RSA NETWITNESS® PLATFORM

NetWitness Endpoint Agent Installation Guide

for RSA NetWitness® Platform 11.5

Contact Information

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

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

Distribution

March 2021

Contents

Introduction

Note: The information in this guide applies to Version 11.1 and later.

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

Windows

The agent software runs on the following Windows operating systems:

- Windows 7 (32 and 64-bit)
- Windows 8 (32 and 64-bit)
- Windows 8.1 (32 and 64-bit)
- Windows 10 (32 and 64-bit) (up to version 20H2)
- Windows 2008 R2 (32 and 64-bit)
- Windows 2012 Server
- Windows 2012 Server R2
- Windows 2016 Server
- Windows 2019 Server

Linux

The agent software runs on either i386 or x84_64 architecture and on the following Linux operating systems:

- CentOS 6.x, 7.x, and 8.x
- Red Hat Enterprise Linux 6.x, 7.x, and 8.x
- SUSE Linux Enterprise Server 12 SP3, 12 SP4, 12 SP5 and 15 SP1
- Ubuntu 16.04 LTS, 18.04 LTS, and 20.04 LTS

Mac

The agent software runs on the following Mac operating systems:

- macOS X 10.9 (Mavericks)
- macOS X 10.10 (Yosemite)
- macOS X 10.11 (El Capitan)
- macOS X 10.12 (Sierra)
- macOS 10.13 (High Sierra)
- macOS 10.14 (Mojave)
- macOS 10.15 (Catalina)
- macOS 11 (Big Sur) - Intel

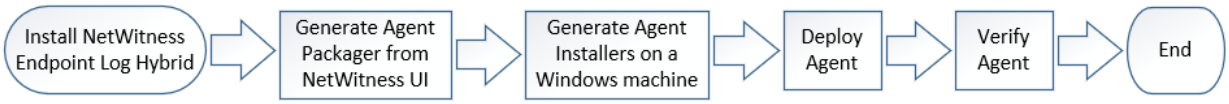
Hardware Requirements

The following are the minimum hardware requirements to run an agent in a host (laptops, workstations, servers, physical or virtual):

- 256 MB RAM
- 300 MB disk space
- Single-core CPU

Installation Flowchart

The following flowchart illustrates the Endpoint agent installation process:



Prerequisites

- Install RSA NetWitness Platform. 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*.
- To migrate an existing NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.5 and later, seehttps://community.rsa.com/docs/DOC-113735 to import the NetWitnes Endpoint 4.4.0.x configurations (file status, certificate status and blocked hashes).

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 Guide*.

Generate an Endpoint Agent Packager

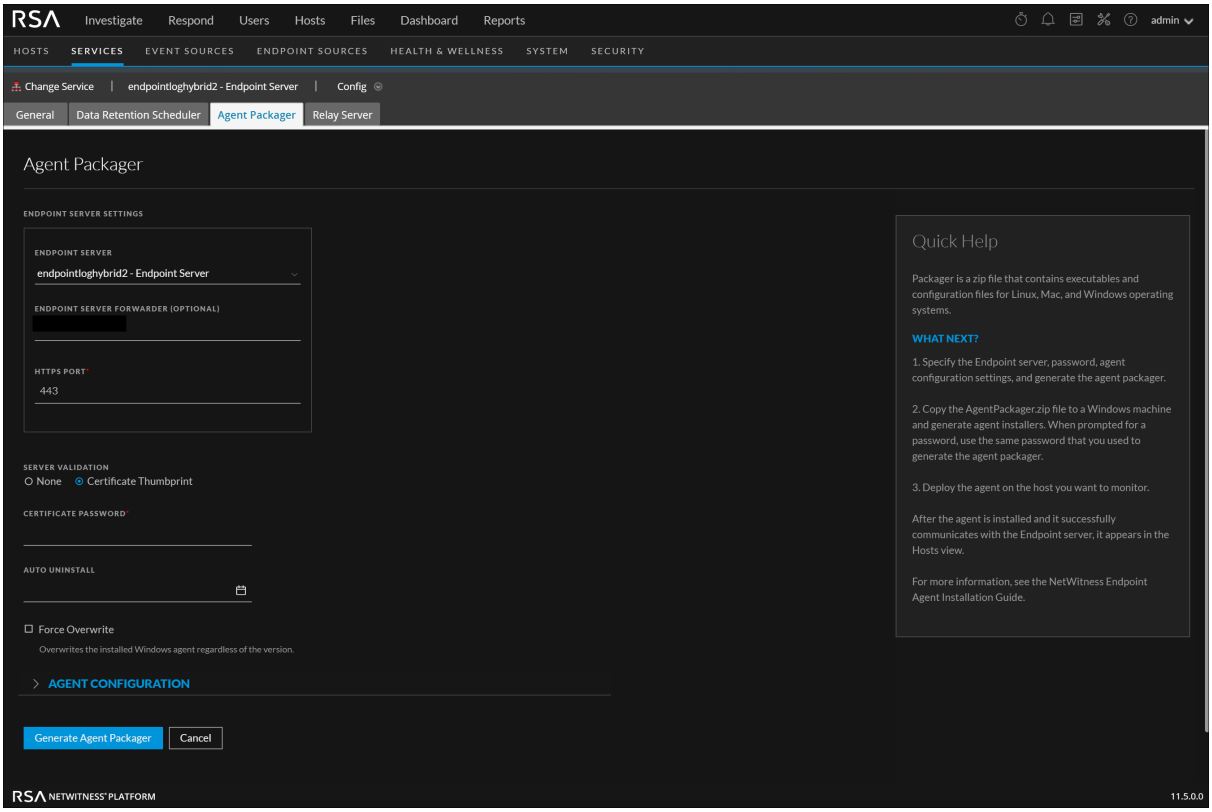
To generate an agent packager to collect endpoint data from hosts:

1. Log in to NetWitness Platform.

   Type `https://<NW-Server-IP-Address>/login` in your browser to get to the NetWitness Platform 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. Enter the values in the following fields:

Field	Description
Endpoint Server	Displays all the available Endpoint servers in the deployed.
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. For example, netwitness.
Auto Uninstall	Date and time the agent automatically uninstalls. You can leave it blank if not required.
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.	
Service	
Service Name	Name of the agent service. For example, NWEAgent.
Display Name	Display name of the agent service. For example, RSA NWE Agent.

Field	Description
Description	Description of the agent service. For example, RSA 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, RSA NWE Driver.
Driver Description	Description of the driver service. For example, RSA 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 Platform 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)
   - NWE000064.msi (for Windows)
   - nwe-agent.pkg (for Mac)
   - nwe-agent.i686.rpm (for RPM based Linux 32-bit)
   - nwe-agent.x86_64.rpm (for RPM based Linux 64-bit)
   - nwe-agent.i686.deb (for Debian based Linux 32-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.i686.rpm** (for 32-bit) or **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 names, you can enter one of the following commands:

`rpm -iv nwe-agent.i686.rpm` (for i386 architecture)

`rpm -iv nwe-agent.x86_64.rpm` (for x84_64 architecture)

Note: To upgrade RPM based Linux agents, run **rpm -Uvh nwe-agent.i686.rpm** or **rpm -Uvh nwe-agent.x86_64.rpm**.

Debian based Linux

Run the **nwe-agent.i686.deb** (for 32-bit) or **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 names, you can enter one of the following commands:

`dpkg -i nwe-agent.i686.deb` (for i386 architecture)

`dpkg -i nwe-agent.x86_64.deb` (for x84_64 architecture)

(Enter the administrator password when prompted.)

Note: To upgrade Debian based Linux agents, run **dpkg -i nwe-agent.i686.deb** or **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.

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/system.log | grep NWEAgent | grep Version
  ```

Uninstall Agents

This section provides the commands to uninstall the agent.

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 upgrade the 11.3.x and later versions of Endpoint agent to 11.5 or later.

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.

To upgrade from 11.3.x and later, download the 11.5 agent packager, deploy and verify agents. For more information, see Generate an Endpoint Agent Packager and Deploy and Verify Endpoint Agents.

Upgrade from 4.4.0.9 and 4.4.1.x is supported only for version 11.3. For more information, see *NetWitness Endpoint 4.4.1.x to NetWitness Platform 11.3 Migration Guide*.

To upgrade an agent from 4.4.0.x to 11.5, uninstall the agent and perform a fresh installation.

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 RSA 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