Dell Data Protection | Endpoint Security Suite Enterprise
Endpoint Security Suite Enterprise Support for VDI v1.3
Endpoint Security Suite Enterprise Support for VDI

2017 - 02

Rev. A02
## Contents

1 Introduction ................................................................................................................................. 4
   VDI Deployment Models .............................................................................................................. 4
   Supported Features .................................................................................................................... 4
      Encryption .......................................................................................................................... 4
      Advanced Threat Prevention .............................................................................................. 5
   Contact Dell ProSupport ........................................................................................................ 5

2 Requirements .............................................................................................................................. 6
   Server Deployment Recommendations ....................................................................................... 6
   Unsupported Features ................................................................................................................. 7

3 Dell Server Policy and Configuration Requirements ................................................................. 8
   VDI Endpoint Group Policy ........................................................................................................ 8
   VDI User Policy ....................................................................................................................... 9
   Enable Activations ................................................................................................................... 10

4 Provision the VMware VDI Clone Pool ...................................................................................... 11

5 Provision the Citrix VDI Clone Pool ............................................................................................ 12

6 Prepare VMware Removable Media .......................................................................................... 13

7 Licensing Considerations .......................................................................................................... 14
   Persistent VDI ........................................................................................................................ 14
   Non-Persistent VDI ............................................................................................................... 14
   Key Material .......................................................................................................................... 15
Introduction

There are two main Virtual Desktop Infrastructure (VDI) architectures used by the Dell Cloud Client-Computing (CCC) team: VMware and Citrix. Endpoint Security Suite Enterprise - Support for VDI integrates the Citrix architecture and Endpoint Security Suite Enterprise. It also includes support for Endpoint Security Suite Enterprise in VMware VDI environments.

VDI Deployment Models

There are two models for Virtual Desktop Infrastructure (VDI) deployment: Persistent and Non-Persistent. Endpoint Security Suite Enterprise supports the Persistent and Non-Persistent VDI models with Citrix and VMware.

Persistent VDI - After the image is deployed, it can be modified by each end user. Users' changes are saved for future sessions and these changes persist until the VDI clone pool is rebuilt. Also, VDI persistence dedicates a specific Virtual Machine in the VDI pool to a specific user and only that user can access that specific Virtual Machine. The user can store data in the personal vdisk that resides within the Virtual Machine.

**NOTE:** The personal vdisk is not saved after a VDI clone pool rebuild.

Non-Persistent VDI - After the image is deployed, the image cannot be modified and then saved by the end user. The session is dedicated to a single user while in use and is then returned to the pool at log-off.

Deployments of a VDI persistent pool can vary greatly. An example of a large-scale VDI environment may be considered to be a delivery group of 150-200 simultaneous Virtual Machines. The VDI clone pool reconstruction may be needed for several reasons. For example, updates to the applications or operating system in the VDI environment would require the updates to be made in the VDI template master, the current VDI clone pool torn down and rebuilt or updated, based on the updated VDI template master. Impact to this methodology will be taken into account with regards to Phase 1 and any discrepancies will be considered in future releases.


Supported Features

Supported features include Encryption and Advanced Threat Prevention.

Encryption

The encryption feature includes encryption of both removable media (External Media Shield, or EMS) and fixed drives (Policy-Based Encryption).

External Media Shield protects removable media (for example, flash drives) by encrypting them. Use the user roaming key.

Policy-Based Encryption protects files on local fixed drives by encrypting their files and folders. Use either the common or user key types.
Advanced Threat Prevention

The Advanced Threat Prevention feature protects the VDI Virtual Machine clones from malware and virus attacks.

The Dell Enterprise Server architecture is based on Microsoft Windows Server 2012 R2. Virtual Desktop Infrastructure architecture uses the Virtual Edition architecture because it is based on the Microsoft Windows Server 2012 R2 with Hyper-V as the hypervisor.

**NOTE:**

Persistent and non-persistent clients' Protected status differs in the Dell Server Remote Management Console:

- **Persistent** - Following the first restart after activation, the client status is Protected.
- **Non-Persistent** - The client status does not change to Protected after activation, since the virtual machine does not retain the client instance after restart.

Contact Dell ProSupport

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

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

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

For phone numbers outside of the United States, check Dell ProSupport International Phone Numbers.
The following components are required to run Endpoint Security Suite Enterprise - Support for VDI.

**Required Components**

- Virtual Desktop Infrastructure Thin Clients (for example, Wyse 7020) on standard endpoints

  **NOTE:** Protection of Virtual Desktop Infrastructure Thin Clients will be handled in future releases.

- Virtual Desktop Infrastructure Clone Pool Protection

**Server Deployment Recommendations**

**Software Prerequisites (Citrix VDI)**

- Virtual Desktop Infrastructure Architecture
- Windows Server 2012 R2 with Hyper-V enabled
- System Center Virtual Machine Manager (SCVMM) 2012 R2
- XenDesktop 7.8
- Dell Data Protection architecture components
- Dell Enterprise Server v9.6
- Endpoint Security Suite Enterprise v1.3

For more information, see "Software Inventory" in the document, *Dell Data Protection | Endpoint Security Suite Enterprise for Citrix*.

**Software Prerequisites (VMware VDI)**

- VMware ESXi v 6 Update 2a
- VMware Horizon View v7.0.1
- VMware Appliance v 6.0.0
- VMware Composer v 7.0.1
- Microsoft SQL Server 2014 Standard Edition
Software Prerequisites (VMware VDI)

- Dell Enterprise Server v9.6
  
or
- Virtual Edition v9.6

- Endpoint Security Suite Enterprise v1.3

- Certificates supported by the operating system

For more information, see "Software Inventory" in the document, *Dell Data Protection | Endpoint Security Suite Enterprise for VMware*.

Client Software Prerequisites VMware VDI

- Windows 10 Enterprise Edition

**NOTE:** Client operating system validation was done on the latest version of the Windows operating system, Windows 10. Refer to Endpoint Security Suite Enterprise Advanced Installation Guide for a complete list of supported operating systems. Refer to the appropriate vendor documentation for information about a specific operating system.

Unsupported Features

This table lists the Endpoint Security Suite Enterprise features that are not supported with VDI:

**Unsupported Features**

- System Data Encryption
- SED Management
- BitLocker Manager
- Advanced Authentication
Before deployment, follow VDI Endpoint Group and User policy and configuration requirements explained in this section:

VDI Endpoint Group Policy

VDI User Policy

Enable Activations

When logging into the VDI master template, user accounts will be non-domain. Use only local administrator accounts to prevent Endpoint Security Suite Enterprise activations.

**NOTE:**
Endpoint Security Suite Enterprise should be installed within the VDI clone pool, into the clone Virtual Machines themselves and not into the master template. Future investigation will include deployment of Endpoint Security Suite Enterprise into the VDI master template.

For the list of unsupported Endpoint Security Suite Enterprise features, refer to [Unsupported Features](#).

**VDI Endpoint Group Policy**

VDI Endpoint Groups are system groups, maintained by Dell Server.

Upon activation, a VDI endpoint is added to the appropriate VDI Endpoint Group on Dell Server, and policies are sent to the endpoint. Persistent VDI Endpoint Groups and Non-Persistent VDI Endpoint Groups are System Endpoint Groups, which are maintained by Dell Server.

Policy settings differ, based on whether persistent or non-persistent VDI is deployed in the environment.

The policy requirements below are for VDI endpoints running Endpoint Security Suite Enterprise. The list includes only policies that are significant for VDI endpoints. VDI User policy settings must also meet certain requirements. See [VDI User Policy](#).

**NOTE:** Ensure that you turn off Advanced Threat Prevention Agent Auto Update. In the left pane of the Remote Management Console, select Management > Services Management > Advanced Threats Agent Auto Update, then select Off.

**NOTE:** With Persistent VDI Groups, ensure that roaming user profiles are configured.

These policy and configuration settings for VDI Endpoint Groups must be configured before VDI client activation:

<table>
<thead>
<tr>
<th>Technology</th>
<th>Category</th>
<th>Policy or Setting</th>
<th>Persistent VDI Group setting</th>
<th>Non-Persistent VDI Group setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Encryption</td>
<td>Self-Encrypting Drive (SED)</td>
<td>Self-Encrypting Drive (SED)</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>
Windows Encryption
  Hardware Crypto Accelerator (HCA)  Hardware Crypto Accelerator (HCA)  Off  Off
Windows Encryption
  Policy-Based Encryption  SDE Encryption Enabled  Not Selected  Not Selected
Windows Encryption
  Policy-Based Encryption  Common Encrypted Folders  <retain default settings>  <retain default settings>
Windows Encryption
  Policy-Based Encryption  Encrypt Windows Paging File  Not Selected  Not Selected
Windows Encryption
  Policy-Based Encryption  Secure Windows Credentials  Not Selected  Not Selected
Windows Encryption
  Policy-Based Encryption  Block Unmanaged Access to Domain Credentials  Not Selected  Not Selected
Windows Encryption
  Policy-Based Encryption  Secure Windows Hibernation File  Not Selected  Not Selected
Windows Encryption
  Policy-Based Encryption  Prevent Unsecured Hibernation  Not Selected  Not Selected
Windows Encryption
  Policy-Based Encryption  Enable Software Auto Updates  Not Selected  Not Selected
Windows Encryption  BitLocker Encryption  BitLocker Encryption  Off  Off
Windows Encryption  Server Encryption  Server Encryption  Off  Off
Threat Prevention
  Advanced Threat Protection  Advanced Threat Protection  On  On
Removable Media Encryption
  Mac Media Encryption  Mac Media Encryption  Off  Off
Port Control
  Windows Port Control  Port Control System  Disabled  Disabled

For more information about policies, refer to AdminHelp, available in the Remote Management Console of the Dell Data Protection Server.

**VDI User Policy**

To manage policy for users in a VDI environment, create a Windows Domain group, associate domain users with that group, and then import the group into Dell Server. This allows Dell Server to manage the users and their policies.

Policy settings differ, based on whether persistent or non-persistent VDI is deployed in the environment.

The policy requirements below are for VDI Users running Endpoint Security Suite Enterprise. The list includes only policies that are significant for VDI Users. VDI Endpoint Group policy settings must also meet certain requirements. See VDI Endpoint Group Policy.

**NOTE:** Ensure that you turn off Advanced Threat Prevention Agent Auto Update. In the left pane of the Remote Management Console, select Management > Services Management > Advanced ThreatsAgent Auto Update, then select Off.

**NOTE:** With Persistent VDI Groups, ensure that roaming user profiles are configured.

These policy and configuration settings for VDI Users must be configured before VDI client activation:

<table>
<thead>
<tr>
<th>Technology</th>
<th>Category</th>
<th>Policy or Setting</th>
<th>Persistent VDI Group setting</th>
<th>Non-Persistent VDI Group setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Encryption</td>
<td>Policy-Based Encryption</td>
<td>Policy-Based Encryption</td>
<td>On</td>
<td>Off</td>
</tr>
</tbody>
</table>
Windows Encryption  | Policy-Based Encryption  | Encrypt Outlook Personal Folders  | Not Selected  | Not Selected  
Windows Encryption  | Policy-Based Encryption  | Encrypt Temporary Files  | Not Selected  | Not Selected  
Windows Encryption  | Policy-Based Encryption  | Encrypt Temporary Internet Files  | Not Selected  | Not Selected  
Windows Encryption  | Policy-Based Encryption  | Encrypt User Profile Documents  | Not Selected  | Not Selected  
Windows Encryption  | Policy-Based Encryption  | Force Logoff/Reboot on Policy Updates  | Selected  | Not Selected  
Removable Media Encryption  | Windows Media Encryption  | Windows Media Encryption  | On  | On  
Removable Media Encryption  | Windows Media Encryption  | EMS Scan External Media  | Not Selected  | Not Selected  

For more information about policies, refer to AdminHelp, available in the Remote Management Console of the Dell Data Protection Server.

Enable Activations

After policy and configuration requirements are met:

- Enable policy for user activations.
- Disable non-domain user activations.

If removable media protection is needed, enable External Media Shield and set the encryption key type to user roaming (which is the default type).
To allow client activation on a refreshed non-persistent image, the image must be refreshed immediately after logoff.

To refresh the image after logoff:

1. In Horizon View, under Catalog, click Desktop Pools.
2. Select the clone pool, and then click Edit.
3. Set the Delete or refresh the machine on logoff parameter to Refresh Immediately.
4. Save the edits.
Provision the Citrix VDI Clone Pool

This section describes how to provision a VDI Clone Pool in a Citrix environment.

**External Media Shield**

To use External Media Shield, configure USB redirection not to use the network share model. In Citrix Studio, enable the USB Redirection policy or add to the existing policy.

![USB Redirection Policy](image)

**NOTE:**
This policy must be enabled for External Media Shield for encryption of removable media to work.

When Thin Client USB devices are connected to a VDI clone as a network share, External Media Shield cannot protect the redirected USB device, because the External Media Shield drivers will ignore network shares. Citrix provides this alternative method of USB redirection, using the USB Redirection policy, that does not use the network share model. This is also discussed in the document, *Dell Data Protection | Endpoint Security Suite Enterprise for Citrix*.

**Activation**

To allow activations, run the `WSDeactivate` tool on all VDI Virtual Machines after the VDI clone pool is deployed but before initial user login. This resolves an interoperability issue between the Virtual Delivery Agent and the Encryption client's vault that blocks encryption activations. The exact cause of the interoperability issue is being investigated.

If desired, use a login script to automate the `WSDeactivate` process.

**IMPORTANT:**
You must run the `WSDeactivate` tool each time the VDI clone pool is rebuilt, before initial user login.
Prepare VMware Removable Media

Refer to Removable Media Encryption (EMS) Install in the document, *Dell Data Protection / Endpoint Security Suite Enterprise for VMware.*
Licensing Considerations

**Persistent VDI**

Client Access Licenses are associated with Virtual Machines in a VDI clone pool. VDI clone pools are often created, torn down, and rebuilt, which causes artificially high usage of Client Access Licenses. Returning the Client Access Licenses to the license pool helps to alleviate this issue.

Currently, the process to return Client Access Licenses is based on removal of the device. SQL statements, run manually in the SQL Management Studio, can mark the devices as removed, which returns the Client Access Licenses to the license pool.

**NOTE:** Contact Dell ProSupport to obtain the SQL statements and the procedure for returning Client Access Licenses to the license pool.

**Non-Persistent VDI**

Client Access Licenses that are allocated to Non-Persistent VDI clients are returned for reuse after the VDI client device lease expires. The default device lease expiration interval is 480 minutes.

**Check for returned licenses**

License expiration is logged in the Security Server. To check for licenses returned for reuse, open `output.log` from the appropriate path:

**Dell Enterprise Server:** Program Files\Dell\Enterprise Edition\Security Server\logs

**VE:** /opt/dell/server/security-server/logs

Sample log entries:

```

2017-01-09 08:17:40,593 INFO com.dell.scheduled.jobs.NonPersistentVdiLicenceExpirationJob [jobsScheduler-2] - Expired 0 non persistent VDI device(s)


```


**Change lease expiration values**

To change the default device lease expiration values, open `application.properties` from the appropriate path:

**Dell Enterprise Server:** `Program Files\Dell\Enterprise Edition\Security Server\conf`

**VE:** `/opt/dell/server/security-server/conf`

Modify the following properties, as desired:

- `vdi.nonpersistent.leaseexpiration.jobfrequency.millis=120000`
- `vdi.nonpersistent.leaseexpiration.initialdelay.millis=30000`
- `vdi.nonpersistent.leaseexpiration.minutes=480`

where

- `vdi.nonpersistent.leaseexpiration.jobfrequency.millis` - Frequency with which the license expiration job runs (in milliseconds).
- `vdi.nonpersistent.leaseexpiration.initialdelay.millis=30000` - Time interval before the license expiration job runs after Security Server startup (in milliseconds).
- `vdi.nonpersistent.leaseexpiration.minutes=480` - Length of time before device lease expiration (in minutes).

**Key Material**

Over time, the Dell Server accumulates an excess of unused key material associated with encrypted endpoints that no longer exist. At the current expected rate, any issue associated with this accumulation should take years to manifest in a Dell Enterprise Server instance based on current information.