TrendAI™

TippingPoint™

TPS Web Management Console Guide

TrendAI™ Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the TrendAI™ website at:

https://docs.trendmicro.com/en-us/tippingpoint/threat-protection-system.aspx

TrendAI™, the Trend Micro t-ball logo, TippingPoint, and Digital Vaccine are trademarks or registered trademarks of TrendAI™ Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2026. TrendAI™ Incorporated. All rights reserved.

Release Date: August 2026

Protected by U.S. Patent No.: Pending

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the TrendAI™ Online Help Center and/or the TrendAI™ Knowledge Base.

Privacy and Personal Data Collection Disclosure

Certain features available in TrendAI™ products collect and send feedback regarding product usage and detection information to TrendAI™. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want TrendAI™ to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that TippingPoint Threat Protection System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by TrendAI™ is subject to the conditions stated in the TrendAI™ Privacy Notice:

https://www.trendmicro.com/privacy

Table of Contents

Chapter 1: TPS Web Management Console

Manually verify the WMC certificate 1-4

Chapter 2: Home

Chapter 3: Upload and install a software package

Chapter 4: Create and export a Tech Support Report

Chapter 5: Download device logs

Index

Index IN-1

Chapter 1

TPS Web Management Console

The TPS Web Management Console (WMC) is a browser-based interface, served directly from the TPS device, for a small set of day-to-day tasks: checking device identity and status, installing software packages, generating a tech support report, and downloading device logs.

Access the WMC

Open a browser and go to the device's management IP address or hostname, for example:

```
https://<device-hostname>
```

Note

If the LSM is enabled on the device, the WMC login page shows a **Legacy LSM** link that opens it at `https://<device-hostname>/lsm`.

Enter your device username and password to log in.

If a login banner (for example, a legal or acceptable-use notice) is configured on the device, it is displayed first as a full-screen dialog. Read the banner and click **Agree** to continue to the login form.

On a successful login, a confirmation message briefly appears and the console opens to the Home page.

Note

Your session token is kept only for the current browser tab. Closing the tab, logging out, or a device reboot all end the session and return you to the login page. Sessions expire after 15 minutes; at this time, you cannot extend a session and must log in again.

To log out, click your user name (**Admin**) in the top-right corner of the header, then click **Logout**. Logging out ends your session on the device immediately.

Reboot the device

Click **Reboot** in the header from any page to restart the device. You are asked to confirm the action before it proceeds.

Important

Rebooting interrupts network traffic while the device restarts. Plan reboots for a maintenance window.

While the device restarts, the WMC shows a full-screen **Rebooting TPS** status screen and automatically returns you to the login page once the device responds again. If the device does not come back within 15 minutes, the WMC shows a timeout message.

Browser support

The WMC is a standard web application and works with current versions of major desktop browsers (tested using Firefox, Safari, Chrome, and Edge). Because the console is served over HTTPS by the device itself, how you handle the certificate depends on which certificate the device is using:

- By default, the WMC uses the device's own self-signed certificate. Your browser cannot be configured to trust this certificate directly, and it warns that the connection is not private. To confirm you are connecting to the genuine device rather than an intercepting proxy, *manually verify the certificate's fingerprint on page 1-4*.

- If a custom certificate has been installed on the device, you can configure your browser to trust it by installing your organization's root CA certificate. Manually verifying the certificate's fingerprint is also possible in this case.

Manually verify the WMC certificate

When you connect to the WMC over HTTPS, your browser shows the certificate the device presents. To confirm you are connecting to the genuine device and not an attacker intercepting the connection, compare the certificate your browser received against the certificate the device actually holds. The device-side value is read over the serial console or SSH CLI, a channel independent of the HTTPS session you are verifying.

The TPS CLI command `show certificate-fingerprints` prints the SHA-1 and SHA-256 fingerprints of the certificate the WMC serves, using whichever certificate is currently in use, either the device's default self-signed certificate, or a custom certificate you installed.

Procedure

1. Connect to the TPS over the serial console or an SSH session, (not through the web browser) and log in with a SuperUser account.
2. At the CLI prompt, run `show certificate-fingerprints` and record the SHA256 fingerprint value.

   Keep this CLI session as your trusted reference.
3. Point a browser at the WMC and open its certificate viewer for the connection.

   If the device is using its default self-signed certificate, the browser shows a certificate-warning page instead of loading the WMC. You do not need to accept the certificate to read its fingerprint.

TABLE 1-1. Viewing the SHA-256 fingerprint by browser

BROWSER	FROM THE CERTIFICATE-WARNING PAGE	IF THE CERTIFICATE IS ALREADY TRUSTED
Firefox	Click **Advanced…**, then **View Certificate**, then read the SHA-256 value under **Fingerprints**.	Click the site-information icon in the address bar, then **More information**, then on the **Security** tab click **View Certificate** and read the SHA-256 value under **Fingerprints**.

Browser	From the certificate-warning page	If the certificate is already trusted
Safari	Click **Show Details**, then **view the certificate**, then expand **Details** and read the SHA-256 Fingerprint.	From the **Safari** menu, choose **Connection Security Details…** (or click the address bar padlock on Safari versions before 18.4), click **Show Certificate**, then expand **Details** and read the SHA-256 Fingerprint.
Chrome / Edge	Click **Not secure** next to the address bar, click **Certificate Details**, and read the SHA-256 value under **Fingerprints**. The same control remains available after you continue to the site.	

(Alternative) If you have OpenSSL installed, you can fingerprint the presented certificate directly: `openssl s_client -connect <device-ip>:443 </dev/null 2>/dev/null | openssl x509 -noout -fingerprint -sha256`

4. Compare the SHA-256 value from the device CLI with the value from the browser (or OpenSSL).

   The comparison is over hex digits and is case-insensitive; separator colons and spacing do not matter.

If the fingerprints match, the certificate your browser received is the exact certificate the device holds. The connection is authentic and not being intercepted, and you can trust it (including saving it as a browser exception for a self-signed certificate).

Important

If the fingerprints differ, stop. Do not enter credentials or accept the certificate. The certificate your browser received is not the one the device is serving. Possible causes include an intercepting proxy or attacker, connecting to the wrong host or IP address, or the device's certificate having legitimately changed since you last connected. Confirm the change was expected before trusting the session.

Chapter 2

Home

The Home page displays read-only identifying information about the device.

TABLE 2-1. Device Information

FIELD	DESCRIPTION
Hostname	The configured hostname of the device.
Model	The device hardware model.
Serial Number	The device serial number.
TOS Version	The version of the TippingPoint Operating System (TOS) currently running.
DV Version	The version of the currently installed Digital Vaccine (DV) package.
Aux DV Version	The version of the currently installed auxiliary DV package, if any.

Note

If the device information cannot be retrieved, the page shows an error message with a **Retry** button.

Chapter 3

Upload and install a software package

The Software page is used to upload and install software packages on the device. The supported package installation types are:

- Digital Vaccine (DV)
- Auxiliary Digital Vaccine (AuxDV)
- TOS upgrade
- License
- Certificate

Important

Software installation through the WMC is not supported while the device is managed by an SMS. When a TPS device is under SMS management, use the SMS to distribute DV, AuxDV, TOS, license, and certificate packages instead of installing them from the WMC.

1. Choose a package file under **Software Upload**.
2. Click **Upload Package**.
3. (Optional) Click **Clear** at any time before installing to remove the selected file and choose a different one.

Once a package finishes uploading, the WMC identifies its type and checks the device's license before allowing installation. If the corresponding license feature is not active or the uploaded package is invalid, the package is removed from the device and an error is shown instead of an install prompt.

Install a Digital Vaccine or Auxiliary DV package

After a DV or AuxDV package uploads, a confirmation dialog shows the currently installed version and the new version. Click **Confirm** to install.

The WMC displays "Installing DV version *x.x.x.x*..." while the install runs and polls the device for progress. When the install finishes, the message updates to "DV version *x.x.x.x* is now installed" and the DV Version (or Aux DV Version) field refreshes automatically.

Install a TOS package

After a TOS package uploads, a confirmation dialog shows the currently running TOS version and the new version.

Note

Installing an older TOS version than the one currently running is not supported.

Important

Installing a TOS package reboots the device automatically and interrupts network traffic and your WMC session while the device restarts, similar to a manual reboot.

Click **Confirm** to start the install. There is no progress indicator for a TOS install. The device reboots as soon as the installation finishes.

Install a license package

After a license package uploads, a confirmation dialog shows the current and new license versions.

1. Click **Confirm** to install.
2. Once the license installs, choose whether to reboot the device:
    - Click **Reboot** to restart the device immediately and apply the new license.
    - Click **Later** to keep working; the new license takes effect after your next reboot.

Install a system certificate package

After a system certificate package uploads, a confirmation dialog warns that installing it reboots the device automatically. Click **Confirm** to install. The device reboots as soon as the install completes.

Chapter 4

Create and export a Tech Support Report

A tech support report bundles diagnostic information from the device for use by Trend Micro support.

Procedure

1. Navigate to the Support page.
2. Choose which optional content to include:
   - Include snapshot
   - Include traffic logs
   - Include crash reports
3. Click **Create** to generate a new report.

   The WMC checks whether a report is already being generated before starting a new one. Once started, it shows progress and polls the device until the report finishes or an error occurs.
4. Once a report is available, click **Export** to download it to your computer.

Chapter 5

Download device logs

Use Log Download to retrieve device logs directly from the WMC, optionally filtered by date, time, or log entry ID.

Procedure

1. Navigate to the Support page.
2. Under **Log Download**, Select a Log Type:
   - System
   - Audit
   - IPS Block
   - IPS Alert
   - Reputation Block
   - Reputation Alert
   - SSL Inspection
3. Select a Format: tab-delimited (`.txt`) or comma-delimited (`.csv`).
4. Optionally narrow the results using one of the following. You cannot select both:

- **Date Range** — Start Date / End Date, with an optional Time Range (Start Time / End Time, in `HH:MM:SS` format) once a date is set.
- **ID Range** — Start ID / End ID, using the numeric log entry sequence numbers.

5. Choose an Output mode:
   - **Download** — saves the log file to your computer.
   - **Open in new tab** — opens the log contents directly in a new browser tab.
6. Click **Download** (or **View Log**, depending on the output mode you selected) to retrieve the log.

Index

TREND MICRO INCORPORATED

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736

www.trendmicro.com