Tenable Nessus to Tenable Vulnerability Management Upgrade Assistant User Guide

Last Revised: June 29, 2023

Table of Contents

Getting Started with Tenable Nessus Upgrade Assistant

> You cannot use the upgrade assistant to upgrade Tenable Nessus to Tenable Vulnerability Management in Federal Risk and Authorization Manage Program (FedRAMP) environments. For more information, see the FedRAMP Product Offering.

In Nessus Professional (version 7.1 and later) and Tenable Nessus Manager (version 8.2 and later), you can use the upgrade assistant to migrate data from a Tenable Nessus deployment to a Tenable Vulnerability Management deployment.

The upgrade migrates configurations on the local Nessus instance into Tenable Vulnerability Management. As a result, all subsequent configurations should be administered through Tenable Vulnerability Management once complete. During migration, the service itself is converted to a Nessus scanner which is then linked to Tenable Vulnerability Management. For Tenable Nessus Manager, any managed scanners and agents are relinked to Tenable Vulnerability Management. Because it is not possible to control when all of these services check in, migration continues running on the local scanner and relinking services as they check in. Optionally, you can move some or all of your scan data to Tenable Vulnerability Management.

> **Note:** Once you start an upgrade, you cannot reverse this action.

- Workflow
- Requirements
- Upgrade Considerations

For assistance with migrating, contact Tenable Support.

Workflow

1. Ensure Tenable Nessus meets the requirements.
2. Review the Upgrade Considerations.
3. If Tenable Nessus is currently linked to Tenable Security Center:
    a. In Tenable Security Center, delete Nessus from Tenable Security Center.
    b. In Tenable Nessus, unlink Nessus.
4. Upgrade from Tenable Nessus to Tenable Vulnerability Management.
5. Review the Migrated Data.
6. Complete or monitor Extended Migration.
7. (Optional) Disable Migration.
8. Learn more about Tenable Vulnerability Management, as described at https://docs.tenable.com/vulnerability-management.

Requirements

Ensure you have met the following requirements:

- Your Tenable Nessus instance is:
  - Nessus version 7.1.0 or later
  - Tenable Nessus Manager version 8.2.0 or later
- You have a Tenable Vulnerability Management administrator account.

Upgrade Considerations

Before you begin, note the following considerations.

While Tenable Nessus is in a suspended state during the upgrade:

- All sessions end, except for the session where the administrator user is performing the upgrade.
- All running scans are canceled.
- All users are logged out and cannot log back in, except for administrator accounts.
- The normal Nessus user interface is disabled, and an upgrade status and control interface appears instead.
- Starting scans manually or via the scheduler is disabled.
- Software updates are disabled.
- Accessing the API and CLI is disabled.

Once the upgrade is complete:

- The service is converted to a Nessus scanner.
- Users can log in to the Tenable Nessus scanner again.
- Scan schedules are configured and managed through Tenable Vulnerability Management.
- API and CLI are enabled.
- You can access the Extended Migration page when logged in to the Nessus scanner. On this page, you can monitor ongoing activity of managed scanners and agents that have not yet been moved to Tenable Vulnerability Management, and select scan history to and provides options for the Administrator to select historic scan data migrate into Tenable Vulnerability Management.

Migrated Data

See the following table for information about the limitations of the upgrade assistant. For more information about Tenable Vulnerability Management, see the Tenable Vulnerability Management documentation.

Nessus Data	Nessus	Tenable Nessus Manager
Agents	N/A	Migrated. You can monitor progress with extended migration.
Agent Groups	N/A	Migrated.
Agent Blackout Windows	N/A	Migrated.
Agent Settings	N/A	Migrated.
Audit files	Migrated	Migrated
Folders	Migrated	Migrated
Local scanner	Migrated **Note:** The local scanner is linked to Tenable Vulnerability Management as a managed scanner at the end of a successful migration.	Migrated **Note:** The local scanner is linked to Tenable Vulnerability Management as a managed scanner at the end of a successful migration.
Managed scanner	N/A	Migrated. You can monitor progress with extended migration. **Note:** There may be complications with migrating linked Nessus scanners and managed Tenable Security Center scanners, which are not supported scenarios. Managed scanners in Tenable Nessus Manager remain as managed scanners in

Nessus Data	Nessus	Tenable Nessus Manager
		Tenable Vulnerability Management.
Plugin rules	Migrated	Migrated
Policies	Migrated	Migrated
Scans	Migrated	Migrated
Scan credentials	Migrated	Migrated
Scan policies	Migrated	Migrated
Scan policy credentials	Migrated	Migrated
Scan history	(Optional) Migrated with extended migration	(Optional) Migrated with extended migration
Users	Migrated	Migrated
User passwords	Not migrated **Note:** Users need to use the **Reset Password** link or have an administrator set a new password for the user in Tenable Vulnerability Management.	Not migrated **Note:** Users need to use the **Reset Password link** or have an administrator set a new password for the user in Tenable Vulnerability Management.
User roles	Migrated	Migrated

Upgrade

The user interface offers a streamlined, guided method to configure and run the upgrade assistant tool.

- Upgrade to Tenable Vulnerability Management
- Migrate Scan History
- Cancel Upgrade
- Disable Migration

Upgrade to Tenable Vulnerability Management

In Nessus (version 7.1 and later) and Tenable Nessus Manager (version 8.2 and later), you can use the upgrade assistant to migrate data from a Tenable Nessus deployment to a Tenable Vulnerability Management deployment.

Before You Begin

- Back up Nessus.
- Review the upgrade considerations and requirements, as described in Getting Started with Tenable Nessus Upgrade Assistant.
- If Tenable Nessus is currently linked to Tenable Security Center:
  1. In Tenable Security Center, delete Nessus from Tenable Security Center.
  2. In Tenable Nessus, unlink Nessus.
- In Tenable Vulnerability Management, generate API keys to use during the upgrade, as described in the Tenable Vulnerability Management User Guide.

To use the upgrade assistant:

1. As an administrator, log in to Tenable Nessus.
2. In the top navigation bar, click **Settings**.
3. In the left navigation bar, click **Upgrade Assistant**.
4. Choose one of the following options:
   - If you already have a Tenable Vulnerability Management account, click **Upgrade Now**.
   - If you do not have a Tenable Vulnerability Management account, click **Sign Up First** and complete the remaining prompts.
5. Type an **Access Key** and **API Secret Key**, the API keys generated by Tenable Vulnerability Management.
6. Type the **Tenable.io Domain** name, which is the email domain of the user you registered for Tenable Vulnerability Management with.

7. Type a **Nessus Identifier**, a label to identify the instance of Nessus that you are upgrading. This identifier is used to represent migrated scanner's configuration in Tenable Vulnerability Management.

8. Click **Upgrade**.

   The **Confirm Upgrade** dialog box appears.

9. Read the upgrade warning, then click **Continue**.

   Your data upgrades from Tenable Nessus to Tenable Vulnerability Management, which may take several minutes.

   When the upgrade is complete, the **Upgrade Complete** screen appears.

10. Click **Continue to Tenable.io**.

    > **Note:** After the upgrade assistant completes, you can find a copy of the upgrade log in your local directory.

11. When the upgrade assistant completes, review the migrated data.

What to Do Next

- Continue with Extended Migration.
- Learn more about Tenable Vulnerability Management: https://docs.tenable.com/vulnerability-management.

Extended Migration

After initial upgrade, you can monitor the **Extended Migration** process, some of which begins automatically, and some of which needs manual intervention.

Extended migration consists of the following parts:

- **Overview**– An overview of the current access and linking keys, which you can update if necessary.
- **Scan History**– A manual migration of some or all of your scan history from Tenable Nessus to Tenable Vulnerability Management.
- **Scanners**– (Tenable Nessus Manager only) An automatic migration of your managed scanners. Some action may be required if scanners fail to link.
- **Agents**– (Tenable Nessus Manager only) An automatic migration of your managed agents. Some action may be required if agents fail to link.

If you choose to disable migration, the extended migration process is interrupted and your Tenable Nessus instance becomes a managed scanner of Tenable Vulnerability Management.

Update Migration Settings

If you regenerated the API keys of the user that you used to do the migration, or the linking key of the scanner or agent, you must update this information in the migration settings. You can update this information as needed on the **Overview** tab of the Extended Migration page.

To update migration settings:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.
2. In the left navigation bar, click **Extended Migration**.

   The **Extended Migration to Tenable Vulnerability Management** page appears. By default, the **Overview** tab is open.
3. Type a new access key, secret key, and/or linking key.
4. Click **Update Settings**.
5. Restart Tenable Nessus for the changes to take effect.

Migrate Scan History

As part of Extended Migration, you can optionally migrate scan history from Tenable Nessus to Tenable Vulnerability Management. Unlike other data that migrates automatically, this process must be launched manually.

Before You Begin

- Perform the initial upgrade, as described in Upgrade to Tenable Vulnerability Management .

To migrate scan history from Tenable Nessus to Tenable Vulnerability Management:

1. As an administrator, log in to Tenable Nessus.
2. In the top navigation bar, click **Settings**.
3. In the left navigation bar, click **Extended Migration**.

   The **Extended Migration to Tenable Vulnerability Management** page appears.
4. Click the **Scan History** tab.
5. In the upper-right corner, click the **Change Settings** button.
6. Type the following to edit the scan history migration settings:
   - **Days of history:** The number of days of scan history you want to upload. Typing 0 uploads all scan history.
   - **Concurrent uploads:** The number of scan history items that Tenable Nessus uploads in parallel. A higher number of concurrent uploads can complete faster but uses more bandwidth. Given dependencies on connectivity with Tenable Vulnerability Management, we recommend not setting this higher than 10.
   - **Seconds to sleep between uploads:** The number of seconds that Tenable Nessus waits before starting the next batch of uploads. Increase the time Nessus waits between uploads if you have limited upload bandwidth.
7. Click **Update Settings**.

   Tenable Nessus filters scan history based on the migration settings and displays a table with the scan history to be upgraded.
8. (Optional) To skip a scan history item, in its row, click ✖.

9. (Optional) To include a skipped scan history item, in its row, click ↻.

10. Click **Migrate**.

    Tenable Nessus migrates the selected scan history items to Tenable Vulnerability Management. The **Status** indicates the progress of the migration.

    > **Note:** This process may take a long period of time, depending on connectivity and the amount of data being migrated. The migration continues to run until complete.

What to Do Next

- Monitor any remaining items on the Extended Migration page. This includes scan history and any scanners and agents that have not yet checked in.
- (Optional) If you are done upgrading scan history and do not plan to upgrade any more data, you can disable migration.
- Learn more about Tenable Vulnerability Management: https://docs.tenable.com/vulnerability-management.

Monitor Managed Scanners Migration

In Tenable Nessus Manager, as part of Extended Migration, managed scanners are automatically relinked from Tenable Nessus to Tenable Vulnerability Management. You can monitor the progress of the migration and manually retry any failed scanners.

Considerations

- There may be complications with migrating linked Nessus scanners and managed Tenable Security Center scanners, which are not supported scenarios.
- Managed scanners in Tenable Nessus Manager remain as managed scanners in Tenable Vulnerability Management.
- A scanner must be version 8.2.0 or later to be migrated to Tenable Vulnerability Management.
- If a scanner is on a lower version than 8.2.0, Tenable Nessus automatically updates a scanner to the latest version before it can be linked. If software updates are disabled, Tenable Nessus temporarily overrides those settings to update the scanner.
- Scans that are configured to use a scanner that is in the process of being migrated do not run until the scanner has successfully relinked to Tenable Vulnerability Management.

Before You Begin

- Perform the initial upgrade, as described in Upgrade to Tenable Vulnerability Management .

To monitor scanner migration progress:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.
2. In the left navigation bar, click **Extended Migration**.

   The **Extended Migration to Tenable Vulnerability Management** page appears.
3. Click the **Scanners** tab.

   Tenable Nessus displays the list of scanners to be upgraded to Tenable Vulnerability Management and their status. It may take several minutes for Tenable Nessus to complete upgrading your scanners to Tenable Vulnerability Management.

> If the scanner needs a software update, it may take longer, depending on the interval the scanner checks for software updates. If a scanner is offline, it does not attempt to check in or relink until it is back online.

4. If a scanner failed to link to Tenable Vulnerability Management, in the scanner row, click ↻ to retry linking.

   Tenable Nessus retries linking the scanner as a managed scanner to Tenable Vulnerability Management.

What to Do Next

- Monitor any remaining Extended Migration items, such as scan history or agents.
- (Optional) If your extended migration is complete and you do not plan to upgrade any more data, you can disable migration.
- Learn more about Tenable Vulnerability Management: https://docs.tenable.com/vulnerability-management.

Monitor Agents Migration

In Tenable Nessus Manager, as part of Extended Migration, agents are automatically relinked from Tenable Nessus to Tenable Vulnerability Management. You can monitor the progress of the migration and manually retry any failed agents.

Considerations

- An agent must be version 7.2.0 or later to be migrated to Tenable Vulnerability Management.
- If an agent is on a lower version than 7.2.0, Tenable Nessus automatically updates an agent to the latest version before it can be linked. If the agent has blackout windows or software updates disabled, Tenable Nessus temporarily overrides those settings to update the agent.
- When an agent is relinked, it is named after the current hostname of the machine the agent is installed on.
- Your migrated agent groups in Tenable Vulnerability Management may initially appear empty but are populated as agents relink to Tenable Vulnerability Management.

Before You Begin

- Perform the initial upgrade, as described in Upgrade to Tenable Vulnerability Management .

To monitor scanner migration progress:

1. In Tenable Nessus, in the top navigation bar, click **Settings**.
2. In the left navigation bar, click **Extended Migration**.

   The **Extended Migration to Tenable Vulnerability Management** page appears.
3. Click the **Agents** tab.

   Tenable Nessus displays the list of agents to be relinked to Tenable Vulnerability Management and their status. It may take over 30 minutes for Tenable Nessus to start migrating your agents to Tenable Vulnerability Management, depending on how many agents you have.
4. If an agent failed to link to Tenable Vulnerability Management, in the agent row, click ↻ to retry linking.

   Tenable Nessus retries linking the agent to Tenable Vulnerability Management.

What to Do Next

- Monitor any remaining Extended Migration items, such as scan history or scanners.
- (Optional) If your extended migration is complete and you do not plan to upgrade any more data, you can disable migration.
- Learn more about Tenable Vulnerability Management: https://docs.tenable.com/vulnerability-management.

Disable Migration

An upgrade is not reversible, and once an upgrade has started, it cannot be canceled. However, if you are finished upgrading all your data, you can disable migration. The Tenable Nessus instance turns into a managed scanner under Tenable Vulnerability Management.

Disabling migration does not remove any data that was already upgraded, but prevents any more scan history from being migrated. Additionally, any scanners and agents that haven’t been migrated to Tenable Vulnerability Management are not migrated, even if they check in.

> **Note:** If you disable migration, you cannot undo this action.

Before you begin

- Ensure you are done monitoring all the items under Extended Migration.

To disable migration:

1. As an administrator, log in to Tenable Nessus.
2. In the top navigation bar, click **Settings**.
3. In the left navigation bar, click **Extended Migration**.

   The **Extended Migration to Tenable Vulnerability Management** page appears.
4. In the upper-right corner, click the **Disable Migration** button.

   Tenable Nessus disables any further scan history from being migrated for this instance of Tenable Nessus.

Cancel Upgrade

An upgrade is not reversible, and once an upgrade has started, it cannot be canceled.

However, if your upgrade encounters an error, it pauses progress. You then have the following options:

- **Continue**, which skips the entity that caused the current error and continues upgrading.
- **Cancel**.

If you choose to cancel an upgrade that was partially complete, you can resume it by going to the **Upgrade Assistant** page again and restarting the upgrade. The upgrade starts where it left off, and retries any error that it encountered before.

> **Note:** If you cancel and do not resume the upgrade at a later date, some successfully upgraded data may remain in Tenable Vulnerability Management. You must manually delete this data from Tenable Vulnerability Management.

Additional Resources

- Upgrade FAQ
- Upgraded Data

FAQ

Consider the following frequently asked questions when planning your upgrade.

Does my environment support the upgrade assistant?

For more information about local machine, Nessus, and Tenable Vulnerability Management requirements, see Requirements.

Will the upgrade assistant transfer all of my Tenable Nessus data?

For information on what data is transferred from Tenable Nessus to Tenable Vulnerability Management, see Migrated Data.

Can I exclude data from the upgrade?

All data described in Migrated Data, except for scan history, is automatically transferred to your instance of Tenable Vulnerability Management. You can optionally choose to upgrade scan history.

Do I need to back up Tenable Nessus before performing the upgrade?

Tenable® recommends backing up Tenable Nessus regularly as a deployment best practice, but the upgrade assistant does not remove any data from Tenable Nessus. Your Tenable Nessus deployment continues running as configured.

Can I use Tenable Nessus as a scanner after I have performed the upgrade?

After you upgrade from Tenable Nessus to Tenable Vulnerability Management, Tenable Nessus becomes a managed scanner. You can no longer use that instance of Nessus as a standalone scanner, but you can log in and see scan history for the upgraded scans.

Can I run the upgrade assistant more than once?

Tenable® recommends running the upgrade assistant only once, from your existing Tenable Nessus deployment to a Tenable Vulnerability Management instance. Once you upgrade your data from Tenable Nessus to Tenable Vulnerability Management, Tenable Nessus becomes a managed scanner, so the option to upgrade again is no longer available.

You can upgrade scan history multiple times, until you disable migration.

Is the upgrade assistant available via the CLI?

The upgrade assistant is currently only available via the Nessus Professional user interface.

How long does it take to run the upgrade assistant?

Upgrade time varies depending on the number and complexity of your scan policies.

How do I manage my data in Tenable Vulnerability Management?

For more information about Tenable Vulnerability Management, see the Tenable Vulnerability Management documentation.

Migrated Data

See the following table for information about the limitations of the upgrade assistant. For more information about Tenable Vulnerability Management, see the Tenable Vulnerability Management documentation.

Nessus Data	Nessus	Tenable Nessus Manager
Agents	N/A	Migrated. You can monitor progress with extended migration.
Agent Groups	N/A	Migrated.
Agent Blackout Windows	N/A	Migrated.
Agent Settings	N/A	Migrated.
Audit files	Migrated	Migrated
Folders	Migrated	Migrated
Local scanner	Migrated **Note:** The local scanner is linked to Tenable Vulnerability Management as a managed scanner at the end of a successful migration.	Migrated **Note:** The local scanner is linked to Tenable Vulnerability Management as a managed scanner at the end of a successful migration.
Managed scanner	N/A	Migrated. You can monitor progress with extended migration. **Note:** There may be complications with migrating linked Nessus scanners and managed Tenable Security Center scanners, which are not supported scenarios. Managed scanners in Tenable Nessus Manager remain as managed scanners in

Nessus Data	Nessus	Tenable Nessus Manager
		Tenable Vulnerability Management.
Plugin rules	Migrated	Migrated
Policies	Migrated	Migrated
Scans	Migrated	Migrated
Scan credentials	Migrated	Migrated
Scan policies	Migrated	Migrated
Scan policy credentials	Migrated	Migrated
Scan history	(Optional) Migrated with extended migration	(Optional) Migrated with extended migration
Users	Migrated	Migrated
User passwords	Not migrated **Note:** Users need to use the **Reset Password** link or have an administrator set a new password for the user in Tenable Vulnerability Management.	Not migrated **Note:** Users need to use the **Reset Password link** or have an administrator set a new password for the user in Tenable Vulnerability Management.
User roles	Migrated	Migrated