Tenable Product Debug Data Collection Guide

Last Updated: July 24, 2026

This guide describes how to collect debugging data and diagnostic files across Tenable products to provide to Tenable Support for troubleshooting.

Table of Contents

Tenable Product Debug Data Collection Guide

This guide outlines the steps to collect diagnostic data for Tenable Support. When you open a case with Tenable Support, use this guide to generate a diagnostics file to attach to your support ticket.

Tenable diagnostics and debug logs are the primary tools for resolving complex issues across Tenable products. Administrators utilize these files to provide Tenable Support with a comprehensive snapshot of system health, configuration settings, and scan activities that are otherwise invisible in the user interface. These logs are crucial for investigating scan failures, performance bottlenecks, and authentication errors. By enabling "debug mode" for a targeted period, users capture data that helps engineers replicate local environments and identify the root cause of service disruptions, ensuring a more stable and accurate vulnerability management lifecycle.

The following are some use cases for opening a Tenable Support ticket with diagnostic and debug data:

- **Troubleshooting scan failures:** Identifying why a scan hung, stopped prematurely, or failed to launch across specific segments.
- **Resolving Credential Failures:** Analyzing exact handshake or permission errors when authenticated scans fail to access targeted assets.
- **Performance Optimization:** Investigating high CPU or memory usage or database lag that impacts the speed of vulnerability processing.
- **Plugin Debugging:** Verifying why specific plugins did not fire or why they produced suspected false positives or negatives on a host.
- **Upgrade & Installation Errors:** Providing logs to resolve issues encountered during version migrations or initial setup failures.

- **Audit Trail Verification:** Documenting unusual user activity or system changes for compliance and security forensics.
- **Connectivity & Sensor Health:** Diagnosing communication breaks between the management console and remote Tenable Nessus scanners or Tenable Agents.

The steps for collecting data are divided into three phases. Not every Tenable product or issue requires all three phases. You may receive specific instructions to gather some or all of these:

Enable Plugin Debugging and Audit Trails

Use this section when troubleshooting false positives, authentication errors, or compliance checks. Apply these settings before running the scan.

- Tenable Nessus (Pro, Manager, and Scanners)
- Tenable Agents
- Tenable One Vulnerability Management
- Tenable One Web App Scanning

Collect Scan Results

Use this section after the scan has finished. These files allow support to replay the scan results with full diagnostic data.

- Tenable Nessus (Pro, Manager, and Scanners)
- Tenable Agents
- Tenable One Vulnerability Management
- Tenable One Web App Scanning

Collect System Debug Logs and Diagnostics Files

Use this section when troubleshooting software crashes, service failures, or installation errors.

- Tenable Nessus (GUI & CLI)
- Tenable Agents (GUI & CLI)
- Tenable Security Center (Diagnostics File)
- Tenable Security Center (Debugging Logs)
- Tenable One Vulnerability Management
- Tenable Core
- Tenable One OT Exposure
- Tenable Network Monitor

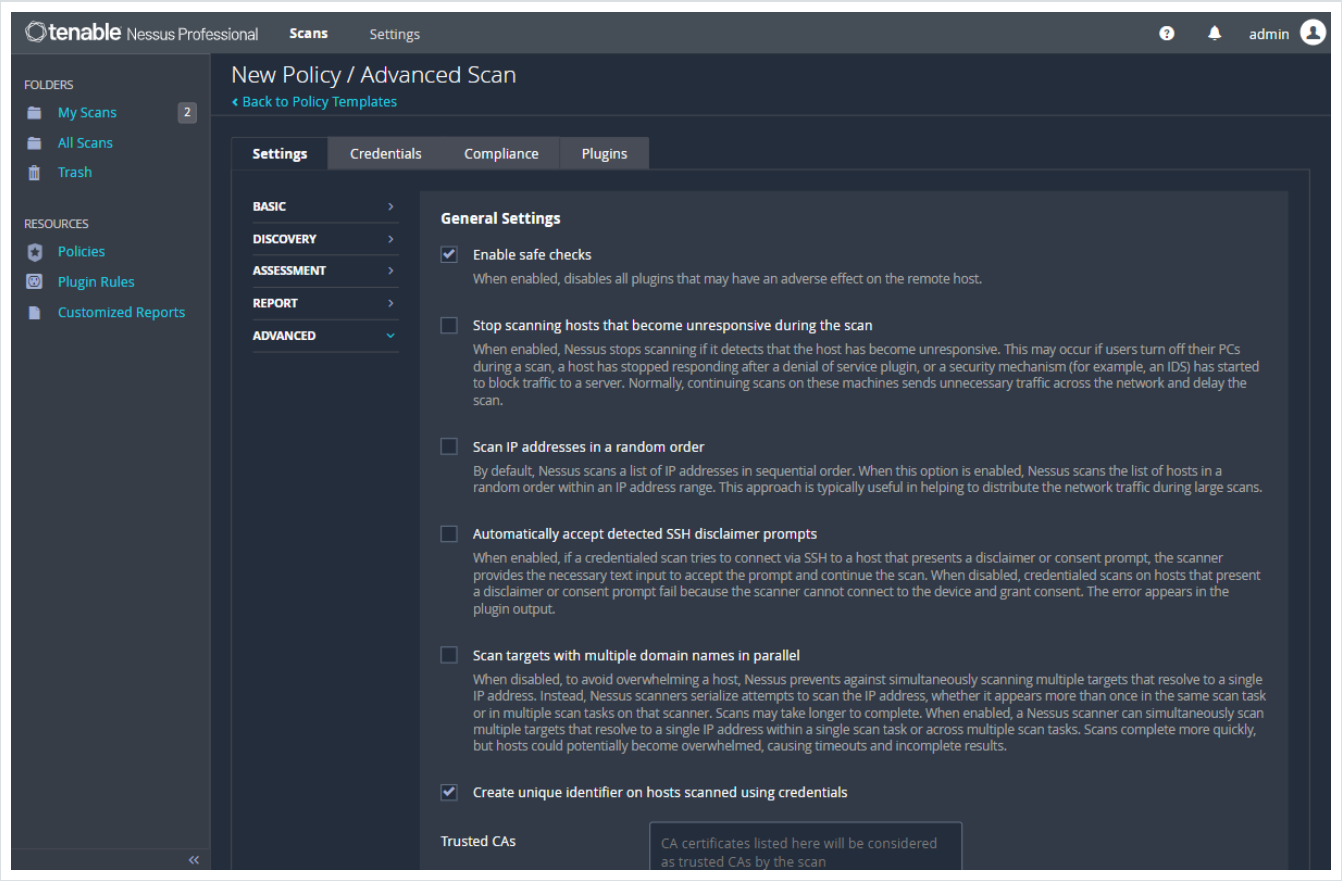
Tenable Nessus

Enable Plugin Debugging and Audit Trails

Use this section when troubleshooting false positives, authentication errors, or compliance checks. Apply these settings before running the scan.

To enable plugin debugging and audit trails for Tenable Nessus:

1. Create or edit your scan policy.
2. Go to **Advanced**. If the screen shows **Scan Type**, set it to **Custom**.



3. Scroll down to the **Debug Settings** section:

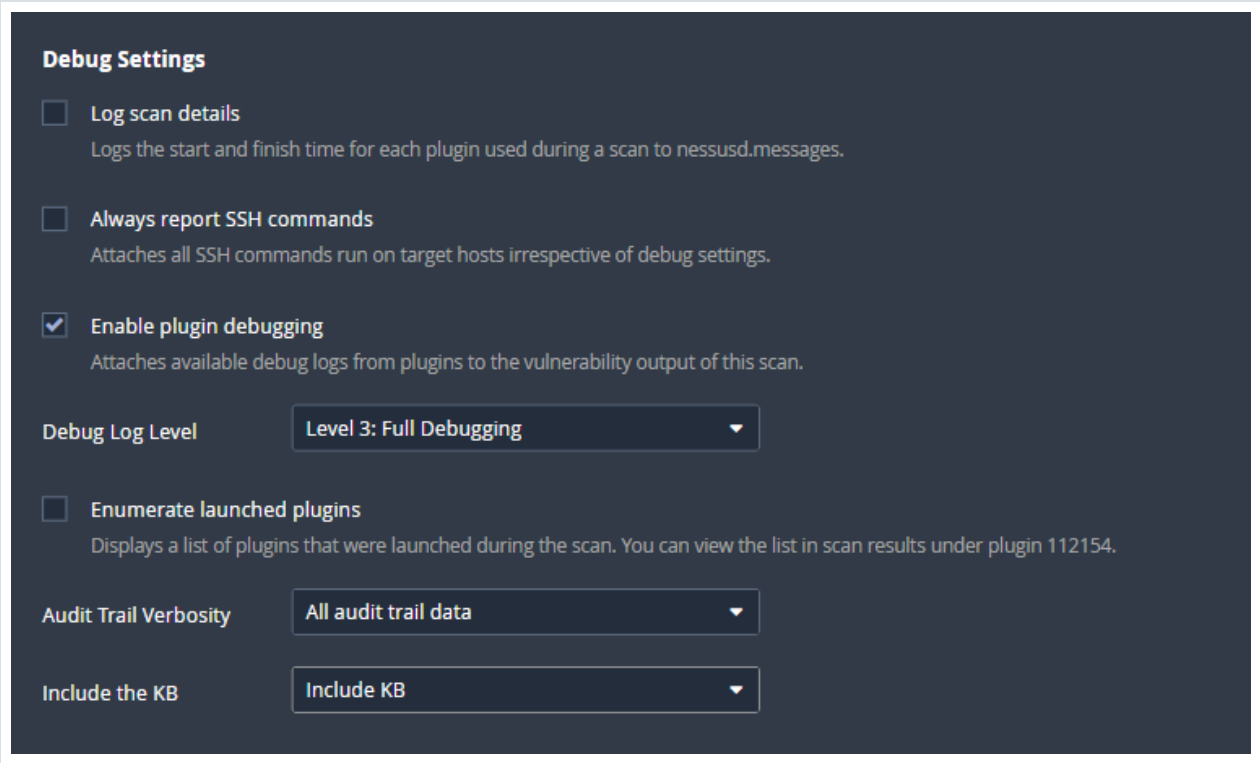
    a. Select **Enable plugin debugging**.

    b. Set **Debug Log Level** to **Level 3**.

    > **Note:** Do not set the **Debug Log Level** to **Level 4** unless instructed to do so by Tenable Support.

    c. Set **Audit Trail Verbosity** to **All audit trail data**.

d. Set **Include the KB** to **Include KB**.

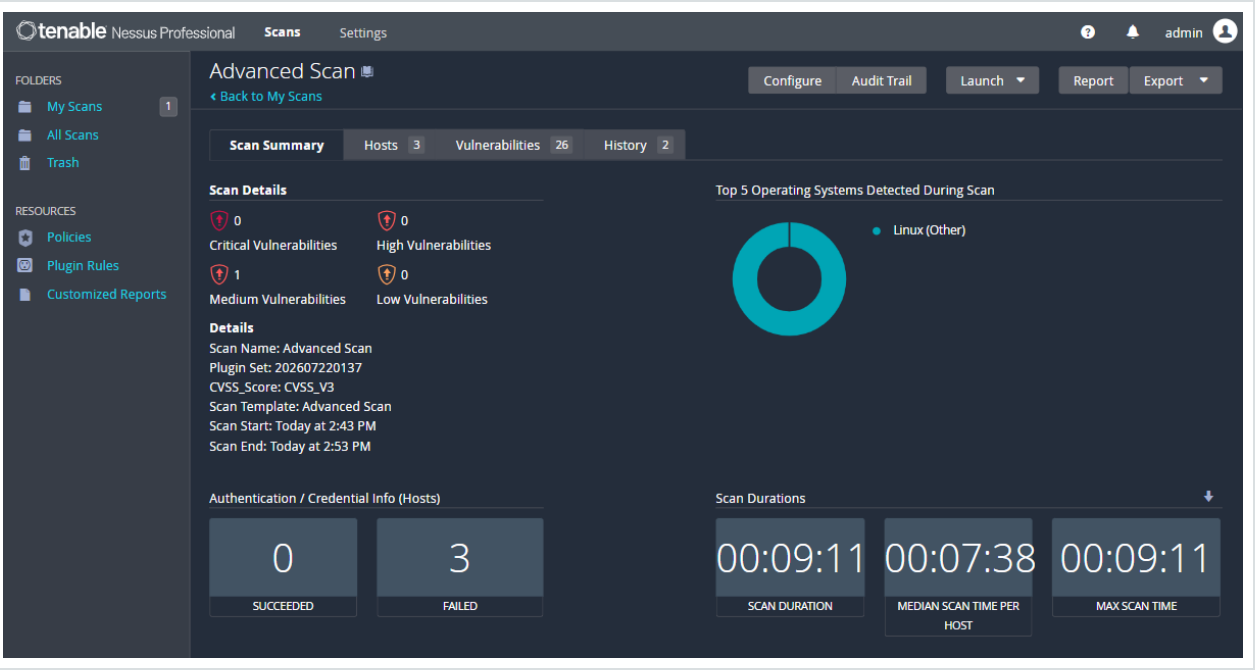


4. Save and run the scan.

5. Ensure the scan has completed with plugin debugging and audit trails enabled:

   a. Select the scan to view the scan details.

   b. In the upper right corner, look for the **Audit Trail** button next to the **Configure** button.



c. In the plugin results, search for the **Debugging Log Report** plugin.

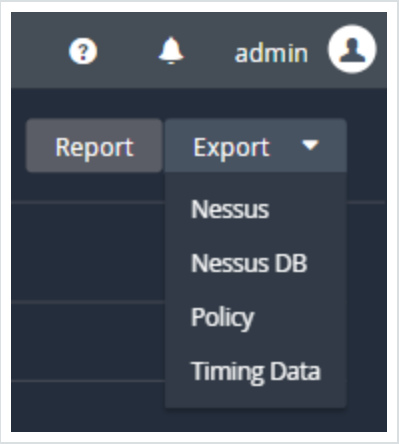
   If the **Audit Trail** button or the **Debugging Log Report** plugin are not visible, try these steps again to enable plugin debugging and audit trails.

Collect Scan Results

Use this section after the scan has finished. These files allow support to replay the scan results with full diagnostic data.

To collect scan results for Tenable Nessus:

1. Ensure the scan has finished with **Plugin Debugging** and **Audit Trails** enabled.
2. Select the scan, and in the upper right corner, click **Export**.



3. Select the **Nessus DB** format.

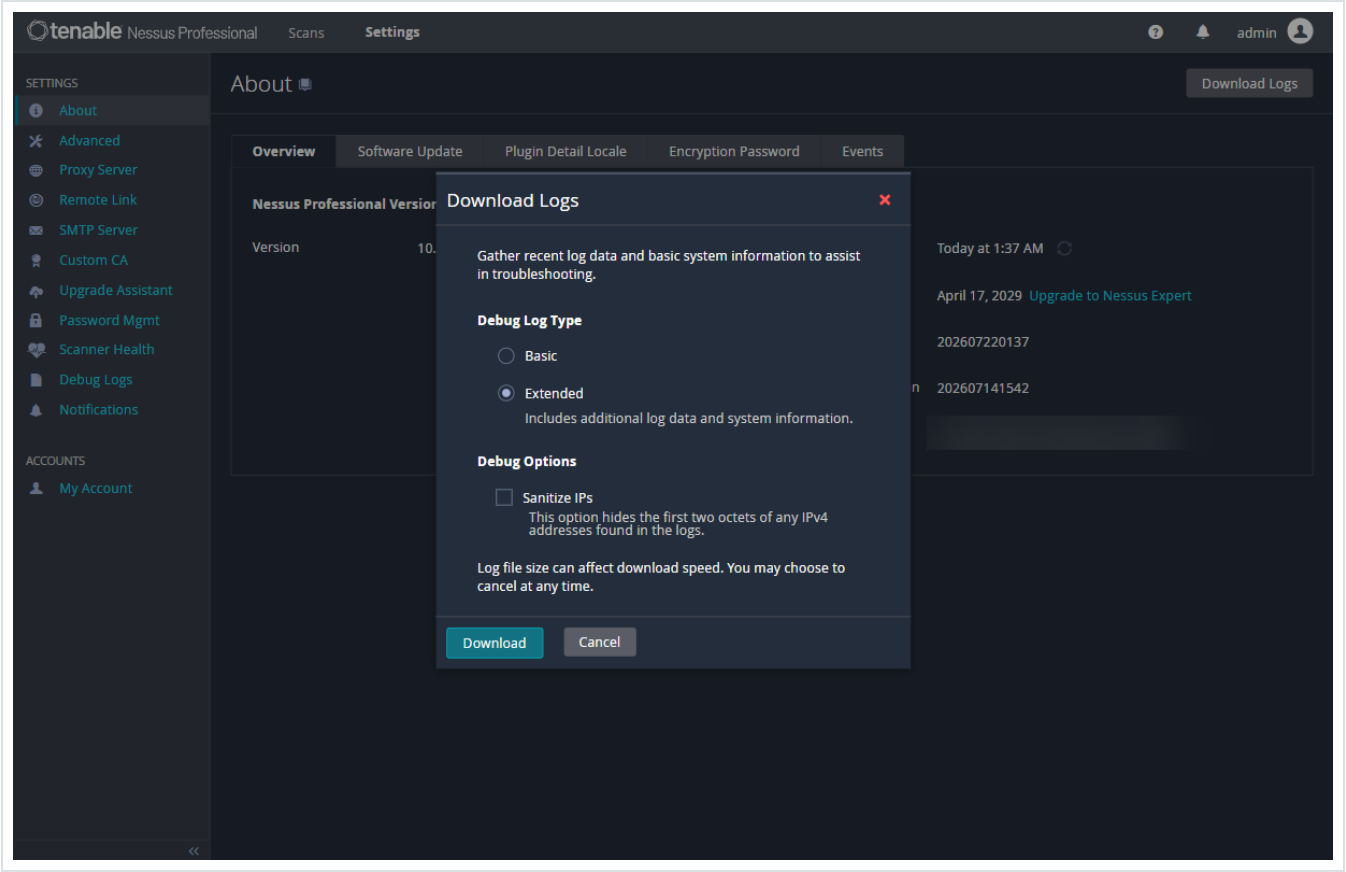
   > **Note:** Set a secure password when prompted. You must provide this password to Tenable Support.

4. Download the file and submit it to your support case.

Collect Debug Logs

Use this section when troubleshooting software crashes, service failures, or installation errors.

- **GUI Method (Nessus 8.x and later):** Go to `https://<nessus_ip>:8834` > **Settings**. In the upper-right corner, click **Download Logs**. Select **Extended** as the debug log type, then click **Download**.



- **CLI (Windows):** Run as Admin: `"C:\Program Files\Tenable\Nessus\nessuscli.exe" bug-report-generator`. Choose **Full Mode**.
- **CLI (Linux):** Run as Root: `/opt/nessus/sbin/nessuscli bug-report-generator`. Choose **Full Mode**.
- **CLI (macOS):** Run as Root: `/Library/Nessus/run/sbin/nessuscli bug-report-generator`.

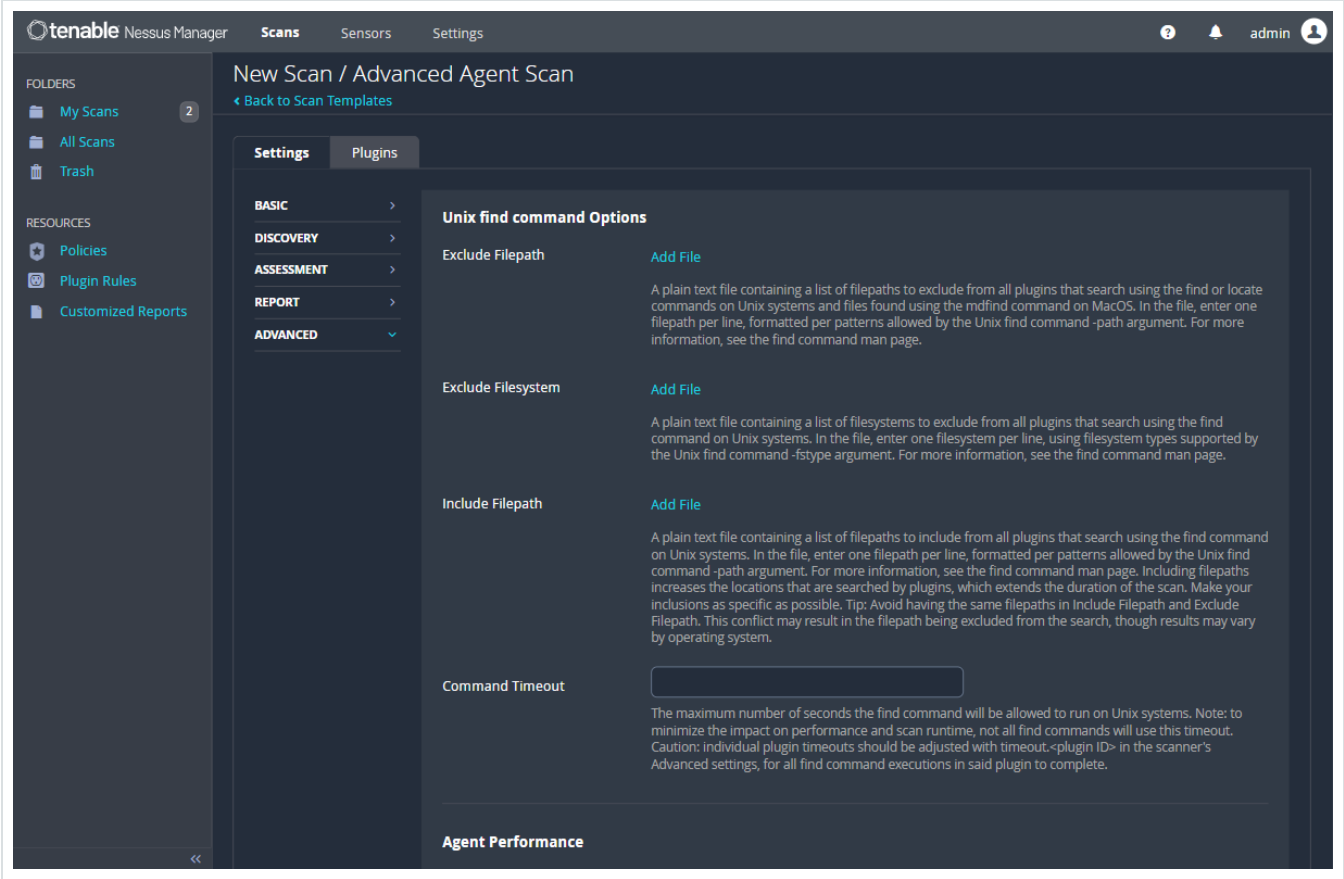
Tenable Agents

Enable Plugin Debugging and Audit Trails

Use this section when troubleshooting false positives, authentication errors, or compliance checks. Apply these settings before running the scan.

To enable plugin debugging and audit trails for Tenable Agents:

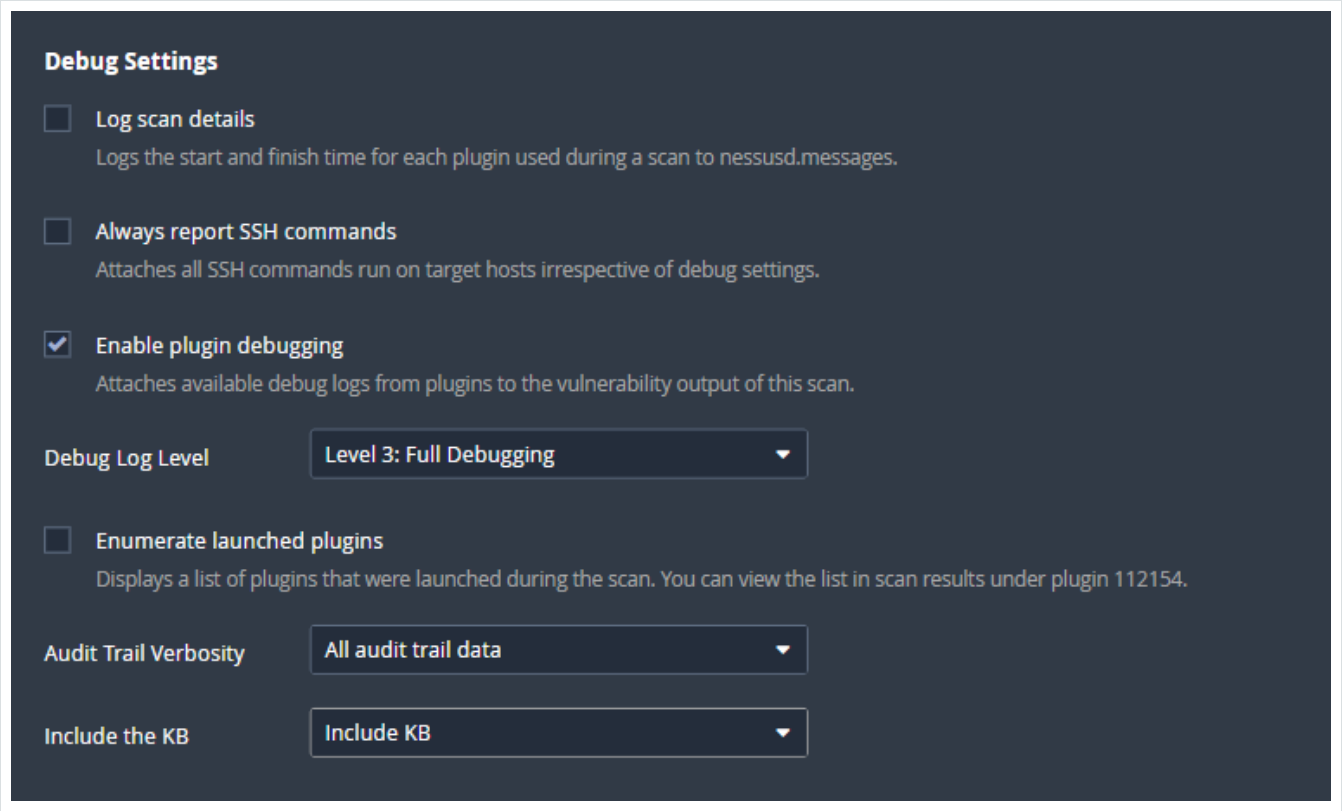
1. Navigate to **Scans** and edit the agent scan policy.
2. Go to **Advanced** (set **Scan Type** to **Custom** if needed).



3. Under **Debug Settings**:
    a. Select **Enable plugin debugging**.
    b. Set **Debug Log Level** to **Level 3**.

c. Set **Audit Trail** to **All audit trail data**.

d. Set **Include the KB** to **Include KB**.



4. Save and run the scan.

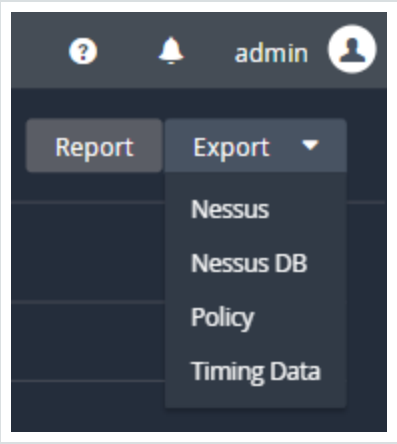
Collect Scan Results

Use this section after the scan has finished. These files allow support to replay the scan results with full diagnostic data.

To collect scan results for Tenable Agents:

1. Ensure the scan has finished with **Plugin Debugging** and **Audit Trails** enabled.

2. Select the scan, and in the upper right corner, click **Export**.



3. Select the **Nessus DB** format.

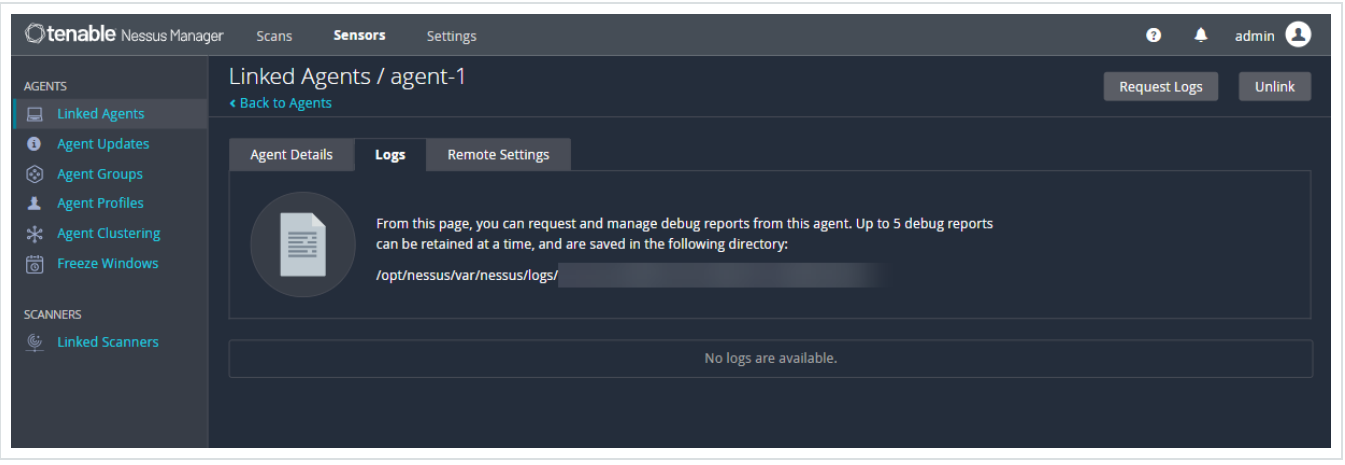
   > **Note:** Set a secure password when prompted. You must provide this password to Tenable Support.

4. Download the file and submit it to your support case.

Collect Debug Logs

Use this section when troubleshooting software crashes, service failures, or installation errors.

- **GUI Method (via Nessus Manager)**: Go to **Sensors**, select the agent, click **The Log**, then **Request Logs**.



- **CLI (Windows)**: Run as Admin: `"C:\Program Files\Tenable\Nessus Agent\nessuscli.exe" bug-report-generator`.
- **CLI (Linux)**: Run as Root: `/opt/nessus_agent/sbin/nessuscli bug-report-generator`.
- **CLI (macOS)**: Run as Root: `/Library/NessusAgent/run/sbin/nessuscli bug-report-generator`.

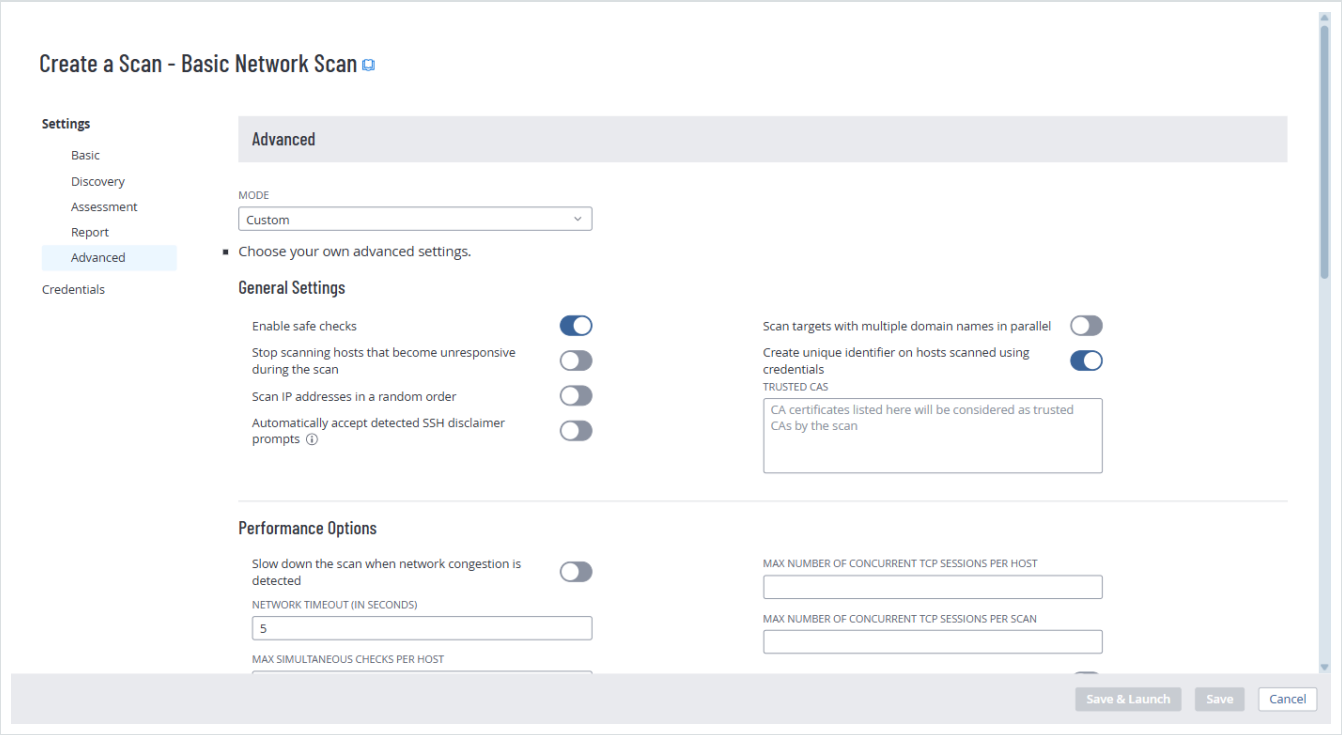
Tenable One Vulnerability Management

Enable Plugin Debugging and Audit Trails

Use this section when troubleshooting false positives, authentication errors, or compliance checks. Apply these settings before running the scan.

To enable plugin debugging and audit trails for Tenable One Vulnerability Management:

1. Create or edit the scan policy.
2. Go to **Advanced** (set **Mode** to **Custom** if visible).

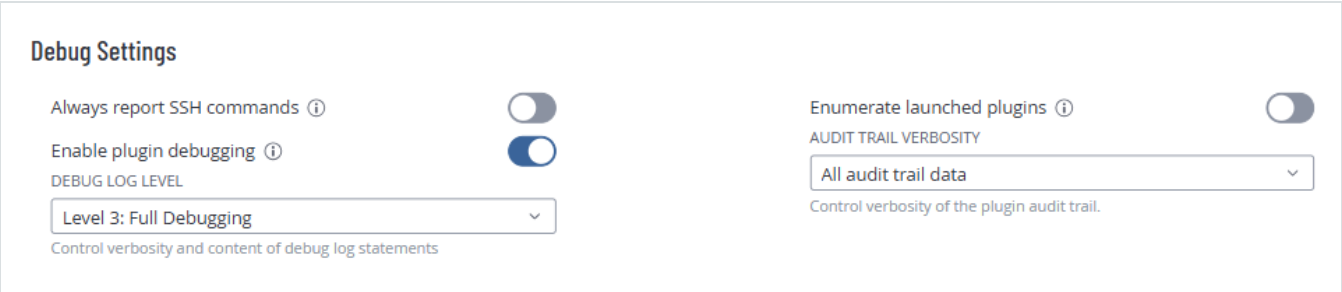


3. Under **Debug Settings**:

    a. Select **Enable plugin debugging**.

    b. Set **Debug Log Level** to **Level 3**.

    c. Set **Audit Trail Verbosity** to **All audit trail data**.



4. Save and run the scan.

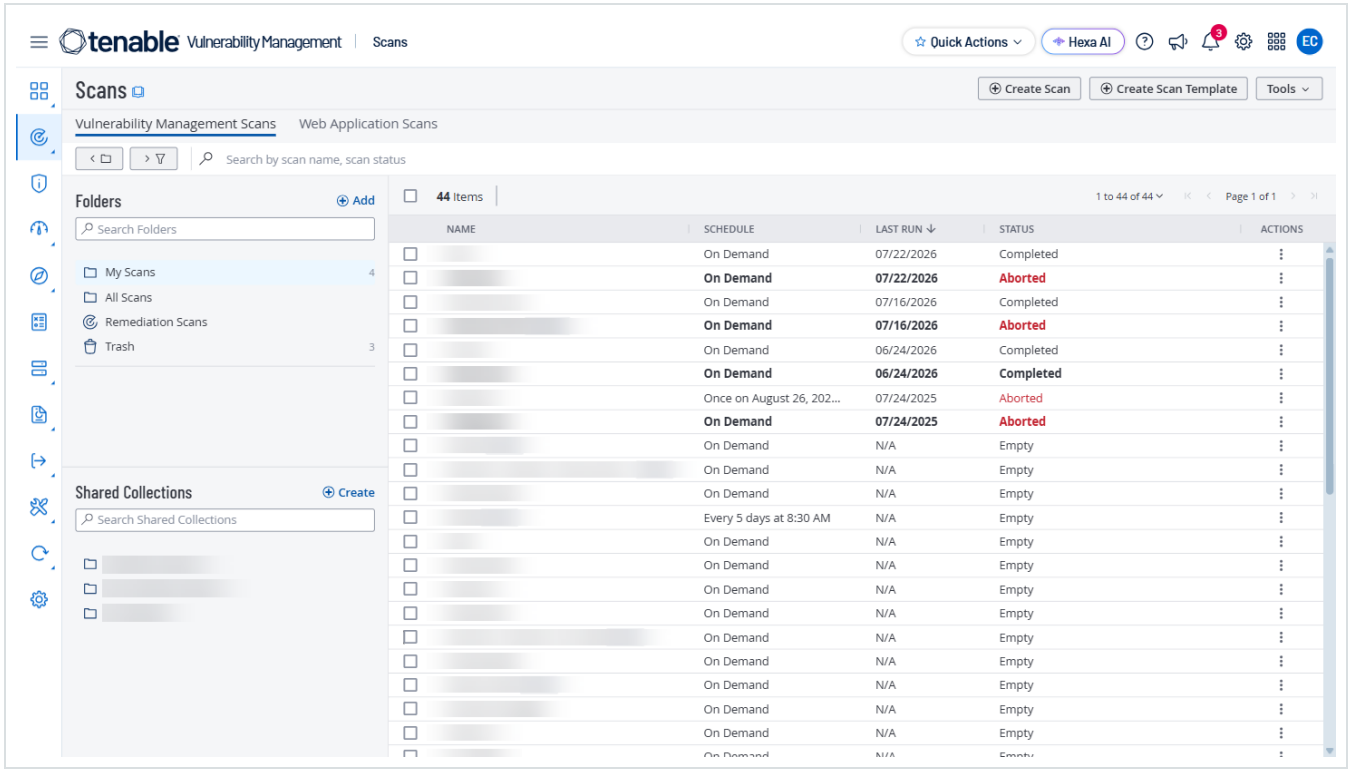
Collect Scan Results

Use this section after the scan has finished. These files allow support to replay the scan results with full diagnostic data.

There are two distinct export paths depending on the scan type.

To collect scan results for standard vulnerability scans:

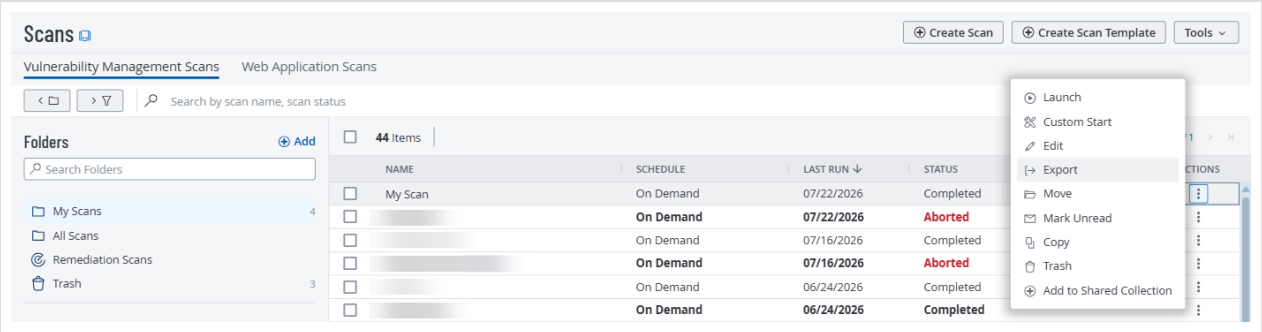
1. In the left navigation, click **Scans**.



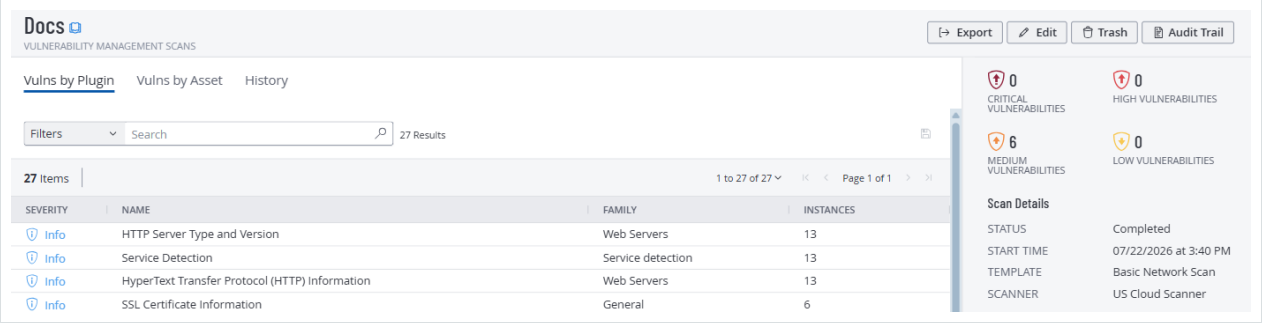
2. Below **Scans**, select **Vulnerability Management Scans**.

3. Do one of the following:

- In the scans table, roll over the scan and click the ⋮ button, then click **Export**.

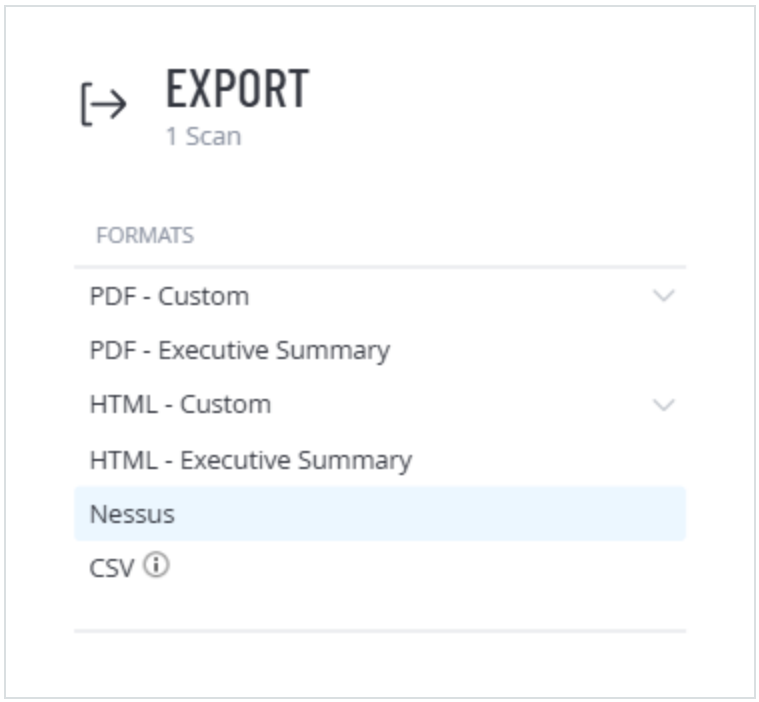


- View scan details, and in the upper right corner, click **Export**.



The **Export** plane appears.

4. Select the **Nessus** format and click **Export**.

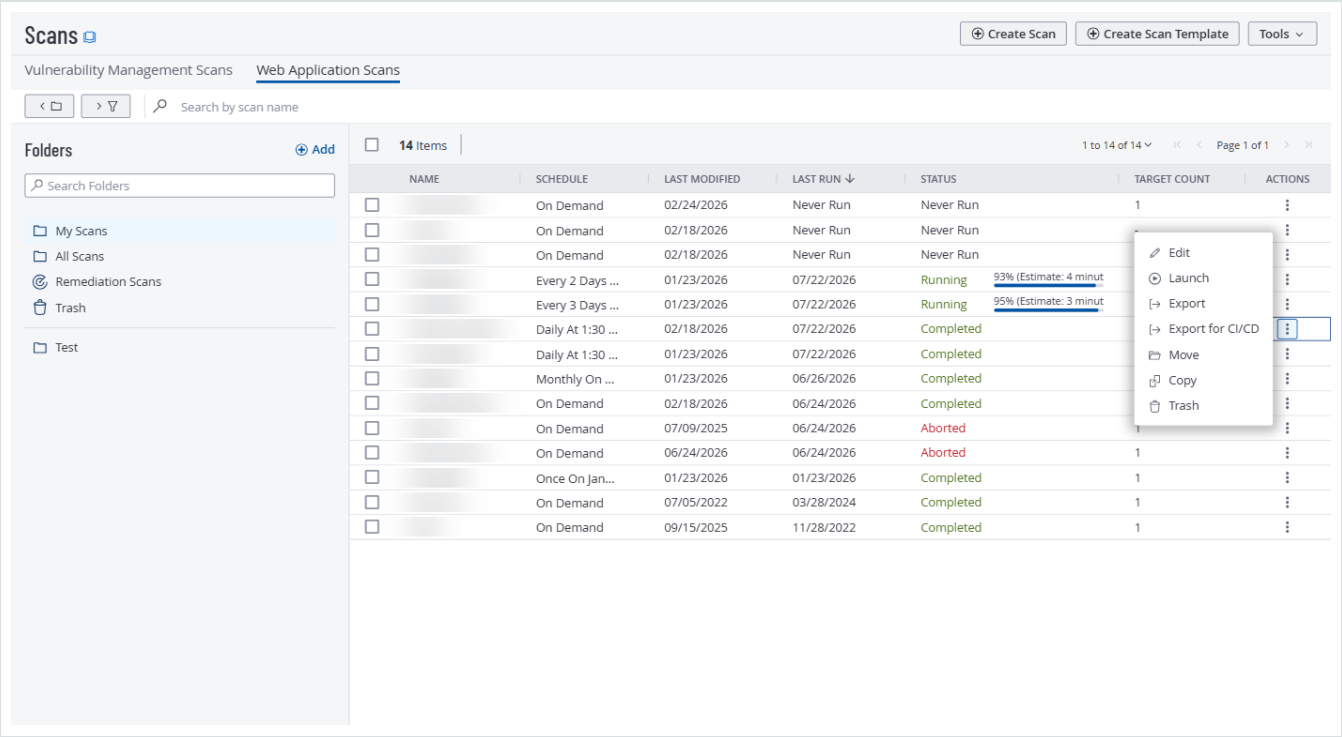


> **Note:** If the scan results are more than 35 days old, only the **Nessus** and **CSV** export formats are available.

5. Submit the downloaded file to your support case.

To collect scan results for web application scans:

1. In the left navigation, click **Scans**.
2. Select the **Web Application Scans** tab (or filter) to locate your scan.
3. Do not open the scan details yet. Instead, look for the **Export** button or the ⋮ menu next to the scan in the list.
4. Select **Export** and select the **Nessus** format.



5. Set a password when prompted.

Collect Debug Logs

Use this section when troubleshooting software crashes, service failures, or installation errors.

To collect system debug logs for Tenable One Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears with **Linked Scanners** selected by default.

2. In the linked scanners table, click the scanner you want logs from.

   The details page for that scanner appears.

3. Click the **Logs** tab.

4. In the upper-right corner, click **Request Logs**.

The log appears as a pending row in the table. Tenable One Vulnerability Management requests the logs the next time the scanner checks in, which may take several minutes.

5. When the log status shows as available, click the download button in that row.

Tenable One Web App Scanning

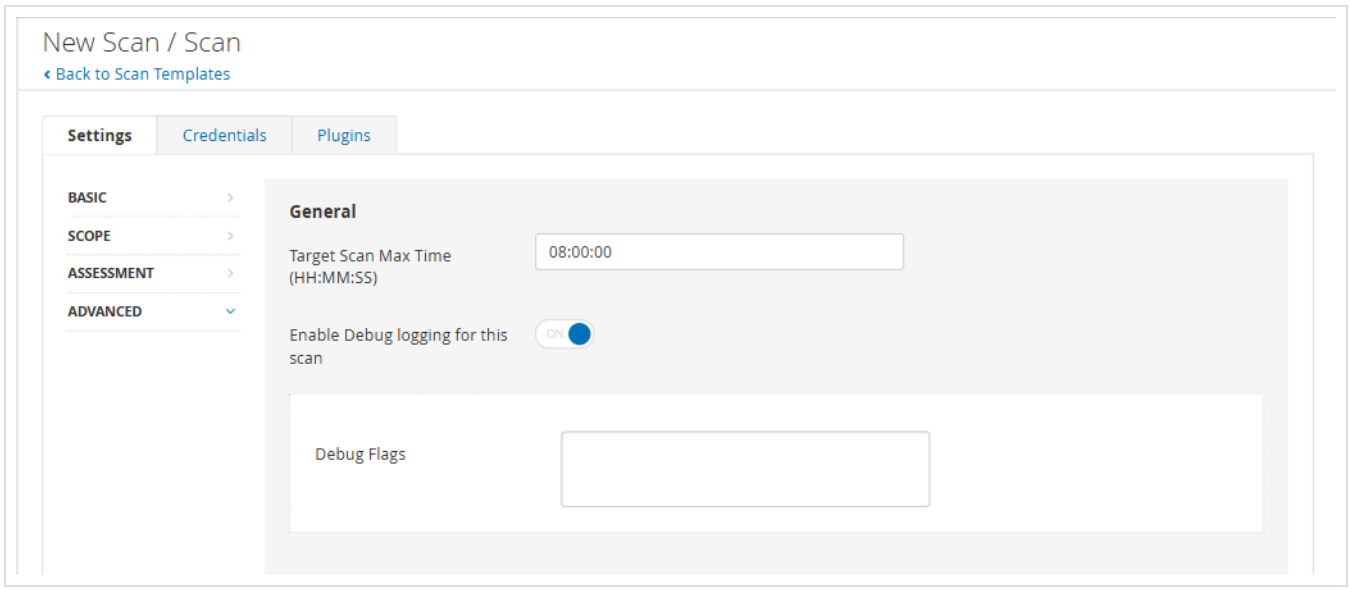
Enable Plugin Debugging and Audit Trails

Use this section when troubleshooting false positives, authentication errors, or compliance checks. Apply these settings before running the scan.

To enable plugin debugging and audit trails for Web App Scanning in Tenable Nessus Expert:

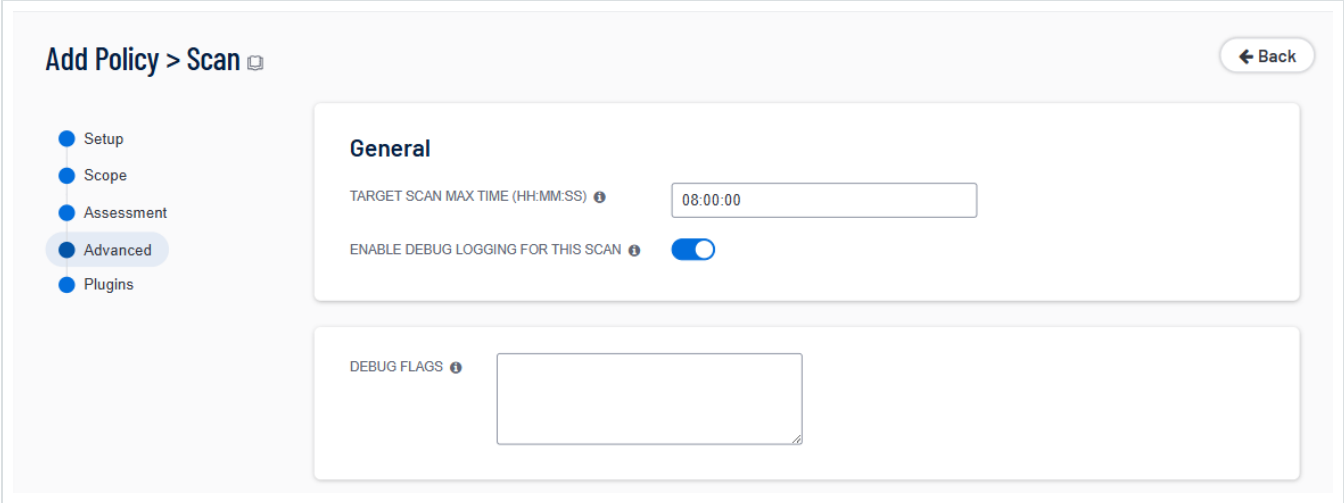
1. In Tenable Nessus Expert, in the policy, go to **Advanced**.
2. Select **Enable Debug logging for this scan**.

   Leave flags empty unless instructed otherwise.



To enable plugin debugging and audit trails for Web App Scanning in Tenable Security Center:

1. In Tenable Security Center, go to **Scans** > **Policies**
2. In the table, select the scan policy.
3. In the **Advanced** section, select **Enable Debug logging for this scan**.

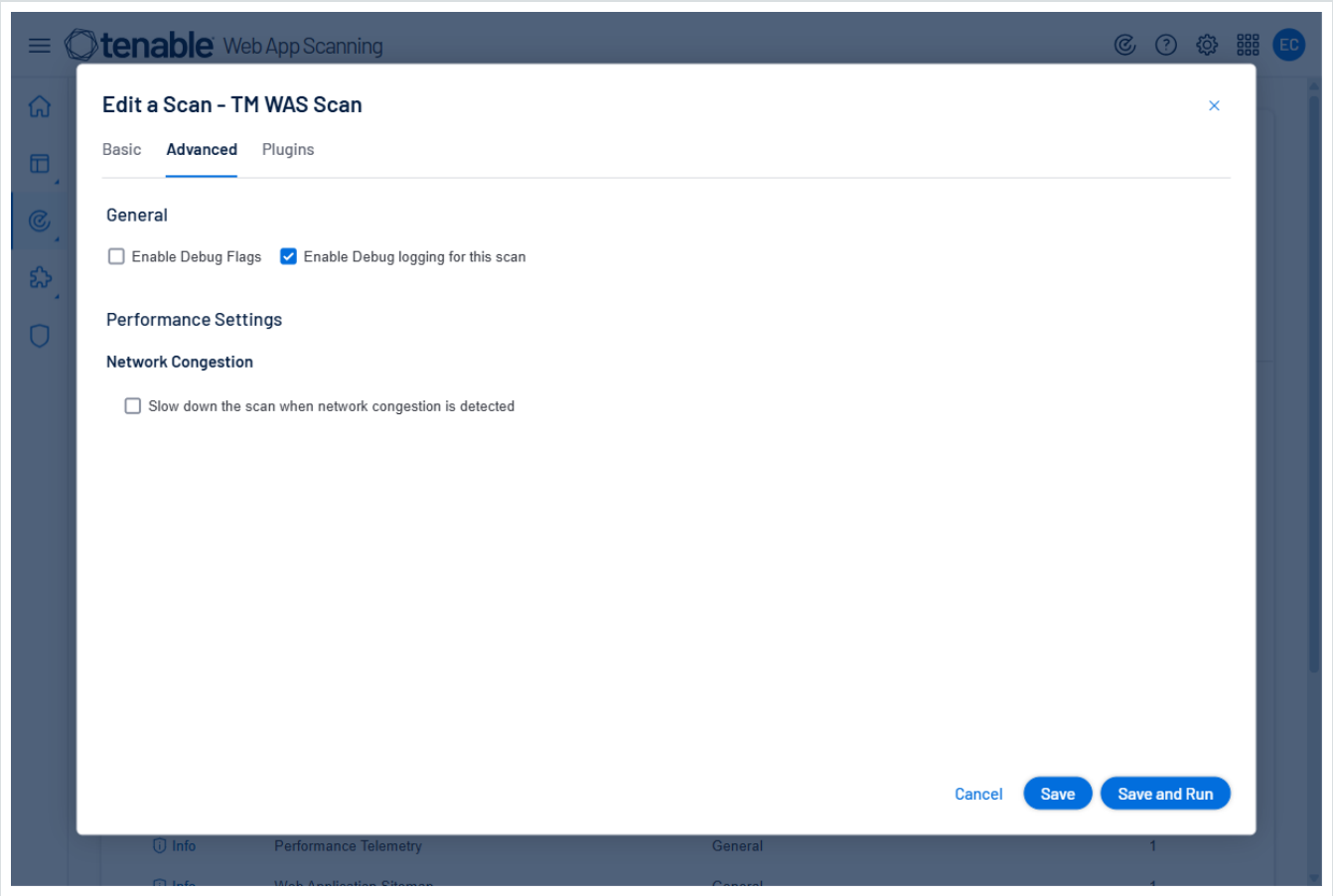


To enable plugin debugging and audit trails for Web App Scanning in Tenable One Vulnerability Management:

1. In Tenable One Web App Scanning, go to **Scans**.
2. In the table, select the scan.

   The **Edit a Scan** window appears.

3. In the **Advanced** tab, select **Enable Debug logging for this scan**.



Collect Scan Results

Use this section after the scan has finished. These files allow support to replay the scan results with full diagnostic data.

To collect scan results for Web App Scanning in Tenable Nessus Expert:

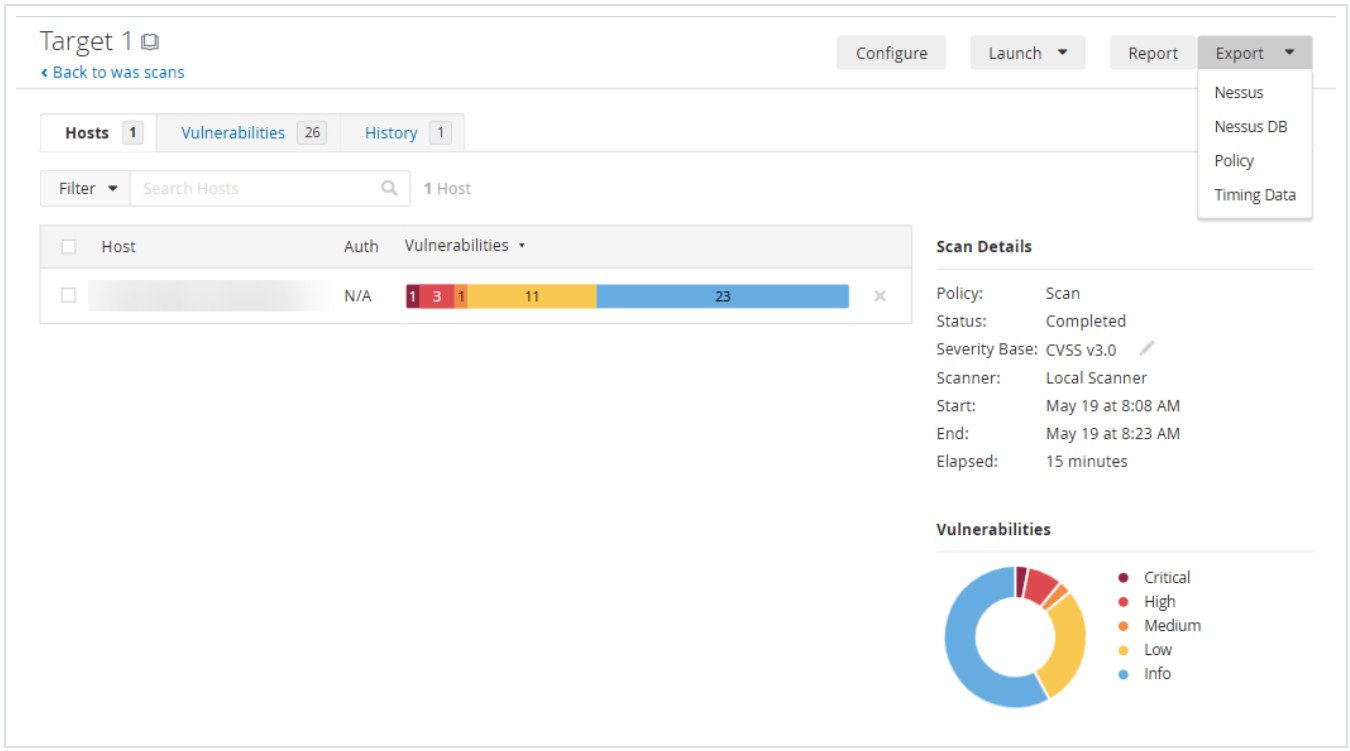
1. In the top navigation bar, click **Scans**.

   The **My Scans** page appears.

2. Click the scan, then click **See All Details**.

The scan details page appears.

3. In the upper-right corner, click **Export**.



4. Select **Nessus DB**.

   a. Type a password to protect the file.

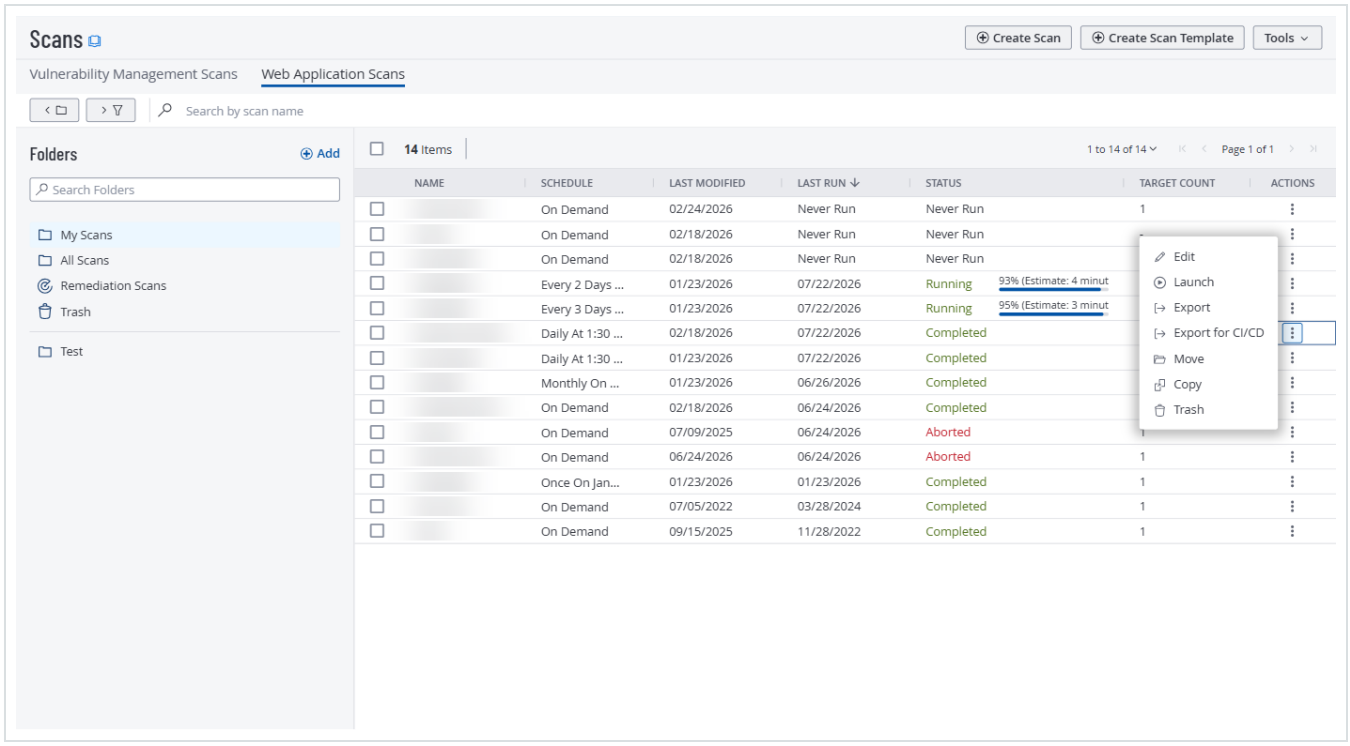
   b. Click **Export**.

> **Note:** You must provide this password to Tenable Support.

5. Submit the downloaded file to your support case.

To collect scan results for Web App Scanning in Tenable One Vulnerability Management:

1. In the left navigation, click **Scans**.
2. Select the **Web Application Scans** tab (or filter) to locate your scan.
3. Do not open the scan details yet. Instead, look for the **Export** button or the ⋮ menu next to the scan in the list.
4. Select **Export** and select the **Nessus** format.



5. Set a password when prompted.

Collect Debug Logs

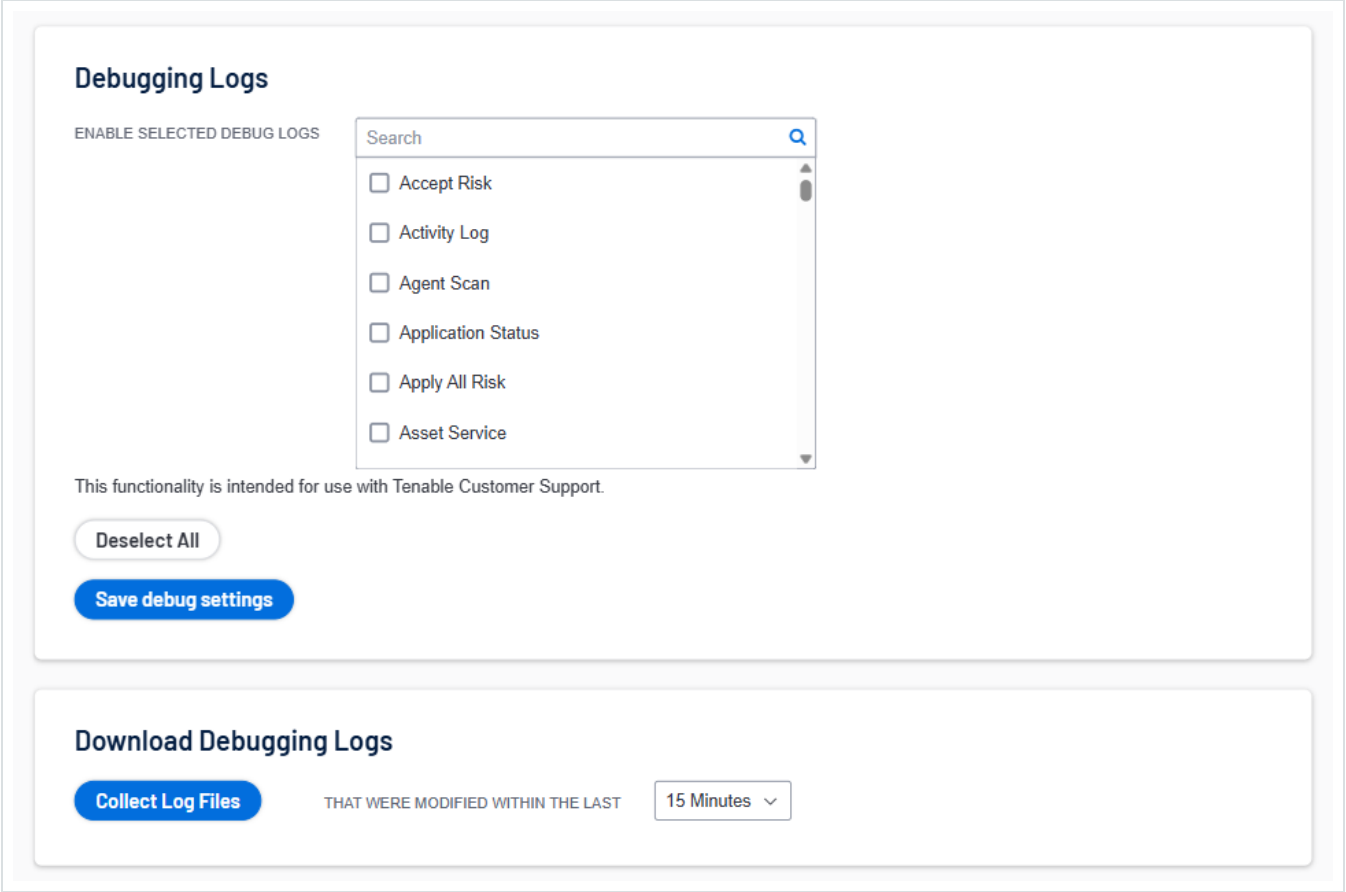
Use this section when troubleshooting software crashes, service failures, or installation errors.

To collect debug logs for Web App Scanning in Tenable Security Center:

1. In the left navigation, click **System** > **Diagnostics**.

   The **Diagnostics** page appears.

2. In the **Debugging Logs** section, select the debugging logs Tenable Support asked you to enable.



3. Click **Save Debug Settings**.

4. Reproduce the issue.

5. In the **Download Debugging Logs** section, click **Collect Log Files**.

6. Click **Download Debug File**.

7. Submit the file to your support case, then disable the debugging logs.

Tenable One OT Exposure

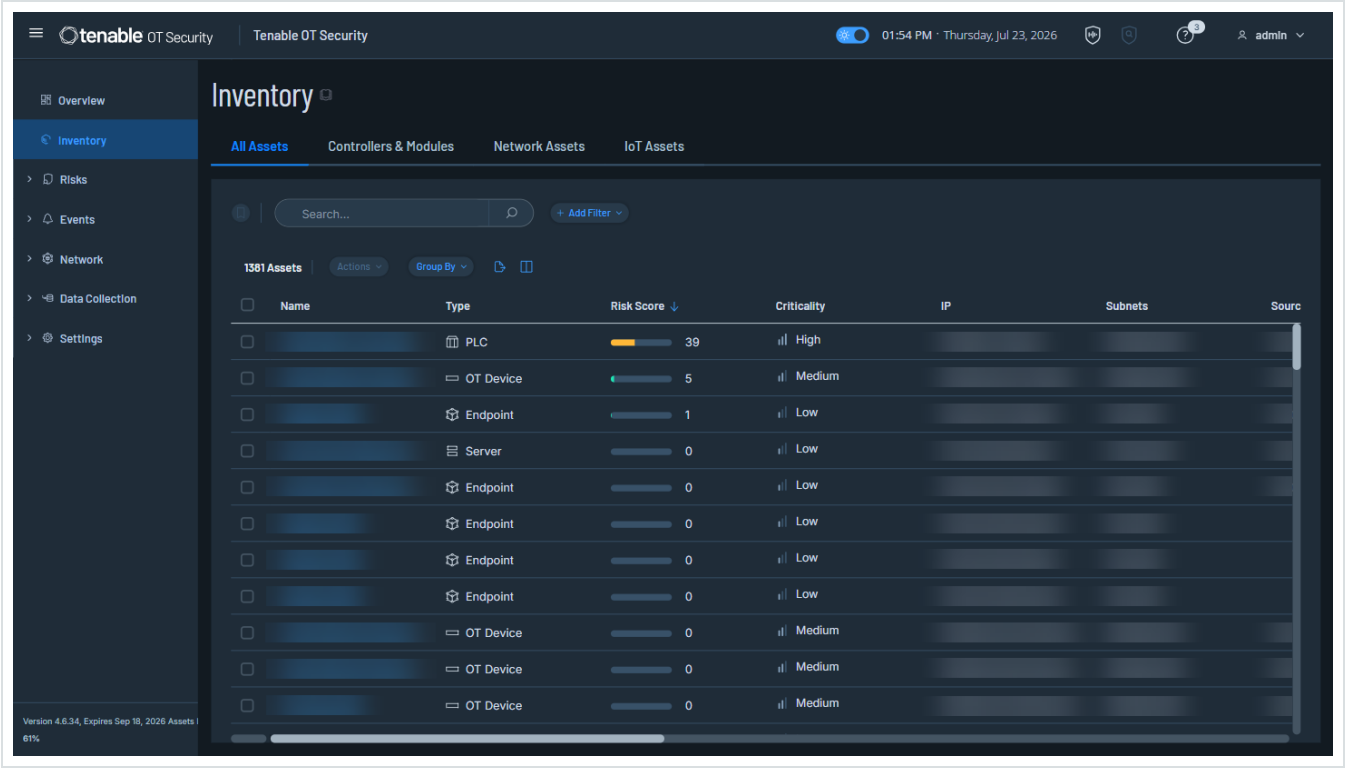
Collect Diagnostics File

Use this section when troubleshooting software crashes, service failures, or installation errors.

To generate a diagnostic report for troubleshooting:

1. In the left navigation bar, go to **Inventory** > **All Assets**.

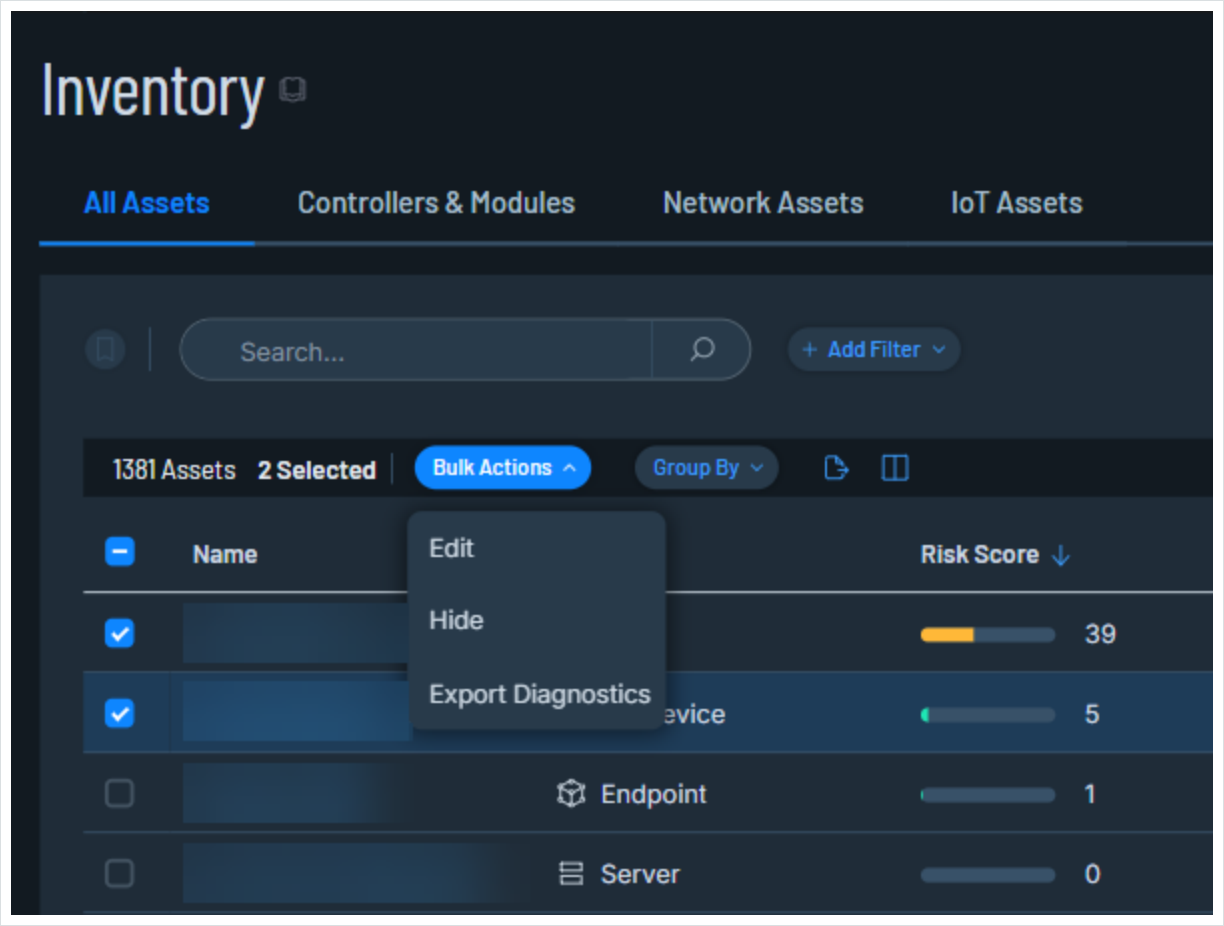
   The **All Assets** page appears.



2. In the All Assets table, select one or more assets to export in the diagnostics report.

3. Do one of the following:

    - For a single asset: In the upper-right corner, click **Actions** > **Export Diagnostics**.
    - For multiple assets: In the upper-right corner, click **Bulk Actions** > **Export Diagnostics**.



    Tenable One OT Exposure downloads the diagnostics report for the selected asset or assets. The diagnostics report is a `tar.gz` file and includes the asset details in a `.json` file.

    The diagnostics report name includes the name of the asset, timestamp, and the Tenable One OT Exposure version. Examples:

    - For a single asset: TOTS_Rouge_3.19.15_2024-06-03T07_05_27.tar.gz
    - For multiple assets: TOTS_AssetsReport_3.19.15_2024-06-03T07_17_54.tar.gz

4. Extract the diagnostics report and share it with Tenable Support for further analysis.

Tenable Security Center

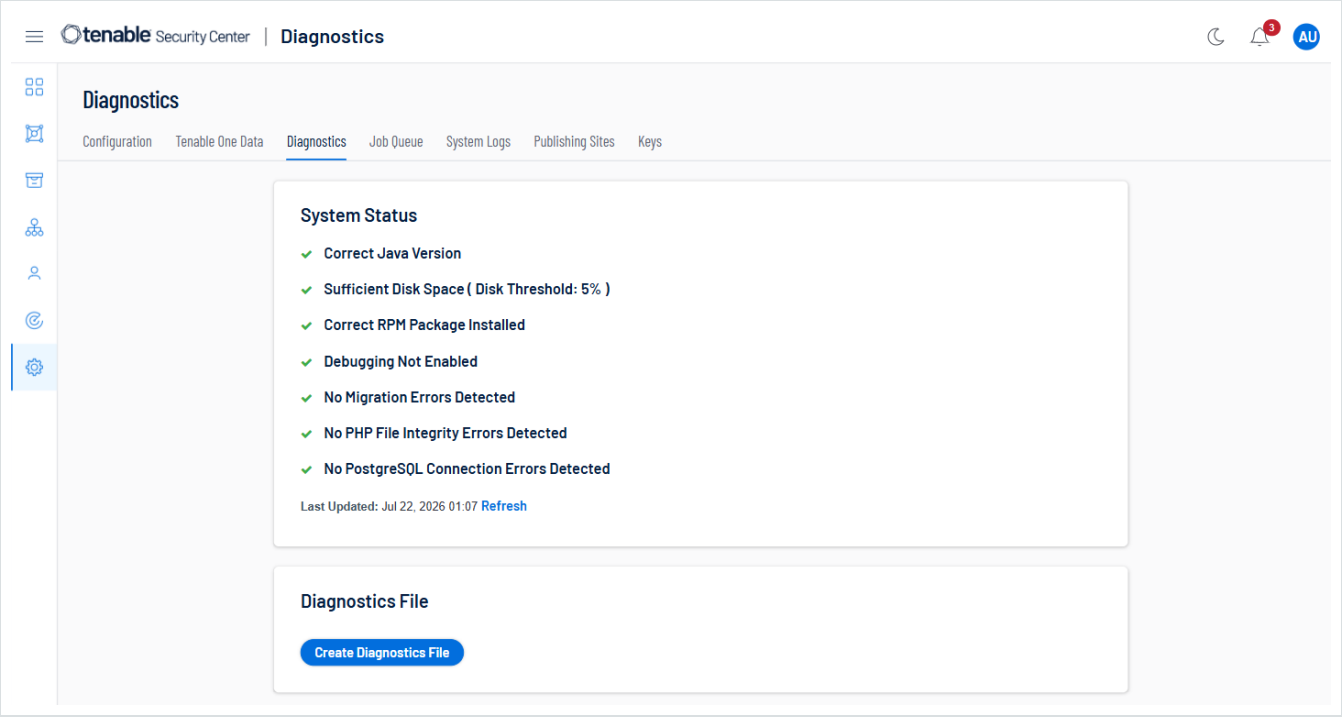
Collect Diagnostics File

Use this section when troubleshooting software crashes, service failures, or installation errors.

To collect a diagnostics file for Tenable Security Center:

1. In the left navigation, click **System** > **Diagnostics**.

   The **Diagnostics** page appears.



2. In the **Diagnostics File** section, click **Create Diagnostics File**.

   The page updates with configuration options.

3. In the **General** section, if you want to omit IP addresses from the file, enable **Strip IPs from Chapters**.
4. In the **Chapters** section, enable the chapters you want to include.
5. Click **Generate File**.
6. Click **Download Diagnostics File**.
7. Submit the `debug.zip` file to your support case.

Collect Debugging Logs

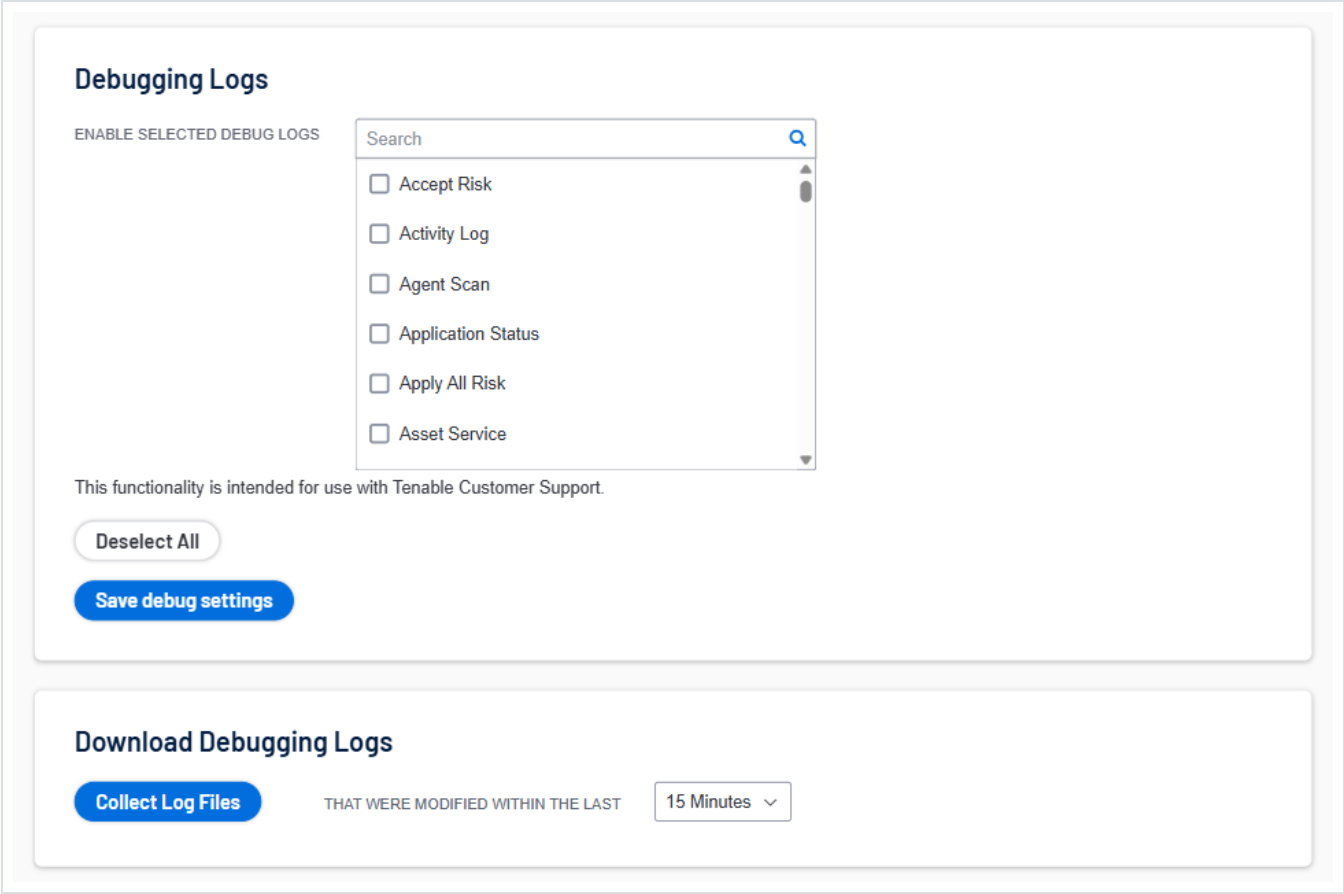
Use this section when troubleshooting software crashes, service failures, or installation errors.

> **Note:** Only enable debugging logs if Tenable Support instructs you to. Disable all debugging settings as soon as troubleshooting is complete to avoid disk and performance issues.

To collect debugging logs for Tenable Security Center:

1. In the left navigation, click **System** > **Diagnostics**.

   The **Diagnostics** page appears.
2. In the **Debugging Logs** section, select the debugging logs Tenable Support asked you to enable.



3. Click **Save Debug Settings**.
4. Reproduce the issue.
5. In the **Download Debugging Logs** section, click **Collect Log Files**.
6. Click **Download Debug File**.
7. Submit the file to your support case, then disable the debugging logs.

Troubleshooting Tenable Security Center Agent Scans

Tenable Security Center cannot run diagnostic Agent scans directly. Because the agent scans are imported as final results, the granular debugging data required for troubleshooting (Plugin Debugging and Audit Trails) is stripped out before it reaches Tenable Security Center.

To troubleshoot issues such as false positives or authentication failures on a Tenable Security Center agent target, you must reproduce the scan on a platform that supports direct agent control (Tenable Nessus Manager or Tenable One Vulnerability Management).

To reproduce the scan:

1. Note the IP address or hostname and the specific policy settings causing the issue in Tenable Security Center.
2. Log in to the Tenable Nessus Manager or Tenable One Vulnerability Management instance where the agent reports.
3. Follow the steps in Tenable Agents for Tenable Agents to enable **Include Audit Trail Data** and **Include KB Data** in the Tenable Nessus Manager settings.
4. Create a scan policy on the Tenable Nessus Manager that matches the settings in Tenable Security Center and run it against the target agent.
5. Once the scan completes, follow the steps in Tenable Agents for Tenable Agents to export the Tenable Nessus DB directly from the Tenable Nessus Manager.
6. Send this Tenable Nessus DB to Tenable Support. The DB contains the diagnostic data that Tenable Security Center could not capture.

Tenable Core

Collect Diagnostics Report

Use this section when troubleshooting software crashes, service failures, or installation errors.

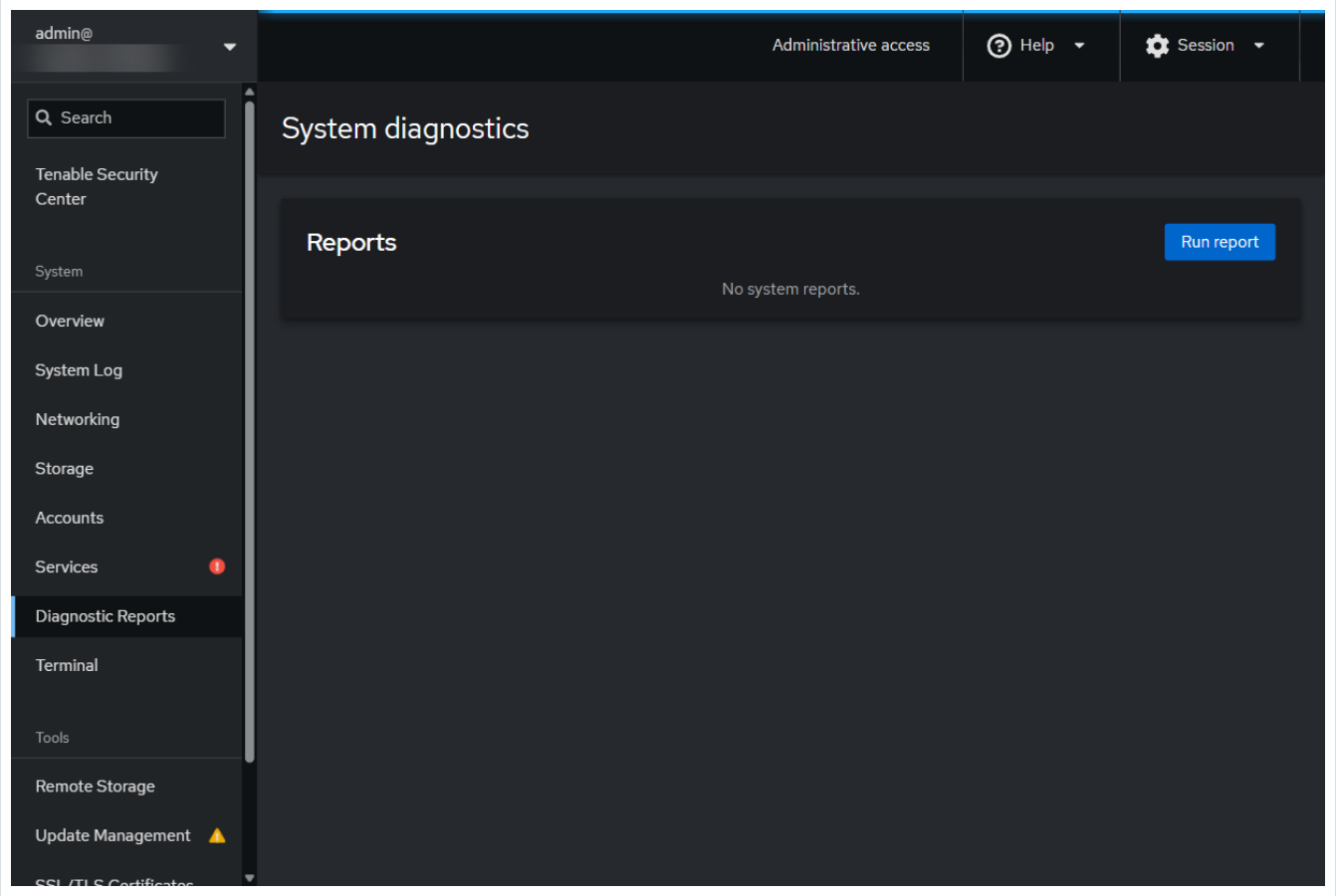
To generate a diagnostic report for troubleshooting:

1. Log in to Tenable Core via the user interface.

   The Tenable Core web user interface page appears.

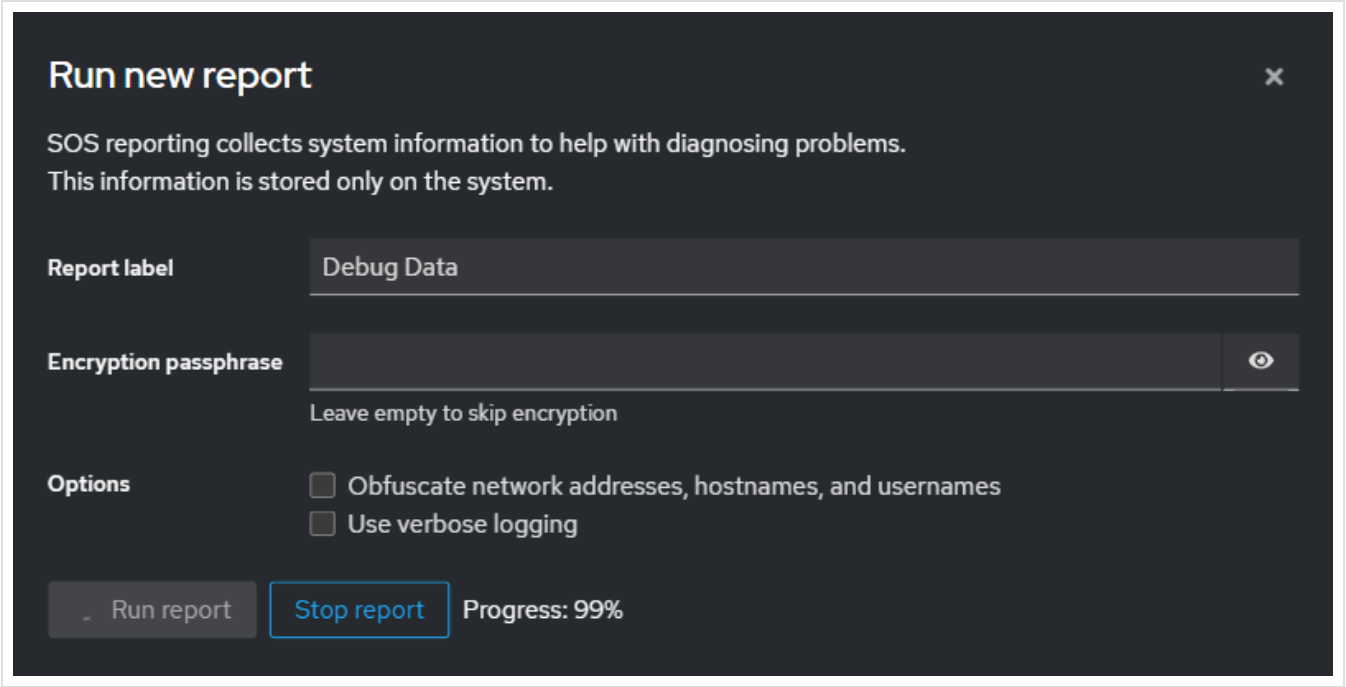
2. In the left navigation bar, click **Diagnostic Reports**.

   The **Diagnostic Reports** page appears.

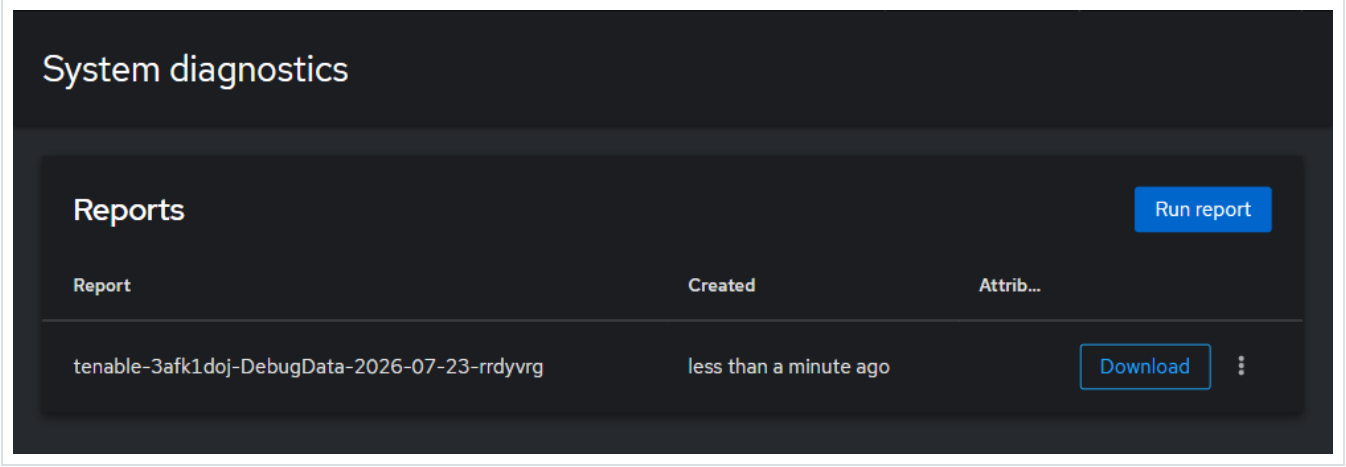


3. Click the **Run report** button.

   A list appears as the report generates.



When the report is complete, the status displays **Done**.



4. Click the **Download** button next to each report that you want to download.

   Note: If you have enabled the setting to password encrypt your downloads, type the password when prompted. You must provide this password to Tenable Support along with the file.

   Tenable Core saves the report.

Note: These steps collect diagnostic information for Tenable Core, not the Tenable product configured with Tenable Core (for example, Tenable Security Center or Tenable Nessus).

Tenable Network Monitor

Collect Debug Logs

Use this section when troubleshooting software crashes, service failures, or installation errors.

To collect Tenable Network Monitor system debug logs on Linux:

- Run the following command:

```
/opt/nnm/bin/debug.sh
```

To collect Tenable Network Monitor system debug logs on Windows:

- Run the following command:

```
C:\Program Files\Tenable\nnm\debug
```