# Troubleshooting

# Advanced Endpoint Protection Troubleshooting Resources

To troubleshoot the Advanced Endpoint Protection components including Traps and the Endpoint Security Manager, use the following resources:

| Resource | Description |
|---|---|
| Endpoint Security Manager | Web interface, which provides reports and logs. The information is useful for monitoring and filtering the logs to interpret unusual behavior on your network. After analyzing a security event, you can choose to create a custom rule for the endpoint or process. |
| DebugWeb log | Indicates information, warnings, and errors related to the Endpoint Security Manager. The DebugWeb log is located in the %ProgramData%\Cyvera\Logs folder of the ESM Server. |
| Server log | Indicates information, warnings, and errors related to the Endpoint Database and ESM Server. The Server log is located in the %ProgramData%\Cyvera\Logs folder of the ESM Server. |
| Service log | Indicates information, warnings, and errors related to the Traps service. The Service log is located in the following folder on the endpoint:<br>• Windows Vista and later: %ProgramData%\Cyvera\Logs<br>• Windows XP: C:\Document and Settings\All Users\Application Data\Cyvera\Logs |
| Console log | Indicates information, warnings, and errors related to the Traps console. The Console log is located in the following folder on the endpoint:<br>• Windows Vista and later: C:\Users\<username>\AppData\Roaming\Cyvera<br>• Windows XP: C:\Document and Settings\<username>\Application Data\Cyvera\Logs |
| Database (DB) Configuration Tool (dbconfig.exe) | Command-line interface that provides an alternative to managing basic server settings using the ESM Console. You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt run as an administrator. For more information, see Database Configuration Tool. |
| Supervisor Command Line Tool (cytool.exe) | Allows you to enumerate protected processes, enable or disable protection features, and enable or disable Traps management actions from a command line interface. For more information, see Cytool. |

# Database Configuration Tool

The DB Configuration Tool is a command-line interface that provides an alternative to managing basic server settings using the ESM Console. You can access the DB Configuration Tool using a Microsoft MS-DOS command prompt run as an administrator. The DB Configuration Tool is located in the Server folder of the Endpoint Security Manager (ESM) Server.

Use the DB Configuration Tool to perform the following functions:

▲ Access the Database Configuration Tool

▲ Manage Endpoint Security Manager Licenses Using the DB Configuration Tool

▲ Set Up Administrative Access to the Endpoint Security Manager Using the DB Configuration Tool

▲ Change the Ninja-Mode Password Using the DB Configuration Tool

▲ Define Communication Settings Using the DB Configuration Tool

▲ Enable External Reporting Using the DB Configuration Tool

## Access the Database Configuration Tool

Run the DB Configuration Tool from the Server folder on an ESM Server to view syntax and usage examples.

All commands run using the DB Configuration Tool are case sensitive.

**Access the Database Configuration Tool**

Step 1 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**, and then press **CTRL**+**SHIFT**+**ENTER**.

Step 2 Navigate to the folder that contains the DB Configuration Tool:

```
C:\Users\Administrator>cd C:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server
```

**Access the Database Configuration Tool**

Step 3 View usage and options for the DB Configuration Tool:

```
c:\Program Files\Palo Alto Networks\Endpoint Security Manager\Server>dbconfig

Usage:

   > DBConfig.exe importLicense [1]

       Add a new license to the database.

       1) CyveraLicense.xml full path

   > DBConfig.exe [1] [2] [3]

       Write a configuration to the database.

       1) Configuration Type (Server, Reflector, UserManagement, Reporting)

       2) Key Name

       3) Value

   > DBConfig.exe [1] show

       Show the values of a specific configuration.

       1) Configuration Type (Server, Reflector, UserManagement, Reporting)


 Examples:


> DBConfig.exe importLicense c:\Foldername\CyveraLicense.xml

> DBConfig.exe server inventoryinterval 200

> DBConfig.exe server show
```

# Cytool

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

You can access the Cytool using a Microsoft MS-DOS command prompt run as an administrator. Cytool is located in the Traps folder on the Endpoint.

Use Cytool to perform the following functions:

- Access Cytool
- View Processes Currently Protected by Traps
- Manage Protection Settings on the Endpoint
- Manage Traps Drivers and Services on the Endpoint
- View and Compare Security Policies on an Endpoint

## Access Cytool

To view syntax and usage examples for Cytool commands, use the /? option after any command.

| **Access Cytool** | |
|---|---|
| Step 1 | Open a command prompt as an administrator:<br>• Select **Start** > **All Programs** > **Accessories**. Right-click **Command prompt**, and then select **Run as administrator**.<br>• Select **Start**. In the **Start Search** box, type **cmd**, and then press **CTRL**+**SHIFT**+**ENTER**. |
| Step 2 | Navigate to the folder that contains Cytool:<br>`C:\Users\Administrator>`**`cd C:\Program Files\Palo Alto Networks\Traps`** |

**Access Cytool**

Step 3 View usage and options for the Cytool command:

```
c:\Program Files\Palo Alto Networks\Traps>cytool /?

Traps (R) supervisor tool 3.1

(c) Palo Alto Networks, Inc. All rights reserved


Usage: CYTOOL [/?] [/a] [command [options]]


Options:

    /?             Display this help message.

    /a             Authenticate as supervisor.

    command        enum | protect | startup | runtime | policy


For more information on a specific command run

    CYTOOL command /?
```

## View Processes Currently Protected by Traps

To view processes that are currently protected by Traps, use the `enum` command on Cytool or view the Protection tab on the Traps console (see View Processes Currently Protected by Traps). By default, both the Traps console and Cytool display only the protected processes initiated by the current user. To view protected processes initiated by all users, specify the `/a` option.

Viewing protected processes initiated by all users requires you to enter the supervisor (uninstall) password.

**View Processes Currently Protected by Traps**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 View protected processes initiated by the current user by entering the `cytool enum` command. To view protected processes for all users on the endpoint, specify the `/a` option, and enter the supervisor password when prompted.

```
c:\Program Files\Palo Alto Networks\Traps>cytool /a enum

Enter supervisor password:

Process ID      Agent Version
1000            3.1.1546
1468            3.1.1546
452             3.1.1546
[...]
```

# Manage Protection Settings on the Endpoint

By default, Traps applies protection to core processes, registry keys, Traps files, and Traps services according to the service protection rules defined in the security policy (for information about configuring service protection rules in the Endpoint Security Manager, see Manage Service Protection). You can use Cytool to override the security rules and manage the following layers of protection that Traps applies on the endpoint:

- Enable or Disable Core Process Protection on the Endpoint
- Enable or Disable Registry Protection Settings on the Endpoint
- Enable or Disable Traps File Protection Settings on the Endpoint
- Enable or Disable Service Protection Settings on the Endpoint
- Use the Security Policy to Manage Service Protection

## Enable or Disable Core Process Protection on the Endpoint

By default, Traps protects core processes including Cyserver.exe and CyveraService.exe based on the service protection rules defined in the local security policy. If required, you can override the behavior of core process protection using the `cytool protect [enable|disable] process` command.

Changing the protection settings requires you to enter the supervisor (uninstall password).

**Enable or Disable Core Process Protection Settings on the Endpoint**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To manage the protection settings of core processes on the endpoint, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect [enable|disable] process
```

The following example displays output for enabling protection of core processes. The `Mode` column displays the revised protection status, either `Enabled` or `Disabled`, or `Policy` when using the settings in the local security policy to protect core processes.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect enable process

Enter supervisor password:


Protection      Mode            State
Process         Enabled         Enabled

Registry        Policy          Disabled

File            Policy          Disabled

Service         Policy          Disabled
```

To use the default policy rule settings to protect core processes on the endpoint, see Use the Security Policy to Manage Service Protection.

## Enable or Disable Registry Protection Settings on the Endpoint

To prevent attackers from tampering with the Traps registry keys, use the `cytool protect enable registry` command to restrict access to the registry keys stored in HKLM\SYSTEM\Cyvera. To disable protection of the registry keys, use the `cytool protect disable registry` command.

Making changes to the registry protection settings requires you to enter the supervisor password when prompted.

**Enable or Disable Registry Protection Settings on the Endpoint**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To manage the protection settings of registry keys on the endpoint, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect [enable|disable] registry
```

The following example displays output for enabling protection of registry keys. The `Mode` column displays the revised protection status, either `Enabled` or `Disabled`, or `Policy` when using the settings in the local security policy to protect registry keys.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect enable registry

Enter supervisor password:


Protection      Mode            State

Process         Policy          Disabled
Registry        Enabled         Enabled

File            Policy          Disabled

Service         Policy          Disabled
```

To use the settings in the local security policy to protect registry keys on the endpoint, see Use the Security Policy to Manage Service Protection.

## Enable or Disable Traps File Protection Settings on the Endpoint

To prevent attackers from tampering with the Traps files, use the `cytool protect enable file` command to restrict access to the system files stored in %Program Files%\Palo Alto Networks\Traps and %ProgramData%\Cyvera. To disable protection of Traps files, use the `cytool protect disable file` command.

Making changes to the Traps file protection settings requires you to enter the supervisor password when prompted.

**Enable or Disable Traps File Protection Settings on the Endpoint**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

### Enable or Disable Traps File Protection Settings on the Endpoint (Continued)

Step 2 To manage the protection settings of Traps files on the endpoint, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect [enable|disable] file
```

The following example displays output for enabling protection of files. The `Mode` column displays the revised protection status, either `Enabled` or `Disabled`, or `Policy` when using the settings in the local security policy to protect Traps files.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect enable file

Enter supervisor password:


Protection      Mode            State

Process         Policy          Disabled

Registry        Policy          Disabled
File            Enabled         Enabled

Service         Policy          Disabled
```

To use the default policy rule settings to protect Traps files on the endpoint, see Use the Security Policy to Manage Service Protection.

## Enable or Disable Service Protection Settings on the Endpoint

To bypass the Traps security policy, attackers can attempt to disable or change the status of Traps services. Use the `cytool protect enable service` command to protect Traps services. To disable protection of Traps services, use the `cytool protect disable service` command.

Making changes to the service protection settings requires you to enter the supervisor password when prompted.

### Enable or Disable Service Protection Settings on the Endpoint

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

**Enable or Disable Service Protection Settings on the Endpoint (Continued)**

Step 2 To manage the protection settings of Traps services on the endpoint, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect [enable|disable] service
```

The following example displays output for enabling protection of services. The `Mode` column displays the revised protection status, either `Policy`, `Enabled`, or `Disabled`, or `Policy` when using the settings in the local security policy to protect Traps services.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect enable service

Enter supervisor password:


Protection     Mode           State

Process        Policy         Disabled

Registry       Policy         Disabled

File           Policy         Disabled

Service        Enabled        Enabled
```

To use the default policy rule settings to protect Traps services on the endpoint, see Use the Security Policy to Manage Service Protection.

## Use the Security Policy to Manage Service Protection

After changing protection settings using Cytool, you can restore the default security policy at any time using the `cytool protect policy <feature>` command.

**Use the Security Policy to Manage Service Protection**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To use the rules in the security policy to manage service protection, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect policy <feature>
```

where `<feature>` is either `process`, `registry`, `file`, or `service`.

The following example displays output for managing the protection on Traps files using the local security policy. The `Mode` column displays the revised protection status as `Policy`.

```
C:\Program Files\Palo Alto Networks\Traps>cytool protect policy file
Enter supervisor password:


Protection     Mode           State
Process        Enabled        Enabled
Registry       Enabled        Enabled
File           Policy         Disabled
Service        Enabled        Enabled
```

## Manage Traps Drivers and Services on the Endpoint

When an endpoint boots, Traps starts drivers (Cyverak, Cyvrmtgn, and Cyvrfsfd) and services (Cyvera and CyveraService) by default. You can use Cytool to override the default behavior and manage the startup or current status of drivers and services on a global or individual basis. Changes to the default startup behavior take effect when the endpoint restarts. Changes to the runtime behavior take immediate effect.

- View Traps Startup Components on the Endpoint
- Enable or Disable the Startup of Traps Components on the Endpoint
- View Traps Runtime Components on the Endpoint
- Start or Stop Traps Runtime Components on the Endpoint

### View Traps Startup Components on the Endpoint

Use the `cytool startup query` command to view the status of startup components on the endpoint. When a service or driver is disabled, Cytool displays the component as Disabled. When a driver is enabled, Cytool displays the component as `System`. When a service is enabled, Cytool displays the component `Startup` as `Automatic`.

**View Traps Startup Components on the Endpoint**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To view the current startup behavior of Traps drivers and services, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool startup query
Service          Startup
cyverak          System
cyvrmtgn         System
cyvrfsfd         System
cyserver         Automatic
CyveraService    Automatic
```

### Enable or Disable the Startup of Traps Components on the Endpoint

Use the `cytool startup [enable|disable]` command optionally followed by the component name to override the default behavior for starting Traps drivers and services on and endpoint.

Making changes to the startup behavior requires you to enter the supervisor password when prompted.

Changes to Traps drivers and services do not take effect until the system restarts. To make changes to Traps drivers and services that take effect immediately, see Start or Stop Traps Runtime Components on the Endpoint.

**Enable or Disable the Startup of Traps Components on the Endpoint**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To change the startup behavior for a specific driver or service, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool startup [enable|disable] <component>
```

where `<component>` is either a driver: `cyverak`, `cyvrmtgn`, `cyvrfsfd`; or a service: `cyserver`, `CyveraService`.

Alternatively, you can omit `<component>` from the command to change the startup behavior for all drivers and services.

The following example displays output for disabling the startup behavior of the cyvrmtgn driver. The **`Startup`** column displays the revised behavior as `Disabled`.

```
C:\Program Files\Palo Alto Networks\Traps>cytool startup disable cyvrmtgn
Enter supervisor password:

Service         Startup
cyverak         System
cyvrmtgn        Disabled
cyvrfsfd        System
cyserver        Automatic
CyveraService   Automatic
```

## View Traps Runtime Components on the Endpoint

Use the `cytool runtime query` command to view the status of Traps components on the endpoint. When a service or driver is active, Cytool displays the component as `Running`. When a service or driver is not running, Cytool displays the component as `Stopped`.

**View Traps Startup Components on the Endpoint**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To view the current runtime state of Traps drivers and services, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool runtime query
Service         State
cyverak         Running
cyvrmtgn        Running
cyvrfsfd        Running
cyserver        Running
CyveraService   Stopped
```

## Start or Stop Traps Runtime Components on the Endpoint

In situations where you do not have permission to change the behavior of Traps from the Endpoint Security Manager but must solve an urgent issue related to Traps drivers and services, you can use the `cytool startup [enable|disable]` command to override the default runtime behavior. The command is useful when you must take immediate action to start or stop all Traps components or start or stop a specific Traps driver or service.

> Changes to the runtime behavior of Traps drivers and services reset when the system restarts. To make changes to the startup behavior of Traps drivers and services, see Enable or Disable the Startup of Traps Components on the Endpoint.

Making changes to the runtime behavior requires you to enter the supervisor password when prompted.

**Start or Stop Traps Runtime Components on the Endpoint**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To start or stop a driver or service, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool runtime start <component>
```

where `<component>` is either a driver: `cyverak`, `cyvrmtgn`, `cyvrfsfd`; or a service: `cyserver`, `CyveraService`.

Alternatively, you can omit `<component>` from the command to change the runtime behavior for all drivers and services.

The following example displays output for stopping the `cyserver` service. The `Startup` column displays the revised component status, either `Running` or `Stopped`.

```
C:\Program Files\Palo Alto Networks\Traps>cytool runtime stop cyserver
Enter supervisor password:

Service         Startup
cyverak         Running
cyvrmtgn        Running
cyvrfsfd        Running
cyserver        Stopped
CyveraService   Running
```

## View and Compare Security Policies on an Endpoint

Using Cytool, you can display details about security policies on the endpoint.

▲ View Details About an Active Policy

▲ Compare Policies

## View Details About an Active Policy

Use the `cytool policy query <process>` command to view details about policies associated with a specific process. The output is helpful when you want to verify that a policy is implemented in the way you intended to configure it.

To view policy details, you must enter the supervisor password when prompted.

**View Details About an Active Policy**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

Step 2 To view the active policy for a process, use the following command:

```
C:\Program Files\Palo Alto Networks\Traps>cytool policy query <process>
```

where `<process>` is either the process name or process ID (PID). For example, to view details about a policy for notepad, enter `cytool policy query notepad`. The following example displays policy details for a process with PID 1234.

```
C:\Program Files\Palo Alto Networks\Traps>cytool policy query 1234
Enter supervisor password:

Generic
  Enable                        0x00000001
  SuspendOnce                   0x00000001
  AdvancedHooks                 0x00000001

[...]
```

## Compare Policies

At regular intervals, Traps requests an updated security policy from the Endpoint Security Manager and stores it in the system registry. When a user starts a process, Traps determines whether or not to protect the process based on the settings in the security policy.

In troubleshooting scenarios where Traps does not behave as expected, use the `cytool policy compare` command to view differences in policies that are applied to processes running on the endpoint. Using the command, you can compare a policy for a process to the default security policy or compare a policy for a process to a policy for another process. In both cases, you can specify either the name of the process or the process ID (PID). Specifying the process name simulates the application of the policy to the process. Specifying the PID queries the effective policy for the running process. Cytool displays the policy settings side-by-side and indicates any differences between policies in red.

To compare policies, you must enter the supervisor password when prompted.

**Compare Policies**

Step 1 Open a command prompt as an administrator and navigate to the Traps folder (see Access Cytool).

## Compare Policies

Step 2 Compare the details of two policies:

- To compare the policy to the default policy, use the following command:

  ```
  C:\Program Files\Palo Alto Networks\Traps>cytool policy compare <process> default
  ```

  where `<process>` is either the process name or process ID (PID).

  The following example displays output for comparing a policy that applies to notepad to the default policy. Differences between the two policies are shown in red.

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

  Generic
    Enable                        0x00000001                           0x00000001
    SuspendOnce                   0x00000001                           0x00000001
    AdvancedHooks                 0x00000001                           0x00000001

  [...]

  DllSec
    Enable                        0x00000001                           0x00000000
    Optimize                      0x00000001                           0x000000011

  [...]
  ```

- To compare the policies for two processes, use the following command:

  ```
  C:\Program Files\Palo Alto Networks\Traps>cytool policy compare <process1> <process2>
  ```

  where `<process1>` and `<process2>` are either the process name or process ID (PID). For example, to compare the policy applied to iexplorer to the policy applied to chrome, enter `cytool policy compare iexplorer chrome`. You can also compare the policies for two PIDs or compare the policy of a process to a policy of a PID.

  The following example displays output for comparing the policies applied to two PIDs, 1592 and 1000. Differences between the two policies are shown in red.

  ```
  C:\Program Files\Palo Alto Networks\Traps>cytool policy compare 1592 1000
  Enter supervisor password:

  Generic
    Enable                        0x00000001                           0x00000001
    SuspendOnce                   0x00000001                           0x00000001
    AdvancedHooks                 0x00000001                           0x00000001

  [...]

  DllSec
    Enable                        0x00000001                           0x00000000
    Optimize                      0x00000001                           0x000000011

  [...]
  ```

# Troubleshoot Traps Issues

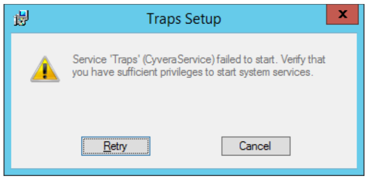
This topic addresses the following issues related to Traps:

- ▲ Why can't I install Traps?
- ▲ Why can't I upgrade or uninstall Traps?
- ▲ Why can't Traps connect to the ESM Server?
- ▲ How do I fix a Traps server certificate error?

## Why can't I install Traps?

### Symptom

Traps Setup reports the following error: Service "Traps" (CyveraService) failed to start. Verify that you have sufficient privileges.


Traps Setup

Service 'Traps' (CyveraService) failed to start. Verify that you have sufficient privileges to start system services.

### Possible Causes

- You do not have administrative privileges to start services on the endpoint.
- The Traps service cannot reach the ESM Server.
- The Traps service cannot retrieve a valid license key from the ESM Server.

### Solution

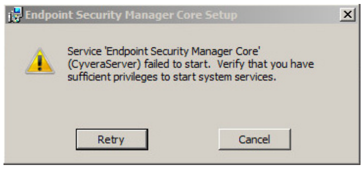
After each step in the following procedure, verify if you can install Traps. If Traps still reports an error, proceed to each subsequent step until the issue is resolved.

| Solution: Why can’t I install Traps? | |
|---|---|
| Step 1 | Verify that you have administrative rights on the endpoint:<br>• Windows 7: Click **Start** > **Control Panel** > **User Accounts** > **Manage User Accounts**. On the users tab, verify that your username is in the Administrators group.<br>• Windows 8: Click **Start** > **Control Panel** > **User Accounts** > **Change User Accounts**. Verify that your account appears as an Administrator.<br>Log in to the endpoint as a valid administrator. |
| Step 2 | Verify that the endpoint can reach the ESM Server by pinging the hostname or IP address of the server. If the server is not reachable:<br>• Verify that the IP address and hostname appear in the hosts file (C:\Windows\System32\drivers\etc) on the ESM Server.<br>• Verify the network and firewall settings on the ESM Server. |
| Step 3 | Verify that the license is valid and has not expired (see Manage Endpoint Security Manager Licenses). |
| Step 4 | The service log file contains information, warnings, and errors related to the Traps service. To further troubleshoot an issue related to the Traps service, open the C:\ProgramData\Cyvera\Logs\Service.log file in a text editor and review any errors in the log file that occurred at the time of the event.<br>By default, the ProgramData folder may be hidden. To view the folder in Windows Explorer, select **Organize** > **Folder and Search Options** > **View** > **Show hidden files and folders**. |
| Step 5 | If the problems persists, contact Palo Alto Networks support. |

## Why can’t I upgrade or uninstall Traps?

### Symptom

Traps Setup reports the following error: Service “Traps” (CyveraService) failed to start. Verify that you have sufficient privileges.



Endpoint Security Manager Core Setup

Service 'Endpoint Security Manager Core' (CyveraServer) failed to start. Verify that you have sufficient privileges to start system services.

### Possible Causes

In earlier versions of Traps, the service protection feature prevents you from modifying or tampering with Traps system files.

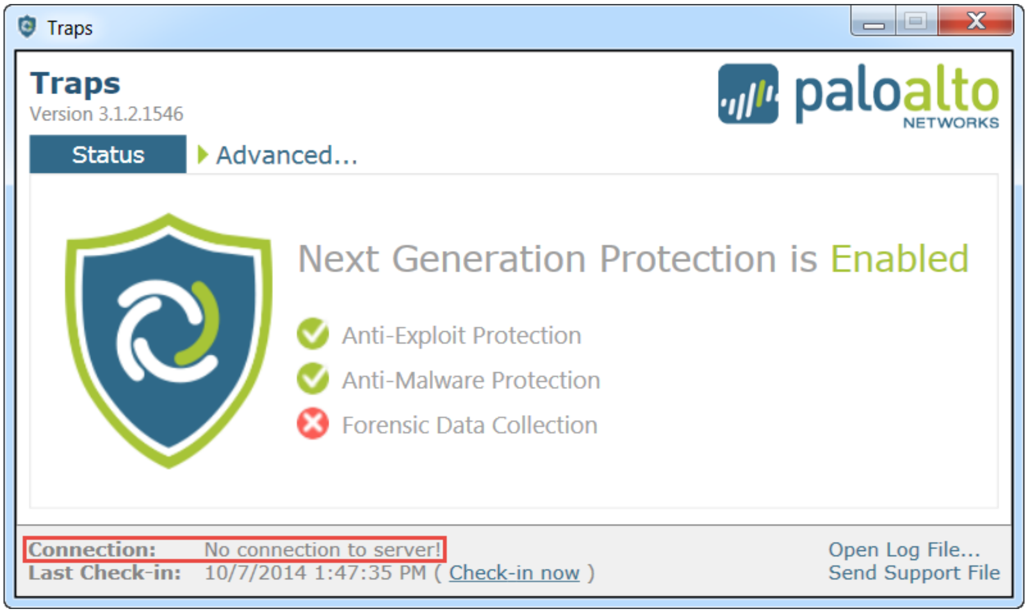
## Solution

| Solution: Why can't I upgrade Traps? | |
|---|---|
| Step 1 | Create an action rule to disable service protection (see Manage Service Protection). |
| Step 2 | Verify that you can install or uninstall Traps. |
| Step 3 | Delete the action rule (see Save and Manage Rules). |
| Step 4 | If the problems persists, contact Palo Alto Networks support. |

# Why can't Traps connect to the ESM Server?

## Symptom

Traps cannot communicate with the ESM Server to retrieve the latest security policy and reports a status of **No connection to server!**.



Connection: No connection to server!
Last Check-in: 10/7/2014 1:47:35 PM ( Check-in now )

## Possible Causes

- The server or endpoint specifications do not meet the installation and criteria prerequisites.
- The Traps service is down on the endpoint.
- The Endpoint Security Manager core service is down on the ESM Server.

- The endpoint is not connected to the network.
- Inbound traffic is not allowed on port 2125.
- The Windows Firewall is enabled on the ESM Server and prevents the server from communicating with the client.

## Solution

After each step in the following procedure, verify if Traps can connect to the ESM Server by selecting **Check-in now**. If Traps still can't connect to the server proceed to each subsequent step until the issue is resolved.

| Solution: Why can't Traps connect to the ESM Server? | | |
|---|---|---|
| Step 1 | Verify that the server and endpoint both meet the prerequisites. | See:<br>• Prerequisites to Install the ESM Server<br>• Prerequisites to Install Traps on an Endpoint |
| Step 2 | Verify that the Traps service is running on the endpoint. | 1. Open the Services Manager:<br>• Windows XP: From the Start Menu, select **Control Panel** > **Administrative Tools** > **Services**.<br>• Windows Vista and later: From the Start Menu, select **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.<br>2. Locate the Traps service (called CyveraService in older versions of Traps) and verify that the service status is **Started**.<br>3. If the service status is **Stopped**, double-click the service, then select **Start**. Click **Close**. |
| Step 3 | Verify that the Endpoint Security Manager core service is running on the ESM Server. | 1. Open the Services Manager:<br>• Windows Server 2008: From the Start Menu, select **Control Panel** > **Administrative Tools** > **Services**.<br>• Windows Server 2012: From the Start Menu, select **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.<br>2. Locate the Endpoint Security Manager core service (called CyveraServer in older versions of the Endpoint Security Manager) and verify that the service status is **Started** (Windows Server 2008) or **Running** (Windows Server 2012).<br>3. If the service status is **Stopped** or **Paused**, double-click the service, then select **Start**. Click **Close**. |
| Step 4 | Verify that you can reach the ESM Server from the endpoint. | From the endpoint, open a command prompt and ping the IP address or hostname of the ESM Server. If the ESM Server is unreachable, examine the network connectivity settings between the devices. |

| **Solution: Why can't Traps connect to the ESM Server? (Continued)** | | |
|---|---|---|
| Step 5 | Verify that you can reach the endpoint from the ESM Server. | From the ESM Server, open a command prompt and ping the IP address or hostname of the endpoint. If the endpoint is unreachable, examine the network connectivity settings between the devices. |
| Step 6 | Verify that port 2125 is open on the Windows Firewall. | 1. To check port access from the endpoint:<br>a. Open a command prompt as an administrator.<br>b. Enter the following command to telnet to port 2125 on the ESM Server:<br>`C:\>`**`telnet <esmservername> 2125`**<br>where `<esmservername>` is the hostname or IP address of the ESM Server.<br>2. If you are unable to telnet to port 2125, create an inbound rule to open that port:<br>a. Open the Windows Firewall advanced settings:<br>– Windows Server 2008: From the Start Menu, select **Control Panel** > **Windows Firewall** > **Advanced Settings**.<br>– Windows Server 2012: From the Start Menu, select **Control Panel** > **System and Security** > **Windows Firewall** > **Advanced Settings**.<br>b. Select **Inbound Rules**.<br>c. Create a new rule to allow Traps to communicate with the Endpoint Security Manager on port 2125 by selecting the New Rule wizard and following the guided instructions.<br>3. Verify that you can now telnet to port 2125 on the ESM Server from the endpoint. |
| Step 7 | Temporarily disable Windows Firewall. | 1. Open the Change Action Center settings:<br>• Windows Server 2008: From the Start Menu, select **Control Panel**. Double-click **Action Center** and select **Change Action Center settings**.<br>• Windows Server 2012: From the Start Menu, select **Control Panel** > **System and Security**. Double-click **Action Center** and select **Change Action Center settings**.<br>2. Deselect the **Network firewall** option.<br>3. Click **OK**. |
| Step 8 | Verify that connectivity is restored between Traps and the ESM Server. | From the Traps console, click **Check-in now**. If the connectivity is established, the connection status appears as **Successful**. If the problems persists, contact Palo Alto Networks support. |

# How do I fix a Traps server certificate error?

## Symptom

The following error appears in the services.log on the endpoint:

"An error occurred while making the HTTP request to https://<hostname>:2125/CyveraServer/. This could be due to the fact that the server certificate is not configured properly with HTTP.SYS in the HTTPS case. This could also be caused by a mismatch of the security binding between the client and the server."

## Possible Causes

When installing the ESM Server software, the following certificate configuration settings are available: No Certificate (no SSL) and External Certificate (SSL). To install Traps, you must select **SSL** if you selected External Certificate during the ESM Server software installation or **No SSL** if you selected No Certificate. The mismatch in settings causes the error reported to the service.log.

## Solution

| Solution: How do I fix a Traps server certificate error? | | |
|---|---|---|
| Step 1 | Reinstall the Traps software. | Verify the SSL settings for the ESM Server and then reinstall Traps on the endpoint, taking care to select the appropriate SSL setting during installation (see Install Traps on the Endpoint). |
| Step 2 | Verify that the error doesn't appear in the log. | Open the services.log on the endpoint and review any recent errors. If the server certificate error persists, contact Palo Alto Networks support. |

# Troubleshoot ESM Console Issues

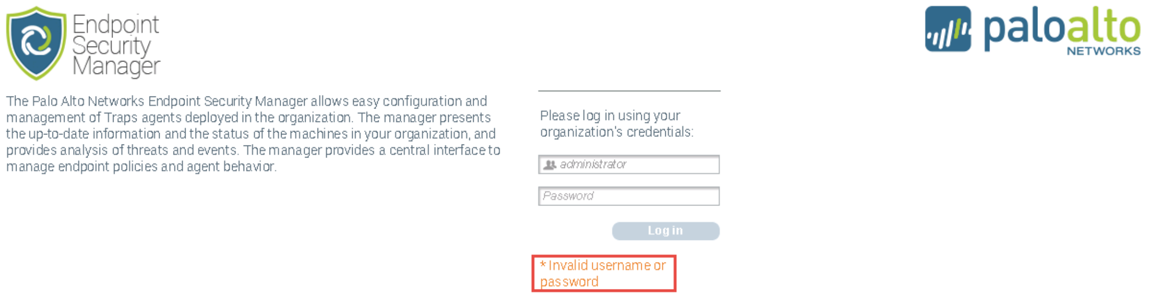
This topic addresses the following issues related to the Endpoint Security Manager (ESM) Console:

- ▲ Why can't I log in to the ESM Console?
- ▲ Why do I get a server error when launching the ESM Console?
- ▲ Why do all endpoints appear as disconnected in the ESM Console?

## Why can't I log in to the ESM Console?

### Symptom

The Endpoint Security Manager (ESM) Console displays an error message that the username or password is invalid.



The Palo Alto Networks Endpoint Security Manager allows easy configuration and management of Traps agents deployed in the organization. The manager presents the up-to-date information and the status of the machines in your organization, and provides analysis of threats and events. The manager provides a central interface to manage endpoint policies and agent behavior.

Please log in using your organization's credentials:

administrator

Password

* Invalid username or password

### Possible Causes

- The username or password was not entered correctly.
- The user specified during the initial installation does not have DB Owner privileges.
- The user was not added as an administrator.
- The user who installed the server was not a local administrator on the server.

### Solution

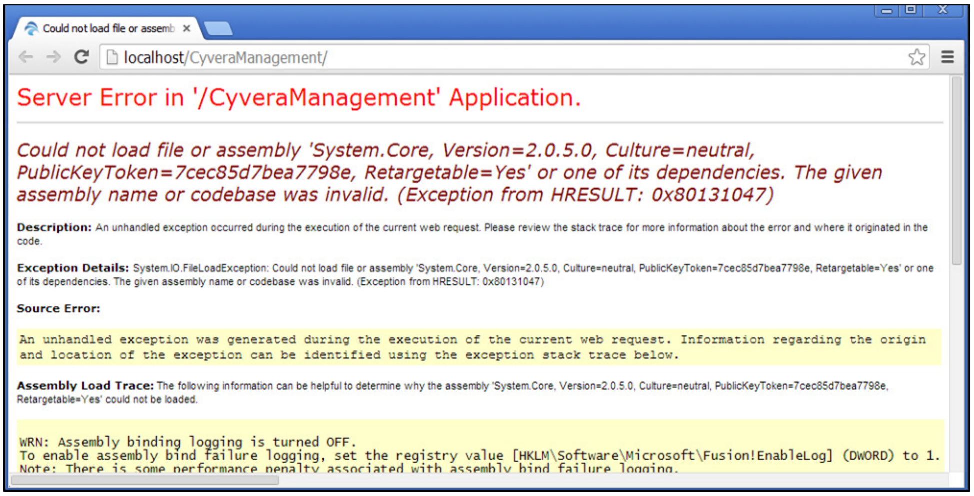
| **Solution: Why can't I log in to the ESM Console?** | |
|---|---|
| Step 1 | Verify that you entered the correct username and password. |
| Step 2 | Verify that the user has DB Owner privileges (see Configure the MS-SQL Server Database). |

| **Solution: Why can’t I log in to the ESM Console?** | |
|---|---|
| Step 3 | Log in as an administrator and verify that the authentication mode is correct and that the user account appears on the User Management page. To add an administrative user, see Set Up Administrative Access to the Endpoint Security Manager Using the ESM Console. Alternatively, you can add the administrator using the Database Configuration Tool (see Set Up Administrative Access to the Endpoint Security Manager Using the DB Configuration Tool). |
| Step 4 | If you cannot log in as an administrator, reinstall the Endpoint Security Manager as a local administrator. |
| Step 5 | Restart IIS: Click **Start** > **Run**, type **IISReset**, and then click **OK**. |
| Step 6 | Verify that you can log in to the Endpoint Security Manager console using the account. If the problems persists, contact Palo Alto Networks support. |

# Why do I get a server error when launching the ESM Console?

## Symptom

When opening the Endpoint Security Manager (ESM) Console, you receive an error in the browser indicating a Server Error in the ‘/CyveraManagement’ or ‘/EndpointSecurityManager’ Application.



Server Error in '/CyveraManagement' Application.

*Could not load file or assembly 'System.Core, Version=2.0.5.0, Culture=neutral, PublicKeyToken=7cec85d7bea7798e, Retargetable=Yes' or one of its dependencies. The given assembly name or codebase was invalid. (Exception from HRESULT: 0x80131047)*

**Description:** An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

**Exception Details:** System.IO.FileLoadException: Could not load file or assembly 'System.Core, Version=2.0.5.0, Culture=neutral, PublicKeyToken=7cec85d7bea7798e, Retargetable=Yes' or one of its dependencies. The given assembly name or codebase was invalid. (Exception from HRESULT: 0x80131047)

**Source Error:**

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin
and location of the exception can be identified using the exception stack trace below.
```

**Assembly Load Trace:** The following information can be helpful to determine why the assembly 'System.Core, Version=2.0.5.0, Culture=neutral, PublicKeyToken=7cec85d7bea7798e, Retargetable=Yes' could not be loaded.

```
WRN: Assembly binding logging is turned OFF.
To enable assembly bind failure logging, set the registry value [HKLM\Software\Microsoft\Fusion!EnableLog] (DWORD) to 1.
Note: There is some performance penalty associated with assembly bind failure logging.
```

## Possible Causes

The server does not meet the prerequisite for .NET Framework 4.0 patched with the KB2468871 update.

## Solution

Install .NET Framework 4.0 and the KB2468871 patch.

## Why do all endpoints appear as disconnected in the ESM Console?

### Symptom

The Health page of the Endpoint Security Manager (ESM) Console reports that all endpoints are disconnected even when the endpoint can reach the ESM Server.

### Possible Causes

- The ESM Server does not meet the prerequisites.
- The Endpoint Security Manager Core service stops and must be restarted. This occurs if you wait more than five minutes to install the license key after initially installing the ESM Console software.
- Inbound traffic is not allowed on port 2125.

### Solution

After each step in the following procedure, verify if Traps can connect to the ESM Server by selecting **Check-in now**. If Traps still can't connect to the server proceed to each subsequent step until the issue is resolved.

| Solution: Why do all endpoints appear as disconnected in the ESM Console? | |
|---|---|
| Step 1 Verify that the server meets the prerequisites. | See Prerequisites to Install the ESM Server. |
| Step 2 Verify that the Traps service is running on the endpoint. | 1. Open the Services Manager:<br>• Windows XP: From the Start Menu, select **Control Panel** > **Administrative Tools** > **Services**.<br>• Windows Vista and later: From the Start Menu, select **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.<br>2. Locate the Traps service (called CyveraService in older versions of Traps) and verify that the service status is **Started**.<br>3. If the service status is **Stopped**, double-click the service, then select **Start**. Click **Close**. |

| Solution: Why do all endpoints appear as disconnected in the ESM Console? (Continued) | | |
|---|---|---|
| Step 3 | Verify that the Endpoint Security Manager core service is running on the ESM Server. | 1. Open the Services Manager:<br>• Windows Server 2008: From the Start Menu, select **Control Panel** > **Administrative Tools** > **Services**.<br>• Windows Server 2012: From the Start Menu, select **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.<br>2. Locate the Endpoint Security Manager core service (called CyveraServer in older versions of the Endpoint Security Manager) and verify that the service status is **Started** (Windows Server 2008) or **Running** (Windows Server 2012).<br>3. If the service status is **Stopped** or **Paused**, double-click the service, then select **Start**. Click **Close**. |
| Step 4 | Verify that port 2125 is open on the Windows Firewall. | 1. To check port access from the endpoint:<br>a. Open a command prompt as an administrator.<br>b. Enter the following command to telnet to port 2125 on the ESM Server:<br>`C:\>telnet <esmservername> 2125`<br>where `<esmservername>` is the hostname or IP address of the ESM Server.<br>2. If you are unable to telnet to port 2125, create an inbound rule to open that port:<br>a. Open the Windows Firewall advanced settings:<br>– Windows Server 2008: From the Start Menu, select **Control Panel** > **Windows Firewall** > **Advanced Settings**.<br>– Windows Server 2012: From the Start Menu, select **Control Panel** > **System and Security** > **Windows Firewall** > **Advanced Settings**.<br>b. Select **Inbound Rules**.<br>c. Create a new rule to allow Traps to communicate with the Endpoint Security Manager on port 2125 by selecting the New Rule wizard and following the guided instructions.<br>3. Verify that you can now telnet to port 2125 on the ESM Server from the endpoint. |
| Step 5 | Temporarily disable Windows Firewall. | 1. Open the Change Action Center settings:<br>• Windows Server 2008: From the Start Menu, select **Control Panel**. Double-click **Action Center** and select **Change Action Center settings**.<br>• Windows Server 2012: From the Start Menu, select **Control Panel** > **System and Security**. Double-click **Action Center** and select **Change Action Center settings**.<br>2. Deselect the **Network firewall** option.<br>3. Click **OK**. |

| Solution: Why do all endpoints appear as disconnected in the ESM Console? (Continued) | | |
|---|---|---|
| Step 6 | Verify that connectivity is restored between Traps and the ESM Server. | From the Traps console, click **Check-in now**. If the connectivity is established, the connection status appears as **Successful**. If the problems persists, contact Palo Alto Networks support. |