

Dell Endpoint Security Suite Enterprise for Linux

Administrator Guide v2.1



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.

© 2012-2018 Dell Inc. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. Registered trademarks and trademarks used in the Dell Encryption, Endpoint Security Suite Enterprise, and Data Guardian suite of documents: Dell™ and the Dell logo, Dell Precision™, OptiPlex™, ControlVault™, Latitude™, XPS®, and KACE™ are trademarks of Dell Inc. Cylance®, CylancePROTECT, and the Cylance logo are registered trademarks of Cylance, Inc. in the U.S. and other countries. McAfee® and the McAfee logo are trademarks or registered trademarks of McAfee, Inc. in the US and other countries. Intel®, Pentium®, Intel Core Inside Duo®, Itanium®, and Xeon® are registered trademarks of Intel Corporation in the U.S. and other countries. Adobe®, Acrobat®, and Flash® are registered trademarks of Adobe Systems Incorporated. Authen tec® and Eikon® are registered trademarks of Authen tec. AMD® is a registered trademark of Advanced Micro Devices, Inc. Microsoft®, Windows®, and Windows Server®, Internet Explorer®, Windows Vista®, Windows 7®, Windows 10®, Active Directory®, Access®, BitLocker®, BitLocker To Go®, Excel®, Hyper-V®, Outlook®, PowerPoint®, Word®, OneDrive®, SQL Server®, and Visual C++® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States or other countries. Box® is a registered trademark of Box. DropboxSM is a service mark of Dropbox, Inc. Google™, Android™, Google™ Chrome™, Gmail™, and Google™ Play are either trademarks or registered trademarks of Google Inc. in the United States and other countries. Apple®, App StoreSM, Apple Remote Desktop™, Boot Camp™, FileVault™, iPad®, iPhone®, iPod®, iPod touch®, iPod shuffle®, and iPod nano®, Macintosh®, and Safari® are either servicemarks, trademarks, or registered trademarks of Apple, Inc. in the United States and/or other countries. EnCase™ and Guidance Software® are either trademarks or registered trademarks of Guidance Software. Entrust® is a registered trademark of Entrust®, Inc. in the United States and other countries. Mozilla® Firefox® is a registered trademark of Mozilla Foundation in the United States and/or other countries. iOS® is a trademark or registered trademark of Cisco Systems, Inc. in the United States and certain other countries and is used under license. Oracle® and Java® are registered trademarks of Oracle and/or its affiliates. Travelstar® is a registered trademark of HGST, Inc. in the United States and other countries. UNIX® is a registered trademark of The Open Group. VALIDITY™ is a trademark of Validity Sensors, Inc. in the United States and other countries. VeriSign® and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. KVM on IP® is a registered trademark of Video Products. Yahoo!® is a registered trademark of Yahoo! Inc. Bing® is a registered trademark of Microsoft Inc. Ask® is a registered trademark of IAC Publishing, LLC. Other names may be trademarks of their respective owners.

2018 - 11

Contents

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

Introduction

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.

Hardware

- At least 500 MB free disk space
- 2 GB RAM
- 10/100/1000 or Wi-Fi network interface card

① | **NOTE: IPv6 is not currently supported.**

Software

The following table details supported software.

Operating Systems (64-bit kernels)

- 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:

Use	Application Protocol	Transport Protocol	Port Number	Destination	Direction
All Communication	HTTPS	TCP	443	Allow all https traffic to *.cylance.com	Outbound
Core Server Communication	HTTPS	TCP	8888	Allows Core Server communication	Inbound/Outbound

- 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.

Features	Policies	Windows	macOS	Linux
File Actions				
	Auto Quarantine (Unsafe)	x	x	x
	Auto Quarantine (Abnormal)	x	x	x
	Auto Upload	x	x	x
	Policy Safe List	x	x	x
Memory Actions				
	Memory Protection	x	x	x
Exploitation				
	Stack Pivot	x	x	x
	Stack Protect	x	x	x
	Overwrite Code	x	n/a	
	RAM Scraping	x	n/a	
	Malicious Payload	x		
Process Injection				
	Remote Allocation of Memory	x	x	n/a
	Remote Mapping of Memory	x	x	n/a
	Remote Write to Memory	x	x	n/a
	Remote Write PE to Memory	x	n/a	n/a
	Remote Overwrite Code	x	n/a	

Features	Policies	Windows	macOS	Linux
	Remote Unmap of Memory	x	n/a	
	Remote Thread Creation	x	x	
	Remote APC Scheduled	x	n/a	n/a
	DYLD Injection		x	x
Escalation				
	LSASS Read	x	n/a	n/a
	Zero Allocate	x	x	
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		
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				
	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		

Features	Policies	Windows	macOS	Linux
	Self Protection Level	x		
	Auto Update	x		
	Run a Detection (from Agent UI)	x		
	Delete Quarantined (Agent UI and Console UI)	x		
	Disconnected Mode	x		x
	Detailed Threat Data	x		
	Certificate Safe List	x	x	n/a
	Copy malware samples	x	x	x
	Proxy Settings	x	x	x
	Manual Policy Check (Agent UI)	x	x	

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

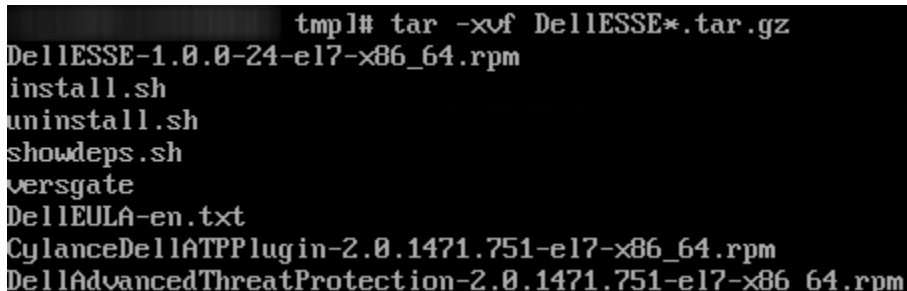
To install the Endpoint Security Suite Enterprise client using the command line, follow the steps below.

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:

```
tar -xvf DellESSE*.tar.gz
```



```

tmp1# tar -xvf DellESSE*.tar.gz
DellESSE-1.0.0-24-el7-x86_64.rpm
install.sh
uninstall.sh
showdeps.sh
versgate
DellEULA-en.txt
CylanceDellATPPlugin-2.0.1471.751-el7-x86_64.rpm
DellAdvancedThreatProtection-2.0.1471.751-el7-x86_64.rpm
  
```

- 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.

```
Dell Endpoint Security Suite Enterprise (ESSE) Installation
Dell Security Management Server Host?
Dell Security Management Server Port?
```

- 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 2:1.5.13-7.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-libEGL    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.

```
Total 452 kB/s | 4.9 MB 00:00:11
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
  Userid      : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
  Fingerprint : 6341 ab27 53d7 8a78 a7c2 7bbl 24c6 a8a7 f4a0 0eb5
  Package     : centos-release-7-3.1611.el7.centos.x86_64 (@anaconda)
  From        : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]:
```

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

```
Dependencies Resolved

=====
Package Arch Version Repository Size
=====
Installing:
DellAdvancedThreatProtection
x86_64 2.0.1461-739 /DellAdvancedThreatProtection-2.0.1461.739-el7-x86_64 149 M

Transaction Summary

=====
Install 1 Package

Total size: 149 M
Installed size: 149 M
Is this ok [y/d/N]:
```

- 9 Enter **y** when prompted to install the *CylanceDellATPPlugin* package.

```
Dependencies Resolved

=====
Package      Arch    Version Repository                               Size
=====
Installing:
CylanceDellATPPlugin
      x86_64 2.2.4-0 /CylanceDellATPPlugin-2.0.1461.739-el7-x86_64 439 k

Transaction Summary
=====
Install 1 Package

Total size: 439 k
Installed size: 439 k
Is this ok [y/d/N]: y
```

- 10 Installation is complete.

```
Installed:
  DellAdvancedThreatProtection.x86_64 0:2.0.1461-739

Complete!
```

- 11 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.

```

Quarantined 17E76B830F9F30A39F078F5A69AD87B3838DB73A28EC893BD06EAF95D6E464E2 /tmp/threats/LINUXTarGz
Archive
Quarantined 20FBC1FDFC96A7E21FB1C700A6517A61711732A0D31FC25A60609710ECBE09 /tmp/threats/LINUXAutoF
lockNoService
Quarantined 2D49A3F81AF3362FE006E417DF2807C960314FF4F271B5B1360964163CB49086 /tmp/threats/LINUXGBL2
Quarantined 52D74BD1555D7C82746112C44F4D9A916B9DA286DD5B14D7665D4167BB1EB5D8 /tmp/threats/LINUXRunni
ngAutoQ
Quarantined 70F193F3C2023A7542338142CA89F1076A238AB7BAAD4202B2DCEDA7286E43D9 /tmp/threats/LINUXTest1
Quarantined 79D8C277F32CD176E4E2DD2198F730C9C79FA00A8F0158E0D519CEC1D068E222 /tmp/threats/LINUXRunni
ngApp
Quarantined B1BC7849F90FB403B9EDE88D40A92769D0AC20640B6A0D310FAF1D6B20E85F8A /tmp/threats/LINUXMaxAr
chive
Quarantined B31D57A77930E60FC151DEED005ED042423A172B4BED7782E33D4D09109BCCB6 /tmp/threats/LINUXGBL1
Quarantined F11C98AADB31D47AD571F6C0FA7F178A6413A0A7E8443709877711FB1CA6E31F /tmp/threats/LINUXAutoF
lockExecution

```

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.00.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:

```

2017.12.12 14:26:02.794 [02390] (00009) I Comm : Received id=ba150b8e-b1d3-44
5a-81e9-426e77fbb843
2017.12.12 14:26:02.795 [02390] (00009) I Comm : ReceivedEdition enterprisese
rver
2017.12.12 14:26:02.847 [02390] (00009) I Comm : Successfully added memory ex
clusions to policy
2017.12.12 14:26:03.322 [02390] (00009) I Comm : new policy seq# 9 received
2017.12.12 14:26:03.385 [02390] (00009) I Comm : registered Centos7-3-64-MH w
ith server
2017.12.12 14:26:03.392 [02390] (00009) I Comm : closing connection to https:
--More-- (39%)

```

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

```

//cedmz.credce.com:8888/agent
2017.12.12 14:27:05.883 [02390] (00009) I Comm : next contact with server sch
eduled for 12/12/2017 8:27:05 PM
2017.12.12 14:27:10.442 [02390] (00005) I Agent : Dell Data Protection stopped
---date--- ---time--- --pid-- -thrid- -subsys- -----
--message-----
2017.12.12 14:27:12.968 [02551] (00005) I Agent : service name is "DellMgmtAge
nt"
2017.12.12 14:27:12.970 [02551] (00005) I Agent : product name is "Dell Data P

```

The enclosed text confirms the three Endpoint Security Suite Enterprise for Linux plugins loaded:

```
2018.02.18 10:51:36.951 [01077] (00005) I Agent : machine name is "centosvm2.ddsdemos.com"
2018.02.18 10:51:36.951 [01077] (00005) I Agent : process is 64-bit
2018.02.18 10:51:36.952 [01077] (00005) I Agent : domain is "(none)"
2018.02.18 10:51:37.059 [01077] (00005) I Agent : loaded plugin "Server Communication Manager" 1.0
Id={CAA1A89F-AF21-4C1E-9407-1E185FFEEB5C} in 69 ms
2018.02.18 10:51:37.059 [01077] (00005) I Agent : loaded plugin "Auditing and Reporting Service" 1.0
Id={0E969074-3164-467F-BF3D-D9E695F48240} in <1 ms
2018.02.18 10:51:37.069 [01077] (00005) I AdvATP : Advanced Threat Prevention Cylance component logging initialized
2018.02.18 10:51:37.069 [01077] (00005) I Agent : loaded plugin "Advanced Threat Prevention" 1.0
Id={96BBD97F-9BF0-4D61-94F8-A9884F8DC287} in 8 ms
2018.02.18 10:51:37.069 [01077] (00005) I Agent : loaded 3 plugins
2018.02.18 10:51:37.090 [01077] (00010) I Comm : AgentID 80397403-c05f-4cbf-b6b4-e15dd577186a
2018.02.18 10:51:37.102 [01077] (00011) I AdvATP : AdvancedAtpManager Starting
2018.02.18 10:51:37.125 [01077] (00011) I AdvATP : management is active
2018.02.18 10:51:37.129 [01077] (00011) 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: 8088ab40-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`

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp --help
usage: atp <options>
options:
  -r, --register=token      : register with Dell Data Security servers with the
                             provided token
  -s, --status              : get status of Advanced Threat Prevention
  -u, --checkupdates        : check for updates
  -b, --start-bg-scan       : start background scan
  -B, --stop-bg-scan        : stop background scan
  -d, --scan-dir=dir        : scan directory
  -l, --getloglevel         : get current log level
  -L, --setloglevel=level   : set log level
  -P, --getpolicytime       : get the policy update time
  -p, --checkpolicy         : check for policy updates
  -t, --threats             : list threats
  -q, --quarantine=id       : quarantine a file by id (hash)
  -w, --waive=id            : waive a file by id (hash)
  -v, --version             : print this tools version
  -h, --help               : 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

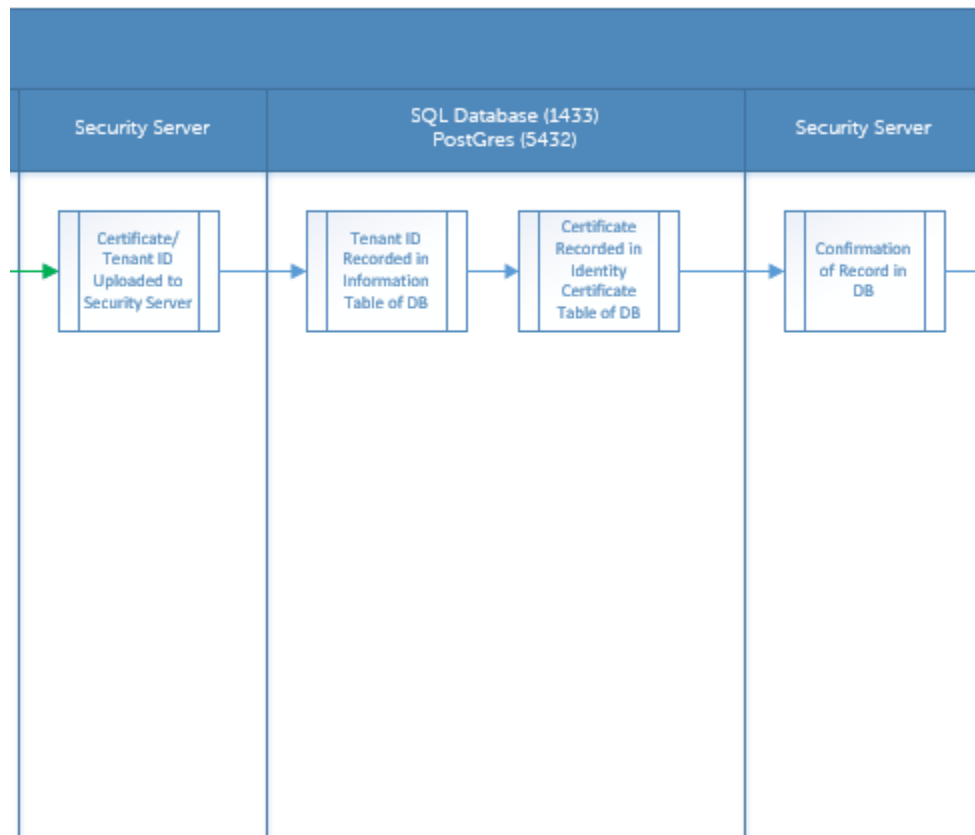
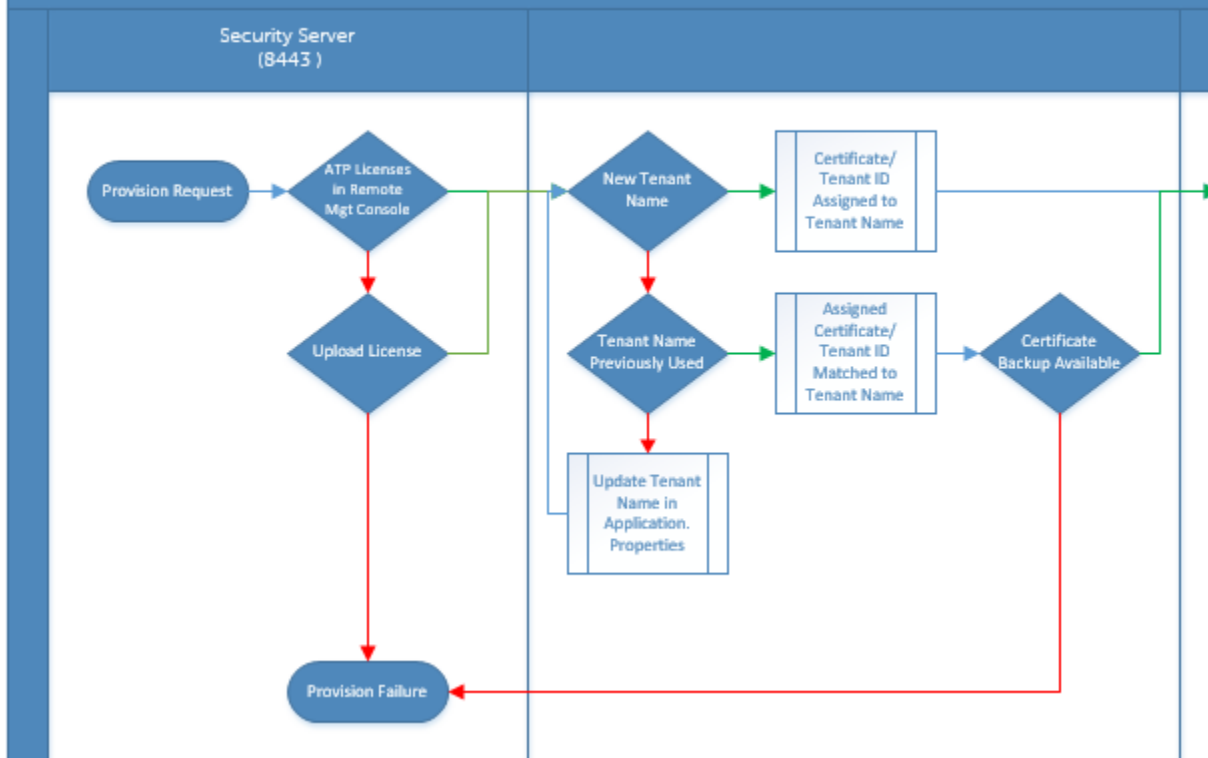
- 1 As a Dell administrator, log in to the Remote Management Console.
- 2 In the left pane of the Management Console, click **Management > Services Management**.
- 3 Click **Set Up Advanced Threat Protection Service**. Import your Advanced Threat Prevention licenses if failure occurs at this point.
- 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**.

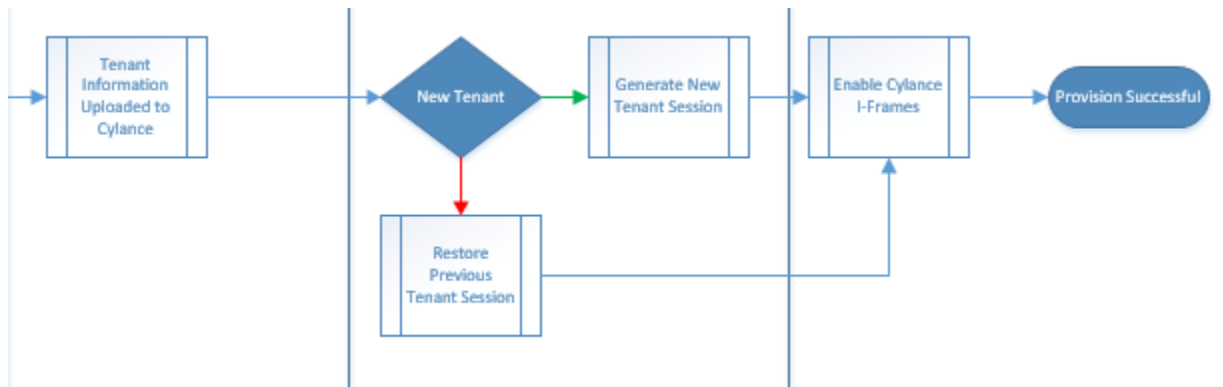
Provisioning Troubleshooting

Provisioning and Agent Communication

The following diagrams illustrate the Advanced Threat Prevention service provisioning process.

Advanced Threat Prevention Service Provisioning Process





The following diagram illustrates the Advanced Threat Prevention agent communication process.

