Sensor Proxy 1.x User Guide

Last Revised: July 25, 2023

Table of Contents

Welcome to Sensor Proxy

Sensor Proxy provides an on-prem cache and single point of traffic between Tenable Vulnerability Management and Tenable Nessus Agents or Tenable Nessus scanners. Sensors send communication to Sensor Proxy, not to Tenable Vulnerability Management directly. As a result, large numbers of sensors can communicate with Tenable Vulnerability Management with less bandwidth usage.

To get started with Sensor Proxy, see Get Started.

Get Started

To get started with Sensor Proxy, see the following:

Prepare and Install

1. Requirements: Ensure you meet the requirements to use Sensor Proxy.
2. Install Sensor Proxy: Install Sensor Proxy and link it to Tenable Vulnerability Management.

Link Sensors

- Link Sensors to Sensor Proxy: Link agents and Tenable Nessus scanners to Sensor Proxy.

Uninstall

1. Relink Sensors Directly to Tenable Vulnerability Management: If you want to uninstall Sensor Proxy, you must first remove sensors from Sensor Proxy and link them directly to Tenable Vulnerability Management instead.
2. Uninstall Sensor Proxy: Remove Sensor Proxy from the communication chain between sensors and Tenable Vulnerability Management.

Review Additional Resources

- File Locations
- Troubleshooting

Requirements

To set up Sensor Proxy, ensure you meet the following requirements:

Software Requirements

- Operating system:
  - Oracle Linux 7, 8, and 9
  - CentOS 7
  - RHEL 7, 8, and 9
- Set up Sensor Proxy on your network where sensors can reach it internally and where Sensor Proxy can reach Tenable Vulnerability Management directly with outbound traffic.

> **Note:** Sensor Proxy does not support content delivery network (CDN)-based scan reports from Tenable Nessus Agents.

Hardware Requirements

Scenario	Minimum Recommended Hardware
Sensor Proxy with up to 50,000 sensors	**CPU:** 4 2GHz cores **Memory:** 8 GB RAM **Disk space:** 100 GB
Sensor Proxy with more than 50,000 sensors **Note:** Each instance of Sensor Proxy can support up to 100,000 linked sensors.	**CPU:** 4 2GHz cores **Memory:** 16 GB RAM **Disk space:** 100 GB

> **Note:** Heavy usage of Sensor Proxy can cause the NGINX access log to grow substantially. Tenable recommends setting up log rotation to prevent running out of disk space.

Tenable Products

- You must have a Tenable Vulnerability Management account.
- You must have Tenable Nessus Agents or Tenable Nessus scanners.

Install Sensor Proxy

Before you begin:

- Ensure you meet the Sensor Proxy requirements.
- Download the Sensor Proxy package.

To install Sensor Proxy:

1. Install Sensor Proxy using the following command, replacing the rpm file name with the Sensor Proxy package you downloaded:

   ```
   # rpm -ivh SensorProxy-versionnumber.el7.x86_64.rpm
   ```

   Sensor Proxy takes several minutes to install, and displays a success message when complete.

2. Link Sensor Proxy to Tenable Vulnerability Management using the following command:

   ```
   #  /opt/sensor_proxy/sbin/configure --link --key=<linking key>
   ```

   Use the linking key for the Tenable Vulnerability Management instance you want to link to. For more information, see Retrieve the Tenable Nessus Agent Linking Key in the *Tenable Vulnerability Management Vulnerability Management User Guide*.

3. Enable the Sensor Proxy service.

   ```
   # systemctl enable sensorproxy
   ```

4. Start the Sensor Proxy service.

   ```
   # systemctl start sensorproxy
   ```

What to do next:

- Save the server certificate files in case you need to recover Sensor Proxy.
- Link sensors to Sensor Proxy.

Link Sensors to Sensor Proxy

To use Sensor Proxy, link sensors to Sensor Proxy rather than linking sensors to Tenable Vulnerability Management directly.

The process for linking sensors depends on the sensor and whether the sensor is currently linked or unlinked.

Use the following table to determine how you should link your sensor to Sensor Proxy:

Sensor you want to link to Sensor Proxy	Action
An agent that is already linked to Tenable Vulnerability Management.	Link an already-linked agent to Sensor Proxy.
An agent that is linked to Tenable Nessus Manager or a different Tenable Vulnerability Management container.	Unlink from the manager, then link an unlinked agent to Sensor Proxy.
An agent that is currently unlinked.	Link an Unlinked Agent to Sensor Proxy
A Tenable Nessus scanner that is already linked to either Tenable Vulnerability Management or Tenable Nessus Manager.	Unlink from the manager, then link a Nessus scanner to Sensor Proxy.
A Tenable Nessus scanner that is currently unlinked.	Link a Tenable Nessus Scanner to Sensor Proxy

Link a Currently-Linked Agent to Sensor Proxy

If you have an agent that is currently linked directly to Tenable Vulnerability Management, you can relink the agent to Sensor Proxy to communicate to the same Tenable Vulnerability Management instance.

> **Note:** You do not need the Tenable Vulnerability Management linking key.

> **Note:** If you have two separate Tenable Vulnerability Management instances, you cannot switch an agent to a differentTenable Vulnerability Management instance using the following procedure. Instead, first unlink the agent from the old instance.
>
> If you have an agent that is linked to Tenable Nessus Manager, you cannot relink to Sensor Proxy directly. Instead, unlink the agent first. After your agent is unlinked, see Link an Unlinked Agent to Sensor Proxy.

Before you begin:

- Install Sensor Proxy.

To relink an agent that is currently linked to Tenable Vulnerability Management:

> **Note:** If you relink an agent, the agent restarts. For several minutes after relinking, the agent does not perform scan jobs.

1. On the agent, use the following command.

   ```
   # nessuscli agent relink --host=<Sensor Proxy IP or hostname> --port=443
   ```

   - For `host`, use the Sensor Proxy IP address or hostname.

   The agent is linked and communicates through Sensor Proxy to Tenable Vulnerability Management.

Link an Unlinked Agent to Sensor Proxy

If you have an agent that is unlinked, you can link it to Sensor Proxy to communicate with Tenable Vulnerability Management.

If you have an agent that is linked to a manager besides the Tenable Vulnerability Management instance you want Sensor Proxy to communicate with, you must first unlink the agent before linking the agent to Sensor Proxy.

Tip: To link an agent that is already linked toTenable Vulnerability Management, see Link a Currently-Linked Agent to Sensor Proxy.

Before you begin:

- Install Sensor Proxy.

To link an unlinked agent to Sensor Proxy:

1. If your agent is already linked to a manager other than Tenable Vulnerability Management, unlink it using the following command:

   ```
   # nessuscli agent unlink
   ```

   The agent is unlinked from its manager.

2. On the agent, link to Sensor Proxy using the following command:

   ```
   # nessuscli agent link --key=<linking key> --host=<Sensor Proxy IP or hostname> --port=443
   ```

   - For `key`, use the Tenable Vulnerability Management linking key. For information on retrieving the linking key, see Link a Sensor in the *Tenable Vulnerability Management Vulnerability Management User Guide*.
   - For `host`, use the Sensor Proxy IP address.

   Note: You can add other agent linking options, except for the `--cloud` option. For more information, see Nessuscli Agent in the *Tenable Nessus Agent User Guide*.

Link a Tenable Nessus Scanner to Sensor Proxy

If you have a Tenable Nessus scanner that is already linked to either Tenable Vulnerability Management or Tenable Nessus Manager, you must first unlink the Tenable Nessus scanner.

For unlinked Tenable Nessus scanners, you can link to Sensor Proxy to communicate via Sensor Proxy to Tenable Vulnerability Management.

> **Note:** If you relink a scanner, the scanner restarts. For several minutes after relinking, the scanner does not perform scan jobs.

Before you begin:

- Install Sensor Proxy.

To link a Tenable Nessus scanner to Sensor Proxy:

1. If your Tenable Nessus scanner is already linked to a manager, unlink it using the following command.

   ```
   # nessuscli managed unlink
   ```

   The scanner is unlinked from its manager.

2. Link the scanner to Sensor Proxy using the following command:

   ```
   # nessuscli managed link --key=<linking key> --host=<Sensor Proxy IP or hostname>
   --port=443
   ```

   - Use the linking key for the Tenable Vulnerability Management instance you want to link to. For more information, see Link a Sensor in the *Tenable Vulnerability Management Vulnerability Management User Guide*.
   - For `host`, use the Sensor Proxy IP address.

   > **Note:** (Optional) You can add other Tenable Nessus linking options, except for the `--cloud` option. For more information, see Nessus CLI in the *Tenable Nessus User Guide*.

Upgrade Sensor Proxy

Before you begin:

From the Tenable Downloads Page, download the latest version of Sensor Proxy.

To upgrade Sensor Proxy:

1. Run the following command:

   ```
   # yum upgrade <Sensor Proxy package>
   ```

   Sensor Proxy upgrades to the latest version.

Migrate Sensor Proxy

Migrating Sensor Proxy to a new machine is simple and does not require you to relink agents. You can migrate Sensor Proxy copying the certificates from the existing Sensor Proxy installation to the new server and linking the new Sensor Proxy to Tenable Vulnerability Management.

Follow the steps in this topic to migrate Sensor Proxy to a new machine.

To migrate Sensor Proxy:

1. Perform the following steps on your current Sensor Proxy machine:

    a. Back up the existing certificates by running the following command:

    ```
    # tar -C /usr/local -cvzf sensorproxybackup.tgz etc/nginx/ssl/
    ```

    b. (Optional) Verify that the correct files have been archived by running the following command:

    ```
    # tar -tvzf sensorproxybackup.tgz
    drwxr-xr-x root/root         0 2023-04-18 21:48 etc/nginx/ssl/
    -rw------- root/root      3247 2023-02-13 15:29 etc/nginx/ssl/ca.key
    -rw-rw-rw- root/root      2000 2023-02-13 15:29 etc/nginx/ssl/ca.pem
    -rw------- root/root      3243 2023-02-13 15:29 etc/nginx/ssl/cert.key
    -rw-rw-rw- root/root      1976 2023-02-13 15:29 etc/nginx/ssl/cert.pem
    ```

    c. Copy the backup archive to a safe location or to the new Sensor Proxy machine by running the following command:

    ```
    # scp ~/sensorproxy.tgz <user>@<ip address>:
    ```

    d. Do one of the following:

    - If your sensors are linked via IP address:

Decommission the existing Sensor Proxy. Once the existing Sensor Proxy machine is decommissioned, start the new Sensor Proxy machine with the same IP address as the previous Sensor Proxy machine. Step 2f is optional.

- If your sensors are linked via hostname:

  Step 2f is required. Continue to step 2a.

2. Perform the following steps on the new Sensor Proxy machine:

   a. Install the latest Sensor Proxy rpm from https://www.tenable.com/downloads/sensor-proxy by running the following command:

   ```
   # rpm -ivh SensorProxy-1.0.7-00.el8.x86_64.rpm
   ```

   b. Copy the backup file to the new Sensor Proxy machine by running the following command:

   ```
   # scp sensorproxy.tgz <user>@<ip address>:
   ```

   The new server must have the same IP as the old server if sensors are linked to Sensor Proxy using IP addresses.

   c. Extract the backup archive on the new machine by running the following command:

   ```
   # tar xvzf sensorproxybackup.tgz -C /usr/local/
   ```

   d. Link the new Sensor Proxy to Tenable Vulnerability Management by running the following command:

   ```
   /opt/sensor_proxy/sbin/configure -link -key=<linking key>
   ```

   e. Enable and start the `sensorproxy` service by running the following commands:

   ```
   systemctl enable sensorproxy
   systemctl start sensorproxy
   ```

f. If your sensors are linked to Sensor Proxy using a hostname, change the DNS for the hostname. Agents connect to the new Sensor Proxy machine as DNS changes propogate.

Agents connect to the new Sensor Proxy instance as they check for jobs and updates.

Remove Sensor Proxy

To remove Sensor Proxy, see the following:

- Relink Sensors Directly to Tenable Vulnerability Management
- Uninstall Sensor Proxy

Relink Sensors Directly to Tenable Vulnerability Management

If you uninstall Sensor Proxy, you remove it from the communication chain between sensors and Tenable Vulnerability Management. Therefore, before you uninstall Sensor Proxy, you must first relink sensors directly to Tenable Vulnerability Management. Otherwise, the sensors cannot communicate with Tenable Vulnerability Management.

To relink an agent (7.5 and later) directly to Tenable Vulnerability Management:

For agents running version 7.5 and later, you can relink the agent directly to Tenable Vulnerability Management and remove Sensor Proxy from the communication chain. You do not need the Tenable Vulnerability Management linking key.

- On the agent, use the following command:

  ```
  # nessuscli agent relink --host=sensor.cloud.tenable.com --port=443
  ```

  The agent unlinks from Sensor Proxy and relinks to Tenable Vulnerability Management directly.

To relink an agent (7.4 and earlier) to Tenable Vulnerability Management:

For agents running 7.4 and earlier, you must first unlink the agent from Sensor Proxy.

1. On the agent, use the following command:

   ```
   # nessuscli agent unlink
   ```

   The agent unlinks from Sensor Proxy.

2. Relink the agent directly to Tenable Vulnerability Management, as described in Link a Sensor in the *Tenable Vulnerability Management Vulnerability Management User Guide*.

To relink a Tenable Nessus scanner to Tenable Vulnerability Management:

1. On the Tenable Nessus scanner, use the following command:

   ```
   # nessuscli managed unlink
   ```

   The scanner unlinks from Sensor Proxy.

2. Relink the scanner directly to Tenable Vulnerability Management, as described in Link a Sensor in the *Tenable Vulnerability Management Vulnerability Management User Guide*.

What to do next:

- (Optional) Uninstall Sensor Proxy

Uninstall Sensor Proxy

If you uninstall Sensor Proxy, you remove it from the communication chain between sensors and Tenable Vulnerability Management.

Caution: Before you uninstall Sensor Proxy, you must first relink sensors directly to Tenable Vulnerability Management. Otherwise, the sensors cannot communicate with Tenable Vulnerability Management.

Before you begin:

- Relink sensors directly to Tenable Vulnerability Management.

To uninstall Sensor Proxy:

1. Unlink Sensor Proxy using the following command:

   ```
   # /opt/sensor_proxy/sbin/configure --unlink
   ```

   Sensor Proxy unlinks from Tenable Vulnerability Management.

2. Uninstall Sensor Proxy using the following command:

   ```
   # rpm -evh SensorProxy
   ```

   Sensor Proxy uninstalls.

Additional Resources

For additional information, see the following:

- File Locations
- Troubleshooting

File Locations

The following are the locations of important logs and files.

- **`/opt/sensor_proxy`** - The directory that contains the Sensor Proxy files.
- **`/usr/local/etc/nginx/ssl`** - Contains server certificates for encrypting the connection between sensors and Sensor Proxy. If you do not use your own certificates, Sensor Proxy generates self-signed certificates with a 10 year expiration.

  The following are the server certificate files:

  - `/usr/local/etc/nginx/ssl/ca.key`
  - `/usr/local/etc/nginx/ssl/ca.pem`
  - `/usr/local/etc/nginx/ssl/cert.key`
  - `/usr/local/etc/nginx/ssl/cert.pem`

  > **Tip**: Tenable recommends backing up these files in case you need to recover Sensor Proxy.

- **`/opt/sensor_proxy/nginx/logs/access.log`** - The NGINX access log, which Sensor Proxy causes to grow substantially.

  > **Tip**: Tenable recommends setting up log rotation to prevent running out of disk space.

- **`/opt/sensor_proxy/logs`** - Location of the Sensor Proxy log files.
  - `sidecar.log` - Logs for the configuration and communication between Sensor Proxy and Tenable Vulnerability Management.
  - `sensorproxy.err` - Error output from monitoring the Sensor Proxy processes.
  - `sensorproxy.out` - Non-error output from monitoring the Sensor Proxy processes.

Troubleshooting

Sensor Proxy Recovery

Scenario:

There was a problem with your Sensor Proxy and you need to install a new Sensor Proxy to allow your sensors to continue communicating with Tenable Vulnerability Management.

Solution:

Sensors that were linked via Sensor Proxy can continue communicating with Tenable Vulnerability Management if:

- the sensors can reach the new Sensor Proxy on the same hostname or IP address as the original Sensor Proxy.
- the new Sensor Proxy is using the same certificates as the original Sensor Proxy.

Do the following:

1. Install the new Sensor Proxy on the same hostname or IP address.
2. Copy the server certificate files that you previously backed up from your initial installation of Sensor Proxy to the same location in the new Sensor Proxy.
3. Start Sensor Proxy.