MST File	180 KB	
	20	Delete	9/01/2016 16:29	MST File	180 KB	
	AL	Rename	9/01/2016 16:28	Setup Information	1 KB	
	j <mark>₿</mark> De	Properties	9/01/2016 16:29	Windows Installer	19,490 KB	
	🖾 setup	r iopeines	9/01/2016 16:30	Application	74,283 KB	

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

岁 Dell	Enterprise Server x64 - InstallShield Wizard
	Welcome to the InstallShield Wizard for Dell Enterprise Server x64
$\sim$	The InstallShield(R) Wizard will install Dell Enterprise Server x64 on your computer. To continue, dick Next.
DELL	NOTICE: This program is protected by one or more U.S. Patents, including: Number 7665125; Number 7437752; and Number 7665118.
	< Back Next > Cancel

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

遐	Dell Enterprise Server x64 - InstallShield	d Wizard
Product Ke Enter Prod		Deel
Enter the 3	2-character Product Key	
InstallShield —	< Back Nex	kt > Cancel
	< DACK INE	

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.

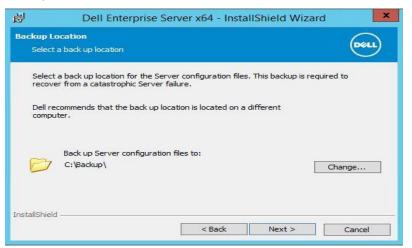
8. Destination Folder



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

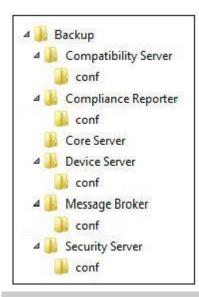
Click Next.

#### 9. Backup Location



Make sure to backup this information. You can change the location by clicking the **Change...** button Click **Next.** 

**Note:** The folder structure created by the installer during this installation step (example shown below) must remain unchanged.



Note: Experience with File System Backups are assumed and therefore not covered in this document.

#### 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

退	Dell Enterprise S	Server x64 - InstallShield Wizard
Creat	e Self-Signed Certificate	(real)
Please e	enter information that will be in	corporated into your self-signed certificate.
Fu	ully-qualified Computer Name: *Required	DD.OSPREY.COM
	Organization:	Г
	Organizational Unit:	
	City:	
	State:	Country (2 letter abbrv:) US
InstallShie	eld	
		< Back Next > Cancel

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

谩	Dell Enterprise S	Server x64 - Ir	stallShield Wizard	d 💌
Create Self	-Signed Certificate			Dell
Please enter in	nformation that will be in	corporated into yo	our self-signed certificate	2.
Fully-qua	alified Computer Name: * Required	DD.OSPREY.CO	M	
	Organization:	<b>I</b>		
	Organizational Unit:	1		
	City:			
	State:		Country (2 letter a	bbrv:) US
InstallShield				
		< Back	Next >	Cancel

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

14. Back End Server Install Setup

岁 D	ell Enterprise Server x64 - InstallShield Wizard
Back End Server	Install Setup
Select ports an	d host names for back end server
	pect or change host and port configuration. Select "Next" to accept the lues are initialized to defaults.
	Edit Hostnames
	Edit Ports
the DMZ.	ont End to communicate wth dients internally in your network or externally in
	ont End to communicate wth dients internally in your network or externally in
Front End Secur	ont End to communicate wth dients internally in your network or externally in <b>ity Server</b>
Front End Secur	ont End to communicate wth dients internally in your network or externally in ity Server Port

Check the ports being used.

Click Edit Ports...

15. Edit Back End Ports

😼 🛛 Dell E	nterprise Ser	ver x64 - InstallShield Wi	zard 🛛 🗙
Edit Back End Ports			Dell
		Port	
Client Authentication	8449	Compatibility Server	1099
Compliance Reporter	8084		
Core Server	8888	Device Server	8081
Key Server	8050	Policy Proxy	8000
Security Server	8443	SMTP	25
	TCP Port	Stomp Port	
Message Broker	61616	61613	
InstallShield			
		ОК	Cancel

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

副	Dell Enterprise Server x64 - Install Shield Wizard
	ise and Install-time Credentials is install-time credentials for the installer to set up the database
required: o use these	er uses these credentials to authenticate to the SQL server. These permissions are reate database, add user, assign permissions. The installed Enterprise Server does not credentials. They are used only during installation.
Databas	e server to use: (i.e. ServerName\InstanceName) V Browse Port:
LT.	V Drowsess Porc
Install-ti	me credentials (not run-time):
• Wind	lows authentication credentials of current user
0.00	
SQL	server authentication using the credentials below
Osqu	server authentication using the credentials below
Login ID	c Contra a contra a la
	c Contra a contra a la
Login ID Basswor	e (CORVERSIONALESSAN
Login ID Passwor Name o	: Total a construction of the second se
Login ID Basswor	: Contract of the second se
Login ID Basswor <u>Name o</u>	: The second sec

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.

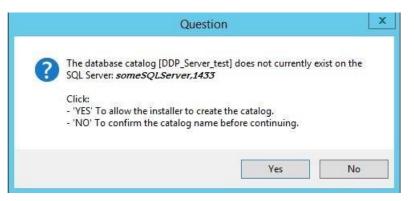
#### OR

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

Dell Enterprise Serve	er x64 - Instal	llShield Wizar	d X		
Service Runtime Account Information Specify authentication credentials for the			DELL		
Specify the user name and password of the of the SQL server. The user account must be in server permissions Default Schema: doo and	the format DOMA	IN\Username and	have the SQL		
<ul> <li>Windows authentication using the credentials below</li> <li>SQL server authentication using the credentials below</li> </ul>					
Service Account Run As User name:					
			Browse		
Password:					
InstallShield					
[	< Back	Next >	Cancel		

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: dbo\_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: dbo\_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

😼 Dell Enterp	orise Server x64 - InstallShield Wizard
	InstallShield Wizard Completed
	The InstallShield Wizard has successfully installed Dell Enterprise Server x64. Click Finish to exit the wizard.
Dell	Launch Remote Management Console
	Show the Windows Installer log
	< Back Einish Cancel

Checkbox Launch Remote Management Console. Click Finish.

## 4.3 Virtual Edition

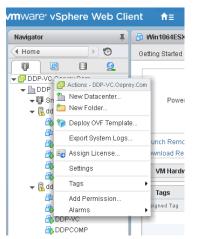
This section details the deployment and configuration of the DDP-VE appliance.

### 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.

ploy OVF Template		?
1 Source	Select source Select the source location	
1a Select source		
1b Review details	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.	
2 Destination		
2a Select name and folder	0 URL	
2b Select a resource		•
2c Select storage	Local file	
3 Ready to complete	Browse	
	Back Next Finish Can	ce

Click Local file, Click Browse... button.

3. Select OVF.

ploy OVF Template		?
1 Source	Calastaaurea	
1a Select source	Look in: 👔 Non-Persistent 🔍 🗢 🗈 💣 📰 -	
1b Review details		ible from your computer,
2 Destination	DDP Enterprise Server - VE v9.6.0 build 1 11/01/2017 14:28 OVA File	
2 a Select name and folder	Recent Places DDP Enterprise Server - VE v9.6.0 build 7 14/12/2016 13:49 OVA File	
2b Select a resource		•
2c Select storage	Desktop	
3 Ready to complete	Librano Allo Consuler Network	
	File name: DDP Enterprise Server - VE v3.6.0 build 14.ova 🔻 Open	
	Files of type: OVF Packages (".ovf, ".ova)  Cancel	
	Back	Finish Cancel

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

ploy OVF Template		
1 Source 1a Selectsource	Review details Verify the OVF tem	plate details
1b Review details	Product	BaseVE
2 Destination	Version	
2a Select name and folder	Vendor	
2b Select a resource	Publisher	No certificate present
2c Select storage	Download size	1.5 GB
3 Ready to complete	Size on disk	3.7 GB (thin provisioned) 80.0 GB (thick provisioned)
	Description	
		Back Next Finish Can

Click Next.

5. Select Name and Folder

Deploy OVF Template		3 H
Deploy OVF Template	Select name and folder Specify a name and location for the deployed template Name: Select a folder or datacenter Search S	The folder you select is where the entity will be located, and will be used to apply permissions to it. The name of the entity must be unique within each vCenter Server VM folder.
		Back Noxt Finish Cancel

Name: *enterName* for VE, Click datacenter Icon Click Next.

### 6. Select storage

1 Source 1a Selectsource	Select storage Select location to store the	files for the deployed tem	iplate			
<ul> <li>1b Review details</li> </ul>	Select virtual disk format:	Thick Provision Lazy Zer	oed 🔹			
2 Destination	VM Storage Policy:	Datastore Default	• 0			
2a Select name and folder	The following datastores	are accessible from the d	estination resource that y	rou selected. Select	the destination of	iatastore for the
2b Select storage	virtual machine configural					
2c Setup networks	Name	Capacity	Provisioned	Free	Type	Storage DR:
3 Ready to complete	🗐 LocalDisk	1.06 TB	1.36 TB	147.93 GB	VMFS	
	4					

Click Next.

7. Setup networks

Deploy OVF Template			?	
1 Source 1 Selectsource	Setup networks Configure the networks the deployed template should use			
<ul> <li>1b Review details</li> </ul>	Source	Destination	Configuration	
2 Destination	bridged	VM Network 2	- O	
2a Select name and folder		~		
2b Select storage				
2c Setup networks				
3 Ready to complete	IP protocol: IPv4	IP allocation: Static -	Manual	
	Source: bridged - Description			
	The bridged network			
	Destination: VM Network 2 - Proto	col settings		
	No configuration needed for this r	network		
		Back	Next Finish Cancel	

Change the networks if needed.

Click Next.

8. Ready to complete

Deploy OVF Template			?
1 Source 1 a Select source	Ready to complete Review your settings selections be	Fore finishing the wizard.	
<ul> <li>1b Review details</li> <li>2 Destination</li> </ul>	OVF file	Nospreyfile/Osprey-Backup/Software/DDP-ESS/DDP-Enterprise-Server-VE-9.4.0.8/DD Enterprise Server VE/DDP Enterprise Server - VE 99.4.0 build 8.ova 1.2.0 B	P
2a Select name and folder     2b Select storage	Size on disk	1.200 80.008 V	
2c Setup networks     3 Ready to complete	Datastore Target	LocalDisk ddp-ese.osprey.com	
	Folder Disk storage Network mapping IP allocation	DDP Thick Provision Lazy Zeroed bridged VM Network 2 Static - Manual, IPv4	
	Power on after deployment		
		Back Next Finish Ca	incel

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

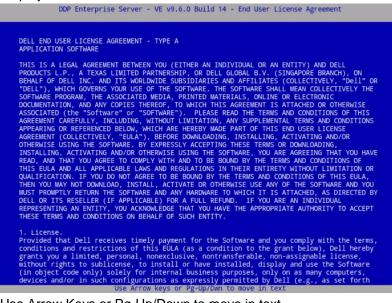
Additional configuration is needed before VE is ready for use. After the steps in section 4.3.1 are completed, power on VE, and a wizard will step you through the configuration.

1. End User License Agreement

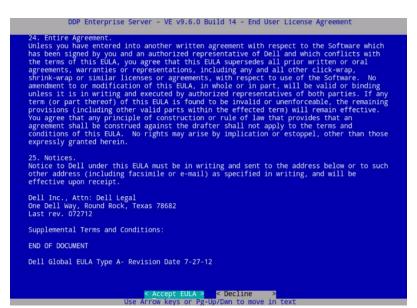
DDP Enterprise Server - VE v9.6.0 Build 14 - End User License Agreement					
Welcome to DDP Enterprise Server - Virtual Edition. Please read and accept terms of this licensed software. Press 'Esc' at any time to go back to the start of the EULA process. Select the language to display the EULA and select < Display EULA > to continue. After reading the EULA you must select <accept eula=""> to proceed with the software initialization</accept>					
( <u>X</u> ) English	( ) German	( ) Spanish			
( ) French	( ) Italian	( ) Japanese			
( ) Korean	( ) Portuguese(Brazilian)	( ) Portuguese (Iberian)			
Seject 1a	< Display EULA >	form or quit			

Press the **Enter Key** to select English, and Use arrow key to navigate to < **Display EULA** >.

#### 2. Display EULA



#### Use Arrow Keys or Pg-Up/Down 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

AsseVE - VMware Remote Console		
VMRC 🕶 📔 🕶 🚭 🖂		*
	Would you like to change the default password for ddpuser?	
	< <u>Yes</u> > KNO >	

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:

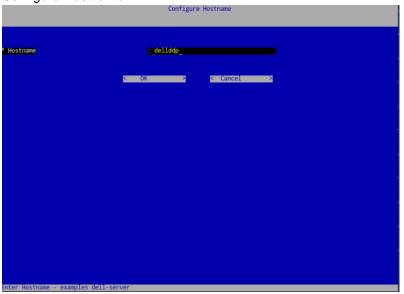
At least 8 characters• At least 1 uppercase letter• At least 1 digit•

At least 1 special character

	Se	t ddpuser Pa	assword	
• Enter Current Password • Enter New Password • Re-enter New Password				
	< 0K	>	< Cancel >	
Enter Current Password				

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

	Configure Network Settings	
* Use DHCP * Static IP * Network Mask * Default Gateway * DHS Server 1 * DHS Server 2 * DHS Server 3	: (X)	
	< OK > < Cancel >	
Press the spacebar to selec	t or de-select DHCP	

You can elect to change network setting here or finish the wizard and change afterwards. Select < OK >.

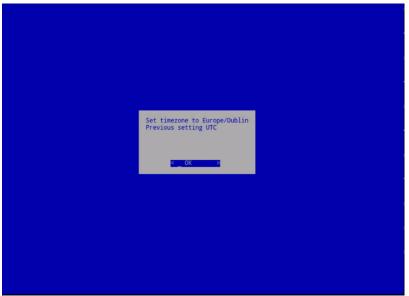
Press the Enter Key.

8. Time Zone

< Europe/Copenhagen ^ >
< Europe/Copenhagen ^ > < Europe/Oublin > < Europe/Gibraltar >
<pre>&lt; Europe/Guernsey</pre>
< Europe/Heisinki >
<pre>&lt; Europe/Istanbul &gt;</pre>
< Europe/Jersey >
<pre>&lt; Europe/Kaliningrad</pre>
< Europe/Kiev [] > < Europe/Lisbon   >
< Europe/Ljubljana
< Europe/London >
< Europe/Luxembourg v >

Select time zone from list. We selected Europe / Dublin as an example.

#### 9. Select TimeZone



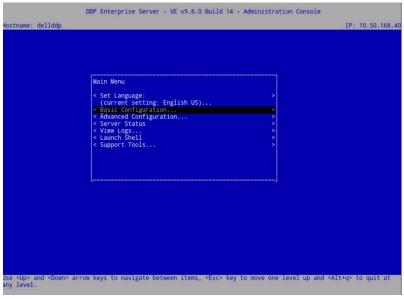
Press the Enter Key.

10. Complete Installation

A BaseVE - VMware Remote Console	
VMRC -	*
The initial virtual appliance configuration has successfully completed. Press <ok> to</ok>	
continue.	
<u>&lt;_ок.</u> >	

Press the Enter Key.

#### 11. Secure Shell



Move down arrow key to **Basic Configuration**... Press the **Enter Key**.

Main Menu	
<pre>&lt; Basic Configuration &lt; &lt; Hostname &lt; &lt; Network Settings &lt; &lt; OWZ Hostname &lt; &lt; Time Zone (current setting: Europe/Dublin) &lt; &lt; Update DDP Enterprise Server - VE &lt; Change User Passwords &lt; File Transfer (FTP) Users &lt; SOH Settings &lt; Start Application &lt;- &lt; Stop Application &lt;- &lt; Rebot Application &lt;- &lt; Rebot Applicate </pre>	>
L	]

Select SSH Setting from menu. Press the **Enter Key**.

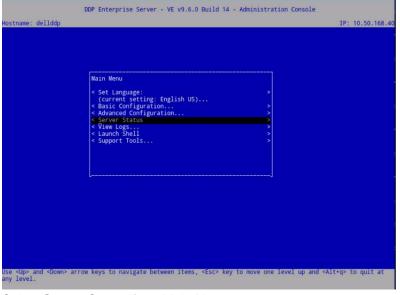
#### 12. SSH Configuration for users

	SSH configuration for ddpsupport, ddpconsole and ddpuser
Enable SSH for ddpsupport for ddpconsole for ddpuser	: (X) : [] : []
	< OK > < Cancel >
Spacebar to select between s	sh enabled/disabled for ddpsupport

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.** 

	Server Status
	Press Enter or Esc key to exit
Dell Message Broker Dell Gompatibility Server Dell Scourity Server Dell Scourity Server Dell Compliance Reporter Dell Core Server Dell Gore Server Handroy Server Dell Forensic Server Dell Forensic Server Dell Policy Proxy	: Running : Running : Running : Running : Running : Running : Running : Running : Running : Running
Press Enter or Esc key to retur fails, it may be that the datal under Main Menu > View Logs.	rn to the menu. Changes in Service status may take several minutes. If a Service basecustomizer process failed. To troubleshoot, check the Database Provisioning Log

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)

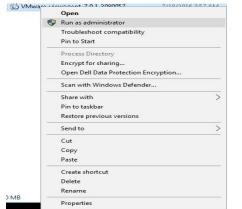
Endpoint Security Suite Enterprise client installation is performed on the master image for both <u>persistent</u> and <u>non-persistent</u> VDI solutions.

## 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.

😸 VMware Horizon Agent		- <u></u>		<
	Welcome to the instal Agent	ler for VMwa	re Horizon	
	VMware Horizon Agent Setup will guide you through the pro wait.			
vMware Horizon™ Agent				
Ċ <sup>™</sup>				
	< Back	Next >	Cancel	

Click Next

3. License Agreement

😸 VMware Horizon Agent		×
License Agreement Please read the following license agr	reement carefully.	5
VMWARE END USER LIC	CENSE AGREEMEI	NT
PLEASE NOTE THAT THI LICENSE AGREEMENT S THE SOFTWARE, REGAR MAY APPEAR DURING TH SOFTWARE.	SHALL GOVERN Y RDLESS OF ANY T	OUR USE OF TERMS THAT
I accept the terms in the license agre	eement	
O I do not accept the terms in the licen		

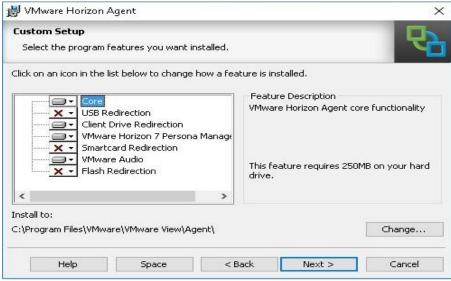
Select I accept the terms in the license agreement. Click Next

#### 4. Network protocol configuration

🚽 VMware Horizon	Agent	×
Network protocol Select the commun	-	2
Specify the protoc	ol to be used to configure this Horizon Agent instan	ce:
IPv4 IPv6	This agent will be configured to choose the IPv4 all connections.	protocol for establishing
	< Back Next	> Cancel

In our example we used IPv4. Click **Next** 

#### 5. Custom Setup



Select USB Redirection.

<b>Select the program f</b>	features you want install	ed.	R
Core X USB Rd This f	ist below to change how edirection eature will be installed eature, and all subfeat	Feature Descript USB Redirection. Horizon 7 Securit on local hard drive. ures, will be installed o	Refer to the VMware v document for quidance
		drive.	
		>	
<			
<		1.59	Change

Select This feature will be installed on local hard drive.

#### 6. VMware Horizon Agent

<b>istom Setup</b> Select the program fe	atures you want ins	stalled.		
ck on an icon in the lis	t below to change h	now a feature is in:	stalled.	
Core		Featu	re Description	
VMware Horizon A				×
🔥 Refert	Agent o the VMware Hor USB redirection sec		ocument for guid	
A Refert	o the VMware Hor		ocument for guid	

Click OK Click Next

7. Register with Horizon 7 Connection Server

👻 - 1997 (1997) (1997) (1997)	on Agent			×
_	Horizon 7 Connection zon 7 Connection Serve		vill connect to.	R
	name of a Horizon 7 Co in credentials to register			
			(hostname or IP ad	ldress)
Authentication:	Authenticate as the	e currently logged o	n user	
	O Specify administral	tor credentials		
		tor credentials	(Domain\U	ser)
	Username:	tor credentials	(Domain\U	ser)

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

😸 VMware Horizon Agent			×
Ready to Install the Program The wizard is ready to begin installation	•		2
VMware Horizon Agent will be installed in C:\Program Files\VMware\VMware View Click Install to begin the installation or C	\Agent\	wizard.	
	< Back	Install	Cancel

Click Install

9. Installer Completed

😸 VMware Horizon Agent	×
	Installer Completed
	The installer has successfully installed VMware Horizon Agent. Click Finish to exit the wizard.
vMware Horizon™ Agent ©PC⊛IP	
	< Back Finish Cancel



10. VMware Horizon Agent Installer Information

闄 VMwa	are Horizon Agent Installe	r Information	×
1	You must restart your sys changes made to VMware effect. Click Yes to restar restart later.	Horizon Agent to take	
	Yes	No	
Click <b>Ye</b>	)e		

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 in section 5.7.1 and 5.7.3 following.
- 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.

From VMWare pull down menu located at top of VDI session, the following Icons should be visible.

🏁 🕎 🚍 Options 🔻 🖞 Connect USB Device 💌 📮 Send Ctrl-Alt-Delete

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



Click Devices, in our example the USB device is an Alcor Micro Mass Storage.

#### Click Alcor Micro Mass Storage.

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

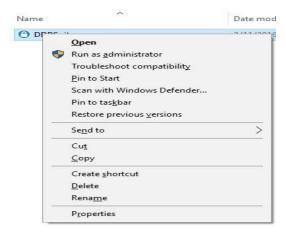
For VDI installations, the Endpoint Security Suite Enterprise client install installs the Encryption client and Advanced Threat Prevention agent. All other software including any VDI agents must already be installed. The Endpoint Security Suite Enterprise client install and setup of registry entries 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 7.2 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

DDP   Endpoint Security Suite	×
Extracting DDP   Endpoint Security Suite	Installer
28% Cancel	
ell Data Protection   Endpoint Security Suite - InstallShield Wizard	×
	DELL
	$\sim$
Setup Status	
Setup Status Dell Data Protection   Endpoint Security Suite is configuring your software may take a couple of minutes.	installation. This
- Dell Data Protection   Endpoint Security Suite is configuring your software	installation. This
Dell Data Protection   Endpoint Security Suite is configuring your software may take a couple of minutes.	installation. This
Dell Data Protection   Endpoint Security Suite is configuring your software may take a couple of minutes.	installation. This
Dell Data Protection   Endpoint Security Suite is configuring your software may take a couple of minutes.	installation. This
Dell Data Protection   Endpoint Security Suite is configuring your software may take a couple of minutes.	installation. This
Dell Data Protection   Endpoint Security Suite is configuring your software may take a couple of minutes.	installation. This
Dell Data Protection   Endpoint Security Suite is configuring your software may take a couple of minutes.	installation. This

Install will continue to the Welcome screen.

#### 3. Welcome

Dell Data Protection   Endpoin	t Security Suite - InstallShield Wizard	×
	Welcome to the InstallShield Wizard for Dell Data Protection   Endpoint Security Suite	
DEL	The InstallShield Wizard will install Dell Data Protection   Endpoint Security Suite on your computer. To continue, click Next.	
	< Back Next > Canc	el

On the Welcome screen, click Next.

#### 4. License Agreement

ease read the following license agreement carefully.	Der
DELL END USER LICENSE AGREEMENT - TYPE A APPLICATION SOFTWARE	^
THIS IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIV ENTITY) AND DELL PRODUCTS L.P., A TEXAS LIMITED PARTNER: GLOBAL B.V. (SINGAPORE BRANCH), ON BEHALF OF DELL INC., WORLDWIDE SUBSIDIARIES AND AFFILIATES (COLLECTIVELY, " "DELL"), WHICH GOVERNS YOUR USE OF THE SOFTWARE. THE SHALL MEAN COLLECTIVELY THE SOFTWARE PROGRAM, THE A MEDIA, PRINTED MATERIALS, ONLINE OR ELECTRONIC DOCUM AND ANY COPIES THEREOF. TO WHICH THIS AGREFMENT IS A	SHIP, OR DELL AND ITS Dell" OR SOFTWARE SSOCIATED MENTATION,
	Print
I accept the terms of the 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

Data Protection   Endpoint Security Suite - InstallShield Wizard	×
II Enterprise Server Setup Please provide the following information about your Dell Enterprise Server.	DELL
Please specify the fully qualified host name of the managing Dell Enterprise Server. This server will be used to activate new users and retrieve their security policies. For example: servername.domain.com Dell Enterprise Server Name	
DDPServerAddr4ess	
Please verify the fully qualified URL of the Dell Device Server. This servlet will be used to activate new users. Dell Device Server URL	I
https://DDPServerAddr4ess:8443/xapi/	
< Back Next > 0	Cancel

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.

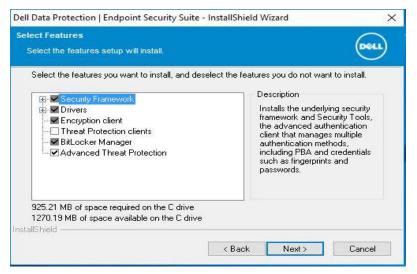
#### 6. Choose Destination Location

Choose Destination Location Select folder where setup will ins	stall files.	Deal
Install Dell Data Protec	ction   Endpoint Security Suite to:	
C:\Program Files\Dell\	Dell Data Protection\	Change
stallShield		

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

eady to Install the Program The wizard is ready to begin installation.		Dell
Click Install to begin the installation.		
If you want to review or change any of yo the wizard.	our installation settings, click Back	Click Cancel to exit
stallShield		95 t

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

#### Click Install.

Data Protection   Endpoint Security Suite - InstallShield Wizard	
	Dell
Setup Status	
Dell Data Protection I Endpoint Security Suite is configuring your software installat may take a couple of minutes.	ion. This
Preparing to Install, please wait	
IIShield	
	Cancel

The installation will take some time to complete.

#### 9. Installation Wizard Complete

Dell Data Protection | Endpoint Security Suite - InstallShield Wizard

Ins	tallShield Wizard Complete
End	e InstallShield Wizard has successfully installed Dell Data Protection   Ipoint Security Suite. Before you can use the program, you must restart your nputer.
	○ Yes, I want to restart my computer now.
	No, I will restart my computer later.
Rei	nove any disks from their drives, and then click Finish to complete setup.

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 Install

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:

From a command prompt do not run from PowerShell: 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:

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"•

The following example installs Advanced Threat Prevention (silent installation, no reboot, installation log file and installation folder in the specified locations)

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

AdvancedThreatProtectionAgentSetup.exe /s /norestart REBOOT=ReallySuppress APPFOLDER="C:\Program Files\Dell\Dell Data Protection\Advanced Threat Protection" /l "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.

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: 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 7.2 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.

#### Open Internet Explorer

1. Go To Tools, Internet Options

		-	nternet	Options		?	2
General	Security	Privacy	Content	Connections	Programs	Adva	nce
Home p	To cre			, type each add /fwlink/p/?Lin			B.
	_	Use cu	rrent	Use default	Use n	ew tab	
Startup	o ———— o						-
	nge how we	ebpages a	re displaye	ed in tabs.	Ta	abs	
Delei form	ng history te tempora informatio velete brow	n.		kies, saved pa:	sswords, and	d web	
				Delete	Set	tings	
Appear	rance —	100					_
(	Colors	Lang	juages	Fonts	Acce	ssibility	•
			0		ancel	Ap	ply

Click Languages.

#### 2. Language Preference



Click Set Language Preferences button.

3. Change your language preferences

Ì₽		Language		- O X
🕘 🍵 🕈 🛊 Control Pa	nel 🔸 All Control Panel	tems > Language	v ¢	Search Control Panel 🔑
Control Panel Home Advanced settings Change date, time, or number formats	Add languages you wa	uage preferences In to use to this list. The language at the top of your list is your primary language (the one you want to see and use most of none Moveup Move down	ften).	
	English (United Kingdom)	Windows display language: Available for download Keyboard layout: United Kingdom Date, time, and number formatting		Options

#### Click Add a language

#### 4. Add a Language

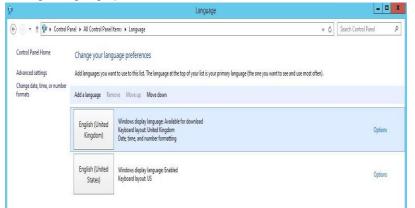
A Condervale	Ali Control Panel items	Language + Add languages		* C S	earch languages
Add a language					
Use the search box to find mor Group languages by: Languages					
Danish	Dari	Divehi	Dutch		^
E					~
English	eesti				=
English	Estonian				_

#### 5. English

			Regional variants			
🔹 🛉 💱 🕻 Control Pane	I + All Control Panel Items +	Language 🕨 Add languages	<ul> <li>Regional variants</li> </ul>		v (	Search regional variant
Add a language						
Use the search box to find mo	re languages.					
English (Australia)	English (Belize)	English (Canada)	English (Caribbean)	English (India)	English (Ireland)	English (Jamaica)
English (Australia)	English (Belize)	English (Canada)	English (Caribbean)	English (India)	English (Ireland)	English (Jamaica)
English (Malaysia)	English (New Zealand)	English (Philippines)	English (Singapore)	English (South Africa)	English (Trinidad and Tobago)	English (United Kingdom)
English (Malaysia)	English (New Zealand)	English (Philippines)	English (Singapore)	English (South Africa)	English (Trinidad and Tobago)	English (United Kingdon
English (United States)	English (Zimbabwe)					
English (United States)	English (Zimbabwe)					

Click English (United States).

6. Change language preference



#### Click first language

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

\$		Language			
🔄 🕘 🔹 🕇 💱 🕻 Control Pi	anel 🔸 All Control Panel	lterns > Language	v C	Search Control Panel	٩
Control Panel Home Advanced settings	Change your lang Add languages you wa	juage preferences In to use to this field. The language at the top of your list is your primary language (the one you want to see and use most of	ten).		
Change date, time, or number formats	Add a language Ren	nove Moveup Movedown			
	English (United States)	Windows display language Enabled Keyboard layout: US Date, time, and number formatting		Options	
	English (United Kingdom)	Windows display language: Available for download Kiejboard layout: United Kingdom		Options	I.

Close the Languages.

## 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



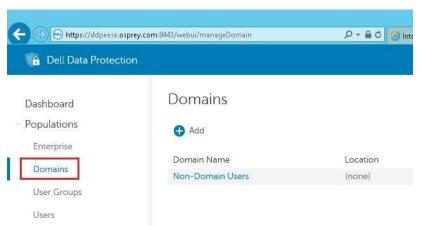
Use the following default username and password to access the management site.

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

Directory URL:		Refresh URL
Host Name:	1	
	Host Name is required	
Port		
Distinguished Name:		
Iser Name:	Enter LDAP username@domain.com	
Password.		
lias.		Add
		Remove Selected

#### 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 Detait io	or: <b>someDomai</b>	11		
Security Policies	Details & Actions	Members	Settings	Key Server
Details				
Domain Name				
Location				
1010111				
LDAP Url				

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

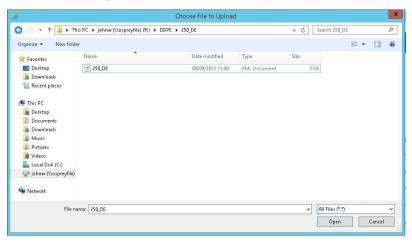
Dashboard	Licens	e Management						
Populations	Upload Li	censes						
Enterprise	Choose	File						
Domains	Choose							
User Groups	Client Li	censes Owned						
Users	Alert	Type	Valid From	Valid To		Count	Status	
Endpoint Groups		Mobile Edition	1/1/1753 12:00 AM	12/31/99	99 11:59 PM	10	None	Delete
Endpoints		Shield for Server	1/1/1753 12:00 AM	12/31/999	9 11:59 PM	4	None	Delete
Administrators		Enterprise Edition	1/1/1753 12:00 AM	12/31/999	9 11 59 PM	10	None	Delete
Compliance Reporter		Cloud Edition	1/1/1753 12:00 AM	12/31/99	9 11:59 PM	10	None	Delete
Management		External Media Edition	1/1/1753 12:00 AM	12/31/99	9 11:59 PM	10	None	Delete
Commit								-
Log Analyzer	I Client Li	cense Usage						
Recover Data	Alert	Туре	Total	Used				
Recover Endpoint		Enterprise Edition	1	0 0				
License Management		Cloud Edition	1	0 0				
		External Media Edition	2	0 0				
Dropbox Management		Mobile Edition	1	D C				
Services Management		BitLocker Manager	2	0				
		Threat Protection	1	0 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

Dell Data Protection			ati	mora 🛔 🌻
Dashboard	Enterprise			
Populations				
Enterprise	Security Policies			
Domains	6 Count O Uncommitted		Sent	eset Policy Canor
User Groups	o then		Policies localiz	ed in English
Users	Windows Encryption	Wincows Threat Prevension	Mac Encryption	
Endpoint Groups	() Self-Encrypting Drive (SED)	() Advanced Threat Protection	O Dell Volume Encryption	
Endpoints	<ul> <li>Hardware Crypto Accelerator (HCA)</li> </ul>	S Threat Protection	Hac Global Settings	
	Q Policy-Based Encryption	@ Malware Protection		
Administration	() BitLocker Encryption	() Web Protection		
Compliance Reporter	() Server Encryption	O Client Firewall		
fanagement				
Commit	Authentication	Removable Media Encryation	+ Part Control	
Log Analyzer	<ul> <li>Windows Auchentication</li> </ul>	P () Windows Media Encryption	Windows Port Control	
	() Microsoft Passport	Mac Media Encryption	Windows Device Control	
Recover Data		Medie Encryption Settings		
Recover Endpoint				
License Management	a Secura Lifecycle	Mobile Protection	Global Settings	
	Cloud Encryption	Mobile Edition - EAS		
Dropbox.Management		Mobile Edition - iDS		
Services Management		O Commercial Anorold		
Notification Management				

Click Enterprise in the left pane.

Under Windows Threat Protection, select Advanced Threat Protection.

#### 2. Security Policies

Enterprise		
Security Policies Threat Events		
€ Return		Show default settings     Save     Cancel
Advanced Threat Protection	Current Volue	
Advanced Threat Protection	on or	
Show advanced settings		

Go to advanced settings to configure additional settings.

Click Show Advanced Settings.

3. Settings

Exclude Specific Folders (includes subfolders)	
Allow Execution of Files in Exclude Folders	
Background Threat Detection	Run Once 🗸
Memory Action: Memory Protection Enabled	
Memory Action: Enable Exclude executable files	No.
	\Windows\System32\CragShieldService.exe \Windows\System32\EMSService.exe

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.

terprise			
Security Policies Threat Events			
leturn		Show default	settings Save Cancel
			A CONTRACT OF A CONTRACT.
Advanced Threat Protection			
Advanced Threat Protection	Current Value		
Advanced Threat Protection Advanced Threat Protection	Current Value on on		

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

Dashboard	Policies		
opulations	Pending Policy Ch	anges: 2	
Enterprise	× · ·	5	
Domains	Comment		
User Groups	ATP Enabled		
Users			
Endpoint Groups	Commit Policies		
Endpoints	Commit History		
Administrators	Date Committed	Changed by	Comment
Compliance Reporter	06/20/16 11:23:03 AM	superadmin	TP off
Management	06/18/16 22:01:24 PM	superadmin	

**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 to add a comment about policies you have changed and reasons for the changes.

Click Commit Policies.

5. Verify ATP is Enabled.

ashboard	Enterprise		
opulations Enterprise	Security Policies Threat Events		
Domains	3 Count O Uncommitted		
User Groups	Windows Encryption	Windows Threat Prevention	Mac Encryption
Users	Self-Encrypting Drive (SED)	P Advanced Threat Protection	O Dell Volume Encryptio
Endpoint Groups	Hardware Crypto Accelerator (HCA)	C Threat Protection	Mac Global Settings
Endpoints	Pile/Folder Encryption (FFE)	Malware Protection	

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

## 6.2.2 ATP Client Verification

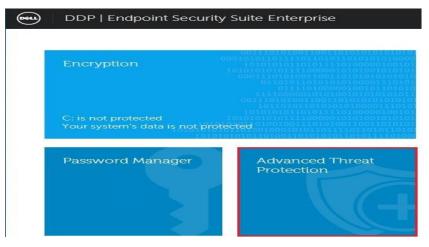
1. Client verification on client desktop.



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

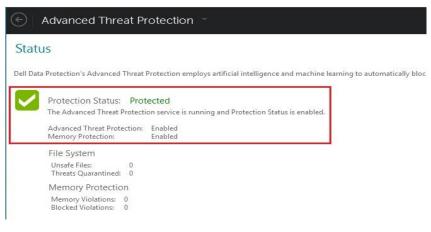
Double-clickthe DDP Console icon.

2. ATP Client



Click the Advanced Threat Protection tile as highlighted above.

#### 3. Status

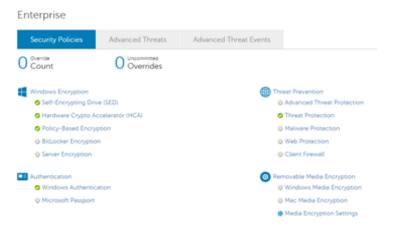


To check that Advanced Threat Prevention enabled for client.

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

Enterprise Security Policies © Return	
Policy-Based Encryption	Current Value
Policy-Based Encryption	Om Off
Application Data Encryption Key	Common 🗸
SDE Encryption Enabled	
SDE Encryption Rules	F#\ - %ENV.SYSTEMDRIVE%\System Volume Information - %ENV.SYSTEMROOT%\dl was assice, man.cat.manifest.policy - %EENV.SYSTEMROOT%\System32 - %EENV.SYSTEMBOOT%\SYSTEM32 - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMS - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMS - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMS - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMS - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMS - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMS - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %EENV.SYSTEMBOOT% - %
Common Encrypted Folders	XENV-SYSTEMDRIVEX \accold.doc.docm.docs.mdb.pdf.ppam.pps.ppsm.ppsx.ppt.pptm.ppt XENV-USERPROFILEX/Desktop XENV-USERPROFILEX/Desktop XENV-USERPROFILEX/Desktop XENV-USERPROFILEX/Pictures ENV-USERPROFILEX/pictures F^XENV-SYSTEMDRIVEX\;dat.ini.xml.txt.log.db.lnk

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

Policies			
🕒 Pending Policy C	hanges: 1		
Comment			
Policy-Based Encryption	4		
Commit Policies			
Commit History			
Date Committed	Changed by	Comment	

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.

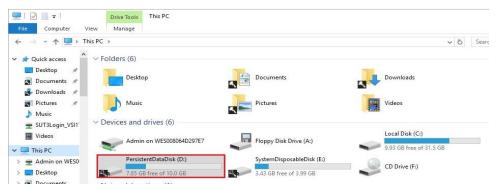
#### 4. Verify policy is active



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

File Home Share	View nis PC > PersistentDataDisk (D:) > Users	» sut3login_vsi1719 > Docu	ments	
🚽 Downloads 💉 ^	Name	Date modified	Туре	Size
💽 Pictures 🛛 🖈	Custom Office Templates	8/3/2016 5:55 PM	File folder	
💧 Music	jw	8/4/2016 9:37 AM	File folder	
🛖 SUT3Login_VSI1'	me me	8/4/2016 9:24 AM	File folder	
Videos	Asd Asd	8/3/2016 5:55 PM	Microsoft Word D	12 K
_	🚮 blah_test	8/3/2016 5:53 PM	Microsoft Word D	0 K
This PC	book1	8/9/2016 11:13 AM	Microsoft Excel W	7 K
🛫 Admin on WESO	book2	8/9/2016 11:05 AM	Microsoft Excel W	7 K
Desktop	PDF1	11/29/2012 10:29	Adobe Acrobat D	1,062 K
Documents	PDF2	11/29/2012 10:29	Adobe Acrobat D	1,098 K

Note: Key icons show that the files are encrypted.

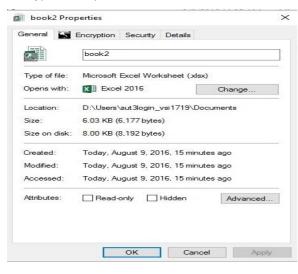
#### 3. Properties

Open	
New	
Print	
Process Directory	
Encrypt for sharing	
Open Dell Data Protection Encryption.	
Scan with Windows Defender	
Open with	
Share with	
Restore previous versions	
Send to	
Cut	
Сору	
Create shortcut	
Delete	
Rename	
Properties	

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

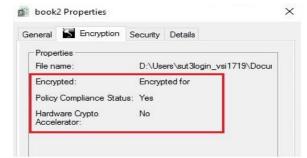
Click Properties.

#### 4. Encryption Properties.



Select the Encryption tab.

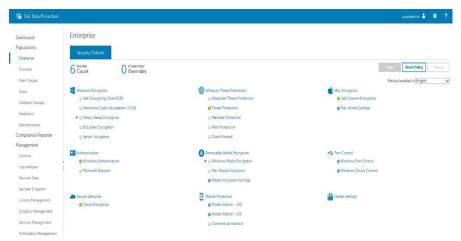
#### 5. File Encrypted properties



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

Enterprise		
Security Policies	Threat Events	
E Return		
Windows Media E	ncryption	
Windows Media Enc	ryption	Current Value
EMS Scan External M	edia	
EMS Access to unShie	elded Media	Read Only V
EMS Block Access to	UnShieldable Media	$\mathbf{\nabla}$
EMS Exclude CD/DVI	) Encryption	
EMS Allow Read-acce	ess to unShielded Media (5.4.x Only)	
EMS Encryption Algo	rithm	AES256 ~
EMS Data Encryption	Key	User Roaming V
EMS Automatic Authe	entication	Local V
EMS Access Encrypte	d Data on unShielded Device	

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

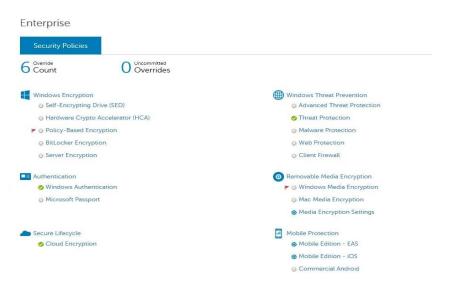
Dashboard	Policies		
Populations	Pending Policy Ch	anges: 1	
Enterprise		2	
Domains	Comment		
User Groups	EMS Enabled		
Users			
Endpoint Groups	Commit Policies		
Endpoints			
Endpoints Administrators	Commit History		
Administrators	Date Committed	Changed by	Comment
Administrators		Changed by superadmin	Comment ATP Enabled
	Date Committed		

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



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

			?	×
Data	Protectio	on	Encr	yption
to enter a comput the devi	this passw ter. ce will be le	ord wh	heneve	r this
	assword to enter a comput the devi	assword for this ex to enter this passw a computer. the device will be le	assword for this external to enter this password wh a computer. the device will be left uns	assword for this external media o to enter this password wheneve

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

External Media Device	Protected		?	×
DØLL	Data Protection	Encryption		
Note that if there were	v files added to this dev unencrypted files on the encrypted state. To als assistance.	his external media p	prior to Shi	ielding,
Volume: (E:\)			0	к

#### 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.

## 7 Appendix

## 7.1 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

# 7.2 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**.

Dell Data Protection			
Dashboard	Enterprise		
Populations Enterprise	Security Policies Advanced Threats	Advanced Threat Events	
Domains	Return		
User Groups			
Users Endpoint Groups	Policy Proxy Polling Interval	360	
Endpoints	Allow Activations	360	
Administrators Reporting	User Experience	-	
Management	Enable Software Auto Updates	-	

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

Dell Data Protection		
Dashboard	Endpoint Groups	
Populations	🕂 Add 🛛 🗑 Delete	
Enterprise		
	Group Name	
Domains	Default Endpoint Group	16
User Groups	Non-Persistent VDI Endpoint Group	10
Users	Opt-In Endpoint Group	0
Users	Persistent VDI Endpoint Group	6
Endpoint Groups		

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

Contraction Dell Data Protection			superadmin 🛔 🔅 🔋
Dashboard	Endpoint Group Detail for: Pe	rsistent VDI Endpoint Group	
<ul> <li>Populations</li> <li>Enterprise</li> </ul>	Security Policies Details & Action	s Members	
Domains	€ Return		Show default settings     Save     Cancel
User Groups			Policies localized in English •
Users	Advanced Threat Protection		
Endpoint Groups	Kadvanced Threat Protection	Current Value	

#### 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.** 

Dell Data Protection	
Dashboard	Policies
<ul> <li>Populations</li> </ul>	O Pending Policy Changes: 15
Enterprise	Comment
Domains User Groups	tum off Activation
Users	Enter a comment for the policy change.
Endpoint Groups	Commit Policies
Endpoints	Commit History
Administrators	Date Committed Changed by Comment
<ul> <li>Reporting</li> <li>Management</li> </ul>	01/12/17 14:42:34 PM superadmin Persistent/DI changes
Commit	

## 7.3 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-suiteenterprise/manuals?rvps=y

## 7.4 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 <u>http://www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research</u>

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 AdminHelp