NetWitness® Platform

Version 12.5.1

Endpoint Agent Installation Guide

NETWITNESS

Platform

Contact Information

NetWitness Community at https://community.netwitness.com contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability. This software is subject to change without notice and should not be construed as a commitment by RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

November, 2024

Contents

Introduction to Endpoint Agent Installation **4**
- Supported Operating Systems 4
- Hardware Requirements 5
- Enable Process Events Tracking on macOS 14 5
- Disable Process Events Tracking on macOS 14 6
- Installation Flowchart 6

Prerequisites **7**

Generate an Endpoint Agent Packager **8**

Generate Endpoint Agent Installers **11**

Deploy and Verify Endpoint Agents **12**
- Deploying Agents (Windows) 12
  - Verifying Windows Agents 12
- Deploying Agent (Linux) 12
  - Verifying Linux Agents 13
- Deploying Agent (Mac) 13
  - Verifying Mac Agents 13

Uninstall Agents **15**
- Uninstalling Agent using UI 15
- Uninstalling Agent Manually 18
  - Uninstalling Windows Agent 18
  - Uninstalling Linux Agent 18
  - Uninstalling Mac Agent 18

Upgrade Agents **19**
- Upgrading Agents Using UI 19
- Upgrading From Previous Versions of Agents 21

Recommendations for Installing Agents in Virtual Desktop Infrastructure (VDI) Environment **23**

Troubleshooting **24**
- Packager Issue 24
- Agent Upgrade via UI Issues 24
- Agent Uninstall via UI Issues 25
- Events Tracking Issues 26

Introduction to Endpoint Agent Installation

Hosts can be laptops, workstations, servers, physical or virtual, where a supported operating system is installed. An Endpoint Agent can be deployed on a host with either a Windows, Mac, or Linux operating system. The installation process involves:

1. (Optional) Configuring the Relay Server

Note: You must set up the default relay server before generating the Agent packager. Whenever the Relay server configuration is modified, agent policy is updated automatically. For more information on configuring the relay server, see *Endpoint Configuration Guide*.

2. Generating an agent packager
3. Generating the agent installer

You can run the agent installer specific to your operating system to deploy agents on the hosts. The agents collect endpoint data and tracking events from these hosts. It monitors key behaviors related to process, file, registry, console, and network, and forwards them as events to the Endpoint Server over HTTPs.

Note: The Endpoint agent can operate either in Insights or Advanced mode depending on the policy configuration. For more information, see the *NetWitness Endpoint Configuration Guide*.

Supported Operating Systems

Note: From version 12.0 and higher, NetWitness Endpoint agents run on ARM devices running on Windows 10 and 11.

Windows	**Linux** *(The agent software runs only on x86_64 architecture)*	**macOS**
Windows 11 (up to version 23H2)		
Windows 11 (up to version 22H2)	CentOS 7.x and 8.x	macOS Sonoma (14) **Note:** For more information on how to enable Process Events tracking on macOS 14, see Enable Process Events Tracking on macOS 14.
Windows 10 Kiosk Mode (64-bit)	Red Hat Enterprise Linux 7.x, 8.x, and 9.x	macOS Ventura (13)
Windows 10 (32 and 64-bit) (up to version 22H2)	SUSE Linux Enterprise Server 12 SP1, 12 SP3, 12 SP4, 12 SP5, 15 SP1, and 15 SP4	macOS Monterey (12)

Windows 8.1 (32 and 64-bit)	Ubuntu 16.04 LTS, 18.04 LTS, and 20.04 LTS	macOS Big Sur (11)
Windows 8 (32 and 64-bit)	Oracle Linux 8.8	macOS Catalina (10.15)
Windows 7 (32 and 64-bit)	Alma Linux 9.0	macOS Mojave (10.14)
Windows Server 2022 Windows Server 2022 Core		macOS High Sierra (10.13)
Windows Server 2019 Windows Server 2019 Core		macOS Sierra (10.12)
Windows Server 2016		OS X El Capitan (10.11)
Windows Server 2012 R2		OS X Yosemite (10.10)
Windows Server 2012		OS X Mavericks (10.9)
Windows Server 2008 R2 (32 and 64-bit)		

Hardware Requirements

The minimum requirements for installing, uninstalling, and upgrading the agent comply with the specific operating system requirements.

Enable Process Events Tracking on macOS 14

You can track Process events on macOS 14 after enabling audit control in your machine.

To enable Process events tracking on macOS 14

Note: The steps 1 and 4 are applicable to you only if the agent is installed and running on your machine. If the agent is not installed on your machine, skip the steps 1 and 4 and perform only the steps 2, 3, and 5.

1. Stop NetWitness agent by running the following command.

   ```
   sudo launchctl unload /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist
   ```

2. Copy the audit service template config file to create a new config by running the following command.

   ```
   sudo cp /etc/security/audit_control.example /etc/security/audit_control
   ```

3. Enable auditd service by running the following command.

   ```
   sudo launchctl enable system/com.apple.auditd
   ```

4. Enable NetWitness agent by running the following command.

   ```
   sudo launchctl load /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist
   ```

5. Reboot the system.

Disable Process Events Tracking on macOS 14

You can disable Process events tracking in your macOS 14 by disabling the already enabled audit control.

To disable Process events tracking on macOS 14

1. Stop NetWitness agent by running the following command.

   ```
   sudo launchctl unload /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist
   ```

2. Disable auditd service by running the following command.

   ```
   sudo launchctl disable system/com.apple.auditd
   ```

3. Remove the audit service config file by running the following command.

   ```
   sudo rm /etc/security/audit_control
   ```

4. Enable NetWitness agent by running the following command.

   ```
   sudo launchctl load /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist
   ```

5. Reboot the system.

Installation Flowchart

The following flowchart illustrates the Endpoint agent installation process:

Prerequisites

- Install NetWitness. For more information, see the *Physical Host Installation Guide* or *Virtual Host Installation Guide*.
- Install NetWitness Endpoint Log Hybrid. For more information, see the *Physical Host Installation Guide* or *Virtual Host Installation Guide*.
- Deploy ESA Rules from the Endpoint Rule Bundle. For more information, see *ESA Configuration Guide*.
- Configure Endpoint Metadata forwarding. For more information, see *NetWitness Endpoint Configuration Guide*.
- Review the default policies and create groups to manage your agents. For more information, see *NetWitness Endpoint Configuration Guide*.
- Configure your RSA Live account and make sure the File Reputation service is enabled. For more information, see *Live Services Management Guide*.

Note: If you are upgrading, make sure that you deploy the latest Endpoint application rules from RSA Live. For more information, see *Live Services Management Guid*.

Generate an Endpoint Agent Packager

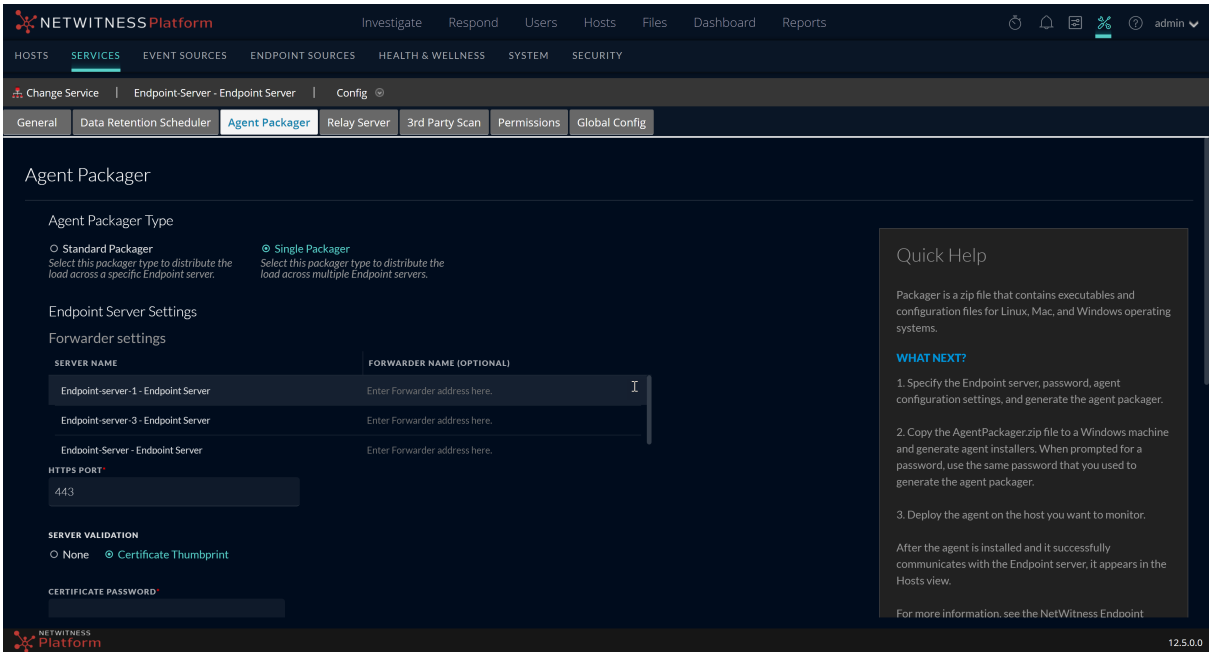
To generate an agent packager to collect endpoint data from hosts:

1. Log in to NetWitness.

   Type `https://<NW-Server-IP-Address>/login` in your browser to get to the NetWitness Login screen.

2. Click  **(Admin) > Services**.

3. Select the **Endpoint Server** service and click  **> View > Config > Agent Packager** tab. The **Agent Packager** tab is displayed.



4. Select the required option in the applicable fields and enter the values in the required fields. The following fields are displayed in the **Agent Packager** tab.

Field	Description
Agent Packager Type	Displays the following 2 options. • **Standard Packager** • **Single Packager** You can select any of the above 2 options as per your requirement. For more information, see NetWitness Endpoint User Guide.
Endpoint Server	Displays all the available Endpoint servers in the deployed.

Field	Description
Endpoint Server Forwarder (Optional)	The optional Endpoint Server Forwarder allows you to enter an alternative Fully Qualified Domain Name (FQDN) or IP address on which the sever can be reached in the case that agents need to go through a NAT or similar in order to reach the Endpoint Server. If specified forwarder is not available, agent will eventually fall back to the packaged address.
HTTPS Port	Port number. For example, 443.
Server Validation	Determines how the agent validates the Endpoint Server certificate: • None – The agent will not validate the server certificate. • Certificate Thumbprint – default selection. The agent identifies the server by validating the thumbprint of the Root CA of the server certificate.
Certificate Password	Password used to download the packager. The same password is used while generating the agent installer. **Note:** The password must be minimum seven characters long and a combination of uppercase and lowercase letters, numbers, and special characters. For example, **Admin@123**.
Auto Uninstall	Date and time the agent automatically uninstalls. You can leave it blank if not required.
Tag Configuration	When you click **Assign Tags** under Tag Configuration, you can do any of the following: • Create new tags and assign them to the hosts. • Select already existing tags and assign them to the hosts. For more information, see Investigate Hosts.
Force Overwrite	Overwrites the installed Windows agent regardless of the version. If this option is not selected, the same installer can be run multiple times on a system, but installs the agent only once. If you enable this option, make sure that you provide the same service name and driver service name as the previously installed agent, while creating a new agent. **Note:** If you want to force overwrite with MSI, run the following command: `msiexec /fvam <msifilename.msi>` After you move an agent from one deployment to another, using Force Overwrite to change the agent incurs an 8-hour delay in communication between the agent and its Endpoint Server on the new deployment. To eliminate the delay, uninstall the agent from the old deployment, and reinstall the agent on the new deployment.
Agent Configuration	
Note: The following Service and Driver fields are applicable only for Windows.	

Field	Description
Service	
Service Name	Name of the agent service. For example, NWEAgent.
Display Name	Display name of the agent service. For example, NWE Agent.
Description	Description of the agent service. For example, NetWitness Endpoint.
Driver	
Driver Service Name	Name of the driver service. For example, NWEDriver.
Driver Display Name	Display name of the driver service. For example, NWE Driver.
Driver Description	Description of the driver service. For example, NetWitness Endpoint Driver.
Generate Agent	Generates an agent packager.

5. Click **Generate Agent**.

   This downloads an agent packager (**AgentPackager.zip**) on the host where you are accessing the NetWitness user interface.

Generate Endpoint Agent Installers

To generate endpoint agent installers to deploy on hosts:

Note: Use a Windows machine to execute the agent packager file.

1. Unzip the **AgentPackager.zip** file. It includes the following:
   - **agents** folder – Contains executables for Linux, Mac, and Windows.
   - **config** folder – Contains configuration file and the certificates required to communicate between the Endpoint Server and the agent.
   - **AgentPackager.exe** file.
2. Run the **AgentPackager.exe** file as administrator by right-clicking the file and selecting **Run as administrator**.
3. Enter the same password used while generating the agent packager and press **Enter**.
   This creates the following installers in the root folder:
   - nwe-agent-package.exe (for Windows)
   - NWE000032.msi (for Windows 32-bit)
   - NWE000064.msi (for Windows 64-bit)
   - NWE00Aa64.msi (for ARM based Windows 64-bit)
   - nwe-agent.pkg (for Mac)
   - nwe-agent.x86_64.rpm (for RPM based Linux 64-bit)
   - nwe-agent.x86_64.deb (for Debian based Linux 64-bit)

   Note: The MSI files should not be renamed.

Deploy and Verify Endpoint Agents

This section provides instruction on how to deploy and verify agents.

Note: By default, the agent is installed in the Insights mode. Depending on the policy assigned, the agent can operate in Insights or Advanced mode. Make sure you review the policy before deploying the agent. For more information, see *NetWitness Endpoint Configuration Guide*.

Deploying Agents (Windows)

To deploy the agent, run the **nwe-agent-package.exe** file on the hosts you want to monitor.

Verifying Windows Agents

After deploying the Windows agents, you can verify if a Windows agent is running by using any of the following methods:

- Using the NetWitness UI

  The Hosts view contains the list of all hosts with an agent. You can look for the host name on which the agent is installed.

  Note: Click **Hosts** or press F5 to refresh the list for latest data.

- Using Task Manager

  Open Task Manager and look for service name that you configured while generating the agent packager on the host machine.

- Using Services.msc

  Open `Services.msc` in run and look for the service name that you configured while generating the agent packager on the host machine.

Deploying Agent (Linux)

To deploy the agent on the hosts you want to monitor:

RPM based Linux

Run the **nwe-agent.x86_64.rpm** (for 64-bit) file. To run the command, open Terminal on the Linux machine and run the following command as `root`:

```
rpm -iv <installer file name>.rpm
```

For example, using the default installer file name, you can enter the following command:

`rpm -iv nwe-agent.x86_64.rpm` (for x86_64 architecture)

Note: To upgrade RPM based Linux agents, run **rpm -Uvh nwe-agent.x86_64.rpm**.

Debian based Linux

Run the **nwe-agent.x86_64.deb** (for 64-bit) file. To run the command, open Terminal on the Linux machine and run the following command as `root`:

```
dpkg -i <installer file name>.deb
```

For example, using the default installer file name, you can enter the following command:

`dpkg -i nwe-agent.x86_64.deb` (for x86_64 architecture)

(Enter the administrator password when prompted.)

Note: To upgrade Debian based Linux agents, run **dpkg -i nwe-agent.x86_64.deb**.

Verifying Linux Agents

After deploying the Linux agents, you can verify if a Linux agent is running by using any of the following methods:

- Using the NetWitness UI

  The Hosts view contains the list of all hosts with an agent.

  Note: Click **Hosts** or press F5 to refresh the list for latest data.

- Using Command Line

  Run the following command to get the PID:

  ```
  pgrep nwe-agent
  ```

- To check the NetWitness Endpoint version, run the following command:

  ```
  cat /opt/rsa/nwe-agent/config/nwe-agent.config | grep version
  ```

Deploying Agent (Mac)

To deploy the agent, run the `nwe-agent.pkg` file on the hosts you want to monitor. On macOS version Catalina (10.15) and higher, you need to move the `nwe-agent.pkg` file to a folder with sufficient access privileges (e.g., `/tmp`) and install the agent from there.

Verifying Mac Agents

After deploying the Mac agents, you can verify if a Mac agent is running by using any of the following methods:

- Using the NetWitness UI

  The Hosts view contains the list of all hosts with an agent.

  Note: Click **Hosts** or press F5 to refresh the list for the latest data.

- Using Activity Monitor

  Open Activity Monitor (/Applications/Utilities/Activity Monitor.app) and look for NWEAgent.
- Using Command Line

  Run the following command to get the PID

  ```
  pgrep NWEAgent
  ```
- To check the NetWitness Endpoint version, run the command:

  ```
  grep a /var/log/NWEAgent.log | grep NWEAgent | grep Version
  ```

Uninstall Agents

You can use one of the following methods to uninstall Endpoint agents. Select a method based on your current Endpoint agent version.

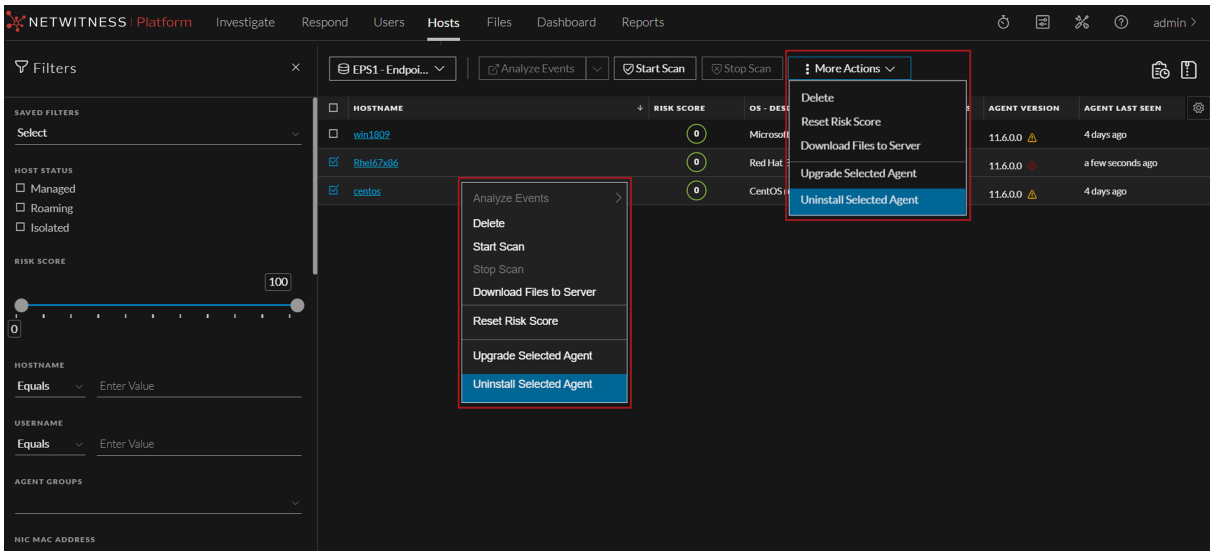
- Uninstalling Agent using UI
- Uninstalling Agent Manually

Uninstalling Agent using UI

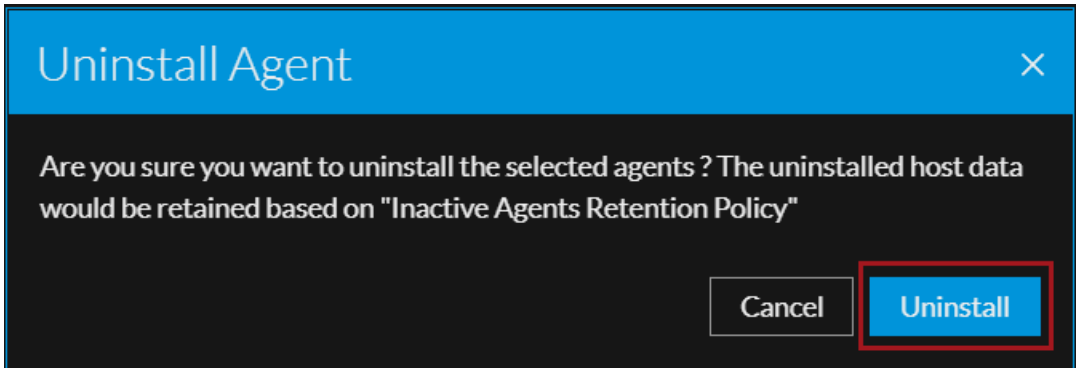
You can uninstall agent using UI by going to **Hosts** and performing one of the following options.

Uninstall one or more agents from Hosts view

1. Select one or more hosts from which you want to uninstall the agents.
2. Selected **More Actions > Uninstall Selected Agent** from the toolbar.



3. In the **Uninstall Agent** dialog, click **Uninstall.**

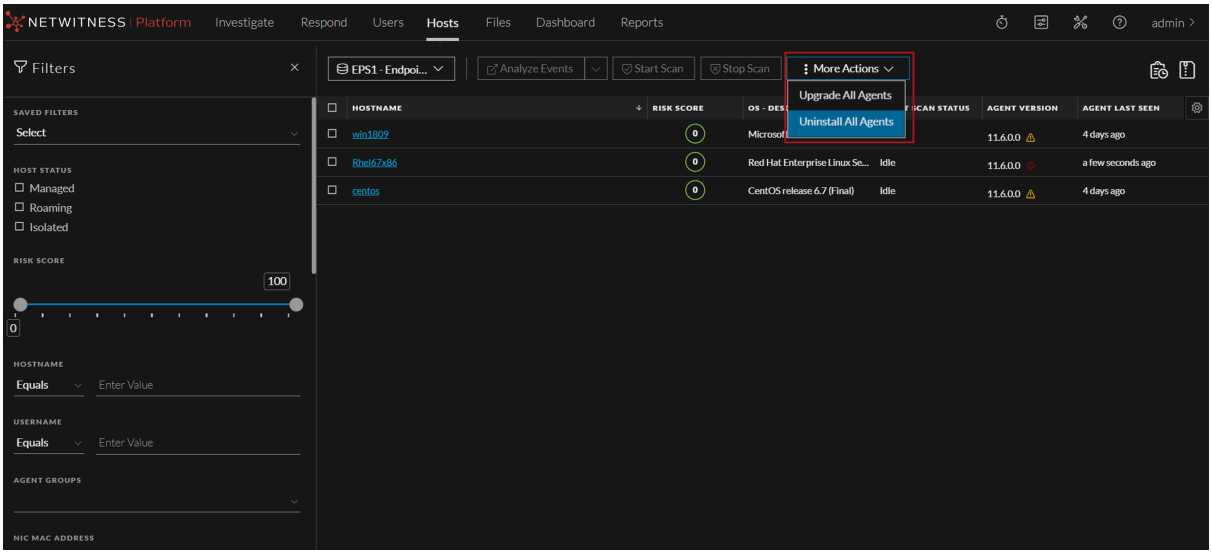


Uninstall all the agents from Hosts view

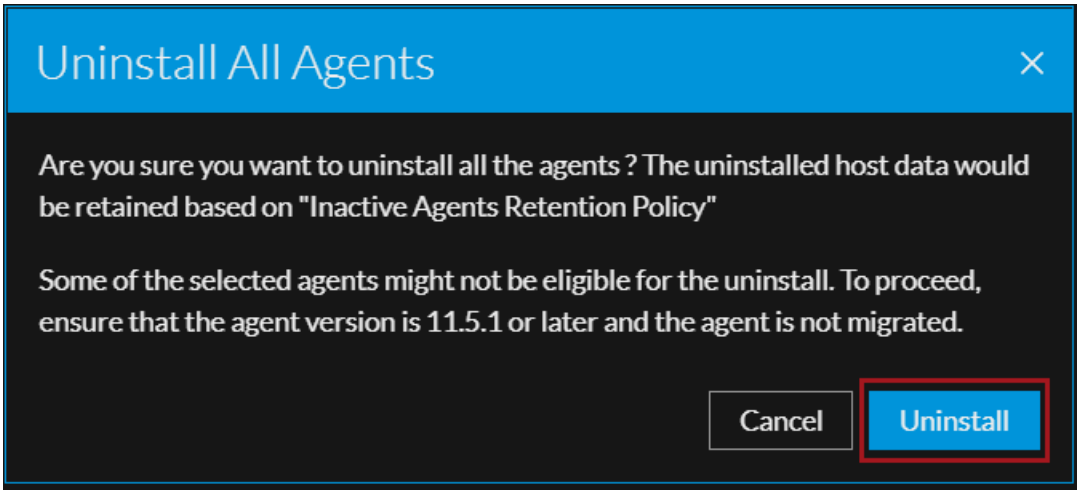
Note: Uninstall All Agents via UI is also supported for Broker service.

1. Select **More Actions > Uninstall All Agents** from the toolbar.

Note: For the uninstall all agents option, you do not need to select the hosts. **Upgrade All Agents** / **Uninstall All Agents** are the default options on the More Actions drop-down. If you select one or more hosts, the More Actions drop-down shows Upgrade Selected Agent / Uninstall Selected Agent as the available options.



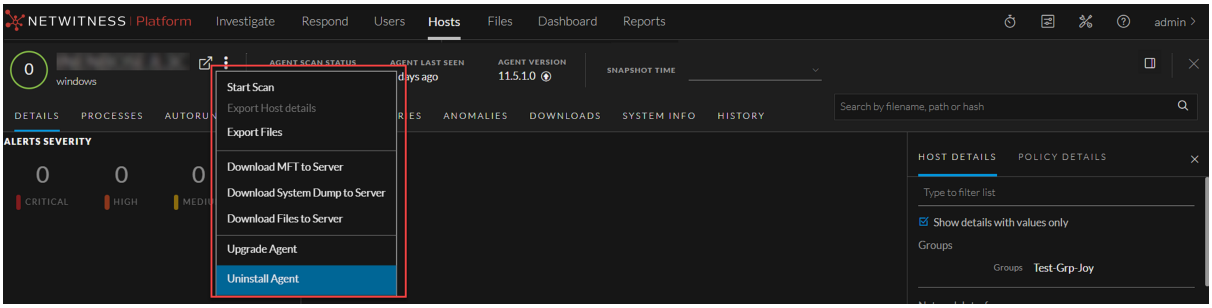
2. In the **Uninstall All Agents** dialog, click **Uninstall.**



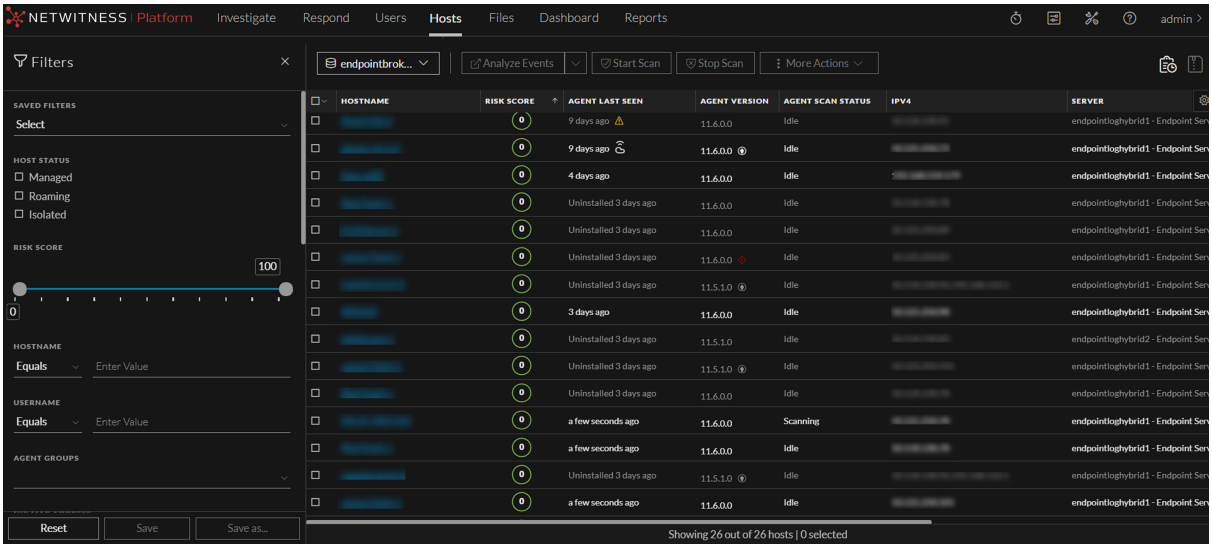
Note: Uninstall All Agents process will require more time to complete depending upon the number of agents selected based on the filters applied.

Uninstall an agent from Host details view

1. Select the hostname to open the host details, click ⋮ (**More Actions**) beside the hostname, and select **Uninstall Agent**.

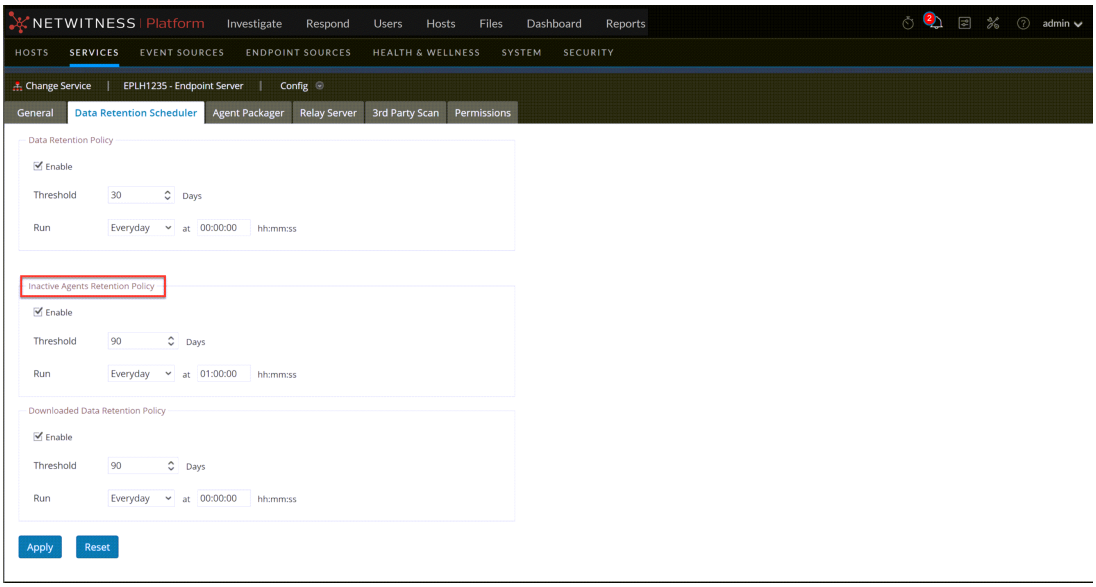


2. In the **Uninstall Agent** dialog, click **Uninstall.**
3. After the agent is uninstalled, **Agent Last Seen** is updated and the host is grayed out in the **Hosts** view.



Note: Once an agent is uninstalled, only **Delete** and **Analyze Events** actions can be performed on it.

IMPORTANT: If you are uninstalling agent using UI, the uninstalled host data would be retained based on **Inactive Agents Retention Policy.**



Uninstalling Agent Manually

Uninstalling Windows Agent

Run the following command as administrator:

```
msiexec /x{63AC4523-5F19-42F0-BC43-97C8B5373589}
```

Uninstalling Linux Agent

For RPM based Linux, run the following command as root:

```
rpm -ev nwe-agent
```

For Debian based Linux, run the following command as root:

```
dpkg -r nwe-agent
```

Uninstalling Mac Agent

Run the following commands:

1. `sudo launchctl unload /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
2. `sudo rm -Rf /usr/local/nwe`
3. `sudo rm -Rf '/Library/Application Support/NWE'`
4. `sudo rm -Rf /Library/LaunchDaemons/com.rsa.nwe.agent.daemon.plist`
5. `sudo pkgutil --forget com.rsa.pkg.nwe`

Upgrade Agents

You can use one of the following methods to upgrade Endpoint agents. Select a method based on your current Endpoint agent version. If you have upgraded the endpoint server recently, you must restart it to see **Upgrade Selected Agent** and **Upgrade All Agents** options on the UI.

- Upgrading Agents Using UI
- Upgrading From Previous Versions of Agents

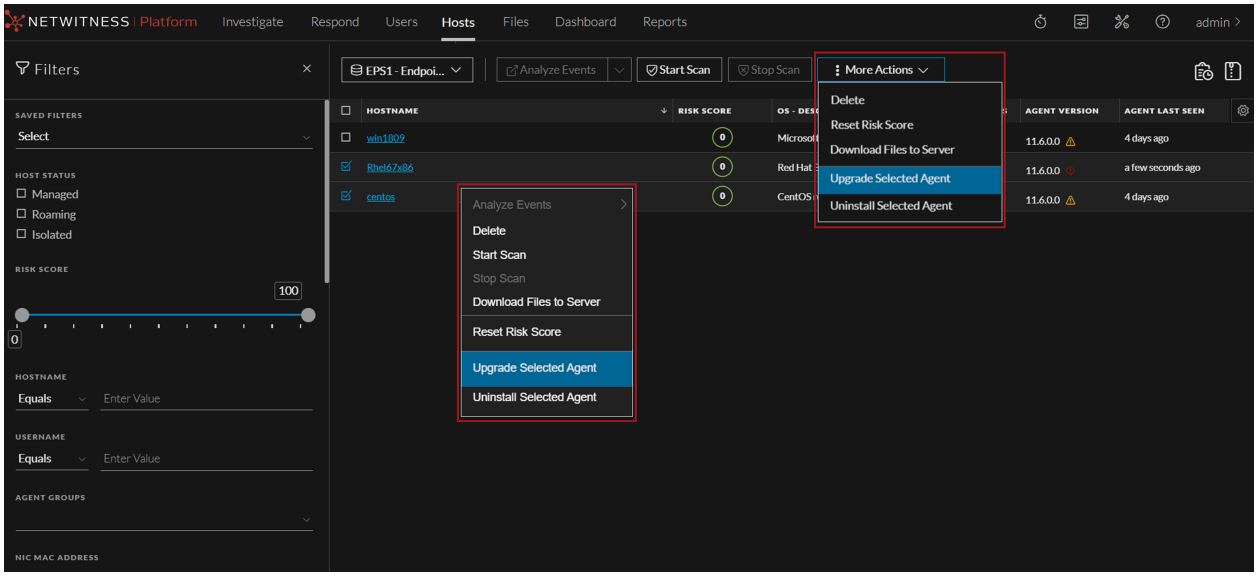
Upgrading Agents Using UI

Note: To upgrade agent from UI, ensure the service user account has both `endpoint-server.agentupdate.manage` and `endpoint-server.ca.manage` permissions. For more information on how to assign roles and permissions, see "Add a Role and Assign Permissions" in the *System Security and User Management Guide*.

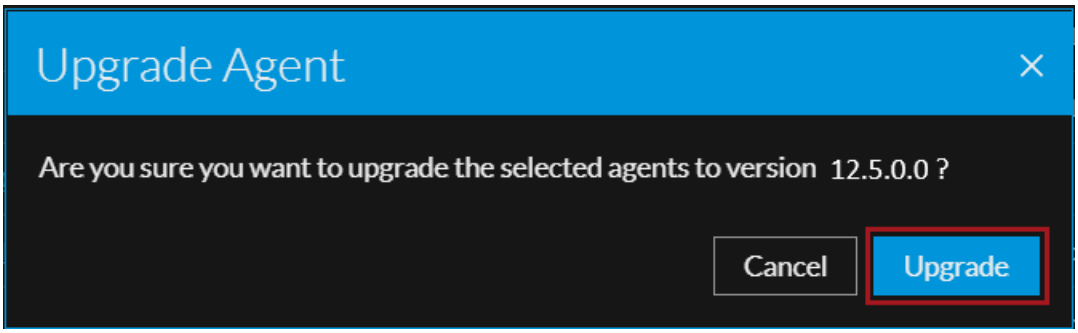
You can upgrade agents using UI by going to **Hosts** and performing one of the following options.

Upgrade one or more agents from Hosts view

1. Select one or more hosts and select **More Actions > Upgrade Selected Agent**



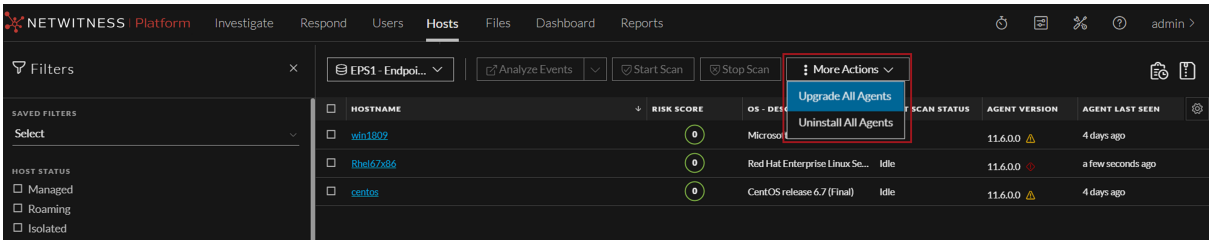
2. In the **Upgrade Agent** dialog, click **Upgrade**.



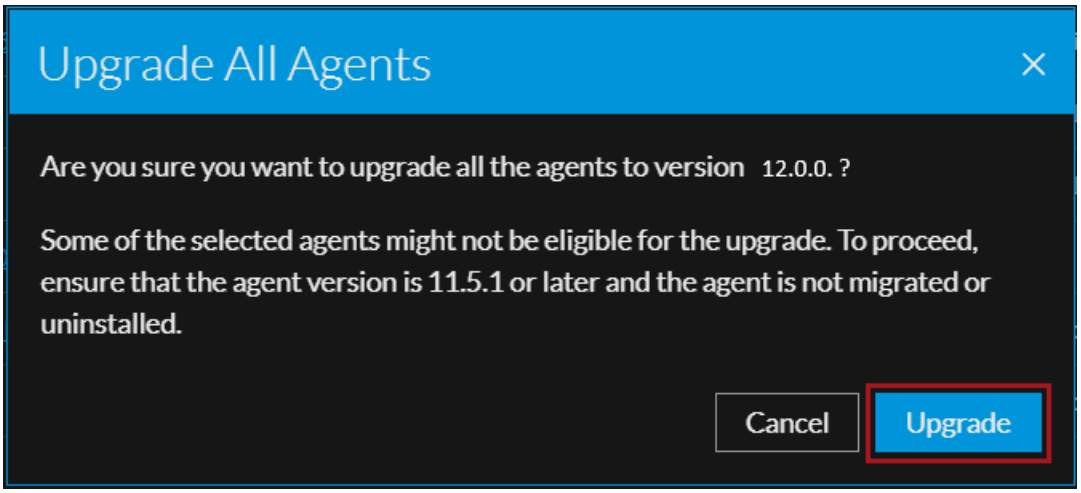
Upgrade all agents from Hosts view

1. Select **More Actions > Upgrade All Agents** from the toolbar, to perform bulk agent upgrade.

Note: For the upgrade all agents option, you do not need to select the hosts. **Upgrade All Agents** / **Uninstall All Agents** are the default options on the More Actions drop-down. When you select one or more hosts, the More Actions drop-down shows Upgrade Selected Agent / Uninstall Selected Agent as the available options.



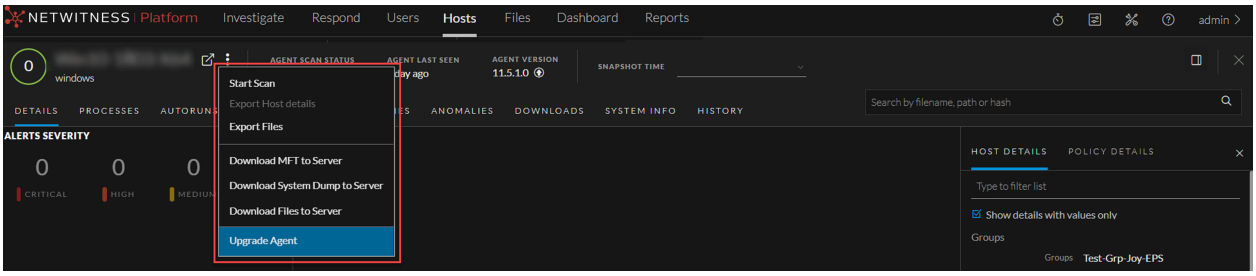
2. In the **Upgrade All Agents** dialog, click **Upgrade**.



Note: Upgrade All Agents process will require more time to complete, depending upon the number of agents selected based on the filters applied.

Upgrade an agent from Hosts details page

Select the hostname to open the host details, click ⋮ (**More Actions**) beside the hostname, and select **Upgrade Agent**.



1. In the **Upgrade Agent** dialog, click **Upgrade**.

The following upgrade status icons are displayed in the **Agent Version** column.

Icons	Upgrade Status	Description
	Upgrade Available	An agent upgrade is available.
	Agent Upgrade Pending	The agent has not yet received the upgrade command.
	In Progress	The agent is being upgraded.
	Failed	Agent upgrade failed. View details in the agent history page.
No Icon	No Upgrade Available	No upgrade available for the agent. Refer to agent eligibility.

You can view the list of commands issued to the agents (by the server or actions performed by any analyst) in the Host view and Host details. By default, commands are sorted based on the command time.

To view the commands:

1. Go to **Hosts**.
2. Do any one of the following,

- To view all commands, click  . You can also filter commands.
  The Agent History view is displayed.
- To view commands specific to a particular host:
  - Click the host for which you want to view the commands.
  - In the Host details view, click **History** tab. You can also filter commands.
    The History view is displayed.

For more information on Agent History, see the "Investigating Hosts" topic in the *NetWitness Endpoint User Guide*.

Upgrading From Previous Versions of Agents

You can upgrade the previous versions of Endpoint agent to the latest version.

Note: In a multi-server Endpoint deployment, during an agent upgrade, make sure that the correct Endpoint server is mentioned in the respective agent policy. In case the agent uses the default policy, ensure to use the agent packager downloaded from the respective Endpoint server to which it is communicating. Using Agent packager from different Endpoint server for agent upgrade will result in migrating the agents to another Endpoint server.

Note: For a subsequent installation or upgrade, use the same service and driver service name.

Recommendations for Installing Agents in Virtual Desktop Infrastructure (VDI) Environment

Agent ID is generated based on various parameters, such as security identifier (SID) and SMBIOS Universal Unique Identifier (UUID). A SMBIOS UUID is a 128-bit number used to uniquely identify a host.

Note: While cloning the VDI image where an agent is already installed, the agent ID automatically changes for Windows and Mac agents if `uuid.action = keep` is not set in the .vmx file. For more information, see Configure a Virtual Machine to change the UUID.
For Linux agents, the agent ID does not change automatically on VDI clone.

When you clone a VDI image:

- If you do not change the agent ID for each VDI clone, make sure that the SMBIOS UUID remains the same.
- If you change the agent ID for each VDI clone, make sure that the SMBIOS UUID is also changed.

To avoid duplication of agent IDs, make sure that the SMBIOS UUID changes on the following VDIs:

- Citrix XenServer
- VMWare Workstation
- VMware vCloud Director

  For more information, see VMware Knowledge Base.
- vCenter hosted ESXi Server

To get the SMBIOS UUID on a Windows virtual host, execute the following command:

```
wmic csproduct get UUID
```

Troubleshooting

This section provides information about possible issues when using the NetWitness Endpoint.

Packager Issue

Issue	Failed to generate the agent installers.
Explanation	Some encryption software may create additional files that fails to generate the agent installers.
Resolution	Copy the packager to a machine that does not have antivirus or encryption software and then generate the agent installers.

Issue	Failed to generate agent installers for MAC.
Explanation	Agent packager `AgentPackager.exe` fails to generate MAC agent installer (`nwe-agent.pkg`) with the error message "Failed to generate table of content for package" or "Failed to create config file C:\AgentPackager (4)\agents\mac\Plugins\NWEInstallerPlugin.bundle\Contents\Resources\config.cfg".
Resolution	Run the `AgentPackager.exe` as administrator by right-clicking the file and selecting **Run as Administrator**.

Issue	Agent packager generates temporary agent installers for MAC.
Explanation	Agent packager `AgentPackager.exe` generates MAC agent installer as `nwe-agent_tmp.pkg` instead of `nwe-agent.pkg`.
Resolution	Run the `AgentPackager.exe` as administrator by right-clicking the file and selecting **Run as Administrator**. The MAC agent package `nwe-agent.pkg` will be generated as expected

Agent Upgrade via UI Issues

Issue	Agent upgrade not available.
Explanation	1. The agent version might not be supported for upgrade from UI. Agent version has to be latest for upgrade via UI. 2. Logged in user may not have appropriate permission for upgrade from UI. 3. Agent version is up-to date.
Resolution	1. Use the manual upgrade method for upgrading the version.

	2. Use admin user which have following permissions, endpoint-server.agentupdate.manage and endpoint-server.ca.manage. 3. No upgrade required. Agent version is already up-to date and no further upgrade is available.

Issue	Agent upgrade is in Pending state.
Explanation	The hosts for which the command is shown in pending could be in offline or inactive state.
Resolution	Ensure Hosts/agents are communicating with Endpoint server directly or via Relay server for it to receive the upgrade command from server. Verify "Agent Last seen" time in Host listing page.

Issue	Agent upgrade failed.
Explanation	1. Agent upgrade fail with any of the following reasons: • Service Name or Driver name mismatch • Checksum mismatch • Installer size mismatch 2. Agent installer could not be created.
Resolution	1. Retry upgrading the agent. If it continues to fail, use the manual upgrade method. 2. Check the permissions for the user initiated the upgrade command. User can be viewed in **Host** > **Agent History** page. User should have following permissions, `endpoint-server.agentupdate.manage` and `endpoint-server.ca.manage`.

Issue	Linux agent upgrade fails with an error, sudo not found.
Resolution	Make sure that the sudo package is installed on the agent machine.

Agent Uninstall via UI Issues

Issue	Agent uninstalled failed.
Explanation	Agent uninstall fails due to several unknown reasons.
Resolution	1. Retry uninstalling the agent. 2. Use the manual uninstall method. For more information, see Uninstalling Agent Manually.

Events Tracking Issues

Issue	Process events cannot be tracked on macOS 14 agent machine.
Explanation	The audit() framework used to track process events is deprecated in macOS 11 and disabled by default in macOS 14. As a result, the process events cannot be tracked on macOS 14 agent machine.
Resolution	For workaround, see **Enable Process Events Tracking on macOS 14** section in Introduction to Endpoint Agent Installation.