# Table of Contents

## Traps Agent 4.2 for Windows

- Traps Agent for Windows Requirements .................................................. 7
- Install the Traps Agent for Windows .......................................................... 8
  - Install the Traps Agent Using the MSI .................................................. 8
  - Install the Traps Agent Using Msiexec ................................................ 9
- Verify Connectivity from the Endpoint ...................................................... 10
- Set Up a Non-Persistent VDI ................................................................. 11
  - VDI Installation Considerations ......................................................... 11
  - Configure the Golden Image for Non-Persistent VDI ....................... 11
  - Traps VDI Tool CLI ............................................................................. 14
  - Configure Storage for a VDI .............................................................. 16
  - Tune and Test the VDI Policy .............................................................. 18
- Use Traps Agent for Windows ............................................................... 20
- Uninstall Traps Agent for Windows ......................................................... 23
  - Manually Uninstall the Traps Agent for Windows ......................... 23
  - Uninstall the Traps Agent for Windows Using Msiexec .......... 23
- Troubleshooting Resources for Traps Agent for Windows .................. 25
  - Cytool for Windows ........................................................................... 25

## Traps Agent 4.2 for Mac

- Traps for Mac Requirements ................................................................. 35
- Install the Traps Agent for Mac .............................................................. 36
- Use the Traps Agent for Mac ................................................................. 38
- Uninstall the Traps Agent for Mac ........................................................ 41
- Troubleshooting Resources for the Traps Agent for Mac .................. 42
  - Cytool for Mac ................................................................................. 42

## Traps Agent 4.2 for Linux

- Traps for Linux Requirements ............................................................... 51
- Install the Traps Agent for Linux ........................................................... 52
- Use the Traps Agent for Linux ............................................................... 54
- Uninstall the Traps Agent for Linux ....................................................... 59
- Troubleshooting Resources for the Traps Agent for Linux .................. 60
The Traps™ agent protects Windows endpoints by preventing known and unknown malware from running on those endpoints and by halting any attempts to leverage software exploits and vulnerabilities. The Traps agent enforces Security policy for your organization as defined in your Traps Endpoint Security Manager. When a security event occurs on an endpoint, the Traps agent collects forensic information about that event that you can use to analyze the incident.

The following topics describe how to install and use the Traps agent for Windows:

> Traps Agent for Windows Requirements
> Install the Traps Agent for Windows
> Set Up a Non-Persistent VDI (There are no additional steps for Persistent VDI)
> Use Traps Agent for Windows
> Uninstall Traps Agent for Windows
> Upgrade Traps from the ESM Console (see the *Traps Endpoint Security Manager Administrator’s Guide*)
> Troubleshooting Resources for Traps Agent for Windows
## Traps Agent for Windows Requirements

Traps™ agent 4.2 for Windows has the following requirements:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version parity</td>
<td>The Traps agent version must not exceed the ESM Server and ESM Console version.</td>
</tr>
<tr>
<td>Processor</td>
<td>• Intel Pentium 4 or later with SSE2 instruction set support</td>
</tr>
<tr>
<td></td>
<td>• AMD Opteron/Athlon 64 or later with SSE2 instruction set support</td>
</tr>
<tr>
<td>RAM</td>
<td>512MB minimum; 2GB recommended</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>200MB minimum; 20GB recommended</td>
</tr>
<tr>
<td>Operating system versions</td>
<td>Palo Alto Networks supports Traps on many operating systems, virtual environments, and virtual applications. To determine the minimum Traps release for a specific operating system, environment, or application, refer to Where Can I Install the Traps Agent? in the Palo Alto Networks® Compatibility Matrix.</td>
</tr>
<tr>
<td>Networking</td>
<td>Allow communication on the TCP port from clients to server (the default is port 2125). Allow communication on the TCP port 443 if you enable secure communication.</td>
</tr>
<tr>
<td>.NET</td>
<td>Windows operating systems require the following minimum .NET version or a later release:</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 and earlier releases—.NET 3.5 SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows 8—.NET 4.5</td>
</tr>
<tr>
<td></td>
<td>• Windows 8.1—.NET 4.5.1</td>
</tr>
<tr>
<td></td>
<td>• Windows 10 and later releases—.NET 4.6</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2003—.NET 3.5 SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008—.NET 3.5 SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012—.NET 4.5</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 and later releases—.NET 4.5.1</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2016—.NET 4.5.1</td>
</tr>
<tr>
<td>Applications and utilities</td>
<td>• BITS client</td>
</tr>
<tr>
<td></td>
<td>• Windows Accessories (Notepad) to view logs</td>
</tr>
<tr>
<td>Localization</td>
<td>To set the language (English, German, Japanese, Spanish, French, Chinese Simplified, Chinese Traditional) of the Traps console, you must install the corresponding language pack.</td>
</tr>
</tbody>
</table>
Install the Traps Agent for Windows

Before installing Traps™ agent 4.2 on a Windows endpoint, verify that the system meets the requirements described in Traps Agent for Windows Requirements.

Install Traps agents using a software distribution tool of your choice or use one of the following methods:

- Install the Traps Agent Using the MSI
- Install the Traps Agent Using Msiexec

Traps agents also support installation on both a persistent and a non-persistent virtual desktop infrastructure (VDI). You are not required to complete additional actions when you install a Traps agent on a persistent VDI but you must perform additional tasks when you Set Up a Non-Persistent VDI.

Install the Traps Agent Using the MSI

Use the following workflow to install the Traps agent using the MSI file.

**STEP 1 |** Initiate the Traps software installation. You can also install Traps using Msiexec (see Install the Traps Agent Using Msiexec).

*The version(s) of Traps that you install on your endpoints must be the same as or older than the ESM Server and ESM Console version.*

1. Obtain the software from your Palo Alto Networks Account Manager, reseller, or from Customer Support Portal (https://support.paloaltonetworks.com).
2. Unzip the zip file and double click the **Traps** installation file; choose either the x64 (64-bit) or x86 (32-bit) version depending on your endpoint’s OS.
3. Click **Next**.
4. Select **I accept the terms in the License Agreement** and then click **Next**.

**STEP 2 |** Configure the Traps agents to connect to the ESM Server.

1. Provide the following information for the ESM Server:
   - **Host Name**—Enter the FQDN or IP address of the ESM Server.
   - **Port**—Change the port number, if required (default is 2125).
   - Select **SSL** to encrypt communication to the server (default) or **No SSL** to not encrypt communication (not recommended).
2. Click **Next > Install**.

**STEP 3 |** Click **Finish**.
STEP 4 | After you complete the installation, restart the endpoint.

STEP 5 | Verify Connectivity from the Endpoint.

Install the Traps Agent Using Msiexec

As an alternative to using the Windows MSI installer, you can use Windows Msiexec to install the Traps agent on Windows endpoints. Msiexec provides full control over the installation process and allows you to install, modify, and perform operations on a Windows Installer from the command line interface (CLI). You can also use Msiexec to log any issues encountered during installation.

You can also use Msiexec in conjunction with a System Center Configuration Manager (SCCM), Altiris, Group Policy Object (GPO), or other MSI deployment software to install Traps on multiple endpoints for the first time.

When you install Traps with Msiexec, you must install Traps per-machine and not per-user.

After installing Traps on an endpoint and establishing an initial connection with the ESM Server, you can upgrade or uninstall Traps from one or more endpoints by creating an action rule (see the Traps Endpoint Security Manager Administrator Guide).

Use the following workflow to install the Traps agent 4.2 using Msiexec.

STEP 1 | Use one of the following methods to open a command prompt as an administrator.

- Select Start > All Programs > Accessories. Right-click Command prompt and Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

STEP 2 | Run the msiexec command followed by one or more of the following options or properties:

Although Msiexec supports additional options, Traps installers support only the options listed here. For example, with Msiexec, the option to install the software in a non-standard directory is not supported—you must use the default path.

- Install, display, and logging options:
  - /i <installpath>\<installerfilename>.msi—Install a package. For example, msiexec /i c:\install\traps.msi.
  - /l*v <logpath>\<logfile>.txt—Log verbose output to a file. For example, /l*v c:\logs\install.txt.
  - /qn—Displays no user interface (quiet installation). At minimum, you must also specify the host server name or IP address using the CYVERA_SERVER property.

For a full list of Msiexec parameters, see https://docs.microsoft.com/en-us/windows/desktop/Msi/command-line-options

- Public properties:
  - CYVERA_SERVER=<servername>—Primary host server name or IP address (default is ESMserver)
  - CYVERA_SERVER_PORT=<serverport>—Primary host server port (default is 2125)
  - USE_SSL_PRIMARY=[0|1]—(Quiet installation only) Set encryption preferences on the primary server by specifying 0 to not use SSL (not recommended) or 1 to use SSL (default)
For example, to install Traps without a user interface, specify a server named TrapsServer that does not use SSL encryption on a port other than the default (for example on port 5212, a non-standard port), and create an installation log in C:\temp, enter the following:

```
msiexec
/i c:\install\traps.msi /l*v C:\temp\trapsinstall.log /qn
CYVERA_SERVER=TrapsServer
CYVERA_SERVER_PORT=5212 USE_SSL_PRIMARY=0
```

STEP 3 | After you complete the installation, restart the endpoint.

STEP 4 | Verify Connectivity from the Endpoint.

Verify Connectivity from the Endpoint

After successfully installing Traps, the Traps agent should be able to connect to the ESM Server. To verify the agent can connect:

STEP 1 | Launch the Traps Console using one of the following methods:
- From the notification area (system tray), double-click the Traps icon (or right-click the icon and select Console).
- Run CyveraConsole.exe from the Traps installation folder.

STEP 2 | Verify the status of the server connection. If Traps is connected to the server, the Connection status reports that the connection is successful. If the Traps agent is unable to establish a connection with the primary or secondary server, the Traps Console reports a disconnected status.

STEP 3 | If you cannot connect, verify network connectivity on the endpoint and then Check In Now.

STEP 4 | As an additional verification step, you can verify connectivity from the ESM Console. See the Traps Endpoint Security Manager Administrator’s Guide.
Set Up a Non-Persistent VDI

To set up a non-persistent virtual machine, you must configure a template policy known as a golden image. The settings in the golden image are used to create each new VDI clone. To prevent each new VDI clone from starting with a cache of unknown files and verdicts, you must collect all PE files that exist on the system and request their verdicts from WildFire.

Obtaining verdicts for all the PEs on the image is a multi-step process. After you collect all portable executable (PE) files, you use the Traps VDI tool (either the graphical interface or the command-line interface) to create a WildFire cache file containing the verdicts for all the PE files detected on the golden image including any that WildFire determined to be malicious. Then configure additional settings depending on the type of storage you want to use in your non-persistent VDI deployment. You can also use the Traps VDI tool to identify the golden image as a VDI instance in the Windows registry.

- VDI Installation Considerations
- Configure the Golden Image for Non-Persistent VDI
- Traps VDI Tool CLI
- Configure Storage for a VDI
- Tune and Test the VDI Policy

VDI Installation Considerations

- Optimize the default session policy on the VDI test pool to assure stable session spawning when the VDI is recompiled.
- Every new VDI creation will start with the initial policy as configured on the golden image. When the golden image is active and communicating with the ESM Server, test the policy on the VDI test pool and push it to the VDI Traps agents. Then fine tune the policy.
- Issues on restricted non-persistent sessions are harder to investigate because there is no forensic data after the session closes. Consider the following options to ensure forensic data is available:
  - Configure an agent setting rule on all non-persistent hostnames to enable the Traps agent to send the memory dumps automatically.
  - Reproduce the issue on a persistent session to collect logs and memory dumps and allow additional troubleshooting.
- Set a fixed number of session hostnames (not random) as licenses are issued by the ESM according to hostname. All naming conventions are supported.
- The ESM Server automatically revokes a license when an agent logs off of a VDI session. In cases where the VDI session is not properly closed, the ESM server waits for a timeout before automatically revoking the license to make it available for other agents. If another VDI session needs to use the license before the license revocation period expires, you can forcefully remove an endpoint from the ESM Console. This action returns the license to the license pool and removes the VDI session from the ESM Console.
- After you upgrade the Traps agent on a non-persistent from Traps 3.4 or earlier releases, you must mark the golden image as a VDI using the Traps VDI Tool (see Configure the Golden Image for Non-Persistent VDI).

Configure the Golden Image for Non-Persistent VDI

To avoid starting your VDI with a cache of unknown executable files, you can use the Traps VDI tool to request verdicts for all known PEs on your golden image. The Traps VDI tool is available on the Customer Support Portal (Updates > Software Updates > Traps Endpoint Protection Agent).
There are two versions of the VDI tool: 32-bit and 64-bit. Use the version of VDI tool that matches the VDI architecture.

STEP 1 | Before you begin:

1. Install the Traps Agent for Windows and any software that you plan to have on the VDI instances.
   
   If after completing the process to configure the golden image, you need to install additional software, you must recreate the WildFire cache file using the Traps VDI tool. This ensures that Traps obtains verdicts for the new software.

2. Verify that the Traps agent on the golden image can access the ESM Server.
   
   On the Traps agent, click **Check In Now** to obtain the latest verdicts from the ESM Server. If the ESM Server is reachable, the status on the console displays **Connected**.

3. Use the **Cytool for Windows** to stop Traps services (including local analysis) on the endpoint.

   Note that the Traps Reporting Service remains running after you stop services.

4. Collect all PE files available on the golden image using Sigcheck. This tool creates a file for you to use as input for the Traps VDI tool.
   
   
   2. Open a command prompt as an administrator and navigate to the directory to which you downloaded Sigcheck.
   
   3. Run Sigcheck recursively to find executable files regardless of extension and output the hashes in comma-separated format to a folder and file name of your choice.

   The Sigcheck parameters are subject to change. To display available usage guidelines, run the `sigcheck` command without options.

   The following examples show the commands you can use in two different versions of Sigcheck:

   **Sigcheck version 2.54**

   ```
   sigcheck
   /s /c /e /h C:\ > C:\temp\outfilename.csv
   ```

   **Sigcheck version 2.2**

   ```
   sigcheck /accepteula -s -h
   -e -c C:\ > C:\temp\outfilename.csv
   ```

STEP 2 | Use the Traps VDI Tool to obtain verdicts for all PE files

   A command-line version of the Traps VDI tool is also available. See **Traps VDI Tool CLI**.

   To ensure that the Traps VDI tool can obtain verdicts for all unknown files, we recommend that you verify the ESM Server can access WildFire ([https://wildfire.paloaltonetworks.com](https://wildfire.paloaltonetworks.com)).

   The Traps VDI tool communicates with the ESM Server to request any verdicts the server has stored in its server cache. The Traps VDI tool then creates a WildFire cache which can contain any of the following verdicts for each hash: malicious, benign, or unknown. A hash has an unknown verdict if the ESM Server has not submitted the sample to or received an updated verdict from WildFire.
1. Open the Traps VDI tool.
2. Configure the following settings:

- **ESM server address**—IP address or hostname of the ESM Server used for checking the hashes. This server must be able to connect to WildFire.
- **ESM server SSL binding**—Set the value to True if the server uses an SSL binding (default is False).
- **Input file**—Path of the comma-separated value (CSV) file created by the Sigcheck tool that contains all the hashes.
- **Password**—Enter the agent's uninstall password. This password is required to read data from protected locations when Service Protection is enabled.
- **ESM server port**—Port number for the ESM server (default is 2125).
- **Hash bulk size**—Hashes will be reported to the server in fragments of this size (default is 300; range is 1 to 500).
- **Tool timeout in hours**—Time in hours to wait for the Traps VDI tool to finish obtaining verdicts. If the Traps VDI tool exceeds the timeout, it stops generating the WildFire cache (default is 24 hours).
- **Wait for WildFire verdicts**—Select False to skip uploading unknown hashes and creating the cache file.
- **WildFire verdicts check interval**—Time in minutes between inquiries to check for new verdicts (default is 10).
- **Write malware to cache**—Select True to write malware verdicts to the cache file (default is False).
3. Click **Start**.

   The Traps VDI tool uses the results of the verdict lookup to create the WildFire cache of verdicts.
4. Wait two hours for the ESM Server to query WildFire for any unknown verdicts and then proceed to the next step. During this time, the ESM Server populates the server cache with any verdicts for hashes WildFire has previously analyzed.

**STEP 3** | Submit any remaining unknown executable files for analysis.

   The Traps VDI tool uploads the files to the ESM Server which then sends the files to WildFire for inspection. After the ESM Server submits the samples, the server queries WildFire every 10 minutes for updated verdicts. The entire process can take up to 24 hours to obtain verdicts for all unknown files.

1. Open the Traps VDI tool.
2. Change the **Wait for WildFire verdicts** setting to **True**. This setting enables the Traps VDI tool to send any remaining unknown executable files and wait for the WildFire verdict.
3. Click **Start**.

After the verdict lookup is complete, the Traps VDI tool recreates the WildFire cache containing the hashes and their verdicts.

**STEP 4 | Review any PE files that WildFire determined to be malicious.**

1. From the ESM Console, go to the Policies > Malware > Hash Control page.
2. Use the **Hash Control** search conditions to identify malware detected on the golden image:

![Hash Control search条件](image)

3. Perform one of the following actions for each malicious PE file:
   - Remove the malicious PE file from the golden image.
   - If you believe the WildFire verdict is incorrect:
     1. Override the verdict for the PE file on the **Hash Control** page of the ESM Console.
     2. Ensure that the Traps agent receives any verdict overrides. To do this, run the Traps VDI tool with the **Wait for WildFire verdicts** set to **True**. This enables the Traps VDI tool to obtain the changed verdicts from the ESM Server. This step typically finishes within ten minutes.

**STEP 5 | Configure the golden image as a non-persistent VDI using the Traps VDI tool.**

This ensures that the agent on each spawned machine registers with the ESM as a new agent. This also ensures the ESM revokes licenses for the VDI when the session is inactive or ends.

1. On the golden image, open the Traps VDI tool.
2. Select **Menu > Mark as VDI**.
3. Enter the Traps uninstall password and click **Mark as VDI**.

The Traps VDI tool identifies the machine in the Windows registry as a non-persistent VDI.

**Traps VDI Tool CLI**

The Traps VDI Tool requests verdicts for all the PE files detected on the golden image and outputs the verdicts to a WildFire cache file. You can use the command-line interface (CLI) version of the Traps VDI Tool to automate the creation of this file.

Consider the following usage guidelines for the Traps VDI Tool CLI:

- If you run the Traps VDI Tool with at least one command line argument, it will run in unattended mode (no user interface). If you issue the `TrapsVdiTool` command without any arguments, the user interface opens.
- By default, arguments with flag values—yes or no—default to yes. Therefore, to use the default value, you can specify the argument without the value (e.g. use `-ssl` instead of `-ssl:y`).
- If a path value contains one or more spaces, surround the entire path argument with double quotes, for example: 
  ```bash
  -i:c:\temp\sig file.csv
  ```
- You cannot use the Traps VDI Tool to check hashes and mark the computer as a VDI—using the `-m` argument—at the same time. Therefore, you must execute these actions separately.
- To write output to a log file, use the > redirect to send output to a filename of your choice, for example:
  ```bash
  TrapsVdiTool -m > TrapsVDI.log
  ```

**STEP 1 | Download the Traps VDI Tool package from the Support Portal.**
STEP 2 | Copy and then unzip the package on the golden image.

STEP 3 | Open a command prompt as an administrator:

- Select Start > All Programs > Accessories. Right-click Command prompt, and then select Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

STEP 4 | Navigate to the folder that contains the Traps VDI Tool CLI:

C:\Users\Administrator>cd C:\TrapsVDItool

STEP 5 | View usage and options for the DB Configuration Tool:

```
c:\TrapsVDItool> TrapsVdiTool -help

    TrapsVdiTool -m:password

    -help          Displays the help screen.
    -silent        Perform tasks in silent mode (no log displays).
    -i:path        Input file (must be CSV). Specifies the path of the
                   file produced by the sigcheck tool. No default. Surround the entire path
                   argument with double quotes to specify a path that contains spaces, for
                   example: "-i:c:\temp\sig file.csv".
    -e:address     Specifies the ESM server address (FQDN or IP).
    -p:port        Specifies the ESM server port. Default: 2125
                   ESM server SSL binding. Indicates use of secured
                   server connection. 'y' for using SSL, 'n' otherwise. Default: n
    -b:size        Hash bulk size. Specifies the bulk size for hash
                   transfers. Default: 300
    -to:hours      Tool timeout in hours. Limits execution time to
                   specified number of hours. Default: 24
    -v[:flag]      Wait for WildFire verdicts. Indicates if should wait
                   for WildFire verdicts. 'y' for waiting, 'n' - otherwise. Default: n
    -c:minutes     Specifies WildFire verdicts check interval in
                   minutes. Default: 10
    -r[:flag]      Instructs the tool to continue from where it left
                   off previously. Default: n
    -w[:flag]      Write malware verdicts to cache. Default: n
    -g[:flag]      Write grayware verdicts to cache. Default: y
    -s:password    The agent’s uninstall password. Required to read
                   data from protected locations when Service Protection is enabled.
    -m:            Instructs the Traps VDI Tool to identify this computer as VDI
                   using the uninstall password and skips performing hash checks. No default. Do not
                   use this option if you want the Traps VDI Tool to perform hash checks.

    CLI execution examples.
    TrapsVdiTool -i:c:\temp\sig.csv -e:192.168.70.100 -ssl -to:1
```
STEP 6 | Specify arguments to create the WildFire cache file or to mark the golden image as a VDI instance. For example:

- **TrapsVdiTool -i:c:\temp\sig.csv -e:192.168.70.100 -ssl -to:1**

  The Traps VDI Tool requests verdicts for the hashes in the c:\temp\sig.csv input file, from the ESM Server with the IP address 192.168.70.100, over a secure connection, and limits the execution time to 1 hour. All the other arguments are set to their default values.

- **TrapsVdiTool "-i:c:\temp\sig file.csv" -v -w**

  The Traps VDI Tool requests verdicts for the hashes in the c:\temp\sig file.csv input file from the default ESM Server, and creates the cache file only after it has received verdicts for all hashes. Note the file path is enclosed in quotes because the filename contains a space.

- **TrapsVdiTool -m:password**

  The Traps VDI Tool identifies the golden image as a VDI instance without performing hash checks.

Configure Storage for a VDI

With a persistent VDI, each user runs a desktop session independently. The settings for users are typically saved to the logical desktop while the user data is stored on a separate logical drive. Both the settings and data remain after the user session ends.

- Configure Traps for a Persistent Storage Scenario
- Configure Traps for a Non-Persistent Storage Scenario

Configure Traps for a Persistent Storage Scenario

If utilizing a VDI machine to offload to a local storage area, you need to make additional changes to the golden image, including changes to the Traps service properties and the startup and shutdown scripts.

STEP 1 | Create a symbolic link from the machine's standard drive to the machine's local storage each time the VDI boots.

On the golden image, run the startup script using GPO or schedule it to run as a task or local policy.

```
set drivepath=D:\
set datapath=%drivepath%\ProgramData\Cyvera
```
set policypath=%ProgramData%\CyveraNotInUse\LocalSystem\Data\ClientPolicy.json

IF EXIST %drivepath% (
    IF EXIST %ProgramData%\Cyvera (rename %ProgramData%\Cyvera CyveraNotInUse)
    %windir%\system32\cmd.exe /c mklink /J %ProgramData%\Cyvera %datapath% 2>&1
    IF NOT EXIST %datapath% (
        mkdir %datapath%
    )
    IF NOT EXIST %datapath%\Everyone\Data (
        mkdir %datapath%\Everyone\Data
    )
    IF NOT EXIST %datapath%\Everyone\Temp (
        mkdir %datapath%\Everyone\Temp
    )
    IF NOT EXIST %datapath%\LocalSystem (
        mkdir %datapath%\LocalSystem
    )
    IF NOT EXIST %datapath%\LocalSystem\ClientPolicy.* (del /F %datapath%\LocalSystem\ClientPolicy.*
    )
    IF NOT EXIST %datapath%\LocalSystem\Data (mkdir %datapath%\LocalSystem\Data copy %policypath% %datapath%\LocalSystem\Data\ClientPolicy.json
    )
    IF NOT EXIST %datapath%\Logs (mkdir %datapath%\Logs
    )
    IF NOT EXIST %datapath%\Prevention (mkdir %datapath%\Prevention
    )
    IF NOT EXIST %datapath%\Quarantine (mkdir %datapath%\Quarantine
    )
    IF NOT EXIST %datapath%\Administrators\Temp (mkdir %datapath%\Administrators\Temp
    )
)
sc start cyserver
sc start cyveraservice
net start tlaservice

To configure GPO for startup scripts:
1. Run gpmc.msc (Group Policy Management) on your domain controller and then create a new GPO.
2. Give the GPO a meaningful name and click OK.
3. Right-click on the newly created GPO and select Edit.
4. In the left pane of the Group Policy Management Editor, navigate to Scripts (Startup/Shutdown), and then go to the right pane and double-click Startup.
5. Click Add, navigate to your script, select your script, and click OK.

STEP 2 | Reset the services state before the image is sealed and migrated into a test or production environment.
On the golden image, create a batch file using the shutdown script and then run it.

```bash
::Stop Cyvera services
net stop CyveraService
net stop CyServer
net stop tlaservice
rd c:\ProgramData\Cyvera /q
ren c:\ProgramData\CyveraNotInUse Cyvera

net start CyveraService
net start CyServer
```

**STEP 3 | Configure Traps services.**

1. Open services.msc: Click **Start** > **Run**, enter services.msc, and then press **Enter**.
2. Right-click the **Traps** service and select **Properties**.
3. From the service **Startup type** drop-down, select **Manual**.
4. Click **Apply** and **OK**.
5. Repeat the process for the **Traps Dump Analyzer Service** and **Traps Reporting Service**.

**Configure Traps for a Non-Persistent Storage Scenario**

In a non-persistent storage scenario, you must configure the Traps service dependency on the Spooler Service (or any of the other last loading services) per the following Microsoft KB [http://support.microsoft.com/kb/193888](http://support.microsoft.com/kb/193888).

**STEP 1 |** Open the Windows Registry and locate the CyveraService key in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\`

**STEP 2 |** Double-click the **DependOnService** multistring.

**STEP 3 |** Add **Spooler** to the Value data list.

**STEP 4 |** Click **OK**.

**Tune and Test the VDI Policy**

After you configure the golden image, tune and test the policy using the following workflow.

**STEP 1 |** Fine-tune the exploit and malware protection policies for your VDI.
If your organization supports a mixed environment of VDI and non-VDI instances, you can apply the Condition for VDI Machine to each rule that applies to only the VDI instances. For example, you can configure Traps to:

**STEP 2 |** Use the golden image to spawn a small pool of persistent sessions (2 or 3). Deploy the sessions in a production environment and imitate the expected day-to-day user behavior, such as browsing, development, and dedicated application usage.

**STEP 3 |** Gather additional information during this period to further optimize the default session policy and test any special restrictions applied to the non-persistent sessions. Typically, clients deployed in persistent mode enable better forensics collection than clients deployed in non-persistent mode.

**STEP 4 |** Resolve any stability issues on the test machine and on the test VDI pool that were caused by the exploit or malware protection policies.

**STEP 5 |** After the VDI server spawns a session from the golden image and connects to the ESM Server, disconnect the golden image. Then revise the VDI policy so that WildFire integration is enabled, EPM Injection is set according to the configuration tested on the golden image, heartbeat and reporting settings use longer intervals (60 minutes is recommended), and memory dumps are sent automatically.

Traps will replace the initial golden image with the revised VDI policy. Changing the VDI policy affects all spawned session on the next restart.

**STEP 6 |** Recompile the golden image.
   1. Restart the image.
   2. Verify that the image can connect to the ESM Server.
   3. Shut down the image and then recompile it.

**STEP 7 |** Log into the ESM Console and verify the health of the VDI instances on the Monitor > Agent > Health page. If your organization uses a mixed environment, you can filter the machine Type column to show only VDI instances. The ESM Console should display the status of the VDI instances as connected.
Use Traps Agent for Windows

Traps™ agent installs in the C:\Program Files (x86)\Palo Alto Networks\Traps folder. If you enabled access to the console, the Traps console is also accessible from the notification area (system tray).

Use the following topics to use and manage the Traps agent for Windows:

- Open the Traps application.
- View status information about the Traps agent.
- Manually connect to the server.
- View and send logs.
- View recent security events that occurred on your endpoint.
- View running processes that are currently protected by the Traps agent.
- View changes to the endpoint security policy.
- Change the display language for the Traps console.

- Open the Traps application.
  
  Use one of the following methods:
  
  - Browse to C:\Program Files\Palo Alto Networks\Traps and run the CyveraConsole.exe application.
  - If you enabled access to Traps from the notification area, double-click the Traps icon (👨‍💻) to launch the agent interface.

- View status information about the Traps agent.
  
  The console displays active and inactive features by displaying a ☑️ or ❌ to the left of the feature type. Select the Advanced tab to display additional tabs along the top of the console. The tabs allow you to navigate to pages that display additional details about security events, protected processes, and updates to the security policy. Usually, an end user will not need to run the Traps Console, but the information can be useful when investigating a security-related event. You can choose to hide the tray icon that launches the console, or prevent its launch altogether.

- Advanced Endpoint Protection—Displays the overall protection status of the endpoint as enabled if one or more protection features are enabled, or disabled if no protection features are enabled.
  
- Anti-Exploit Protection—Indicates whether or not exploit prevention rules are active in the endpoint security policy.
  
- Anti-Malware Protection—Indicates whether restriction or malware protection modules are enabled in the endpoint security policy.
• **Forensic Data Collection**—Indicates whether or not WildFire integration is enabled.
• **Version**—Displays the Traps agent version.
• **Connection**—Displays the connection status and, if connected, includes the server to which the agent is connected.
• **Last Check-in**—Displays the local time on the endpoint of the last check-in with the server.

- Manually connect to the server.

  The Traps agent periodically communicates with the server to send status information and retrieve the latest security policy. The Traps agent performs this operation transparently at regular intervals so it is not typically necessary to connect to the server manually. If your Connection status is Not Connected, you can try to manually connect. This option is available if you do not want to wait for the automated communication interval to become active.

  To initiate a manual check-in with the server, **Check In Now** from the home page of the Traps console. If the agent successfully establishes a connection with the server, the Connection status changes to Connected.

- View and send logs.

  - **View logs**—**Open Log File** to view logs generated by the Traps agent. The logs display in your default text editor in chronological order with the most recent logs at the bottom.
  - **Send logs**—**Send Support File** to collect Traps logs and send them to the Traps Endpoint Security Manager. The logs help you to analyze any recent security events and Traps issues that you encounter.

- View recent security events that occurred on your endpoint.

  1. Click **Advanced**, if necessary, to display additional actions that you can perform from the Traps console.
  2. Click **Events**.

     For each event, the Traps console displays the local **Time** that an event occurred, the name of the **Process** that exhibited malicious behavior, the **Module** that triggered the event, and the mode specified for that type of event (Termination or Notification).

- View running processes that are currently protected by the Traps agent.

  1. Click **Advanced**, if necessary, to display additional actions that you can perform from the Traps console.
  2. Click **Protection**.
- View changes to the endpoint security policy.
  For each policy change, the Traps console displays the rule name or description of the change and the
date and time of the change.

  1. Click Advanced, if necessary, to display additional actions that you can perform from the Traps
  console.
  2. Click Policy.

- Change the display language for the Traps console.

  The Traps console is localized in the following languages: English, German, French, Spanish, Chinese
(traditional and simplified), and Japanese. To set the language, you must install the corresponding
language pack.

  1. Click Advanced, if necessary, to display additional actions that you can perform from the Traps
  console.
  2. Click Settings.
  3. Select the display language for Traps (default is English).
Uninstall Traps Agent for Windows

You can uninstall the Traps™ agent using any of the following methods on a Windows endpoint:

- **Uninstall from the Traps Endpoint Security Manager** (Refer to how you Uninstall the Traps Agent in the Traps Endpoint Security Manager Administrator’s Guide.)
- Manually Uninstall the Traps Agent for Windows
- Uninstall the Traps Agent for Windows Using Msiexec

After you uninstall the agent, the endpoint is no longer protected by the Security policy of your company and the license returns to the pool of available licenses.

Manually Uninstall the Traps Agent for Windows

Use the following workflow to manually uninstall Traps.

**STEP 1 |** Select Start > Control Panel > (Programs) > Programs and Features.

**STEP 2 |** Select Traps from the list and then Uninstall.

**STEP 3 |** When prompted to continue uninstalling, click Yes and acknowledge any notifications.

**STEP 4 |** Enter the uninstall password and click Next.

Uninstall the Traps Agent for Windows Using Msiexec

Use the following workflow to uninstall Traps using Msiexec.

**STEP 1 |** Use one of the following options to open a command prompt as an administrator:

- Select Start > All Programs > Accessories. Then right-click Command prompt and Run as administrator.
- Select Start. In the Start Search box, type cmd. Then, to open the command prompt as an administrator, press CTRL+SHIFT+ENTER.

**STEP 2 |** Run the msiexec command followed by one or more of the following options or properties:

- Uninstall and logging options:
  - /x <installpath>\<installerfilename>.msi—Uninstall a package.
  - /l*v <logpath>\<logfileaname>.txt—Log verbose output to a file.

  For a full list of Msiexec parameters, see https://docs.microsoft.com/en-us/windows/desktop/Msi/command-line-options

- Public properties:
  - UNINSTALL_PASSWORD=<uninstallpassword>—Specify the administrator password. You must specify the UNINSTALL_PASSWORD property to successfully uninstall a package.

For example, to uninstall Traps using the traps.msi installer with the specified password and log verbose output to a file called uninstallLogFile.txt, enter the following command:

C:\Users\username>msiexec
Troubleshooting Resources for Traps Agent for Windows

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traps™ installation log</td>
<td>Specifies any errors encountered during installation of Traps components. Use this log file when you need to troubleshoot installation issues. On Windows endpoints, the installer stores the log files in the %temp% or C:\Users&lt;user_name&gt;\AppData\Local\Temp folder.</td>
</tr>
<tr>
<td>Traps service log</td>
<td>Indicates information, warnings, and errors related to the Traps service. The Service log is located in the following folder on the endpoint:</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista or a later Windows OS—%ProgramData%\Cyvera Logs</td>
</tr>
<tr>
<td></td>
<td>• Windows XP—C:\Document and Settings\All Users \Application Data\Cyvera\Logs</td>
</tr>
<tr>
<td>Traps console log</td>
<td>Indicates information, warnings, and errors related to the Traps console. The Console log is located in the following folder on the endpoint:</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista or a later Windows OS—C:Users&lt;username&gt; \AppData\Roaming\Cyvera</td>
</tr>
<tr>
<td></td>
<td>• Windows XP—C:\Document and Settings&lt;username&gt; \Application Data\Cyvera\Logs</td>
</tr>
<tr>
<td>Supervisor Command Line Tool (cytool.exe)</td>
<td>Allows you to manage Traps features and perform advanced troubleshooting on the local endpoint from a command line interface. For more information, see Cytool for Windows.</td>
</tr>
<tr>
<td>Unknown files for analysis</td>
<td>Traps stores unknown files to send to the Endpoint Security Manager in the C:\ProgramData\Cyvera\Temp folder. After the Endpoint Security Manager submits a file to WildFire®, the Traps agent deletes the file from the Temp folder.</td>
</tr>
<tr>
<td></td>
<td>In some cases, third-party Antivirus (AV) applications raise an alert for this folder. If this occurs, we recommend that you whitelist this folder in the third-party AV application.</td>
</tr>
</tbody>
</table>

Cytool for Windows

Cytool is a command-line interface (CLI) that is integrated into Traps and enables you to query and manage both basic and advanced functions of Traps. Any changes you make using Cytool are active until Traps receives the next heartbeat communication from the ESM Server.

On Windows endpoints, you can access Cytool using a Microsoft MS-DOS command prompt that you run as an administrator. Cytool is located in the C:\Program Files\Palo Alto Networks\Traps folder on the endpoint.

The following table displays the Cytool options available on Windows endpoints.
<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>enum</strong></td>
<td>Enumerate protected processes.</td>
</tr>
<tr>
<td>Usage: <code>cytool enum</code></td>
<td></td>
</tr>
<tr>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td>C:\Program Files\Palo Alto Networks\Traps&gt; <code>cytool enum</code></td>
<td></td>
</tr>
<tr>
<td>Process ID</td>
<td>Agent Version</td>
</tr>
<tr>
<td>6396</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>6316</td>
<td>N/A</td>
</tr>
<tr>
<td>5788</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>8576</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>5532</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>7244</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>7160</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>8596</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>1064</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>7820</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>5156</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td>6904</td>
<td>4.2.0.33808</td>
</tr>
<tr>
<td><strong>protect</strong></td>
<td>Enable or disable a protection feature.</td>
</tr>
<tr>
<td>Usage: <code>cytool protect &lt;action&gt; &lt;feature&gt;</code></td>
<td></td>
</tr>
<tr>
<td>where:</td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;action&gt;</code>—Changes protection for a Traps feature. Options are: <code>enable</code>, <code>disable</code>, <code>policy</code>, and <code>query</code>. The query option displays the protection status for each feature.</td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;feature&gt;</code>—Specifies the feature for which you want to change the protection status. Options are <code>process</code> for Traps core processes, <code>registry</code> for Traps registry keys, <code>file</code> for Traps files, and <code>service</code> for Traps services.</td>
<td></td>
</tr>
<tr>
<td>For example:</td>
<td></td>
</tr>
<tr>
<td>C:\Program Files\Palo Alto Networks\Traps&gt; <code>cytool protect disable process</code></td>
<td></td>
</tr>
<tr>
<td>Enter supervisor password:</td>
<td></td>
</tr>
<tr>
<td>Protection</td>
<td>Mode</td>
</tr>
<tr>
<td>Process</td>
<td>Disabled</td>
</tr>
<tr>
<td>Registry</td>
<td>Policy</td>
</tr>
<tr>
<td>File</td>
<td>Policy</td>
</tr>
<tr>
<td>Service</td>
<td>Policy</td>
</tr>
<tr>
<td><strong>startup</strong></td>
<td>Enable, disable, or query the startup state of Traps components.</td>
</tr>
<tr>
<td>Usage: <code>cytool startup &lt;action&gt; &lt;component&gt;</code></td>
<td></td>
</tr>
<tr>
<td>where:</td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;action&gt;</code>—Changes startup action for a Traps component. Options are: <code>enable</code>, <code>disable</code>, and <code>query</code>. The query option displays the startup status for each component.</td>
<td></td>
</tr>
<tr>
<td>• <code>&lt;component&gt;</code>—Specifies the component for which you want to change the startup action. To change the startup action for multiple components, list them</td>
<td></td>
</tr>
<tr>
<td>Command Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| runtime        | Stop or start product components. Usage: `cytool runtime <action> <component>` where:  
  - `<action>`—Changes startup runtime action for a Traps component. Options are: `start`, `stop`, and `query`. The query option displays the startup status for each component.  
  - `<component>`—Specifies the component for which you want to change the runtime action, or you can specify all components by not including any in this command. To change the runtime action for a subset of components, list them with spaces separating each component. Options are: `cyverak`, `cyvrmtgn`, `cyvrfsfd`, `cyserver`, `tlaservice`, `CyveraService`, and `twdservice`. For example:  
    
    ```bash
    C:\Program Files\Palo Alto Networks\Traps> cytool runtime stop cyserver cyverak
    Enter supervisor password:
    Service         State
    cyverak         Stopped
    cyvrmtgn        Running
    cyvrfsfd        Running
    cyserver        Stopped
    CyveraService   Stopped
    tlaservice      Stopped
    twdservice      Stopped
    ```  
| policy         | Query or compare the applied policy for a process. Usage: `cytool policy <action> <process>` where:  
  - `<action>`—Options are: `query` and `compare`. The `query` option displays the current applied policy for the process; the `compare` option enables you to compare the policy against the policy for another process or against the default policy. For example:  
    
    ```bash
    C:\Program Files\Palo Alto Networks\Traps> cytool policy query <process>
    ```
<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <code>&lt;process&gt;</code>—Either the process name or process ID (PID).</td>
<td></td>
</tr>
</tbody>
</table>

For example, to query the policy for future executions of notepad.exe:

C:\Program Files\Palo Alto Networks\Traps> cytool policy query notepad.exe
Enter supervisor password:

<table>
<thead>
<tr>
<th>Generic</th>
<th>Enable</th>
<th>0x00000001</th>
</tr>
</thead>
<tbody>
<tr>
<td>LongHooks</td>
<td>0x00000000</td>
<td></td>
</tr>
<tr>
<td>StaticHooks</td>
<td>0x00000000</td>
<td></td>
</tr>
<tr>
<td>NoCallSplitting</td>
<td>0x00000000</td>
<td></td>
</tr>
<tr>
<td>InitSecurityCookie</td>
<td>0x00000000</td>
<td></td>
</tr>
<tr>
<td>DontInjectThinApp</td>
<td>0x00000001</td>
<td></td>
</tr>
<tr>
<td>LeanInjection</td>
<td>0x00000000</td>
<td></td>
</tr>
</tbody>
</table>

B01
| Enable | 0x00000000 |
| BlockAPI | 0x00000000 |

[...]

For example, to compare the policy for future executions of notepad.exe to the default policy:

C:\Program Files\Palo Alto Networks\Traps> cytool policy compare notepad.exe default
Enter supervisor password:

<table>
<thead>
<tr>
<th>Generic</th>
<th>Enable</th>
<th>0x00000001</th>
</tr>
</thead>
<tbody>
<tr>
<td>LongHooks</td>
<td>0x00000000 0x00000000</td>
<td></td>
</tr>
<tr>
<td>StaticHooks</td>
<td>0x00000000 0x00000000</td>
<td></td>
</tr>
<tr>
<td>NoCallSplitting</td>
<td>0x00000000 0x00000000</td>
<td></td>
</tr>
<tr>
<td>InitSecurityCookie</td>
<td>0x00000000 0x00000000</td>
<td></td>
</tr>
<tr>
<td>DontInjectThinApp</td>
<td>0x00000001 0x00000000</td>
<td></td>
</tr>
<tr>
<td>LeanInjection</td>
<td>0x00000000 0x00000000</td>
<td></td>
</tr>
</tbody>
</table>

B01
| Enable | 0x00000000 |
| BlockAPI | 0x00000000 |

[...]

log
Operate product log sessions.
Usage: cytool log <action>
where `<action>` is one of the following:
<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>start</strong> &lt;log_size&gt;</td>
<td>Starts the log session and logs the results to a file with a maximum size in MB (up to 25MB).</td>
</tr>
<tr>
<td><strong>stop</strong></td>
<td>Stop the log session.</td>
</tr>
<tr>
<td><strong>reset</strong></td>
<td>Reset all logging configurations to their defaults. If an active logging session exists, it will be restarted.</td>
</tr>
<tr>
<td><strong>set</strong> &lt;component&gt; &lt;log_level&gt; &lt;flag&gt;</td>
<td>where:</td>
</tr>
<tr>
<td>&lt;component&gt;</td>
<td>can be either <strong>all</strong> (set the log level for all components) or one of the following individual components: cyvrlpc, cyvrsfd, cyverak, cyvrmtn, cyreport, cyserver, cyapi, cylnk, cyprptui, cytray, tlaservice, tlaworker, tlccore, cytool, cyverau, cyinjct, cyvrrtp, cyvera, ntntnativeapi, winutils, or panwd.</td>
</tr>
<tr>
<td>&lt;log_level&gt;</td>
<td>can be one of the following log levels: <strong>NONE</strong>, <strong>CRITICAL</strong>, <strong>ERROR</strong>, <strong>WARNING</strong>, <strong>INFO</strong>, <strong>VERBOSE</strong>, <strong>DEBUG</strong>, or <strong>ALL</strong>.</td>
</tr>
<tr>
<td>&lt;flag&gt;</td>
<td>is the mask (hex) of one or more trace flags (a maximum of 31) separated by spaces that Traps assigns to each trace when a program runs on the endpoint (for example 0x7FFFFFFF, or 0x5). The trace flag is a property of a trace provider (in this case, Traps) and determines which events Traps generates. You can use the trace flag to filter events that Traps traces.</td>
</tr>
</tbody>
</table>

- **convert** <etl_file> [tmf_file]>—Extract the encoded event trace log (ETL) file using a trace message format (TMF) file as a key to a file with the same name and store the result in `%ProgramData%\Cyvera\Logs\Log.txt`. When a TMF file is not supplied, Cytool uses the default TMF file stored in the `%ProgramData%\Cyvera\Logs\` folder to convert the ETL file. | *This command is not supported on Windows XP SP3.* |

**Examples:**

```
CYTOOL log convert %ProgramData%\Cyvera\logs\traps_native_log.4.0.0.0.etl
Converts the default log file (.etl) with log.tmf that is located in the same folder.
```

```
CYTOOL log set cyvrrttrap ERROR 0x5
Sets cyvrrttrap's configuration to produce ERROR traces of first and third flags.
```

```
CYTOOL log set all VERBOSE 0x7FFFFFFF
Sets all components configuration to produce VERBOSE traces with all flags.
```

**quarantine** | View and restore quarantined files. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usage:</strong></td>
<td></td>
</tr>
<tr>
<td>• cytool quarantine list—List all quarantined files.</td>
<td></td>
</tr>
<tr>
<td>• cytool restore &lt;ID&gt; [path]—Restore files to their original location or to a path, if specified, by specifying the file ID.</td>
<td></td>
</tr>
</tbody>
</table>

**stat** | Query Traps statistics from a running process. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usage:</strong></td>
<td></td>
</tr>
<tr>
<td>cytool stat &lt;pid&gt;</td>
<td></td>
</tr>
</tbody>
</table>
where `<pid>` is the process ID (PID).

For example, to display statistics about the Chrome process identified by PID 4080:

```bash
c:\Program Files\Palo Alto Networks\Traps> cytool stat 4080
DllSec Invocations: 0
DllSec Time: 00:00:00.0
G01 Invocations: 0
G01 Time: 00:00:00.0
G01 Thunk 00 Resolution: 0
G01 Thunk 01 Resolution: 0
G01 Thunk 02 Resolution: 0
G01 Thunk 03 Resolution: 0
G01 Thunk 04 Resolution: 0
G01 Thunk 05 Resolution: 0
G01 Thunk 06 Resolution: 0
G01 Thunk 07 Resolution: 0
G01 Thunk 08 Resolution: 0
G01 Thunk 09 Resolution: 0
G01 Thunk 10 Resolution: 0
G01 Thunk 11 Resolution: 0
G01 Thunk 12 Resolution: 0
G01 Thunk 13 Resolution: 0
G01 Thunk 14 Resolution: 0
G01 Thunk 15 Resolution: 0
G01 Stack Walk Resolution: 0
J01 Minimum Stack Depth: 166
J01 Checks: 25
J01 Stack Walk Checks: 0
```

**tla**

View the history of the Traps local analysis module.

Usage: `cytool tla query`

For example:

```bash
C:\Program Files\Palo Alto Networks\Traps> cytool tla query
FileType: Executable
Build: 589
Timestamp: Sunday, February 11, 2018, 12:32:36

FileType: Dynamically Linked Library
Build: 585
Timestamp: Wednesday, January 10, 2018, 12:37:20

FileType: Visual Basic Application Macro
Build: 591
Timestamp: Monday, February 12, 2018, 11:11:04
```

**info**

Display general Traps information.

Usage: `cytool info [query]`

To display the Traps version, run the `cytool info` command without any additional arguments. To display additional details about Traps, such as the version of the default policy and the specific build number, add the query argument. For example:
### Command Option

<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cytool info</strong></td>
<td>General Traps information. Usage: <code>cytool info query</code></td>
</tr>
<tr>
<td><strong>cytool image</strong></td>
<td>Display image information about a specific PE file. Usage: <code>cytool image &lt;process_path&gt;</code> For example:</td>
</tr>
<tr>
<td><strong>cytool wf</strong></td>
<td>WildFire operations. Usage: <code>cytool wf query [&lt;&lt;hash&gt;&gt;]</code></td>
</tr>
</tbody>
</table>
The Traps agent protects Mac endpoints by preventing known and unknown malware from running and halting attempts to leverage software exploits and vulnerabilities. The Traps agent enforces your organization’s security policy as defined in the Traps Endpoint Security Manager. When a security event occurs on an endpoint, Traps collects forensic information about that event which you can use to analyze the incident further.

The following topics describe how to install and use the Traps agent for Mac:

> Traps for Mac Requirements
> Install the Traps Agent for Mac
> Use the Traps Agent for Mac
> Upgrade Traps from the ESM Console (see the Traps Endpoint Security Manager Administrator’s Guide)
> Uninstall the Traps Agent for Mac
> Troubleshooting Resources for the Traps Agent for Mac
# Traps for Mac Requirements

The Traps agent for Mac has the following requirements:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version parity</td>
<td>The Traps agent version must not exceed the ESM Server and ESM Console version.</td>
</tr>
<tr>
<td>Processor</td>
<td>• Intel Pentium 4 or later with SSE2 instruction set support</td>
</tr>
<tr>
<td></td>
<td>• AMD Opteron/Athlon 64 or later with SSE2 instruction set support</td>
</tr>
<tr>
<td>RAM</td>
<td>512MB minimum; 2GB recommended</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>200MB minimum; 20GB recommended</td>
</tr>
<tr>
<td>Operating system versions</td>
<td>Palo Alto Networks supports Traps on many operating systems. To determine the minimum Traps release for a specific operating system, refer to Where Can I Install the Traps Agent? in the Palo Alto Networks® Compatibility Matrix.</td>
</tr>
<tr>
<td>Networking</td>
<td>Allow communication on the TCP port from clients to server (the default is port 2125). Allow communication on TCP port 443 if you enable secure communication.</td>
</tr>
</tbody>
</table>
Install the Traps Agent for Mac

Before installing Traps on a Mac endpoint, verify that the system meets the requirements described in Traps for Mac Requirements.

Install Traps using a software distribution tool of your choice (such as JAMF) or using the following workflow:

STEP 1 | Download the installation package you want to install from the ESM Console.

STEP 2 | Copy the installation package to the endpoint on which you want to install the Traps software. For more information, see the Traps Endpoint Security Manager Administrator's Guide.

STEP 3 | Install the Traps software.
1. Unzip the installation package and run the `Traps.pkg` installation file.
2. Click Continue to proceed with the installation.
3. If prompted to confirm the destination, click Continue.
4. Click Install to begin the installation.
5. Enter the User Name and Password of the administrator with access to install software on the endpoint, and then click Install Software.
6. Click Close.
7. Click Keep if you want to retain the install package and Traps Uninstaller.
8. If prompted, allow Traps to install system extensions:
   
   *The installer displays a System Extension Blocked warning on macOS 10.13 and later releases if you have not previously allowed software from Palo Alto Networks to install system extensions. If you later reinstall the app, the installer does not prompt you again.*

1. Dismiss the System Extension Blocked warning.
2. Go to System Preferences > Security & Privacy > General and select Allow.

![Configuration Settings](image)

**STEP 4** | After the installation completes, verify your connection.

1. To open the Traps console, click the Traps icon in the menu bar, and select Open Console.
2. Click **Check In Now** to initiate a connection with the ESM Server. If successful, the **Last Check-In** field updates to display the recent check-in date and time.

![Connection Verification](image)
Use the Traps Agent for Mac

See the following topics to use or manage the Traps agent for Mac:

- Open the Traps application.
- View status information about the Traps agent:
- Manually connect to the server.
- View and send logs.
- View recent security events that occurred on your endpoint.
- View protected processes on the Mac endpoint.
- Configure proxy communication.

- Open the Traps application.
  Use one of the following methods:
  - Browse to the Traps application in Finder.
  - If you enabled access to the Traps console, click the Traps icon ( ![Traps Icon](image.png)) in the menu bar, and select Open Console.

- View status information about the Traps agent:

  ![Traps Application Screenshot](image.png)

  - **Version**—Displays the Traps agent version.
  - **Protection**—Displays the active policies in bold.
• **Connection**—Displays the connection status and, if connected, includes the server to which the agent is connected.

• **Last Check-in**—Displays the local time on the endpoint of the last check-in with the server.

• Manually connect to the server.

The Traps agent periodically communicates with the server to send status information and retrieve the latest security policy. The Traps agent performs this operation transparently at regular intervals so it is not typically necessary to connect to the server manually. If your **Connection** status is **Not Connected**, you can manually retry your connection. This option is available if you do not want to wait for the automated communication interval to begin.

To initiate a manual check-in with the server: On the home page of the Traps console, click **Check In Now**. If the agent successfully establishes a connection with the server, the **Connection** status changes to indicated the service to which the agent is connected.

• View and send logs.

  • Send logs—Click **Send Support File** to collect Traps logs. The logs can help you further analyze any recent security events and Traps issues that you encountered.

  • View logs—Click **Open Log File** to view logs generated by the Traps agent. The logs display in your default text editor in chronological order with the most recent logs at the bottom.

• View recent security events that occurred on your endpoint.

For each event, the Traps console displays the local **Time** an event occurred, the name of the **Process** that exhibited malicious behavior, the **Module** that triggered the event, and the mode specified for the type of event (Termination or Notification).
• View protected processes on the Mac endpoint.

The Protection tab of the Traps console displays all running processes in which Traps is injected to prevent malicious execution or behavior. The Traps console also indicates the process ID (PID) associated with each process.

• Configure proxy communication.

Traps can communicate with the ESM Server using the system proxy server that you define for the endpoint. For information on How to Enter Proxy Settings, see the documentation for your Mac operating system version.
Uninstall the Traps Agent for Mac

From the ESM Console you can uninstall the Traps agent on an endpoint (see Uninstall the Traps Agent in the Traps Endpoint Security Manager Administrator's Guide). You can also uninstall the agent from the endpoint directly. On Mac endpoints, you can use the Mac installation program (in this case, the Traps Installer) to uninstall a program. After you uninstall the agent, the endpoint is no longer protected by your company's security policies and the license returns to the pool of available licenses.

**STEP 1 |** Run the Traps installer to uninstall the Traps agent.

**STEP 2 |** Click **OK** through any prompts.
### Troubleshooting Resources for the Traps Agent for Mac

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
</table>
| Traps Console log                 | Indicates information, warnings, and errors related to the Traps console. The Console log is located in the following folder on the endpoint:  
  - Mac OS X 10.10 and OSX 10.11—/var/log/traps/agent/  
  - macOS 10.12 and later releases—View logs from the Console application                                                                                                  |
| Traps Service log                 | Indicates information, warnings, and errors related to the Traps service. The Service log is located in the following folder on the endpoint:  
  - Mac OS X 10.10 and OSX 10.11—/var/log/traps/  
  - macOS 10.12 and later releases—View logs from the Console application                                                                                          |
| Supervisor Command Line Tool (Cytool) | Allows you to manage Traps features and perform advanced troubleshooting on the local endpoint from a command line interface. For more information, see [Cytool for Mac](#).      |

### Cytool for Mac

Cytool is a command-line interface that is integrated into Traps that enables you to query and manage both basic and advanced functions of Traps. Any changes that you make using Cytool are active until Traps receives the next heartbeat communication from the ESM Server.

On Mac endpoints, you can access Cytool as a super user using a terminal. Cytool is located in the `/Library/Application Support/PaloAltoNetworks/Traps/bin` directory on the endpoint.

The following table displays the Cytool options available on Mac endpoints.

<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| `-h --help`    | Traps-Mac:bin Traps$ sudo ./cytool  
Usage: cytool<options>  
cytool - Support tool  
Options:  
-h --help  
information.  
enum  
processes protected by Traps.  
esm <connect | disconnect> [address=hostname:port]  
startup query  
status for Traps agent and daemons.  
Connect/  
List startup status for Traps agent and daemons.  
Display help information.                                                                                           |
<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>startup &lt;enable</td>
<td>disable&gt; &lt;process_name</td>
</tr>
<tr>
<td>runtime query</td>
<td>List runtime status for agent, daemons, and kernel extensions.</td>
</tr>
<tr>
<td>runtime &lt;start</td>
<td>stop&gt; &lt;process_name</td>
</tr>
<tr>
<td>persist list</td>
<td>Display persistent databases.</td>
</tr>
<tr>
<td>persist export &lt;db_name</td>
<td>db_path&gt;</td>
</tr>
<tr>
<td>persist import &lt;db_name</td>
<td>db_path&gt; &lt;file_name&gt;</td>
</tr>
<tr>
<td>persist print &lt;db_name</td>
<td>db_path&gt; [csv]</td>
</tr>
<tr>
<td>log &lt;log_level&gt; &lt;process_name</td>
<td>all&gt;</td>
</tr>
<tr>
<td>log collect</td>
<td>Generate support file archive.</td>
</tr>
<tr>
<td>wakeup</td>
<td>Wake up from OS incompatibility state.</td>
</tr>
<tr>
<td>dump &lt;enable</td>
<td>disable</td>
</tr>
<tr>
<td>checkin</td>
<td>Update Traps from server.</td>
</tr>
<tr>
<td>opswat &lt;installed</td>
<td>running</td>
</tr>
</tbody>
</table>

**enum**

Enumerate protected processes.

Usage: `sudo ./cytool enum`

For example:

```
Traps-Mac:bin Traps$ sudo ./cytool enum
List of protected processes:
<table>
<thead>
<tr>
<th>Process name</th>
<th>Process ID</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photos</td>
<td>2047</td>
<td>Traps</td>
</tr>
<tr>
<td>Mail</td>
<td>2099</td>
<td>Traps</td>
</tr>
</tbody>
</table>
```

**esm**

Connect or disconnect from an ESM Server.

Usage: `sudo ./cytool connect http[s]://<hostname|IP address>:<port>`

Usage: `sudo ./cytool disconnect`

Use http or https depending on the communication settings of the ESM Server.

For example:

```
Traps-Mac:bin Traps$ sudo ./cytool disconnect
Traps-Mac:bin Traps$ sudo ./cytool connect http://203.0.113.35:2125
```
<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>startup</strong></td>
<td>Enable, disable, or query the startup state of Traps components.</td>
</tr>
<tr>
<td><strong>runtime</strong></td>
<td>Stop or start product components.</td>
</tr>
</tbody>
</table>

**startup**

Enable, disable, or query the startup state of Traps components.

Usage: `sudo ./cytool startup <action> <component>`

where:

- `<action>`—Change startup action for a Traps component. Options are: `enable`, `disable`, `query`. The query option displays the startup status for each component.
- `<component>`—Target component for which to set the startup action. To change the startup action for multiple components, list them with spaces separating each component. Options are: `traps_agent`, `trapsd`, `authorized`, `pmd`, `kproc-ctrl`

For example:

```
Traps-Mac:bin Traps$ sudo ./cytool startup disable traps_agent pmd
Process name                Startup status
traps_agent                      Disabled
trapsd                      Enabled
authorized                      Enabled
pmd                      Disabled
kproc-ctrl                      Loaded
Traps-Mac:bin Traps$ sudo ./cytool startup enable all
Process name                Startup status
traps_agent                      Enabled
trapsd                      Enabled
authorized                      Enabled
pmd                      Enabled
kproc-ctrl                      Loaded
```

**runtime**

Stop or start product components.

Usage: `sudo ./cytool runtime <action> <component>`

where:

- `<action>`—Change startup runtime action for a Traps component. Options are: `start`, `stop`, `query`. The query option displays the startup status for each component.
- `<component>`—Target component for which to set the runtime action, or all components if no components are specified. To change the runtime action for multiple components, list them with spaces separating each component. Options are: `traps_agent`, `trapsd`, `authorized`, `pmd`, `kproc-ctrl`

For example:

```
Traps-Mac:bin Traps$ sudo ./cytool runtime query
Name    PID         User              Status  Command  
traps_agent   1055        Traps             Running  /Library/ Application Support/PaloAltoNetworks/Traps/bin/traps_agent.app/ Contents/MacOS/traps_agent
trapsd    906         root             Running  /Library/ Application Support/PaloAltoNetworks/Traps/bin/trapsd
authorized    927  _traps_panw             Running  /Library/ Application Support/PaloAltoNetworks/Traps/bin/authorized
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pmd</td>
<td>909</td>
<td>root</td>
</tr>
<tr>
<td>kproc-ctrl</td>
<td>159</td>
<td>root</td>
</tr>
</tbody>
</table>

**Usage:**

```
Traps-Mac:bin Traps$ sudo ./cytool runtime stop all
```

```
Name    PID         User              Status  Command
authorized    N/A          N/A             STOPPED  N/A
pmd    N/A          N/A             STOPPED  N/A
traps_agent    N/A          N/A             STOPPED  N/A
trapsd   N/A          N/A             STOPPED  N/A
kproc-ctrl    N/A          N/A            Unloaded  N/A
```

```
Traps-Mac:bin Traps$ sudo ./cytool runtime start all
```

```
Name    PID         User              Status  Command
authorized   1883  _traps_panw             Running  /Library/
pmd   1889         root             Running  /Library/
traps_agent   1899        Traps           Running  /Library/
trapsd   1901         root             Running  /Library/
kproc-ctrl    160         root              Loaded  com.paloaltonetworks.driver.kproc-ctrl
```

**Persist**

Traps stores policy and security event information such as the list of trusted signers, local verdicts, and one-time actions in local databases on the endpoint. To troubleshoot policy issues and security events, you can use cytool persist operations to import, export, and view information stored in the local database.

**Usage:**

```
sudo ./cytool persist <action>
```

where `<action>`:

- **list**—List the local databases on the endpoint.
- **export** [`<database name>` | `<database path>`]—Export database table to a file in the `/Library/Application Support/PaloAltoNetworks/Traps/bin/` directory.
- **import** [`<database name>` | `<database path>`] `<file name>`—Add records in a JSON file to the database.
- **print** [`<database name>` | `<database path>`]—Print the database, in comma-separated values (CSV) format, to the command prompt.

To view a list of all local databases, use the `cytool persist list` command.

```
Traps-Mac:bin Traps$ sudo ./cytool persist list
```

**Persistent database list:**

- `fvhash.db` Database of blacklisted fvhashes
- `hash_override.db` Database of hashes override (Admin exceptions)
- `hashes.db` Database of the verdicts received from WildFire
- `trusted_signers.db` Database of trusted signers
- `post_detection.db` Database of post-detection candidates
<table>
<thead>
<tr>
<th>Command</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| logging | log | Set log level for the desired process. Usage: `sudo ./cytool log <log_level> <components>` where:  
  * `<log_level>` is an integer value corresponding to the log level:  
    * 0—Disable logging  
    * 1—Fatal  
    * 2—Critical  
    * 3—Error  
    * 4—Warning  
    * 5—Notice  
    * 6—Information  
    * 7—Debug  
    * 8—Trace  
  * `<components>` is all or one or more of the following Traps component: `trapsd`, `authorized`, `pmd`, `traps_agent`, `kproc-ctrl`. For example:  
    ```
    Traps-Mac:bin Traps$ sudo ./cytool log 2 all
    ```  
    Then use the `sudo ./cytool log collect` command to generate a support file archive of all logs in a TGZ file. On Mac endpoints running OS X 10.10 and OSX 10.11, Cytool outputs the logs to the `/var/log/traps` directory. On Mac endpoints running macOS 10.12, you can view logs from the Console application. |
| wake up | wakeup | Wake up the endpoint from an OS incompatibility state. |
| dumps | dump | Enable or disable dump generation or restore policy settings. |

```bash
Traps-Mac:bin Traps$ sudo ./cytool
SIGTERM caught
```
<table>
<thead>
<tr>
<th>Command Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| checkin        | Initiate check-in to the server.  
Usage: `sudo ./cytool checkin`  
To verify the checkin, view the check-in time on the Traps console. |
| opswat         | Check Traps Agent status and version.  
Usage: `sudo ./cytool opswat <parameter>`  
where `<parameter>` is:  
- `installed`—Display the Traps installation status (true if the `com.paloaltonetworks.pkg.traps` package is installed or false if the package is not installed). You must also supply the Traps supervisor password to view the status.  
- `running`—Display the running status of Traps daemons (true if running or false).  
- `protected`—Display the applied policy status (true if applied or false).  
- `version`—Display the version of Traps.  
- `last_update_time`—Display the date and time of the last successful check-in with the ESM Server. |

```
Traps-Mac:bin Traps$ sudo ./cytool opswat version
4.2.0.1042
Traps-Mac:bin Traps$ sudo ./cytool opswat installed
Password: true
Traps-Mac:bin Traps$ sudo ./cytool opswat running
true
Traps-Mac:bin Traps$ sudo ./cytool opswat protected
true
Traps-Mac:bin Traps$ sudo ./cytool last_update_time
Password: Fri Jun 22 09:24:20 2018 -0700 (%a %b %d %H:%M:%S %Y %z)
```
The Traps agent protects Linux servers by preventing attackers from leveraging software exploits or vulnerabilities to compromise an endpoint. The Traps agent enforces your organization’s security policy as defined in the Traps Endpoint Security Manager. When a security event occurs on an endpoint, Traps collects forensic information about that event which you can use to analyze the incident further.

The following topics describe how to install and use the Traps agent for Linux:

- Traps for Linux Requirements
- Install the Traps Agent for Linux
- Use the Traps Agent for Linux
- Upgrade Traps from the ESM Console (see the Traps Endpoint Security Manager Administrator’s Guide)
- Uninstall the Traps Agent for Linux
- Troubleshooting Resources for the Traps Agent for Linux
# Traps for Linux Requirements

The Traps agent for Linux has the following requirements:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Minimum Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version parity</td>
<td>The Traps agent version must not exceed the ESM Server and ESM Console version.</td>
</tr>
<tr>
<td>Processor</td>
<td>2.3 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>4GB; 8GB recommended</td>
</tr>
<tr>
<td>Hard disk space</td>
<td>10GB</td>
</tr>
<tr>
<td>Architecture</td>
<td>x86 64-bit</td>
</tr>
<tr>
<td>Operating system versions</td>
<td>See Where Can I Install the Traps Agent? in the Palo Alto Networks® Compatibility Matrix.</td>
</tr>
<tr>
<td>Kernel version</td>
<td>2.6.32</td>
</tr>
<tr>
<td>Software packages</td>
<td>• ca-certificates</td>
</tr>
<tr>
<td></td>
<td>• openssl 1.0.0 or a later release</td>
</tr>
<tr>
<td></td>
<td>• Distributions with SELinux in enforcing or permissive mode:</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 6, CentOS 6, and Oracle Linux 6—policycoreutils-python</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 7, CentOS 7, and Oracle Linux 7—policycoreutils-python and selinux-policy-devel</td>
</tr>
<tr>
<td></td>
<td>• SUSE—policycoreutils-python and selinux-policy-devel</td>
</tr>
<tr>
<td></td>
<td>• Debian and Ubuntu—policycoreutils and selinux-policy-dev</td>
</tr>
<tr>
<td>Networking</td>
<td>Allow communication on the TCP port from clients to server (the default is port 2125). Allow communication on TCP port 443 if you enable secure communication.</td>
</tr>
</tbody>
</table>
Install the Traps Agent for Linux

Traps for Linux is designed to protect Linux servers and operates transparently in the background as a system process. After you install Traps for Linux, it is typically not necessary to interact with the Traps agent; however, to perform common actions, such as initiating a manual check in with the Traps Endpoint Security Manager, you can use the command-line utility (also available for Mac and Windows) named Cytool. Cytool is available in the /opt/traps/bin/cytool directory and must be run as root or with root permissions.

Before installing Traps on a Linux server, verify that the system meets the requirements described in Traps for Linux Requirements.

If you intend to use SELinux, make sure to enable it before you proceed with the Traps installation. This ensures that Traps disables any injection-based modules which cause compatibility issues. If you later enable SELinux, you must reinstall Traps to avoid any compatibility issues.

You can then install Traps using software distribution tools that support Linux such as Satellite or Chef, or you can manually install Traps using the following workflow:

**STEP 1 |** Download the Traps installation script from the ESM Console.
For more information, see the Traps Endpoint Security Manager Administrator's Guide.

**STEP 2 |** Copy the installation package to the Linux server on which you want to install the Traps software.
For example, to copy the file securely from a local machine to the Linux server:

```
user@local ~
$ scp Traps_Linux_installer_4.2.0.660.tar.gz root@ubuntu.example.com:/tmp
Traps_Linux_installer_4.2.0.660.tar.gz                     100%  21MB
1.2MB/s   00:18
```

**STEP 3 |** Log on to the Linux server and unpack the Traps software.

```
user@local ~
$ ssh root@ubuntu.example.com
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-1041-aws x86_64)
* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
Get cloud support with Ubuntu Advantage Cloud Guest: http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

Last login: Tue Dec 26 22:14:15 2017 from 192.168.1.100
root@ubuntu:/$ cd /tmp
root@ubuntu:/tmp$ tar -xzf Traps_Linux_installer_4.2.0.660.tar.gz
root@ubuntu:/tmp$ ls
```

© 2018 Palo Alto Networks, Inc.
The software package contains several scripts that are needed for the installation. Use the `traps-installer.sh` script as described in the following step and ensure that you run the script from the same folder as the other files.

**STEP 4**

Run the install script (`traps-installer.sh`) as root or with root permissions.

For example:

```bash
root@ubuntu:/tmp$ ./traps-installer.sh
Starting Traps for Linux installer with the following params:
traps_version: 4.2.0.660
installer_path: /tmp/traps_linux-4.2.0.660.sh
servers_xml_path: /tmp/Servers.xml

Verifying archive integrity... 100%  All good.
Uncompressing Traps traps_installer installer  100%
[1] Checking prerequisites
  Verifying Debian (dpkg) packages:
    * openssl ... OK
    * ca-certificates ... OK
  Done
[2] Installing Traps at /opt/traps
  Done
[3] Creating logger directory
  Done
[4] Installing AppArmor policies
  Done
[5] Defining Traps local services (systemd)
  Created symlink from /etc/systemd/system/multi-user.target.wants/traps_trapsd.service to /etc/systemd/system/traps_trapsd.service.
  Created symlink from /etc/systemd/system/multi-user.target.wants/traps_pmd.service to /etc/systemd/system/traps_pmd.service.
  Created symlink from /etc/systemd/system/multi-user.target.wants/traps_authorized.service to /etc/systemd/system/traps_authorized.service.
  Done
[6] Starting Traps security services
  Done
```

The script installs the files for the Traps app for Linux in the `/opt/traps` folder with the Cytool utility available at `/opt/traps/bin/cytool`.

After the Traps agent successfully connects to the server for the first time and retrieves a valid license, the agent begins protecting the Linux server.
Use the Traps Agent for Linux

After you install Traps for Linux, Traps operates transparently in the background as a system process. Typically, it is not necessary to interact with the Traps agent; however, to perform common actions, such as initiating a manual check in with the ESM Server, you can use the command-line utility (also available for Mac and Windows) named Cytool. Cytool is available in the `/opt/traps/bin/cytool` directory and must be run as root or with root permissions.

To use the Traps agent for Linux:

- Display the Cytool help.
- List processes protected by Traps.
- Start or stop Traps daemons.
- View the Traps security policy.
- Collect logs.
- Manually initiate a check in with the server.
- View the version of Traps.
- Display the Cytool help.

From the Linux server, run the `cytool` command without any arguments or with `-h` or `--help` options.

```
root@ubuntu:~$ /opt/traps/bin/cytool
Usage: cytool<options>
    cytool - Support tool

Options:
    -h --help                                           Display help
    enum                                                List processes protected
    by Traps.
    startup query                                       List startup status for
    traps endpoint agent(s) and daemon(s).
    startup <enable | disable> <process_name | all>     Enable/Disable agent(s)
    and daemon(s) after reboot.
    runtime query                                       List runtime status for
    agent(s), daemon(s) and kernel extensions.
    runtime <start | stop> <process_name | all>         Start/Stop agent(s),
    daemon(s) and kernel extensions immediately.
    persist list                                        Display list of
    persistent databases.
    persist export <db_name | db_path>                 Export database(s) to
    the file(s) in JSON format.
    persist import <db_name | db_path> <file_name>     Import data into the
    database from the given JSON file.
    persist print <db_name | db_path> [csv]            Print database to the
    command prompt.
    log set-level <log_level> <process_name | all>     Set log level for the
desired process.
    log collect archive.                                Generate support file
    dump <enable | disable | restore>                   Enable/Disable dump
generation or restore policy settings.
    checkin                                            Initiate Check In Now
```

From the Linux server, run the `cytool` command without any arguments or with `-h` or `--help` options.
Follow the usage guidelines to run additional Cytool commands.

- List current running processes protected by Traps.
  Enter the `cytool enum` command.

```bash
root@ubuntu:~$ cytool enum
-----------------------------------
Traps list of protected processes:
-----------------------------------
  PID  CMD                           UID
 1098 /usr/sbin/cron -f               0
 1131 /usr/sbin/rsyslogd -n         104
```

To view processes for all users including those initiated by the operating system, specify the `/a` option.

- Start or stop Traps daemons.
  The Traps agent comprises the trapsd, authorized, and pmd daemons. To start or stop one or all daemons, enter either the `cytool runtime [start | stop] [<process_name> | all]` command or the `cytool startup [enable | disable] [<process_name> | all]` command. The behavior of both commands changes both the current running state and the startup registration status of the daemons when the server boots.

For example:

```bash
root@ubuntu:~$ /opt/traps/bin/cytool runtime stop trapsd
Name    PID       User       Status       Command
trapsd  N/A       N/A        STOPPED      N/A
authorized   2179       root       Running      /opt/traps/bin/authorized
pmd   2164       root       Running      /opt/traps/bin/pmd
root@ubuntu:~$ /opt/traps/bin/cytool runtime start all
Name    PID       User       Status       Command
trapsd  26427       root       Running      /opt/traps/bin/trapsd
authorized   2179       root       Running      /opt/traps/bin/authorized
pmd   2164       root       Running      /opt/traps/bin/pmd
```

- View the Traps security policy.
  Traps stores policy and security event information such as the list of trusted signers, local verdicts, and one-time actions in local databases in the `/opt/traps/persist/` directory. To troubleshoot policy issues and security events, you can use Cytool to import, export, and view information stored in the local database.

To view a list of all local databases, use the `cytool persist list` command.

```bash
root@ubuntu:~$ /opt/traps/bin/cytool persist list
Persistent database list:
  post_detection.db Database of post-detection candidates
  agent_actions.db Database of one time actions
  cloud_frontend.db Database of Cloud frontend settings
  hashes_lru.db Least recently used verdicts database
```
cloud_reports.db  Database of Cloud reports
hashes.db  Database of the verdicts received from WildFire
esm_frontend.db  Database of ESM frontend settings
policy.db  Policy database
fvhash.db  Database of blacklisted fvhashes
trusted_signers.db  Database of trusted signers
hash_paths.db  Database of file paths
hash_override.db  Database of hashes override (Admin exceptions)
esm_reports.db  Database of ESM reports
security_events.db  Database of security events (preventions)
file_upload.db  Database of files being uploaded to ESM
hashes_retransmit.db  Database of hashes to be retransmitted
agent_settings.db  Database of agent settings

To view the records of a database, use the `cytool persist print [<database_name> | <database_path>]` command where you specify either the name of database (see the `cytool persist list` command) or the path to the database. Or, to export the records of a database to a JSON file, use the `cytool persist export [<database_name> | <database_path>]` command. For example:

```
root@ubuntu:~$ /opt/traps/bin/cytool
persist print security_events.db
```

Database security_events:
persistence::DB: /opt/traps/persist/security_events.db: Open
persistence::DB: /opt/traps/persist/security_events.db: Open: IO error:
lock /opt/traps/persist/security_events.db/LOCK: Resource temporarily unavailable
3c34dcc1-bc37-ffef-ed55-f5512df05884,
Prevention ID: 3c34dcc1-bc37-ffef-ed55-f5512df05884
Timezone offset (min): 240
Module ID (CyveraComponent): 277
Module status (CyStatus): 0xC0400015
Blocked: false
Source process ID: 14818
Source process terminated: true
Source process command line: /root/Desktop/Linux_testers/ROP/lighttpd system 0
Source process file index: 0
Target process ID: 0
Target process terminated: false
Target process command line: 
Target process file index: 0
User ID: 0
User name: 
Traps version: 4.2.0.601
OS name: Linux
OS version: Red Hat Enterprise Linux Server release 6.9 (Santiago)
Machine name: ubuntu
Dump path: /opt/traps/forensics/3c34dcc1-bc37-ffef-ed55-f5512df05884/
Content version: 17-2805
IP Address: 10.200.0.55
Verdict (WildFire/Hash Control): 0
1 Files:
  Name: lighttpd
  Path: /root/Desktop/Linux_testers/ROP
  Size: 0
  Hash: 8630c9e57ca58fb7966c80525c36f572416e0a8db617b8a43c946d4fa966a71c
  Version: 

To add records to the database, use the `cytool persist import [<database_name> | <database_path>] <input_filename>` command where `<input_filename>` is a JSON file.

- **Collect logs.**
  
  Use the `cytool log set_level <log_level> [<process_name> | all]` command to change the log level of a Traps component where:
  
  - `<log_level>` is an integer value corresponding to the log level:
    
    - 1—Fatal
    - 2—Critical
    - 3—Error
    - 4—Warning
    - 5—Notice
    - 6—Information
    - 7—Debug
    - 8—Trace
  
  - `<process_name>` is the traps component: `trapsd`, `authorized`, or `pmd`.
  
  Then use the `cytool log collect` command to collect all logs in a TGZ file.

- **Manually initiate a check in with the server.**

  Use the `cytool checkin` command to initiate the manual check-in. To verify the status of the check-in on the ESM Console, view the LAST SEEN date from the additional details view of an endpoint on the Endpoints page.

- **Connect or disconnect from an ESM Server.**

  Use the `cytool disconnect` command to disconnect from an ESM Server or `cytool connect <hostname|IP address>:<port>` command to connect to a specific ESM Server and port. Use http or https depending on the communication settings of the ESM Server.

  For example:

  root@ubuntu:~$ /opt/traps/bin/cytool esm disconnect
• View the version of Traps.

To view the version of Traps on the Linux server, open or read the version.txt file in the /opt/traps/ directory. To read the version, you must run the command run as root or with root permissions.

For example:

```bash
root@ubuntu:~$ cat /opt/traps/version.txt
traps_linux-4.2.0.1040
ce1707dadb9b67effb7f08cedee60d9508377
```
Uninstall the Traps Agent for Linux

From the ESM Console you can uninstall the Traps agent on a Linux server (see Uninstall the Traps Agent in the Traps Endpoint Security Manager Administrator's Guide). You can also uninstall the agent directly on the server. Successfully uninstalling the Traps program effectively removes the Traps agent from the server. On Linux servers, you can use the uninstall.sh script found in the /opt/traps/scripts directory to uninstall Traps. After you uninstall the agent, your server will no longer be protected your company's security policies.

STEP 1 | On the Linux server, run the uninstall.sh script and confirm you want to uninstall the Traps.

By default, the script removes all logs, keys, and other files related to the Traps agent. If you want to preserve the logs, run the uninstall script in light mode using the -l option.

To use the uninstall script, you must run it from the default location in the scripts directory.

```
root@ubuntu:/opt/traps/scripts/uninstall.sh
This operation will uninstall Traps, are you sure? [y/N]: y
[1] Shutting down Traps services
  Done
[2] Waiting on active AppArmor policy updates
  Done
[3] Removing AppArmor policies
  * traps
  Done
[4] Stopping Traps security services (systemd)
  Removed symlink /etc/systemd/system/multi-user.target.wants/traps_trapsd.service.
  Removed symlink /etc/systemd/system/multi-user.target.wants/traps_pmd.service.
  Removed symlink /etc/systemd/system/multi-user.target.wants/traps_authorized.service.
  Done
[5] Removing Traps
  Done
```

STEP 2 | Confirm that the Traps agent is no longer installed.

From the Linux server you can verify the removal of the traps folder in /opt/. You can also verify that the server was removed from the Endpoints page in the ESM Console.
# Troubleshooting Resources for the Traps Agent for Linux

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traps logs</td>
<td>Indicates information, warnings, and errors related to the Traps service. Traps logs are located in the following directory on the endpoint: /var/log/traps/</td>
</tr>
</tbody>
</table>