

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

Re	visions	<u>.</u>	2
1	Introd	luction	5
	1.1	Purpose	5
	1.2	Scope	5
	1.3	Configuration prerequisites	5
2	Soluti	ion 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	Hardv	ware 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	Softw	are 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	t 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	Endpo	pint 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	Apper	ndix	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 <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

6

- 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.

8

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 place 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
TOTALS	20	43	6	846

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	e View	Manage			~	
🖻 💿 🕶 🕇 👪 « I	installers 🕨 Ente	rprise Server 🕨 x64 🕨	~ 0	, Search x64		ρ
 ★ Favorites ■ Desktop ▲ Downloads ▲ Recent places 	Name 0x040c 0x040c 0x0407 0x0409 0x0409		Date modified 22/06/2010 14:35 16/03/2012 14:50 23/03/2010 16:44 22/06/2010 14:37	Type Configuration Sett Configuration sett Configuration sett Configuration sett	Size 26 KB 26 KB 26 KB 22 KB 25 KB	
🌉 This PC	a) Oxf	Open	6/03/2012 12:55	Configuration sett	15 KB	
🗣 Network	Oxe Oxe	Run as administrator Troubleshoot compatibility Pin to Start Share with Restore previous versions Send to Cut Copy Paste	2/04/2012 14:44 2/06/2010 14:40 2/06/2010 14:41 9/01/2016 16:29 9/01/2016 16:29 9/01/2016 16:29 9/01/2016 16:29 9/01/2016 16:29 9/01/2016 16:29	Configuration sett Configuration sett MST File MST File MST File MST File MST File MST File MST File MST File MST File	14 KB 24 KB 25 KB 192 KB 32 KB 184 KB 188 KB 184 KB 284 KB 284 KB	
	20 20 AL	Create shortcut Delete Rename	9/01/2016 16:29 9/01/2016 16:29 9/01/2016 16:28	MST File MST File Setup Information	180 KB 180 KB 1 KB	
	Setup	Properties	9/01/2016 16:29 9/01/2016 16:30	Windows Installer Application	19,490 KB 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

	Dell Enterprise Server x64 - InstallShield Wizard
చ ి	ell Enterprise Server x64 requires the following items to be installed on your computer. lick Install to begin installing these requirements.
Status	Requirement
Pending	Microsoft Visual C++ 2013 Redistributable Package (x64) Pgsql
Pending	Microsoft Visual C++ 2010 SP1 Redistributable Package (x64)
Pending	Microsoft SQL Server 2012 Native Client (x64)
	Install Cancel

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

	DELL END	USER LICENSE		IT - TYPE A		
THIS ENT GLO WO WH COL MAT	IS A LEGAL AGREEME TY) AND DELL PRODU BAL B.V. (SINGAPORE RLDWIDE SUBSIDIARI CH GOVERNS YOUR U LECTIVELY THE SOFTW FRIALS, ONLINE OR EI REOF, TO WHICH THIS	NT BETWEEN Y CTS L.P., A TEX. BRANCH), ON ES AND AFFILI JSE OF THE SOF (ARE PROGRAM LECTRONIC DO S AGREEMENT 1	OU (EITHER AS LIMITED BEHALF OF ATES (COLLE TWARE, TH M, THE ASSO CUMENTAT IS ATTACHE	AN INDIVIDU PARTNERSHIP DELL INC. AND CTIVELY, "Dell E SOFTWARE CLATED MEDI ION, AND ANY D OR OTHERW	AL OR AN , OR DELL ITS " OR "DELL"), SHALL MEAN A, PRINTED COPIES ISE	
1116						

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 Wizard	×
Product K Enter Pro	k ey oduct Key	DELL
Enter the 3	32-character Product Key	
	+ + + + + + + + + + + + + +	
InstallShield —	- Back Next >	Cancel
	< Back Next >	Lancer

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

遐	Dell Enterprise Server x64 - InstallShield Wizard							
Instal	I SSL Certificate							
Se	elect a Digital Certificate for this server:							
0	O Import an existing certificate.							
	Import an existing certificate that was purchased from a Certificate Authority (CA).							
۲	Create a self signed certificate and import it to key store.							
	Create a self signed certificate and import it to key store.							
Note: I authori	t is highly recommended that a digital certificate is utilized from a trusted certificate ty.							
Select ' certifica	Select "Cancel" to quit the installation process and independently purchase a 3rd party certificate.							
InstallShi	eld							
	< Back Next > Cancel							

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

il De	ell Enterprise S	Server x64 -	InstallShi	eld Wizard	i 🔽
Create Self-Sign	ied Certificate				Dett
Please enter inform Fully-qualified	ation that will be in Computer Name: * Required	corporated into	your self-sig COM	ned certificate	•
	Organization:	1			
Or	ganizational Unit:				
	City:]	
	State:	J	Coun	itry (2 letter ab	obrv:) US
InstallShield —					
		< Bac	k	Next >	Cancel

Fill in Information as needed.

Click Next.

12. Install SSOS Certificate

😥 🛛 Dell Enterprise	Server x64 - Instal	IShield Wizard	t 🗙						
Install 5505 Certificate									
Select a Digital Certificate for this ser	Select a Digital Certificate for this server to use for SSOS:								
O Import an existing certificate.									
Import an existing certificate that was purchased from a Certificate Authority (CA).									
Create a self signed certif	icate and import it to	key store.							
Create a self signed certificate and import it to key store.									
Note: It is highly recommended that a digital certificate is utilized from a trusted certificate authority.									
Select "Cancel" to quit the installation process and independently purchase a 3rd party certificate.									
InstallShield									
	< Back	Next >	Cancel						
Import an existing certifi Create a self signed certific Create a self signed certific Note: It is highly recommended that a authority. Select "Cancel" to quit the installation certificate. InstallShield	cate that was purchased icate and import it to ificate and import it to ke a digital certificate is utiliz process and independen < Back	I from a Certificate A key store . ed from a trusted control of the store of the	Authority (CA). ertificate party Cancel						

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

13. Create Self-Signed Certificate

岁 Dell Enterprise S	Server x64 - InstallShield Wizard
Create Self-Signed Certificate	Dest
Please enter information that will be in Fully-qualified Computer Name: * Required	corporated into your self-signed certificate. DD.OSPREY.COM
Organization:	Π
Organizational Unit:	
State:	Country (2 letter abbrv:)
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

i₿	Dell Enterprise Se	erver x64 - Insta	IIShield Wizar	d 🗙
Back Er	d Server Install Setup			\bigcirc
Sele	t ports and host names for bac	k end server		Dell
Click be configu	low to inspect or change host a ration. Values are initialized to o	and port configuration defaults.	n. Select "Next" to a	ccept the
	Ec	dit Hostnames		
		Edit Ports		
U Wo the	ks with Front End to communica DMZ.	ate w <mark>th d</mark> ients interna	ally in your network	or externally in
Host	ild Security Server	Port		
		8443		
InstallShie	d			

Check the ports being used.

Click Edit Ports...

15. Edit Back End Ports



😼 Dell Er	nterprise Se	rver 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			
A DOGINA HONE		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

6	Dell Enterprise S	erver x64 - Inst	allShie	ld Wizard	×
Datab Speci	ase and Install-time Creder ify install-time credentials for the	ntials e installer to set up	the datab	ase	Dest
The install equired: use these Databa	er uses these credentials to au create database, add user, ass credentials. They are used only se server to use: (i.e. ServerN	thenticate to the SQ ign permissions. The v during installation. ame\InstanceName))L server. e installed	These permi Enterprise S	ssions are erver does not
1		~ Brow	vse	Port:	
WinSQL	dows authentication credentials server authentication using the	of current user credentials below			
Login II Passwo	D: Crossian Low wd:	desendentiation			
Name o	of database catalog:				
Name o	of database catalog: Server				Browse
Name of DOP_3	of database catalog: Server Id				Browse

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.

	Question	3
?	The database catalog [DDP_Server_test] does not currently exist on the SQL Server: <i>someSQLServer</i> ,1433	
	Click: - 'YES' To allow the installer to create the catalog. - 'NO' To confirm the catalog name before continuing.	
	Ver	

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 Server x64 - InstallShield Wizard	ĸ
Service Runtime Account Information Specify authentication credentials for the services to use	
Specify the user name and password of the domain service account Dell services will use to access the SQL server. The user account must be in the format DOMAINUJsername and have the SQL server permissions Default Schema: doo and Database Role Membership: db_owner, public.	
 Windows authentication using the credentials below SQL server authentication using the credentials below 	
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

谩	Dell Enterprise Server x64 - InstallShield Wizard	×
Ready The wi	o Install the Program rard is ready to begin installation.	
Click Ir If you exit th	stall to begin the installation. want to review or change any of your installation settings, click Back. Click Cancel to e wizard.	
InstallShield	< Back Install Cancel]

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.

Deploy OVF Template		? Þ
Deploy OVF Template 1 Source 1 Source 1 B Select Source 2 Destination 2 a Select name and folder 2b Select a resource 2c Select storage 3 Ready to complete	Select source Select the source location Enter a URL to download and install the OVF package from the internet, or browse to a location accessible from your compute such as a locating drive, a network share, or a CD/DVD drive. URL Local file Browse	(?))) H,
	Back Next Finish Ci	ancel

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

Deploy OVF Template			(? H
1 Source ✓ 1a Select source	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 Finis	sh Cancel

Click Next.

5. Select Name and Folder

Deploy OVF Template		?
Deploy OVF Template Source Solid Source Destination Solid Soli	Select name and location for the deployed template Name: Select a folder or datacenter Select a folder or datacenter Select name DDP-VC Osprey Com DDP-VE Osprey Cem Select Area Select name	The folder you select is where the entity will be located, and will be used to apply permissions to it.
	Test Test Test MiwareViewComposerReplicaFolder	The name of the entity must be unique within each vCenter Sener VM folder.
		Back Next Finish Cancel

Name: enterName for VE,

Click datacenter Icon

Click Next.

6. Select storage

Deploy Ovi Template							0
1 Source 1 Selectsource	Select storage Select location to store the	e files for the deployed	template				
1b Review details	Select virtual disk format:	Thick Provision Lazy	Zeroed	•			
2 Destination	VM Storage Policy:	Datastore Default		-			
2a Select name and folder	The following datastores	are accessible from th	e destination reso	urce that	you selected. Select	the destination d	atastore for the
2b Select storage	virtual machine configurat	ion files and all of the	virtual disks.				
2c Setup networks	Name	Capacity	Provisione	ed	Free	Туре	Storage DRS
3 Ready to complete	LocalDisk	1.06 TB	1.36 TB		147.93 GB	VMFS	

Click Next.

7. Setup networks

1 Source	Setup networks Configure the networks the deployed template should use				
1a Selectsource 1b Review details 2 Destination	Source bridged	Destination VM Network 2	Configuration		
2a Select name and folder 2b Select storage 2c Setup networks					
/ 3 Ready to complete	IP protocol: IPv4 Source: bridged - Description The bridged network	IP allocation: State - M	tanual		
	Destination: VM Network 2 - Pro No configuration needed for this	tocol settings			

Change the networks if needed.

Click Next.

8. Ready to complete

D¢l

Deploy OVF Template						(?) H
Deploy OVF Template 1 Source 1 Source 1 Source 1 B Select source 2 Destination 2 2 Select name and folder 2 2 Select storage 2 C Setup networks 3 Ready to complete	Ready to complete Review your settings selections be OVF file Download size Size on disk Name Datastore Target Folider Disk storage Network mapping IE allocation	fore finishing the wizard. Nospreyfile/Osprey-Backup/Softwar Enterprise Server/VEI/DDP Enterpri 1.2.08 80.0.08 V V LocalDisk ddp-ese.osprey.com DDP Thick Provision Lazy Zeroed bridged to M Network 2	re\DDP-ESS\DD se Server - VE v	0P-Enterprise 9,4.0 build 8.0	Server-VE-9.4.	(?) N 0.8(DDP
	IP allocation	Static - Manual, IPv4	Back	Next	Finish	Cancel

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

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)
Select 1	< Display EULA >	form or quit

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

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"), DEASE READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY, "ULLUIN, 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 BOWNLOADING, 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 ENTRETY WITHOUT LIMITATION OR QUALIFICATION. IF YOU DO NOT AGREE TO BEDWIND BY THE TERMS AND CONDITIONS OF THIS EULA AND ALL APPLICABLE LAWS AND REGULATIONS IN THEIR ENTRETY WITHOUT LIMITATION OR QUALIFICATION. IF YOU DO NOT AGREE TO A BROWN BY THE TERMS AND CONDITIONS OF THIS EULA, ND THAT YOU DANGREE TO ARBEE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS EULA, AND ALL APPLICABLE LAWS AND REGULATIONS IN THEIR ENTRETY WITHOUT LIMITATION OR DUAL FICATION. IF YOU DO NOT AGREE TO A FOLL REFUND. IF YOU ARE AN INDIVIDUAL THEN YOU MAY NOT DOMNLOAD, INSTALL, ACTIVATE OR OTHERWISE USE ANY OF THE SOFTWARE AND YOU MUST PROMPTLY RETURN THE SOFTWARE AND ANY HARDWARE TO WHICH IT IS ASTLCHED AS DIRECTED BY DELLOR ITS RESELLER (IF APPLICABLE) FOR A FULL REFUND. IF YOU ARE AN INDIVIDUAL REPRESENTING AN ENTITY, YOU ACKNOMLEDGE

License. rovided that Dell receives timely payment for the Software and you comply with the terms, anditions and restrictions of this EULA (as a condition to the grant below), Dell hereby rants you a limited, personal, nonexclusive, nontransferable, non-assignable license, ithout 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, evices and/or in such configurations as expressly permitted by Dell (e.g., as set forth Use Arrow keys or Pg=Up/Own to move in text

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



Use arrow key to select < Accept EULA >.

Press the Enter Key.

Select Default Mode. 3.



Press the Enter Key.

4. Change ddpuser password

📌 BaseVE - VMware Remote Console		
VMRC 🕶 🔢 🕶 🖧 🖽		*
1.		
	Would you like to change the default	
	password for ddpuser?	
	< Yes > < No >	



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

	Set ddpuser Password	
* Enter Current Password * Enter New Password * Re-enter New Password		
	< OK > < Cancel >	

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 • DNS Server 1 • DNS Server 2 • DNS Server 3	: (X)	
	< OK > < Cancel >	
Press the spacebar to select	: 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

<pre>< Europe/Copenhagen < Europe/Dublin < Europe/Gibraltar</pre>		
< Europe/Guernsey < Europe/Helsinki	>	
< Europe/Isle_of_Man < Europe/Istanbul	>	
< Europe/Jersey < Europe/Kaliningrad	>	
< Europe/Kiev < Europe/Lisbon		
< Europe/Ljubljana < Europe/London		
]	

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

	DDP Enterprise Server - VE v9.6.0 Build 14 - Ad	ministration Console	
lostname: dellddp			IP: 10.50.168.40
	Main Menu		
	< Set Language:	\$	
	(current setting: English US)		
	<pre>< Basic Configuration < Advanced Configuration</pre>	>	
	< Server Status	>	
	< Launch Shell		
	< Support Tools	2	
Use <up> and <down> arr</down></up>	ow keys to navigate between items. <esc> key to</esc>	move one level up and <	Alt+g> to guit at
iny level.	the state of the s	and the rest of and	and, to dare at

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

SSH configuration for ddpsupport, ddpconsole and ddpuser			
Enable SSH for ddpsupport for ddpsupport for ddpuser	: (X) : [] : []		
	< OK > < Cancel >		
spacebar to select between s	ssh 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 E	sc key to exit	
Dell Message Broker Dell Identity Server Dell Compatibility Server Dell Scompitibility Server Dell Compliance Reporter Dell Core Server Dell Core Server HA Dell Inventory 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 datab under Main Menu > View Logs.	i to the menu. Changes in So asecustomizer process faile	ervice status may take seven d. To troubleshoot, check th	al minutes. If a Service ne 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

	Open	
•	Run as administrator	
	Troubleshoot compatibility	
	Pin to Start	
	Process Directory	
	Encrypt for sharing	
	Open Dell Data Protection Er	cryption
	Scan with Windows Defende	r
	Share with	>
	Pin to taskbar	
	Restore previous versions	
	Send to	>
	Cut	
	Сору	
	Paste	
	Create shortcut	
	Delete	
	Rename	
	Properties	

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.

闄 VMware Horizon Agent	- 🗆 🗙		
	Welcome to the installer for VMware Horizon Agent		
	VMware Horizon Agent Setup is preparing the installer which will guide you through the program setup process. Please wait.		
VMware Horizon [™]			
Agent			
ĊPC@IP			
	< Back Next > Cancel		

Click Next

3. License Agreement

🛃 VMware Horizon Agent			×
License Agreement Please read the following license agre	ement carefully.		6
VMWARE END USER LIC	ENSE AGREI	EMENT	^
PLEASE NOTE THAT THE LICENSE AGREEMENT S THE SOFTWARE, REGAR MAY APPEAR DURING TH SOFTWARE.	E TERMS OF HALL GOVER DLESS OF A HE INSTALLA	THIS END U RN YOUR US NY TERMS 1 TION OF TH	SER SE OF THAT E
 I accept the terms in the license agree 	ement		
O I do not accept the terms in the licens	e agreement		
	< Back	Next >	Cancel

Select I accept the terms in the license agreement.

Click Next

4. Network protocol configuration

😸 VMware Horizon Agent		×
Network protocol configuration Select the communication protocol		2
Specify the protocol to be used to c IPv4 IPv6 all connections	onfigure this Horizon Agent instanc be configured to choose the IPv4 p ,	e: rotocol for establishing
	< Back Next >	Cancel

In our example we used IPv4.

Click Next

5. Custom Setup

🛃 VMva	/are Horizon A	gent				×
Custon Select	n Setup : the program fe	atures you want ir	nstalled.			P
Click on	an icon in the lis	t below to change direction rive Redirection e Horizon 7 Persona ard Redirection e Audio edirection	how a feal	ture is ins Featur VMware This fea drive.	italled. e Description e Horizon Agent coi ature requires 2501	re functionality 48 on your hard
<			>			
C:\Progr): ram Files\VMwar	e\VMware View\Aç	jent\			Change
	Help	Space	< B	ack	Next >	Cancel

Select USB Redirection.

Select the program features	; you want installed.	2
Core Core Core Core Core Core Core Core	v to change how a feature is Fea USE will be installed on local h and all subfeatures, will b	s installed. ature Description 3 Redirection. Refer to the VMware izon Z Security document for guidance and drive. e installed on local hard drive.
<	driv	e.
nstall to:		Change

Select This feature will be installed on local hard drive.

6. VMware Horizon Agent

				and the second second
istom Setup				
Select the program f	eatures you want insta	lled.		
k on an icon in the li	st below to change how	v a feature is ins	talled.	
- Core		Featur	e Description	
VMware Horizon . 	Agent to the VMware Horiza USB redirection secul	on 7 Security de rely.	ocument for guidar	×
VMware Horizon . 	Agent to the VMware Horizo USB redirection secu	on 7 Security d rely.	ocument for guidar	X nce on
VMware Horizon .	Agent to the VMware Horizo USB redirection secu	on 7 Security de rely.	ocument for guidar	X nce on OK
VMware Horizon . Refer using	Agent to the VMware Horizo USB redirection secu	on 7 Security de rely.	ocument for guidar	OK Change

Click OK

Click Next

7. Register with Horizon 7 Connection Server

VMware Hori	zon Agent			×
Register with	Horizon 7 Connectio	n Server		
Enter the Hor	izon 7 Connection Serve	er that this machine v	vill connect to.	
Enter the server administrator log	r name of a Horizon 7 Co gin credentials to registe	onnection Server (st. er this machine with t	andard or replica inst he Horizon 7 Connec	tance) and tion Server. 2 address)
I			(noscialite of 1	0001000)
Authentication:	Authenticate as the second	he currently logged (on user	000,000
Authentication:	 Authenticate as the second seco	he currently logged a ator credentials	on user	000000
Authentication:	Authenticate as the standard of the second secon	he currently logged a ator credentials	on user	claic, c, c
Authentication:	Authenticate as the second	he currently logged a ator credentials	nuser (Domair	n\User)
Authentication:	Authenticate as the specify administrative specify administrative specify administrative specific s	he currently logged a ator credentials	on user (Domair	n\User)
Authentication:	Authenticate as the second secon	he currently logged a ator credentials	on user (Domain	n\User)
Authentication:	Authenticate as the second secon	he currently logged a ator credentials	(riostriance of a	n\User)

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.			6
VMware Horizon Agent will be installed in			
C:\Program Files\VMware\VMware View\	Agent\		
Click Install to begin the installation or Ca	ancel to exit the	e 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					
	< Back Finish Cancel				

Click Finish

10. VMware Horizon Agent Installer Information

谩 VMwa	re Horizon Agent Installer	r Information	×
1	You must restart your sys changes made to VMware effect. Click Yes to restarl restart later.	tem for the configuratior Horizon Agent to take t now or No if you plan to	ו ס
	Yes	No	

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 lcons should be visible.
 - b. 🌋 🕎 = Options 🗸 🛊 Connect USB Device 🖌 🖨 Send Ctrl-Alt-Delete
 - 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

O DDP Tenapoint Security Suite	×
Extracting DDP Endpoint Security Suite Instal	ller
28% Cancel	
Dell Data Protection Endpoint Security Suite - InstallShield Wizard	×
	Dell
Setup Status	
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes.	ion. This
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes. Installing Prerequisites, please wait	ion. This
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes. Installing Prerequisites, please wait	ion. This
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes. Installing Prerequisites, please wait	ion. This
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes. Installing Prerequisites, please wait	ion. This
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes. Installing Prerequisites, please wait	ion. This
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes. Installing Prerequisites, please wait	ion. This
Dell Data Protection Endpoint Security Suite is configuring your software installati may take a couple of minutes. Installing Prerequisites, please wait	on. This

Install will continue to the Welcome screen.

3. Welcome



On the Welcome screen, click Next.

4. License Agreement

ease read the following license agreement carefully.	Del
DELL END USER LICENSE AGREEMENT - TYPE A APPLICATION SOFTWARE	^
THIS IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL O ENTITY) AND DELL PRODUCTS L.P., A TEXAS LIMITED PARTNERSHIP, OF GLOBAL B.V. (SINGAPORE BRANCH), ON BEHALF OF DELL INC. AND ITS WORLDWIDE SUBSIDIARIES AND AFFILIATES (COLLECTIVELY, "Dell" OF "DELL"), WHICH GOVERNS YOUR USE OF THE SOFTWARE. THE SOFTW, SHALL MEAN COLLECTIVELY THE SOFTWARE PROGRAM, THE ASSOCIAT MEDIA, PRINTED MATERIALS, ONLINE OR ELECTRONIC DOCUMENTATI AND ANY COPIES THEREOF. TO WHICH THIS AGREEMENT IS ATTACHED	ARE ED ON, OR
I accept the terms of the license agreement	Print
I do not 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

ell Data Protection Endpoint Security Suite - InstallShield Wizard	×
Dell 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/	
stallShield	
< 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

Dell Data Protection	n Endpoint Security	Suite - InstallShield W	/izard	×
Choose Destination	on Location ere setup will install files	s.		Dell
Install C:\Pro	Dell Data Protection E)gram Files\Dell\Dell Da	ndpoint Security Suite t ata Protection\	o:	Change
InstallShield		< Back	Next >	Cancel

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

Click Next.

7. Select Features

C
e features you do not want to install. Description Installs the underlying security framework and Security Tools, the advanced authentication client that manages multiple authentication methods, including PBA and credentials such as fingerprints and passwords.

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 ye the wizard.	our installation settings, click Back. C	lick Cancel to exit

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

Click Install.

	\sim
	Dell
ietup Status	
ell Data Protection Endpoint Secur nay take a couple of minutes.	ity Suite is configuring your software installation. This
Preparing to Install, please wait	
Shield	

The installation will take some time to complete.

9. Installation Wizard Complete

Dell Data Protection | Endpoint Security Suite - InstallShield Wizard



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" /I*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, nonmanaged 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





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



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



54 Dell Data Protection | Endpoint Security Suite Enterprise for VDI with VMware | January 2017



14. English

0.0	. [0						16
€ 6	🔹 🕆 💱 🕻 Control Panel	All Control Panel Items	Language 🕨 Add languages	 Regional variants 		¥ (Search regional variari
	Add a language Use the search box to find more	e 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 Kingdor
	English (United States)	English (Zimbabwe)					

- 16. Click English (United States).
- 17. Change language preference



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

(€) - ↑ 🗣 • Contro	ol Panel 🕨 All Control Panel	Items 🕨 Language	v 🖒 Search Control Panel
Control Panel Home Advanced settings	Change your lang Add languages you wa	juage preferences nt 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 moo	st often).
Change date, time, or numbe formats	er Add a language Ren	nove Move up Move down	
	English (United States)	Windows display language Enabled Keyboard layout: US Date, time, and number formatting	0
	English (United Kingdom)	Windows display language: Available for download Keyboard layout: United Kingdom	a

- 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

https://ddpeese.c	sprey.com:8443/webui/manageDomain	S≣÷Q
🔞 Dell Data Protect	ion	
Dashboard	Domains	
Populations	🕂 Add	
Enterprise	Domain Namo	location
Domains	Non-Domain Users	(none)
User Groups		
Users		

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:		
User Name:	Enter LDAP username@domain.com	
Password:		
Alias		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

Security Policies	Details & Actions	Members	Settings	Key Server
Details				
Domain Name				
Location				
LDAP Url				
Comment	Cood			

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	icenses							
Enterprise									
Domeins	Choose								
User Groups	Client Li	icenses Owned							
Users	Alert	Туре	Valid From	Valid To		Count	5	Status	
Endpoint Groups		Mobile Edition	1/1/1753 12:00 AM	12/31/999	9 11:59 PM		10 1	None	Delete
Endpoints		Shield for Server	1/1/1753 12:00 AM	12/31/999	99 11:59 PM		4 1	None	Delete
Administrators		Enterprise Edition	1/1/1753 12:00 AM	12/31/999	P9 11 59 PM		10 1	Nome	Delote
Compliance Reporter		Cloud Edition	1/1/1753 12:00 AM	12/31/999	9 11:59 PM		10 1	None	Delete
Management		Estantial Made Estimat	1/1/1763 12-00 444	12/31/000	0 11 CO DAA		10.1	Marine 1	Datara
Commit		Electric media Edition	1/ 1/ 1/ 33 10, 550 PMT		12.22.33.114		200.000	(HORM)	Desete
Log Analyzer	1 Client Li	icense Usage							
Recover Data	Alert	Туре	Total	Used					
Recover Endpoint		Enterprise Edition	10	0					
License Management		Cloud Edition	10	0					
Contract of the second second		External Media Edition	20	0					
Dropbox Management		Mobile Edition	10	0					
Services Management		BitLocker Manager	20	0					
Alizaba Managamana a		Threet Protection	10	0					
wents management		Shield for Caner							

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

		Choose File to Upload	ł			
🔿 💿 👻 🕆 📕 🕨 Thi	is PC → johnw (\\aspreyfile) (R	b) > DDPE > 250_DE		v 🖒 Search i	50_DE	,P
Organize New folde	r				III • 🔲	
🔆 Favorites	Name	Date modified	Туре	Size		
E Desktop	250_DE	09/09/2013 13:48	XML Document	3 KB		
🚴 Downloads						
Secent places						
This PC						
Desktop						
Downloads						
Music						
Pictures						
Videos						
🏭 Local Disk (C:)						
😪 johnw (\\ospreyfile)						
🙀 Network						
File na	me: 250_DE			✓ All File	(*.*)	
				0	en Canc	el

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

3. Upload License

0	1 license(s) uploaded successfully. 0 license(s) failed to upload.
	Success: • The Enterprise Edition license () successfully uploaded.

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

16 Del Data Protection					spece 4 0 ?
Dashboard Reputations	Enterprise Secury Policies				
Domine User Groups	6 Count	0 Overrides			Rear Pulsy Const
Users Endpoint Groups Endpoints Admendments Compliance Reporter	 Ninkow Encryption Gali-throughing D Handware Crypto Onlog-texast Drop Biologies Encryption Server Encryption 	ner BADI Acasianson SI-CAI ygman an	Birecout Thread Prevention Ordencout Thread Prevention Ordencout Thread Prevention Walknew Prevention Orden Thread Thread Orden Thread	Arec Drougenes Cost Internet Transform Mite Clobel Series	
Manapement Convert Log Assigner Recover Deta	Authentication O Microsoft Passpor	cuincin e	Ferrosstöle Media Entryston Voltaberi Media Entryston Media Entryston Media Entryston Media Entryston Media Entryston	 ≪Ge Port-Carend ♦ Stractions Fort Carend ♦ Windows Events 	
Recover Endpoint Examps Vanegement Displace Menagement Services Menagement	Secure Unity de		 Michie Protection Wolder Edition - 163 Michie Ostene - 203 Conversited Marcel 	Global Serings	

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	Seve	Cancel
Advanced Threat Protection	Comm Value				
Advanced Threat Protection	On OF				
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	
	\Windows\System32\CmgShieldService.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.

erprise		
curity Policies Threat Events		
um.		Show default settings
Advanced Threat Protection		
Advanced Threat Protection	Current Value or or	
File Action: Unsafe Executable Auto Quarantine With Executable Control Enabled	8	
File Action: Unsafe Executable Auto Upload Enabled	2	

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

Click On to enable protection.

Click Save.

4. Commit

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



Dashboard	Enterprise		
Populations Enterprise	Security Policies Threat Events		
Domeine	3 Count O Overrides		
User Groups	Windows Encryption	Windows Threat Prevention	Mac Encryption
Users	O Self-Encrypting Drive (SED)	P 🖉 Advanced Threat Protection	O Dell Volume Encryptic
Federalet Genues	Q Hardware Crypto Accelerator (HCA)	P @ Threas Protection	Mac Global Sattings
	O File/Folder Encryption (FFE)	O Malware Protection	
Endpoints	O BisLocker Encryption	O Web Protection	
Administrators	o Server Encryption	() Client Frewall	

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



Enterprise Security Policies	
Return	
Policy-Based Encryption	Current Value
Policy-Based Encryption	On Off
Application Data Encryption Key	Common V
SDE Encryption Enabled	
SDE Encryption Rules	F#3 - ASUNY-SYSTEMBORYSS/System Volume Information - ASUNY-SYSTEMBOOTSS-SILease ays accuman cat-manifest policy - ASUNY-SYSTEMBOOTSS/System32 - ASUNY-SYSTEMBOOTSS/SYSTEM32 - ASUNY-SYSTEMBOOTSS/SYSTEM32/cmd.exc.oxe - ASUNY-SYSTEMBOOTSS/SYSTEM32/cmd.exc.oxe
K Common Encrypted Folders	XENV:SYSTEMDRIVEX \accdb.doc.docm.docx.mdb.pdf.ppam.pps.ppam.ppsx.ppt.pptm.ppt XENV.USERPROFILEX/Dosktop XENV.USERPROFILEX/Downloads XENV.USERPROFILEX/Documes \~XENV.SYSTEMDRIVEX\dat.ini.xml.pt.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	n		
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

÷ → × ↑ 🖹 > Th	is 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 WES0	book2	8/9/2016 11:05 AM	Microsoft Excel W	7 K
E 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	

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

Click Properties.

4. Encryption Properties.

erierai 🔼	Encryption Security	Details	
	book2		
Type of file:	Microsoft Excel Works	sheet (xlsx)	
Opens with:	Excel 2016		Change
Location:	D:\Users\sut3login_v	si 1719\Docu	ments
Size:	6.03 KB (6,177 bytes)		
Size on disk:	8.00 KB (8,192 bytes)		
Created:	Today, August 9, 201	6, 15 minutes	ago
Modified:	Today, August 9, 201	6, 15 minutes	ago
Accessed:	Today, August 9, 201	6, 15 minutes	ago
Attributes:	Read-only	idden	Advanced

Select the Encryption tab.

5. File Encrypted properties

eneral	5	Encryptic	on Se	ecurity	Details		
Prope	erties						
File n	ame:			D:\Us	ers\sut3log	gin_vsi1719	9\Docu
Encry	pted:			Encryp	ted for		
Policy	Com	pliance S	tatus:	Yes			
Hard	ware C lerator	Crypto		No			

This indicates that the file is encrypted.

6.2.5 EMS Policy Configuration

1. Removable Media Policy Configuration



1 Del Data Protection				speratres 1 0 ?
Dashboard Populations	Enterprise Secury Police			
Domains User Croups	6 Count	0 Overrides		News Publicy Const
Unors Endedier Concern	Windows Encryption () Self-Encryption	ng Dave (SED)	Windows Threat Preventions () Advanced Threat Protections	Muc Excryption OVI Volume Encryption
Endpoince	© Hertikere Cry P. Q. Policy-Devel	pto Accelentor 9-CAI Encryption	Threat Protection Allowing Protection	 Mac Global Lettings
Administrators Compliance Reporter	© Brüccher End	-ypion	© Web Protection © Clarit Frend	
Management.	Authentication		Removable Media Encryption	+Q+ Ten Control
Log Analytier	 Kimbows Auth Microsoft Peo 	tension aport	 Windows Media Encryption Wat: Media Encryption 	e Windows Fort Control e Windows Device Control
Recover Deta Recover Enclosert			Made Encryption Settings	
Conta Nanagement	 Secure Lifecycle Oraud Encrypt 	con	Mobile Protection	Cichel Gerings
Services Management			Hotole Edition - ICS O Conversitied Antinoid	
Notification Management				

Click Enterprise in the left pane.

Select Removable Media Encryption.

2. Windows Media Encryption

Enterprise		
Security Policies	Threat Events	
Eturn		
Windows Media E	ncryption	
Windows Media End	cryption	Current Value
EMS Scan External M	ledia	
EMS Access to unSh	ielded Media	Read Only 🗸
EMS Block Access to	UnShieldable Media	Y
EMS Exclude CD/DV	D Encryption	
EMS Allow Read-acc	cess to unShielded Media (5.4.x Only)	
EMS Encryption Algo	prithm	AES256 V
EMS Data Encryption	n Key	User Roaming 🗸
EMS Automatic Auth	entication	Local V
EMS Access Encrypt	ed Data on unShielded Device	N

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

C Dell Data Protection			
Dashboard	Policies		
 Populations Enterprise 	Pending Policy Ch Comment	anges: 1	
Domains User Groups	EMS Enabled		
Users			
Endpoint Groups	Commit Policies		
Endpoints Administrators	Commit History		
Compliance Reporter	Date Committed	Changed by	Comment
compliance Reporter	06/20/16 11:45:56 AM	superadmin	ATP Enabled
Management	06/20/16 11:23:03 AM	superadmin	TP off
Commit	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

Enterprise	
Security Policies	
6 Count 0 Uncommitted Overrides	
Windows Encryption	Windows Threat Prevention
Self-Encrypting Drive (SED)	Advanced Threat Protection
Hardware Crypto Accelerator (HCA)	O Threat Protection
Policy-Based Encryption	Malware Protection
BitLocker Encryption	 Web Protection
© Server Encryption	Client Firewall
Authentication	Removable Media Encryption
Windows Authentication	Windows Media Encryption
Microsoft Passport	Mac Media Encryption
	Media Encryption Settings
Secure Lifecycle	Mobile Protection
Cloud Encryption	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

Inprotected Media	Found	?	×
D¢LL	Data Protection Er	ncryption	
Based on security or	olicies, data moved from this co	mouter to any ex	vternal
media device must b If you select "No", y	e encrypted. Would you like to you will be granted read-only ac	cess to the devic	e.

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

Enter New Password			?	×
D¢LL	Data	Protecti	on Enc	ryption
Please create a new You may be prompted device is inserted into If you select "Cancel you will be granted re Volume: (E:\)	password d to enter a compu , the dev ad-only a	for this ex this passw ter. rice will be le access to th	ternal media ord whenev eft unshield ne device.	a device. ver this ed but
New Password: [Retype Password: [1			
		OK	Ca	ancel

New Password: thisIsYourPassword

Retype Password: *thisIsYourPassword*

Click OK.

7. Shielding External Device

Shielding External Device		?	×
DØLL	Data Protection	Encrypti	on
Your external device until this process is co	is being shielded. Do not omplete!	eject your d	evice
-			

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**.

1 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
Administrators	Allow Activations	0
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	1		
Dashboard	Endpoint Groups		
Populations	Add Telete		
Enterprise	•		
	Group Name	Count	
Domains	Default Endpoint Group	16	
User Groups	Non-Persistent VDI Endpoint Group	10	
11	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.

1 Dell Data Protection		superadmin 🛔 🔍 ?
Dashboard	Endpoint Group Detail for: Persistent VDI Endpoint Group	
 Populations Enterprise 	Security Policies Details & Actions Members	
Domains	€ Return	Show default settings Save Cancel
User Groups		Policies localized in English
Users	Advanced Threat Protection	
Endpoint Groups	Advanced Threat Protection On On	
Endersietz		

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				
Populations	O Pending Policy Changes: 15				
Enterprise	Comment Turn off Activeton Enter a comment for the policy change.				
User Groups					
Endpoint Groups	Commit Polides				
Endpoints Administrators	Commit History				
Reporting	Date Commenta Changeo by Comment. 0/1/2/174-4234PM supersonin Pensitient/00/changes.				
- Management					
Comme	1				

A.3 Recommended VDI policies

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

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 <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 Admin Help