Sensor Proxy 1.x User Guide

Last Revised: October 15, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Sensor Proxy **5**

Get Started 5

Prepare and Install 5

Link Sensors 5

Uninstall 6

Review Additional Resources 6

Requirements 6

Software Requirements 6

Hardware Requirements 6

Port Requirements 7

Inbound Traffic 8

Outbound Traffic 8

Tenable Products 8

Install Sensor Proxy **9**

Link Sensors to Sensor Proxy **11**

Link a Tenable Agent to Sensor Proxy 11

Link a Tenable Nessus Scanner to Sensor Proxy 12

Link a Tenable One Web App Scanning Scanner to Sensor Proxy 13

Link a Tenable One Web App Scanning Docker Image Scanner 14

Link a Tenable Core + Web Application Scanning Scanner 14

Relink Sensors **15**

Relink a Tenable Agent 16

Relink a Tenable Nessus Scanner 16

Upgrade Sensor Proxy **17**

Migrate Sensor Proxy **18**

Uninstall Sensor Proxy **22**

Certificate Authority Rotation 22

Requirements and Considerations 23

Rotate the Certificate Authority 24

Configure FIPS Mode 26

Configure Sensor Proxy to Use a Third-Party HTTP Proxy 27

Configure Tenable Agent Fallback 28

Deployment Recommendations for Ephemeral Agents 30

Reduce Agent Accumulation 31

Unlink Agents Before Decommissioning 31

Check Linked Agent Count 32

File Locations 32

Identification Files 34

Prerequisites for Linking Sensor Proxy to Tenable Security Center 34

Prepare for Linking 36

(Optional) Gather Information 38
Determine the Origin of Your Tenable Security Center Server Certificate 38
Determine the Creation Date of Your Tenable Security Center Server Certificate 39
Ensure Your Tenable Core Server Certificate Matches One of Your Trusted Certificate Authorities 39
Troubleshooting 40
Check Sensor Proxy Status 40
Scenario 40
Solution 40
Steps 40
Recover Sensor Proxy 41
Scenario 41
Solution 41
Steps 41

Welcome to Sensor Proxy

Last Updated: October 15, 2026

Sensor Proxy provides an on-premises cache and single point of traffic between Tenable Agents and Tenable Nessus scanners to Tenable One Vulnerability Management or Tenable One Web App Scanning scanners to Tenable Security Center. Sensors send communication to Sensor Proxy, not to Tenable One Vulnerability Management or Tenable Security Center directly. As a result, large numbers of sensors can communicate with Tenable One Vulnerability Management or Tenable Security Center with less bandwidth usage. Additionally, Sensor Proxy alleviates overall network traffic by caching agent plugins and updates and distributing differential agent updates.

> **Note:** Tenable Security Center 6.5 only supports Sensor Proxy linked with Tenable One Web App Scanning scanners. Tenable Nessus scanners and Tenable Agents are currently unsupported. Tenable One Vulnerability Management supports Sensor Proxy linked with all sensors except Tenable One Web App Scanning scanners.

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 One Vulnerability Management or Tenable Security Center.

Link Sensors

- Link Sensors to Sensor Proxy – Link Tenable Agents, Tenable Nessus scanners, and Tenable One Web App Scanning scanners to Sensor Proxy.

Uninstall

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

Review Additional Resources

- Additional Resources

Requirements

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

Software Requirements

- Supported operating systems:
  - Oracle Linux 8 and 9
  - Red Hat Enterprise 8 and 9
  - Tenable Core
- Set up Tenable Sensor Proxy on your network where sensors can reach it internally and where Tenable Sensor Proxy can reach Tenable One Vulnerability Management or Tenable Security Center directly with outbound traffic.

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

Hardware Requirements

Scenario	Minimum Recommended Hardware
Tenable Sensor Proxy with up to 50,000 sensors connected to Tenable One Vulnerability Management	**CPU** – 4 2GHz cores **Memory** – 8 GB RAM **Disk space** – 100 GB
Tenable Sensor Proxy with more than 50,000 sensors connected to Tenable One Vulnerability Management **Note:** Each instance of Tenable Sensor Proxy can support up to 100,000 linked sensors.	**CPU** – 4 2GHz cores **Memory** – 16 GB RAM **Disk space** – 100 GB
Tenable Sensor Proxy with up to 250 Tenable One Web App Scanning scanners connected to Tenable Security Center	**CPU** – 4 2GHz cores **Memory** – 16 GB RAM **Disk space** – 100 GB

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

Port Requirements

Sensor Proxy requires access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 22	Provides administrative SSH access for OS-level maintenance.
TCP 443	Communication to Sensor Proxy from Tenable sensors.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 8837	Communication from Sensor Proxy to Tenable Security Center.
TCP 443	Communication from Sensor Proxy to Tenable One Vulnerability Management.

Tenable Products

- You must have a Tenable One Vulnerability Management account or a Tenable Security Center account.
- For Tenable One Vulnerability Management, you must have Tenable Agents or Tenable Nessus scanners. For Tenable Security Center, you must have Tenable One Web App Scanning 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:

   ```
   # dnf install SensorProxy-<version number>.<os>.<architecture>.rpm
   ```

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

2. Link Sensor Proxy to either Tenable One Vulnerability Management or Tenable Security Center:

   - **Link to Tenable One Vulnerability Management**

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

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

     For `key`, use the Tenable One Vulnerability Management linking key. For information on retrieving the linking key, see Link a Sensor in the *Tenable One Vulnerability Management Vulnerability Management User Guide*.

     > **Note:** The `--name` argument is optional. If no name is provided, the name defaults to *Sensor Proxy*.

- **Link to Tenable One Vulnerability Management FedRAMP**

  Link Sensor Proxy to Tenable One Vulnerability Management FedRAMP using the following command:

  ```
  # /opt/sensor_proxy/sbin/configure --link --key=<linking key> --host=fedcloud.tenable.com --
  name=<name>
  ```

  For `key`, use the Tenable One Vulnerability Management linking key. For information on retrieving the linking key, see Link a Sensor in the *Tenable One Vulnerability Management User Guide*.

  > **Note:** The `--name` argument is optional. If no name is provided, the name defaults to *Sensor Proxy*.

- **Link to Tenable Security Center**

  Link Sensor Proxy to Tenable Security Center using the following command:

  ```
  # /opt/sensor_proxy/sbin/configure --link --key=<linking_key> --host=<linking_host> --
  port=8837 --ca-path=</path/to/security_center_CA> [--name=<sensor_proxy_name>]
  ```

  For `key`, use the Tenable Security Center linking key. For `ca-path`, use the standard Tenable Security Center CA certificate file and path (**/opt/sc/data/CA/TenableCA.crt**) or, if applicable, your organization's customer certificate and path.

  For information on adding Sensor Proxy to Tenable Security Center, see Sensor Proxies the *Tenable Security Center User Guide*.

  > **Note:** The `--name` argument is optional. If no name is provided, the name defaults to `Sensor Proxy`.

3. Enable and start the Sensor Proxy service by running the following command:

   ```
   # systemctl enable --now sensorproxy
   ```

> **Tip:** If you have trouble linking Sensor Proxy to Tenable Security Center, see Prerequisites for Linking Sensor Proxy to Tenable Security Center for troubleshooting information.

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 One Vulnerability Management or Tenable Security Center directly.

> **Note:** Tenable Security Center 6.5 only supports Sensor Proxy linked with Tenable One Web App Scanning scanners. Tenable Nessus scanners and Tenable Agents are currently unsupported. Tenable One Vulnerability Management supports Sensor Proxy linked with all sensors except Tenable One Web App Scanning scanners.

The process for linking sensors varies depending on the sensor type.

Link a Tenable Agent to Sensor Proxy

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

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

If you have an agent that is already linked to Tenable One Vulnerability Management but want it to route through Sensor Proxy, you must relink the agent using the Sensor Proxy host and port. You can either use the `nessuscli agent relink` command or unlink the agent and then link it to Sensor Proxy.

Before you begin:

- Install Sensor Proxy.

To link an agent to Sensor Proxy:

1. If your agent is already linked to a manager other than Tenable One Vulnerability Management, unlink it using the following command. If your agent is already linked to Tenable One Vulnerability Management but not through Sensor Proxy, skip to step 2 and use `nessuscli agent relink` instead of `nessuscli agent link`.

   ```
   # 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 One Vulnerability Management linking key. For information on retrieving the linking key, see Link a Sensor in the *Tenable One 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 Agent User Guide*.

   Note: If the agent is already linked to Tenable One Vulnerability Management, use the following command to relink it to Sensor Proxy without unlinking first:

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

Link a Tenable Nessus Scanner to Sensor Proxy

If you have a Tenable Nessus scanner that is already linked to either Tenable One 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 One 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
   ```

   - For `key`, use the Tenable One Vulnerability Management linking key. For information on retrieving the linking key, see Link a Sensor in the *Tenable One 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*.

Link a Tenable One Web App Scanning Scanner to Sensor Proxy

Sensor Proxy supports two types of Tenable One Web App Scanning scanners: those deployed from the Tenable One Web App Scanning Docker image and those deployed with Tenable Core + Web App Scanning.

> **Note:** Tenable One Web App Scanning scanners linked to Sensor Proxy are only supported with Tenable Security Center.

Before you begin:

- Install Sensor Proxy.

Link a Tenable One Web App Scanning Docker Image Scanner

1. Access the Tenable One Web App Scanning Docker image at https://hub.docker.com/r/tenable/was-scanner.
2. Run the following command to start the Docker container:

   ```
   docker run -d -e WAS_SCANNER_NAME=<my_scanner> -e WAS_LINKING_KEY=<my_linking_key> -e WAS_PLATFORM_URL=<sensor_proxy_url> tenable/was-scanner
   ```

   Replace <*my_scanner*> with a unique scanner name, replace <*my_linking_key*> with your linking key, and replace <*sensor_proxy_url*> with the URL of the Sensor Proxy the scanner will be linked to.

For more information about the Tenable One Web App Scanning Docker image, see Deploy Tenable Web App Scanning as a Docker Image in the *Tenable One Web App Scanning User Guide*.

Link a Tenable Core + Web Application Scanning Scanner

1. Download the Tenable Core + Web Application Scanning installer from the Tenable Core download page.
2. Install Tenable Core + Web Application Scanning.

3. From the Tenable Core + Web Application Scanning **Overview** page, click **Web Application Scanner** in the left-side navigation pane.

   The **Web Application Scanner** page appears.

4. Click ☑ next to **Tenable Management Platform URL**.

   A window appears.

5. Enter the following information:

   - **Linking Key** – The linking key from your Tenable Security Center instance. For more information, see Sensor Proxies the *Tenable Security Center User Guide*.
   - **Scanner Name** – The name of the scanner that you want to appear in Tenable Security Center.
   - **Tenable Management URL** – The URL of your Sensor Proxy instance (`https://<sensor_proxy_host>`).
   - **Connect Using Proxy** – Leave this unselected.

6. Click **Activate Scanner**.

   A success message appears and your Tenable One Web App Scanning scanner appears in the scanner list on Tenable Security Center.

For more information about Tenable Core + Web App Scanning, see the Tenable Core + Web App Scanning User Guide.

Relink Sensors

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

Note: If you are connecting to Tenable One Vulnerability Management through Tenable Nessus scanners or Tenable Agents located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

Note: Tenable Security Center 6.5 only supports Sensor Proxy linked with Tenable One Web App Scanning scanners. Tenable Nessus scanners and Tenable Agents are currently unsupported. Tenable One Vulnerability Management supports Sensor Proxy linked with all sensors except Tenable One Web App Scanning scanners.

Relink a Tenable Agent

You can relink the agent directly to Tenable One Vulnerability Management and remove Sensor Proxy from the communication chain. You do not need the Tenable One 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 One Vulnerability Management directly.

Relink a Tenable Nessus Scanner

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

```
# nessuscli managed unlink
```

The scanner unlinks from Sensor Proxy.

2. For Tenable One Vulnerability Management, link the scanner directly as described in Link a Sensor in the *Tenable One Vulnerability Management Vulnerability Management 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 sensors. You can migrate Sensor Proxy by copying the certificates from the existing Sensor Proxy installation to the new server and linking the new Sensor Proxy to Tenable One Vulnerability Management or Tenable Security Center.

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. (This step is not required if the system is a Tenable Core + Sensor Proxy system that already has Sensor Proxy installed and running.) Install the latest Sensor Proxy rpm from https://www.tenable.com/downloads/sensor-proxy by running one of the following commands:

      - **EL8 and EL9**

        ```
        # dnf install SensorProxy-1.x.x-00.elx.x86_64.rpm
        ```

      - **EL7**

        ```
        # yum install SensorProxy-1.x.x-00.elx.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 Sensor Proxy to either Tenable One Vulnerability Management or Tenable Security Center:

- **Link to Tenable One Vulnerability Management**

  Link Sensor Proxy to Tenable One Vulnerability Management by running the following command:

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

  For `key`, use the Tenable One Vulnerability Management linking key. For information on retrieving the linking key, see Link a Sensor in the *Tenable One Vulnerability Management Vulnerability Management User Guide*.

  > **Note:** The `--name` argument is optional. If no name is provided, the name defaults to *Sensor Proxy*.

- **Link to Tenable Security Center**

  Link Sensor Proxy to Tenable Security Center by running the following command:

  ```
  # /opt/sensor_proxy/sbin/configure --link --key=<linking_key> --host=<linking_host> --
  port=8837 --ca-path=</path/to/security_center_CA> [--name=<sensor_proxy_name>]
  ```

  For `key`, use the Tenable Security Center linking key. For `ca-path`, use the standard Tenable Security Center CA certificate file and path (**/opt/sc/data/CA/TenableCA.crt**) or, if applicable, your organization's customer certificate and path.

  For information on adding Sensor Proxy to Tenable Security Center, see Sensor Proxies the *Tenable Security Center User Guide*.

  > **Note:** The `--name` argument is optional. If no name is provided, the name defaults to `Sensor Proxy`.

e. Enable and start the Sensor Proxy service by running the following command:

```
# systemctl enable --now sensorproxy
```

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

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

Uninstall Sensor Proxy

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

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

To uninstall Sensor Proxy:

1. Unlink Sensor Proxy using the following command:

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

   Sensor Proxy unlinks from the manager.

2. Uninstall Sensor Proxy using the following command:

   ```
   # rpm -evh SensorProxy
   ```

   Sensor Proxy uninstalls.

Certificate Authority Rotation

Certificate authority (CA) rotation is a process that allows you to manage and change Sensor Proxy's CA without disrupting existing agent connections. By leveraging specific command line (CLI) flags, you can generate or install new certificates, distribute the updated CA to agents safely, and apply the new server certificates seamlessly.

The CA rotation process occurs in three main stages to ensure continuous connectivity:

1. New certificates (either self-signed or custom) are generated or installed alongside the existing ones in a designated directory. Sensor Proxy then begins distributing the updated CA to all currently connected agents through its standard workflow. New agents connecting via a link will also automatically receive the updated CA.
2. Monitor the migration status using a built-in reporting tool to verify that your active agents have successfully received the new CA.
3. Once you confirm your active agents are updated, you rotate the certificates. This action moves the old certificates to a timestamped backup directory and applies the new server certificates for immediate use.

Rotating your CA is a critical security practice. This feature ensures that you can perform necessary certificate updates without causing agent disconnects or blind spots in your vulnerability management coverage. By allowing agents to receive and trust the new CA before the server certificates are actually swapped, it guarantees a seamless transition and continuous agent communication.

For instructions on how to rotate the CA, see Rotate the Certificate Authority.

Requirements and Considerations

- You must restart Sensor Proxy after generating or installing new CAs to begin distribution.
- You must restart Sensor Proxy again after the final certificate rotation for the changes to take effect.

  > **Caution:** Do not rotate and apply the new server certificates until the CA report confirms 100% of your agents have the updated CA. After rotation, any agents that have not updated to the latest CA might fail to connect.

- If issues arise after a rotation, you can revert to a previous state by restoring your backed-up certificates. To manually restore them, follow these steps:
  1. Copy the backed-up certificate files from the timestamped directory to the active SSL directory. For example:

```
sudo cp /usr/local/etc/nginx/ssl/certs-<date>-<time>/*
/usr/local/etc/nginx/ssl/
```

2. Restart Sensor Proxy to apply the restored certificates by running the following command:

```
sudo systemctl restart sensorproxy
```

Rotate the Certificate Authority

You can use the Sensor Proxy command line interface to rotate your certificate authority (CA) or service certificates without disrupting agent connections. This ensures your agents maintain seamless communication with Sensor Proxy during security updates.

For more information about CA rotation, see Certificate Authority Rotation.

To rotate the CA or server certificates:

1. Generate or install the new certificates:
    - To generate a new server certificate without regenerating the CA, run:

```
/opt/sensor_proxy/sbin/configure -nextCert
```

    - To generate both the new self-signed CA and server certificates, run:

```
/opt/sensor_proxy/sbin/configure -nextCert -appendCA
```

    - To install custom certificates, run:

```
/opt/sensor_proxy/sbin/configure -installCert -ca <path/to/custom_ca_
certificate> -publicKey <path/to/custom_server_certificate_public> -
privateKey <path/to/custom_server_certificate_private>
```

2. Restart Sensor Proxy to begin distributing the new CA to connected agents Run the following command:

```
sudo systemctl restart sensorproxy
```

3. Monitor the CA rotation status to verify agents receive the new CA by running:

```
/opt/sensor_proxy/sbin/configure -agent-ca-report
```

   - (Optional) To export details of all agents, use the `-export-all-agents` flag. By default, this flag exports data in JSON format.
   - (Optional) To export details of agents that have not yet migrated, use the `-export-agents-not-migrated` flag. flag. By default, this flag exports data in JSON format.

     Note: You can use the `-export-all-agents` and `-export-agents-not-migrated` flags with or without the `-agent-ca-report` flag.

   - (Optional) If you set the `-export-all-agents` or `-export-agents-not-migrated` flag, you can append `-force-pull-agentdata` to force an immediate data pull from Tenable One Vulnerability Management instead of waiting for the standard 12-hour interval.
   - (Optional) If you set the `-export-all-agents` or `-export-agents-not-migrated` flag, you can append `-csv` to export the report data to a CSV file instead of the default JSON format.

4. Review the output to verify that your active agents have updated to the latest CA. Based on your active agent status, decide whether you are ready to proceed with the certificate rotation.

   Caution: Do not rotate and apply the new server certificates until the CA report confirms 100% of your agents have the updated CA. After rotation, any agents that have not updated to the latest CA might fail to connect.

5. Apply the new server certificates and automatically back up the old ones by running:

```
/opt/sensor_proxy/sbin/configure -rotateCert
```

6. Restart Sensor Proxy to finalize the rotation and use the newly applied certificates.

Configure FIPS Mode

You can enable or disable the Federal Information Processing Standard (FIPS) mode on Tenable Sensor Proxy from the command line. Tenable Sensor Proxy mirrors the FIPS mode setting of the underlying operating system.

For more information about FIPS mode, refer to the FIPS 140-2 Compliance in Oracle Linux 8 topic in the Oracle documentation.

Note: Tenable recommends that you discuss with your organization's system auditor any further questions about FIPS mode operation or compliance.

Note: Tenable Sensor Proxy versions earlier than 1.2.0 do not support FIPS mode. FIPS mode is not supported in Enterprise Linux 7 environments.

To enable or disable FIPS mode:

1. Open your command line tool of choice.
2. (Optional) View the current state of FIPS mode by running the following command:

   ```
   fips-mode-setup --check
   ```

3. Run one of the following commands to enable or disable FIPS mode:
   - To enable FIPS mode, run:

     ```
     fips-mode-setup --enable
     reboot
     ```

   - To disable FIPS mode, run:

```
fips-mode-setup --disable
reboot
```

Tenable Sensor Proxy updates according to the new FIPS mode setting.

Configure Sensor Proxy to Use a Third-Party HTTP Proxy

Sensor Proxy supports integration with third-party HTTP proxy servers, allowing all outbound sensor traffic to be routed through a custom-designated proxy. This enhancement enables your organization to comply with internal security policies that require all outbound network communications to pass through a centralized proxy.

With this feature, you can:

- Configure Sensor Proxy to send all outbound traffic through your organization's approved third-party HTTP proxy.
- Simplify network and firewall management by centralizing sensor communications.
- Maintain compliance with enterprise security requirements and regulatory standards.

Note: Sensor Proxy only supports basic authentication for third-party proxy connections.

To enable Sensor Proxy to use a third-party HTTP proxy:

1. Do one of the following:
   - Create the `proxy.env` file as a symlink by running the following command:

     ```
     ln -s </path/to/your/envfile> /opt/sensor_proxy/config/proxy.env
     ```

   - Create the `/opt/sensor_proxy/config/proxy.env` file, directly add your proxy environment variables following your organization's procedures, and save the file.

     The following lines are examples of custom proxy environment variables in `proxy.env`:

```
https_proxy="http://username:password@tenableproxy.example.com:3128"
no_proxy="localhost,127.0.0.1"
```

Note: You must URL-encode any special characters in the username or password for proxy environment variables, as Sensor Proxy reads these values as URLs.

2. Restart Sensor Proxy and apply your changes by running the following command:

```
systemctl restart sensorproxy
```

To disable third-party HTTP proxy support in Sensor Proxy:

1. Do one of the following:
   - Remove the symlink from `proxy.env` by running the following command:

     ```
     rm /opt/sensor_proxy/config/proxy.env
     ```

   - Open `proxy.env`, comment out or remove your proxy environment variables following your organization's procedures, and save the file.
2. Restart Sensor Proxy and apply your changes by running the following command:

```
systemctl restart sensorproxy
```

Configure Tenable Agent Fallback

In Tenable Sensor Proxy version 1.0.10 and later, you can configure linked Tenable Agents to fall back and connect directly to Tenable One Vulnerability Management if the agents cannot properly connect to Tenable Sensor Proxy. Agent fallback allows agents to remain online and continue scanning in the event of connectivity issues with Tenable Sensor Proxy.

Once an agent is connected to Tenable One Vulnerability Management via fallback, it attempts to reconnect with Tenable Sensor Proxy every 15 minutes.

Agent fallback is disabled by default, but you can enable the fallback setting in the Sensor Proxy `sidecar.json` file.

To configure agent fallback:

1. In your system file manager, navigate to `/opt/sensor_proxy/config/`.
2. Open `sidecar.json`.
3. Between the **SidecarTokenFile** and **AgentAgeOutDays** lines, enter a new line.

```
{
"Version": "1.0.10",
"Port": 8080,
"MeasurementsEnabled": false,
"MetricsPort": ":4242",
"Logfile": "/opt/sensor_proxy/logs/sidecar.log",
"Loglevel": "info",
"LogStdout": false,
"LogDefaultContext": "[service]",
"Upstream": "sensor.cloud.tenable.com",
"DBFile": "/opt/sensor_proxy/cacheDb.db",
"CAPemFile": "/usr/local/etc/nginx/ssl/ca.pem",
"CAKeyFile": "/usr/local/etc/nginx/ssl/ca.key",
"CertPemFile": "/usr/local/etc/nginx/ssl/cert.pem",
"CertKeyFile": "/usr/local/etc/nginx/ssl/cert.key",
"NGINX_port": 443,
"SidecarName": "Sidecar",
"SidecarTokenFile": "/etc/sensor-proxy-token",

"AgentAgeOutDays": 21
}
```

4. In the new line, enter the following information to enable agent fallback:

```
"OverrideFallback": true,
```

The JSON file should now look as follows:

```
{
"Version": "1.0.10",
"Port": 8080,
"MeasurementsEnabled": false,
"MetricsPort": ":4242",
"Logfile": "/opt/sensor_proxy/logs/sidecar.log",
"Loglevel": "info",
"LogStdout": false,
"LogDefaultContext": "[service]",
"Upstream": "sensor.cloud.tenable.com",
"DBFile": "/opt/sensor_proxy/cacheDb.db",
"CAPemFile": "/usr/local/etc/nginx/ssl/ca.pem",
"CAKeyFile": "/usr/local/etc/nginx/ssl/ca.key",
"CertPemFile": "/usr/local/etc/nginx/ssl/cert.pem",
"CertKeyFile": "/usr/local/etc/nginx/ssl/cert.key",
"NGINX_port": 443,
"SidecarName": "Sidecar",
"SidecarTokenFile": "/etc/sensor-proxy-token",
"OverrideFallback": true,
"AgentAgeOutDays": 21
}
```

Alternatively, you can delete the **OverrideFallback** line to disable agent fallback.

5. Save your file changes.
6. Restart Tenable Sensor Proxy to apply the change.

Deployment Recommendations for Ephemeral Agents

Environments that deploy and decommission agents frequently (for example, auto-scaling groups, CI/CD runners, or containerized workloads) require additional configuration to prevent inactive agent records from accumulating in Tenable Sensor Proxy.

Reduce Agent Accumulation

By default, Tenable Sensor Proxy retains inactive agents for 21 days. If retained agent tokens exceed Tenable One Vulnerability Management's 100,000-token limit, bulk polling requests fail and active agents cannot retrieve jobs.

> **Note:** In Tenable Sensor Proxy 1.4.0 and later, agent data is automatically deleted when an agent is unlinked. However, ephemeral agents do not always unlink cleanly–for example, due to a network outage, pod crash, or forced termination. In those cases, the agent record persists until it ages out, so you should still configure a shorter age-out interval.

To reduce this risk, lower the `AgentAgeOutDays` value in `/opt/sensor_proxy/config/sidecar.json`. This process requires root access.

To configure agent age-out:

1. In your system file manager, navigate to `/opt/sensor_proxy/config/`.
2. Open `sidecar.json`.
3. Set `AgentAgeOutDays` to a value lower than the default of 21. For example:

   ```
   "AgentAgeOutDays": 7
   ```

4. Save your file changes.
5. Restart Tenable Sensor Proxy to apply the change.

Unlink Agents Before Decommissioning

For best performance, unlink agents before decommissioning them. When an agent unlinks cleanly, Tenable Sensor Proxy 1.4.0 and later automatically deletes the agent data immediately rather than waiting for the age-out interval to expire.

To unlink an agent as part of your teardown process, run the following command on the agent host before shutting it down:

```
/opt/nessus_agent/sbin/nessuscli agent unlink
```

If you manage ephemeral infrastructure with orchestration tools (such as Kubernetes, Terraform, or auto-scaling groups), add the unlink command to your pre-stop or shutdown hook.

Note: If an agent cannot unlink cleanly (for example, due to a crash or network partition), the agent record remains in Tenable Sensor Proxy until the `AgentAgeOutDays` interval expires. Configure a shorter age-out value to handle these cases.

Check Linked Agent Count

To verify the number of retained agent records in Tenable Sensor Proxy, run the following command:

```
/opt/sensor_proxy/sbin/configure -agent-ca-report
```

Tip: Run this command periodically to confirm that your age-out configuration prevents agent accumulation. If the count continues to grow despite a short age-out interval, verify that agents are unlinking before decommissioning.

- (Optional) To export details of all agents, use the `-export-all-agents` flag. By default, this flag exports data in JSON format.
- (Optional) If you set the `-export-all-agents` flag, you can append `-force-pull-agentdata` to force an immediate data pull from Tenable One Vulnerability Management instead of waiting for the standard 12-hour interval.
- (Optional) If you set the `-export-all-agents` flag, you can append `-csv` to export the report data to a CSV file instead of the default JSON format.

File Locations

The following are the locations of important logs and files:

Location	Purpose
`/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 recoverSensor 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`	Contains Sensor Proxy log files: • `sidecar.log` – Logs for the configuration and communication between Sensor Proxy and Tenable One Vulnerability Management. • `sensorproxy.err` – Error output from monitoring the Sensor Proxy processes.

	• `sensorproxy.out` – Non-error output from monitoring the Sensor Proxy processes.

Identification Files

Sensor Proxy has two identification files:

Identification File	Description

UUID	Sensor Proxy creates the UUID and saves it to `/etc/sensor-proxy-uuid` when you start the Sensor Proxy service for the first time. You can also find the UUID in `/opt/sensor_proxy/logs/sidecar.log`:
	`2023/12/11 05:47:00.331866 [info] [service] Sensor Proxy is identified by <UUID>`
	`2023/12/11 05:47:00.920269 [info] [link] Linked successfully to http://sensor.cloud.tenable.com`

Authorization token	Sensor Proxy obtains the authorization token from Tenable One Vulnerability Management or Tenable Security Center when Sensor Proxy successfully links to it and saves the token to `/etc/sensor-proxy-token`. **Note:** Whether a Tenable Agent or Tenable Nessus scanner links directly to Tenable One Vulnerability Management or to a Sensor Proxy, they similarly obtain and store an authorization token in the secure preferences database (`nessus-fetch.db`). When linking to a Sensor Proxy, they obtain the token from the Sensor Proxy.

Prerequisites for Linking Sensor Proxy to Tenable Security Center

To successfully link standalone or Tenable Core instances of Sensor Proxy to Tenable Security Center, your Tenable Security Center SSL/TLS certificate must meet certain requirements.

To determine if the current Tenable Security Center certificates meet those requirements, use the following procedure:

1. Log in to the Sensor Proxy or Tenable Security Center system via SSH.
2. Run one of the following commands, depending on which system you are logged into:
    - Sensor Proxy system

      ```
      openssl s_client -connect <securitycenter_hostname_or_ip>:443 < /dev/null 2> /dev/null | openssl x509 -noout -text | grep -A 1 'Subject Alternative’
      ```

    - Tenable Security Center system

      ```
      openssl x509 -noout -text -in /opt/sc/support/conf/SecurityCenter.crt | grep -A 1 'Subject Alternative Name'
      ```

3. Depending on what command output you see, proceed in one of the following ways:
    - If no output is shown when you run the command, see Regenerate the Tenable Security Center Server Certificate in the *Tenable Security Center User Guide* and regenerate the server certificate. After you regenerate the server certificate, proceed to Prepare for Linking.
    - If output like the following is shown but neither the hostname nor the IP address shown match the FQDN or IP address of the Tenable Security Center system, see Regenerate the Tenable Security Center Server Certificate in the *Tenable Security Center User Guide* and regenerate the server certificate.

      ```
      X509v3 Subject Alternative Name:
      DNS:sc-host-name, IP Address:10.10.10.10
      ```

      After you regenerate the server certificate, proceed to Prepare for Linking.

- If the output is shown and the hostname and IP address shown match the FQDN or IP address of the Tenable Security Center system, proceed to Prepare for Linking.

Prepare for Linking

Based on details about your organization's Tenable Security Center + Sensor Proxy setup and certificate details, you may need to perform additional checks and steps before or during the Sensor Proxy linking process.

Use the following grid to determine what linking and installation steps you need to take based on your Sensor Proxy installation type, Tenable Security Center installation type, Tenable Security Center certificates, and root CA type. If you need help finding information about your setup and certificate details, see (Optional) Gather Information.

Tenable Security Center Installation Type	Tenable Security Center Certificates	Root CA Type	Linking and Installation Steps to Take
Any Tenable Security Center installation	n/a	Public	Proceed to Install Sensor Proxy (for standalone Sensor Proxy installation/linking) or Configure Tenable Core + Sensor Proxy in Tenable Core (for Tenable Core + Sensor ProxySensor Proxy installation/linking). During either installation/linking process, you do not need to specify a CA path when prompted.

Any Tenable Security Center installation	n/a	Tenable Security Center-generated server certificate	Proceed to Install Sensor Proxy (for standalone Sensor Proxy installation/linking) or Configure Tenable Core + Sensor Proxy in Tenable Core (for Tenable Core + Sensor Proxy installation/linking). During either installation/linking process, you must specify */opt/sc/data/ca/TenableCA.crt* as the CA path.
Non-Tenable Core + Tenable Security Center installations	n/a	Internal or Custom (possibly in `/opt/sc/data/ca`, but with an unknown name)	Proceed to Install Sensor Proxy (for standalone Sensor Proxy installation/linking) or Configure Tenable Core + Sensor Proxy in Tenable Core (for Tenable Core + Sensor Proxy installation/linking). During either installation/linking process, you must specify the custom path to your CA.
Tenable Core + Tenable Security Center installations	n/a	Internal or Custom (possibly on the Tenable Core **Certificate** > **Security Center** tab > **Trusted Certificate Authorities** page)	Proceed to Install Sensor Proxy (for standalone Sensor Proxy installation/linking) or Configure Tenable Core + Sensor Proxy in Tenable Core (for Tenable Core + Sensor Proxy installation/linking).

			During either installation/linking process, you must specify the custom path to your CA.
Tenable Core + Tenable Security Center installations	Created with Tenable Security Center packages with certificate data change	Tenable Core-generated (on the Tenable Core **Certificate** > **Security Center** tab > **Trusted Certificate Authorities** page)	If necessary for your organization, ensure the Tenable Core server certificate matches one of the trusted certificate authorities. Once you have matched the server certificate to a trusted certificated authority, proceed to Install Sensor Proxy (for standalone Sensor Proxy installation/linking) or Configure Tenable Core + Sensor Proxy in Tenable Core (for Tenable Core + Sensor Proxy installation/linking).

(Optional) Gather Information

Determine the Origin of Your Tenable Security Center Server Certificate

1. On the Sensor Proxy system, run the following command:

   ```
   openssl s_client -connect <securitycenter_hostname_or_ip>:443 < /dev/null 2>
   /dev/null | openssl x509 -noout -issuer
   ```

2. On the Tenable Security Center system, run the following command as root/tns:

```
openssl x509 -noout -issuer -in /opt/sc/support/conf/SecurityCenter.crt
```

If the output from either of those commands contains:

- `CN=Locally generated Tenable Core CA`
    - The certificate is Tenable Core-generated.
- `OU = "INSECURE Certificate Authority for Tenable, Inc."`
    - The certificate is Tenable Security Center-generated.
- Other value or values
    - The certificate is publicly or privately generated.

Determine the Creation Date of Your Tenable Security Center Server Certificate

1. On the Sensor Proxy system, run the following command:

    ```
    openssl s_client -connect  <securitycenter_hostname_or_ip>:443 < /dev/null 2>
    /dev/null | openssl x509 -noout -startdate
    ```

2. On the Tenable Security Center system, run the following command as root/tns:

    ```
    openssl x509 -noout -startdate -in /opt/sc/support/conf/SecurityCenter.crt
    ```

    The following is an example of the command output:

    ```
    notBefore=Feb 21 16:38:22 2024 GMT
    ```

Ensure Your Tenable Core Server Certificate Matches One of Your Trusted Certificate Authorities

1. In Tenable Core, click **SSL/TLS Certificates** in the left-side navigation pane.

    The SSL/TLS Certificates page appears.

2. Click **Tenable.sc**.

The Tenable Security Center certificate page appears.

3. Note the **Issuer** and **Issuer Organizational Unit** values in the Server Certificates section.
4. Under Trusted Certificate Authorities, ensure that one of the configured authorities has:
    - A **Subject** that matches the **Issuer** of the server certificate
    - A **Subject Organizational Unit** that matches the **Issuer Organization Unit** of the server certificate.

      If one of the configured authorities meets this criteria, the server configuration is ready for Sensor Proxy linking.
5. If one of the configured authorities does not meet this criteria, add the necessary trusted certificate to Tenable Core and repeat these steps before proceeding.

Troubleshooting

Check Sensor Proxy Status

Scenario

Sensor Proxy appears to be offline or is not communicating with your management console.

Solution

Verify the state of the Sensor Proxy service.

Steps

1. Log in to the remote Sensor Proxy host via SSH to ensure the operating system is functional.
2. Confirm that the Sensor Proxy daemon is running by executing the following command:

```
# service sensorproxy status
```

> **Note:** The output should indicate that the service is running and show a process ID (PID).

3. If the service is not running, start the service:

```
# service sensorproxy start
```

4. Verify the process is active by checking the status again or using the `ps` command:

```
# ps -ef | grep sensorproxy
```

Recover Sensor Proxy

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 One Vulnerability Management or Tenable Security Center.

Solution

Sensors that were linked via Sensor Proxy can continue communicating with Tenable One Vulnerability Management or Tenable Security Center 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.

Steps

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.