Contents

Topic 1  Introduction to Forcepoint Endpoint Solutions. .................................. .3

Topic 2  TRITON AP-ENDPOINT Web. ......................................................... .5
    How to check the status of TRITON AP-ENDPOINT Web ...................... .6
    How to use the TRITON AP-ENDPOINT Web diagnostics tool .............. .7
    Fallback mode ................................................................................. .8
    How to view logs ........................................................................... .9
    How to disable TRITON AP-ENDPOINT Web protection .................... 10

Topic 3  TRITON AP-ENDPOINT DLP. ..................................................... 11
    How to check the status of TRITON AP-ENDPOINT DLP .................. 11
    How to set encryption passwords .................................................. 13
        Decrypting files on a removable media device .............................. 13
        Decrypting files on Windows .................................................... 14
        Decrypting files on Mac ........................................................... 14
    How to view contained files and save them to an authorized location . . 16
    How to view logs ........................................................................... 17
    How to update TRITON AP-ENDPOINT DLP .................................... 18
    How to disable TRITON AP-ENDPOINT DLP ................................... 18
Your organization uses Forcepoint endpoint solutions to protect you and other users against advanced web-based threats and data theft while on and off the corporate network. Endpoint solutions include server software installed on corporate servers and client software installed on your computer.

Forcepoint offers 2 endpoint solutions:

- TRITON AP-ENDPOINT Web defends your computer against web threats.
- TRITON AP-ENDPOINT DLP protects your organization from the unintended loss of data and data theft.

If you see this icon in your task bar, TRITON AP-ENDPOINT Web protection is available and enabled.

This icon means TRITON AP-ENDPOINT DLP (Data Loss Prevention) is protecting you and your organization.

This guide covers the following:

**TRITON AP-ENDPOINT Web**

- How to check the status of TRITON AP-ENDPOINT Web, page 6
- How to use the TRITON AP-ENDPOINT Web diagnostics tool, page 7
- Fallback mode, page 8
- How to view logs, page 9
- How to disable TRITON AP-ENDPOINT Web protection, page 10*

**TRITON AP-ENDPOINT DLP**

- How to check the status of TRITON AP-ENDPOINT DLP, page 11
- How to view logs, page 17
- How to set encryption passwords, page 13
- How to view contained files and save them to an authorized location, page 16
- How to update TRITON AP-ENDPOINT DLP, page 18
• How to disable TRITON AP-ENDPOINT DLP, page 18*

*Note that disabling the endpoint introduces possible vulnerabilities, because you are no longer receiving the protection provided by TRITON AP-ENDPOINT Web or TRITON AP-ENDPOINT DLP or both if both are installed and disabled.
TRITON AP-ENDPOINT Web

TRITON AP-ENDPOINT Web is a software application that runs on your laptop or other endpoint machine, protecting you from malware and enforcing your organization’s acceptable user policy.
How to check the status of TRITON AP-ENDPOINT Web

This applies to Windows operating system users. To view the status of TRITON AP-ENDPOINT Web, hover over the Forcepoint icon in your task bar. Icons serve as a status indicator and an access point to additional diagnostic information:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Enabled Icon]</td>
<td>Enabled</td>
<td>TRITON AP-ENDPOINT Web software is successfully configured and activated.</td>
</tr>
<tr>
<td>![Disabled Icon]</td>
<td>Disabled</td>
<td>You have manually disabled the endpoint software on your computer. It is no longer being protected against web threats. You can re-enable the software manually or it will be enabled when your computer is restarted. The ability to enable/disable endpoint software is allocated by your system administrator. See <em>How to disable TRITON AP-ENDPOINT Web protection</em>.</td>
</tr>
<tr>
<td>![Fallback Icon]</td>
<td>Fallback</td>
<td>Network events prevented your endpoint software from connecting with cloud services. You are no longer being protected against web threats.</td>
</tr>
<tr>
<td>![Fallback Icon]</td>
<td>Fallback</td>
<td>Network events prevented your endpoint software from connecting with cloud services. The system applies filters cached during the last connection to the Internet. Your computer is partially protected against web threats.</td>
</tr>
</tbody>
</table>

Related topics:
- *Fallback mode*, page 8
- *How to disable TRITON AP-ENDPOINT Web protection*, page 10
- *How to use the TRITON AP-ENDPOINT Web diagnostics tool*, page 7
- *How to view logs*, page 9
Important

If you manually disable TRITON AP-ENDPOINT Web, a reboot will always re-enable it.

Note that if your organization is using both TRITON AP-ENDPOINT Web and TRITON AP-ENDPOINT DLP, a TRITON AP-ENDPOINT DLP icon displays on your task bar as well. For more information about TRITON AP-ENDPOINT DLP, see TRITON AP-ENDPOINT DLP, page 11.

How to use the TRITON AP-ENDPOINT Web diagnostics tool

This applies to Windows operating system users. TRITON AP-ENDPOINT Web offers a diagnostics tool that you can access by double-clicking any of the three possible endpoint status icons that display in the task bar. The tool displays information that you can provide to your system administrator to assist with troubleshooting if TRITON AP-ENDPOINT Web is not behaving as expected.

When the tool is launched, each of the diagnostic tests is executed in sequence. If one of the tests results in a failure, the subsequent tests are not automatically run.

Three diagnostic tests are accessed from this tool:

1. System Information - collects basic information related to the specific system on which the TRITON AP-ENDPOINT Web software is installed.
2. Network Diagnostics - collects information related to basic network connectivity.
3. PAC File Status - For endpoints that go through a proxy before connecting to the Internet. Collects information to determine if the PAC file is accessible.

Related topics:

- How to check the status of TRITON AP-ENDPOINT Web, page 6
- Fallback mode, page 8
- How to disable TRITON AP-ENDPOINT Web protection, page 10
- How to view logs, page 9
4. **Cloud Services** - For endpoints that connect directly to the Internet. Collects information to determine if the endpoint can contact the cloud service for disposition information (i.e. whether to block or allow the request).

**Note**

Corresponding log files generated from these new diagnostics can easily be collected with the existing CLIENTINFO.EXE tool. Your Help Desk may ask you to run this tool to collect these files. To run it, click the Collect Endpoint Info... button on the diagnostics screen, as shown below.

The resulting file is placed onto the desktop. Attach the file to an email to your HelpDesk or system administrator.

**Fallback mode**

End User’s Guide | TRITON AP-ENDPOINT Web | Cloud and On-Premises v8.2.x

- How to check the status of TRITON AP-ENDPOINT Web, page 6
- How to disable TRITON AP-ENDPOINT Web protection, page 10
- How to use the TRITON AP-ENDPOINT Web diagnostics tool, page 7
- How to view logs, page 9

TRITON AP-ENDPOINT Web provides a Fallback mode if your network connection to the cloud service is interrupted. Events that may trigger Fallback mode include:

- Changing from Wi-Fi to an Ethernet network connection or vice-versa
- Connecting to a virtual private network (VPN)
- Assigning a new IP address to your laptop
- Disconnecting from the Internet

While in Fallback mode, the Forcepoint icon displayed in your task bar changes to reflect your level of protection.

If you see this icon in your task bar, your system is in Fallback mode and is **not** protected against web threats. When network events prevent endpoints from connecting with cloud services, TRITON AP-ENDPOINT Web is automatically and temporarily bypassed. If this happens, you can continue to access the Internet (provided Internet access is available), but endpoint protection is not provided during this time.
If you see this icon in your task bar, your system is in Fallback mode and is partially protected. When network events prevent endpoints from connecting with cloud services, TRITON AP-ENDPOINT Web applies filters cached from the last connection to the Internet. For example, if the user normally sees a block page when visiting Facebook, then the user would also see a block page when visiting Facebook while in Fallback mode. This block page would indicate that it was a result of cached results.

Once the network issue is resolved, TRITON AP-ENDPOINT Web is automatically re-enabled.

How to view logs

You can see logs about system events related to TRITON AP-ENDPOINT Web. To view the logs, go to the Application section of the Windows system event log. Examples of log notifications you might see are these:

- EventID 258: “User disabled Forcepoint SaaS Service.”
- Event ID 257: “Forcepoint SaaS Service has entered cloud enforce mode.”

These logs may be helpful to share with your system administrator. All logs are in English.
How to disable TRITON AP-ENDPOINT Web protection

Disabling the TRITON AP-ENDPOINT Web endpoint software removes the protection provided by the endpoint service, and stops it from intercepting traffic and securing your workstation from web threats. Sometimes, it may be useful to manually disable the endpoint software to troubleshoot issues with the assistance of your system administrator.

If your organization allows you to disable TRITON AP-ENDPOINT Web, when you right click the endpoint icon, you'll see the option to **Disable** it. Select **Disable** to disable the endpoint at any time.

If you see an authentication page asking for your username and logon credentials, you need to change your proxy auto-config (PAC) file settings in Internet Explorer. Contact your system administrator for assistance with changing your PAC file settings.

To re-enable TRITON AP-ENDPOINT Web, click **Enable**.

**Important**

If you manually disable TRITON AP-ENDPOINT Web, a reboot will always re-enable it.
TRITON AP-ENDPOINT DLP

End User's Guide | TRITON AP-ENDPOINT DLP | Version 8.2.x

TRITON AP-ENDPOINT DLP (Data Loss Prevention) expands protection to sensitive information stored on your computer. Depending on your corporate policy, data could be quarantined or encrypted when you try to email it, print it, or copy it to removable media such as thumb drives, CD/DVD burners, and Android devices. (CD/DVD and Android support depends on your operating system.)

How to check the status of TRITON AP-ENDPOINT DLP

End User's Guide | TRITON AP-ENDPOINT DLP | Version 8.2.x

Related topics:
- How to disable TRITON AP-ENDPOINT DLP, page 18
- How to view contained files and save them to an authorized location, page 16
- How to view logs, page 17
- How to update TRITON AP-ENDPOINT DLP, page 18

To view status information for TRITON AP-ENDPOINT DLP, click the TRITON AP-ENDPOINT DLP icon on your task bar.
On the TRITON AP-ENDPOINT DLP screen, you can:

- See whether your machine is connected to a TRITON AP-DATA server
- Check the IP address of the TRITON AP-DATA server hosting the endpoint server software
- View your endpoint profile name, and when it was last updated
- Determine if TRITON AP-ENDPOINT DLP protection is enabled or bypassed
- View discovery status and details of the last and next discovery scans
Note that if your organization is using both TRITON AP-ENDPOINT Web and TRITON AP-ENDPOINT DLP, a TRITON AP-ENDPOINT Web icon displays on your task bar as well. For more information about TRITON AP-ENDPOINT Web, see TRITON AP-ENDPOINT Web, page 5.

How to set encryption passwords

Some corporate policies dictate that sensitive data be encrypted before being copied to a removable media device such as a USB drive. If this is the case for your organization, you cannot copy files to such media until you set the password to use to decrypt them.

Set the password one time, then any time you copy sensitive data to removable media, it is encrypted and copied along with a Forcepoint Decryption Utility to the device.

You, or any other user accessing the files on endpoints where the TRITON AP-ENDPOINT DLP is not installed, or where the password configured for encryption is different than yours, must enter this password.

Decrypting files on a removable media device

To decrypt the content on your removable media device, you must run a Forcepoint Decryption Utility. Content that was encrypted on Windows can be encrypted on any Windows or Mac machine. (Content cannot be encrypted on Mac, however.)
The Forcepoint Decryption Utility is copied to your removable media device along with the encrypted files.

- Decrypting files on Windows
- Decrypting files on Mac

Decrypted files on Windows

1. Insert the removable device into a Windows laptop or desktop.
2. Unzip either `wsdecrypt_win64.zip` or `wsdecrypt_win32.zip` depending on your environment.
3. Double-click `wsdecrypt.exe`.
4. Enter the encryption password when prompted. A dialog appears and displays lists of subdirectories and files on your system.
5. Navigate to the folder containing the encrypted files. By default, the files are on your removable media device.
6. Select the folders and files to decrypt, right-click, and select Save As.
7. Select the folder in which to save the decrypted files.

Decrypted files on Mac

1. Insert the removable device into a Mac laptop or desktop.
2. Double-click `Forcepoint Decryption Utility.dmg` and mount it as a disk volume.
3. Launch the application `Forcepoint Decryption Utility` in the disk volume.
4. Drag and drop the encrypted files from the removable media device into the application's list window.

5. Select the file to decrypt, and select "Decrypt File As...". If the file selected is not encrypted by the Forcepoint endpoint, the operation is disabled.

6. Enter the encryption password when prompted. A file save dialog appears if the correct password is entered.

7. Enter the file name that you want to save the decrypted file as.

8. If necessary, select the next file to decrypt. No prompt appears as long as it is encrypted by the same password.
The Forcepoint Decryption Utility decrypts the files using the password you provided and places them in this path.

Files that were encrypted with a different password are not decrypted.

How to view contained files and save them to an authorized location

Contained files are those that are held in temporary storage on an endpoint machine.

Files are contained if your organization chose to prevent sensitive information from being written from an endpoint machine to a removable device—such as a USB flash drive, CD/DVD, or external hard disk—and you try to copy a file to a forbidden device. If the file has been modified, the contained file will include these modifications, while removing the modified file from the forbidden device.

You can view the contents of contained files from the endpoint machine, and choose to save them to an authorized location instead.

1. On the TRITON AP-ENDPOINT DLP screen, click **Contained Files**.

2. To see the contents of a file, select the file and click **Open**.

3. To save a file to an authorized location, select the file and click **Save As**, then browse to the new location.

4. Click **Close** when done.
How to view logs

There are two logs available in TRITON AP-ENDPOINT DLP:

- The system log contains information about changes on your machine, for example:
  - Changes of connection status, such as your computer moving from an office to a remote location
  - When TRITON AP-ENDPOINT DLP is enabled or disabled
  - When TRITON AP-ENDPOINT DLP profiles are applied and updated
  - When the client is connected to or disconnected from the TRITON AP-ENDPOINT DLP server
- The content log contains details of file operations that have been picked up by the endpoint policy, and any actions taken by TRITON AP-ENDPOINT DLP as a result.

To see the log details, on the TRITON AP-ENDPOINT DLP screen, click View logs.

To see the latest log information, click Refresh.
How to update TRITON AP-ENDPOINT DLP

Periodically, your corporate policies and TRITON AP-ENDPOINT DLP profile are pushed to your machine to keep them up to date. To update them manually, click Update on the TRITON AP-ENDPOINT DLP screen.

How to disable TRITON AP-ENDPOINT DLP

1. On the TRITON AP-ENDPOINT DLP screen, click Disable.

2. Report the bypass ID to your TRITON AP-DATA administrator.
3. Enter the bypass code supplied by the administrator.
4. Click Enter.

The endpoint client is disabled for the length of time specified when the bypass code was created. The Disable button on the task bar updates to the Default button.

Related topics:
- How to disable TRITON AP-ENDPOINT DLP, page 18
- How to view contained files and save them to an authorized location, page 16
- How to view logs, page 17
- How to update TRITON AP-ENDPOINT DLP, page 18