Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.
1 Introduction................................................................................................................................. 4
  Overview......................................................................................................................................................... 4
  Contact Dell ProSupport................................................................................................................................. 4

2 Requirements........................................................................................................................................... 5
  Hardware................................................................................................................................................................. 5
  Software................................................................................................................................................................. 5
  Ports................................................................................................................................................................. 5
  Endpoint Security Suite Enterprise for Linux and Dependencies........................................................................ 6
  Compatibility......................................................................................................................................................... 6

3 Tasks......................................................................................................................................................... 9
  Installation................................................................................................................................................................. 9
    Prerequisites......................................................................................................................................................... 9
    Command Line Installation........................................................................................................................................ 9
    View Details......................................................................................................................................................... 11
  Verify Installation.................................................................................................................................................. 12
  Troubleshooting.................................................................................................................................................. 13
    Disable SSL Trust Certificate........................................................................................................................................ 13
    Add XML Inventory and Policy Changes to the Logs Folder.............................................................................. 14
  Collect Log Files.................................................................................................................................................. 14
  Provision a Tenant.................................................................................................................................................. 14
    Provision a Tenant.................................................................................................................................................. 15
  Provisioning Troubleshooting...................................................................................................................................... 15
    Provisioning and Agent Communication........................................................................................................... 15
The Endpoint Security Suite Enterprise for Linux Administrator Guide provides the information needed to install and deploy the client software.

**Overview**

Endpoint Security Suite Enterprise for Linux offers Advanced Threat Prevention at the operating system and memory layers, all centrally-managed from the Dell Server. With centralized management, consolidated compliance reporting, and console threat alerts, organizations can easily enforce and prove compliance for endpoints. Security expertise is built in with features such as pre-defined policy and report templates, to help businesses reduce IT management costs and complexity.

Security Management Server or Security Management Server Virtual - provides centralized security policy administration, integrates with existing enterprise directories and creates reports. For the purposes of this document, both Servers are cited as Dell Server, unless a specific version needs to be cited (for example, a procedure is different using Security Management Server Virtual).

Advanced Threat Prevention for Linux has one tar.gz file, which contains the three RPMs.

**Contact Dell ProSupport**

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

Additionally, online support for Dell 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 Tag or Express Service Code available when you call.

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

Client hardware and software requirements are provided in this chapter. Ensure that the deployment environment meets the requirements before continuing with deployment tasks.

Hardware

The following table details the minimum supported hardware.

<table>
<thead>
<tr>
<th>Hardware</th>
</tr>
</thead>
</table>
| • At least 500 MB free disk space  
• 2 GB RAM  
• 10/100/1000 or Wi-Fi network interface card |

⚠️ **NOTE:** IPv6 is not currently supported.

Software

The following table details supported software.

Operating Systems (64-bit kernels)

<table>
<thead>
<tr>
<th>Operating Systems (64-bit kernels)</th>
</tr>
</thead>
</table>
| • CentOS Linux v7.1 - v7.5  
• Red Hat Enterprise Linux v7.1 - v7.5 |

Ports

- Port 443 (https) is used for communication and must be open on the firewall for agents to communicate with the Management Console. If port 443 is blocked for any reason, updates cannot be downloaded, so computers may not have the most current protection. Ensure that client computers can access the following:

<table>
<thead>
<tr>
<th>Use</th>
<th>Application Protocol</th>
<th>Transport Protocol</th>
<th>Port Number</th>
<th>Destination</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Communication</td>
<td>HTTPS</td>
<td>TCP</td>
<td>443</td>
<td>Allow all https traffic to *.cylance.com</td>
<td>Outbound</td>
</tr>
<tr>
<td>Core Server</td>
<td>HTTPS</td>
<td>TCP</td>
<td>8888</td>
<td>Allows Core Server communication</td>
<td>Inbound/Outbound</td>
</tr>
</tbody>
</table>

- For additional information, see [SLN303898](#).
Endpoint Security Suite Enterprise for Linux and Dependencies

Endpoint Security Suite Enterprise for Linux uses Mono and dependencies to install and activate on Linux OS. The installer will download and install required dependencies. Following extraction of the package, you can view which dependencies are being leveraged by using the following command:

```
./showdeps.sh
```

Compatibility

The following table details compatibility with Windows, Mac, and Linux.

n/a - Technology does not apply to this platform.

Blank field - Policy is not supported with Endpoint Security Suite Enterprise.

<table>
<thead>
<tr>
<th>Features</th>
<th>Policies</th>
<th>Windows</th>
<th>macOS</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Actions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Quarantine (Unsafe)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Auto Quarantine (Abnormal)</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Auto Upload</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Policy Safe List</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td><strong>Memory Actions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Protection</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td><strong>Exploitation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stack Pivot</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Stack Protect</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Overwrite Code</td>
<td>x</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAM Scraping</td>
<td>x</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Payload</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Process Injection</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote Allocation of Memory</td>
<td>x</td>
<td>x</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Remote Mapping of Memory</td>
<td>x</td>
<td>x</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Remote Write to Memory</td>
<td>x</td>
<td>x</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Remote Write PE to Memory</td>
<td>x</td>
<td>n/a</td>
<td>n/a</td>
<td></td>
</tr>
<tr>
<td>Remote Overwrite Code</td>
<td>x</td>
<td>n/a</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Features</td>
<td>Policies</td>
<td>Windows</td>
<td>macOS</td>
<td>Linux</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------</td>
<td>---------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>Remote Unmap of Memory</td>
<td>x</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Remote Thread Creation</td>
<td>x</td>
<td>x</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Remote APC Scheduled</td>
<td>x</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>DYLD Injection</td>
<td>x</td>
<td>x</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

**Escalation**

| LSASS Read               | x              | n/a     | n/a   |
| Zero Allocate           | x              | x       | n/a   |

**Protection Settings**

| Execution Control        | x              | x       | x     |
| Prevent service shutdown from device | x               | x     |
| Kill unsafe running processes and their sub processes | x               | x     | x     |
| Background Threat Detection | x               | x     | x     |
| Watch for New Files      | x              | x       | x     |
| Maximum archive file size to scan | x               | x     | x     |
| Exclude Specific Folders | x              | x       | x     |
| Copy File Samples        | x              | x       | x     |

**Application Control**

| Change Window            | x              | x       |
| Folder Exclusions        | x              |         |

**Agent Settings**

| Enable auto-upload of log files | x | x | x |
| Enable Desktop Notifications  | x |   |   |

**Script Control**

<p>| Active Script            | x |   |
| Powershell               | x |   |
| Office Macros            | x | n/a |
| Block Powershell console usage | x |
| Approve scripts in these folders (and subfolders) | x |
| Logging Level            | x |   |</p>
<table>
<thead>
<tr>
<th>Features</th>
<th>Policies</th>
<th>Windows</th>
<th>macOS</th>
<th>Linux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self Protection Level</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Update</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Run a Detection (from Agent UI)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Quarantined (Agent UI and Console UI)</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disconnected Mode</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Detailed Threat Data</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Safe List</td>
<td>x</td>
<td>x</td>
<td></td>
<td>n/a</td>
</tr>
<tr>
<td>Copy malware samples</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Proxy Settings</td>
<td>x</td>
<td>x</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Manual Policy Check (Agent UI)</td>
<td>x</td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Installation

This section guides you through the Endpoint Security Suite Enterprise for Linux installation.

Prerequisites

Dell recommends that IT best practices are followed during the deployment of client software. This includes, but is not limited to, controlled test environments for initial tests and staggered deployments to users.

Before beginning this process, ensure the following prerequisites are met:

- Ensure that the Dell Server and its components are already installed.
- If you have not yet installed the Dell Server, follow the instructions in the appropriate guide below.
  - Security Management Server Installation and Migration Guide
  - Security Management Server Virtual Quick Start Guide and Installation Guide
- Ensure that you have the Dell Server host name and port. Both are needed for client software installation.
- Ensure that the target computer has network connectivity to the Dell Server.
- If a client's server certificate is missing or is self-signed, you must disable the SSL certificate trust on the client side only.

Command Line Installation

To install the Endpoint Security Suite Enterprise client using the command line, follow the steps below.

The `sudo` command must be used to invoke administrative privileges during installation. When prompted, enter your credentials.

Fingerprint approval displays only during the first installation.

1. Locate and download the installation bundle (DellESSE-1.x.x-xxx.tar.gz) using your Dell FTP Account.
2. Extract the tar.gz using the following command:
   ```bash
tar -xvf DellESSE*.tar.gz
   ```
3. The following command executes the installation script for the required RPMs and dependencies:
sudo ./install.sh

4 In *Dell Security Management Server Host?* enter the fully qualified host name of the Dell Server to manage the target user. For example, server.organization.com.

5 In *Dell Security Management Server Port?*, verify the port is set to 8888.

6 Enter **y** when prompted to install the DellESSE package and its dependencies.

```
libxfixes x86_64 5.0.3-1.el7  base  18
libXrender x86_64 0.9.10-1.el7  base  26
libXxf86vm x86_64 1.1.4-1.el7  base  18
libexif x86_64 0.6.21-6.el7  base  347
libjpeg-turbo x86_64 1.2.90-5.el7  base  134
libpng x86_64 2.0.13-7.el7_2  base  213
libtiff x86_64 4.0.3-27.el7_3  base  170
libxcb x86_64 1.12-1.el7  base  211
libxshmfence x86_64 1.2-1.el7  base  7.2
lyx-fonts noarch 2.2.3-1.el7  epel  159
mesa-libGL x86_64 17.0.1-6.20170307.el7  base  82
mesa-libGL x86_64 17.0.1-6.20170307.el7 base  155
mesa-libgbm x86_64 17.0.1-6.20170307.el7 base  32
mesa-libglapi x86_64 17.0.1-6.20170307.el7 base  41
pixman x86_64 0.34.0-1.el7  base  248
```

**Transaction Summary**

Install 1 Package (+27 Dependent packages)

Total size: 96 M
Total download size: 3.8 M
Installed size: 104 M
Is this ok [y/d/N]:

7 Enter **y** if prompted for *Fingerprint* approval.

8 Enter **y** when prompted to install the *DellAdvancedThreatProtection* package.
Enter `y` when prompted to install the `CylanceDellATPPlugin` package.

Installation is complete.

See Verify Endpoint Security Suite Enterprise for Linux Installation.

**Command Line Uninstallation**

To uninstall Endpoint Security Suite Enterprise for Linux using the command line, follow the steps below.

1. Access a Terminal window.
2. Uninstall the package using the following command:
   
   ```
   sudo ./uninstall.sh
   ```
3. Press Enter.
   
   Endpoint Security Suite Enterprise for Linux is now uninstalled, and the computer can be used normally.

**View Details**

After Endpoint Security Suite Enterprise for Linux is installed, it is recognized by the Dell Server as an endpoint.

**atp -t**

The `atp - t` command displays all threats discovered on the device and the action taken. Threats are a category of events that are newly detected as potentially unsafe files or programs and require guided remediation.
These entries detail the action taken, hash ID, and location of the threat.

- **Unsafe** - A suspicious file that is likely to be malware
- **Abnormal** - A suspicious file that may be malware
- **Quarantined** - A file that is moved from its original location, stored in the Quarantine folder, and prevented from executing on the device.
- **Waived** - A file allowed to execute on the device.
- **Cleared** - A file that has been cleared within the organization. Cleared files include files that are Waived, added to the Safe list, and deleted from the Quarantine folder on the device.

For more information about Advanced Threat Prevention threat classifications, see AdminHelp, available in the Dell Server Remote Management Console.

### Verify Installation

Optionally, you can verify that the installation was successful.

- On the client, access a Terminal window.
- Before a policy sequence is received, the client registers with the Dell Server.
- The /var/log/Dell/ESSE/DellAgent.01.log file details communication with the Dell Server and plugin/service interaction. The enclosed text confirms that the client has received policies from the Dell Server:

  ![Terminal output](image1)

  The enclosed text confirms that the Dell service was stopped to load the Advanced Threat Prevention plugin:

  ![Terminal output](image2)
The enclosed text confirms the three Endpoint Security Suite Enterprise for Linux plugins loaded:

```
2018.02.18 18:51:36.951 [01077] (00005) I Agent : machine name is "centoscsm2.ddsdeos.com"
2018.02.18 18:51:36.951 [01077] (00005) I Agent : process is 64-bit
2018.02.18 18:51:36.952 [01077] (00005) I Agent : domain is "none"
Id=C069097-4F21-4C1E-9407-1E105FEEB5C) in 69 ms
2018.02.18 18:51:37.059 [01077] (00005) I Agent : loaded plugin "Server Communication Manager" 1.0
Id=O4E269087-3164-4677-9F3D-98E05F06240) in <1 ms
Id=968869F-8F80-4D61-94FB-A9804F8DC287) in 8 ms
2018.02.18 18:51:37.069 [01077] (00005) I Agent : loaded plugin "Advanced Threat Prevention" 1.0
Id=968869F-8F80-4D61-94FB-A9804F8DC287) in <1 ms
2018.02.18 18:51:37.098 [01077] (00005) I Comm : AgentID 8008a848-e18-43fa-a959-85f44e5ff251
2018.02.18 18:51:37.102 [01077] (00005) I AdvATP : AdvancedAtpManager Starting
2018.02.18 18:51:37.125 [01077] (00005) I AdvATP : management is active
2018.02.18 18:51:37.129 [01077] (00005) I AdvATP : processing new policies - Policy list: count=1
```

**atp -s** - Includes the following:

- Registration Status
- Serial Number - Use this when contacting support. This is the unique identifier of the installation.
- Policy

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp -s
Registration Status: Registered
Serial Number: 8008a848-ce18-43fa-a959-85f44e5ff251
Policy: (Online)
```

The following command details command line variables for Endpoint Security Suite Enterprise for Linux:

```
/opt/cylance/desktop/atp --help
```

The Advanced Threat Prevention atp command is added to the /usr/sbin directory, which is normally included in a shell's PATH variable, so that it can be used in most cases without an explicit path.

**Troubleshooting**

**Disable SSL Trust Certificate**

If a computer's server certificate is missing or is self-signed, you must disable the SSL certificate trust on the client side only.
If you are using an uncommon certificate, import the root certificate to the Linux Certificate Store then restart Endpoint Security Suite for Linux services with the following command:

```
/usr/lib/dell/esse/agentservicecmd.sh restart
```

1. Access a Terminal window.
2. Enter the path to CsfConfig app:
   ```
   /usr/lib/dell/esse/CsfConfig
   ```
3. Run CsfConfig.app:
   ```
   sudo ./CsfConfig
   ```
   The following displays with default settings:
   ```
   Current Settings:
   ServerHost = deviceserver.company.com
   ServerPort = 8888
   DisableSSLCertTrust = False
   DumpXmlInventory = False
   DumpPolicies = False
   ```
4. Type `-help` to list the options.
5. To disable SSL Certificate Trust on the target computer, enter the following command:
   ```
   sudo /usr/lib/dell/esse/CsfConfig -disablecerttrust true
   ```

### Add XML Inventory and Policy Changes to the Logs Folder

To add the inventory.xml or policies.xml files to the Logs folder:

1. Run the CsfConfig app as described above.
2. To change `DumpXmlInventory` to True, enter the following command:
   ```
   sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
   ```
3. To change `DumpPolicies` to True, enter the following command:
   ```
   sudo /usr/lib/dell/esse/CsfConfig -dumppolicies true
   ```
   Policy files are dumped only if a policy change has occurred.
4. To view inventory.xml and policies.xml log files, go to `/var/log/Dell/Dell Data Protection`.

**NOTE:** CsfConfig changes may not immediately apply.

### Collect Log Files

Logs for Endpoint Security Suite Enterprise for Linux are located in the following location: `/var/log/Dell/ESSE`. To generate logs, use the following command: `./getlogs.sh`

For information about how to collect the logs, see [SLN303924](#).

### Provision a Tenant

A tenant must be provisioned in the Dell Server before Advanced Threat Prevention enforcement of policies becomes active.
Prerequisites

- Must be performed by an administrator with the system administrator role.
- Must have connectivity to the Internet to provision on the Dell Server.
- Must have connectivity to the Internet on the client to display the Advanced Threat Prevention online service integration in the Management Console.
- Provisioning is based off of a token that is generated from a certificate during provisioning.
- Advanced Threat Prevention licenses must be present in the Dell Server.

Provision a Tenant

1. As a Dell administrator, log in to the Remote Management Console.
2. In the left pane of the Management Console, click Management > Services Management.
3. Click Set Up Advanced Threat Protection Service. Import your Advanced Threat Prevention licenses if failure occurs at this point.
4. The guided set up begins once the licenses are imported. Click Next to begin.
5. Read and agree to the EULA and click Next.
6. Provide identifying credentials to the Dell Server for provisioning of the Tenant. Click Next. Provisioning an existing Tenant that is Cylance-branded is not supported.
7. Download the Certificate. This is required to recover if there is a disaster scenarios with the Dell Server. This Certificate is not automatically backed up. Back up the Certificate to a safe location on a different computer. Select the check box to confirm that you backed up the Certificate and click Next.
8. Set up is complete. Click OK.

Provisioning Troubleshooting

Provisioning and Agent Communication

The following diagrams illustrate the Advanced Threat Prevention service provisioning process.
The following diagram illustrates the Advanced Threat Prevention agent communication process.