RSA NETWITNESS® PLATFORM

NetWitness Endpoint Agent Installation Guide

for RSA NetWitness® Platform 11.3

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

For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks.

License Agreement

Third-Party Licenses

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

April 2020

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. Generating an agent packager

2. 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.

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 1903)

- 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 and 7.x

- Red Hat Linux 6.x and 7.x

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)

Hardware Requirements

The following are the minimum hardware requirements to deploy an agent:

- 256 MB RAM

- 300 MB disk space

- Single-core CPU

Installation Flowchart

The following flowchart illustrates the Endpoint agent installation process:

```
      ╭─────────────────────╮
      │  Install NetWitness │
      │ Endpoint Log Hybrid │
      ╰─────────────────────╯
                │
                ▼
      ┌─────────────────────┐
      │   Generate Agent    │
      │    Packager from     │
      │    NetWitness UI     │
      └─────────────────────┘
                │
                ▼
      ┌─────────────────────┐
      │   Generate Agent    │
      │   Installers on a    │
      │  Windows machine     │
      └─────────────────────┘
                │
                ▼
      ┌─────────────────────┐
      │    Deploy Agent     │
      └─────────────────────┘
```

Linux Run **nwe-agent.rpm** or **nwe-agent(64-bit).rpm**	Mac Run **nwe-agent.pkg**	Windows Run **nwe-agent-package.exe**

```
      ┌─────────────────────┐
      │    Verify Agent     │
      └─────────────────────┘
                │
                ▼
      ╭─────────────────────╮
      │        End          │
      ╰─────────────────────╯
```
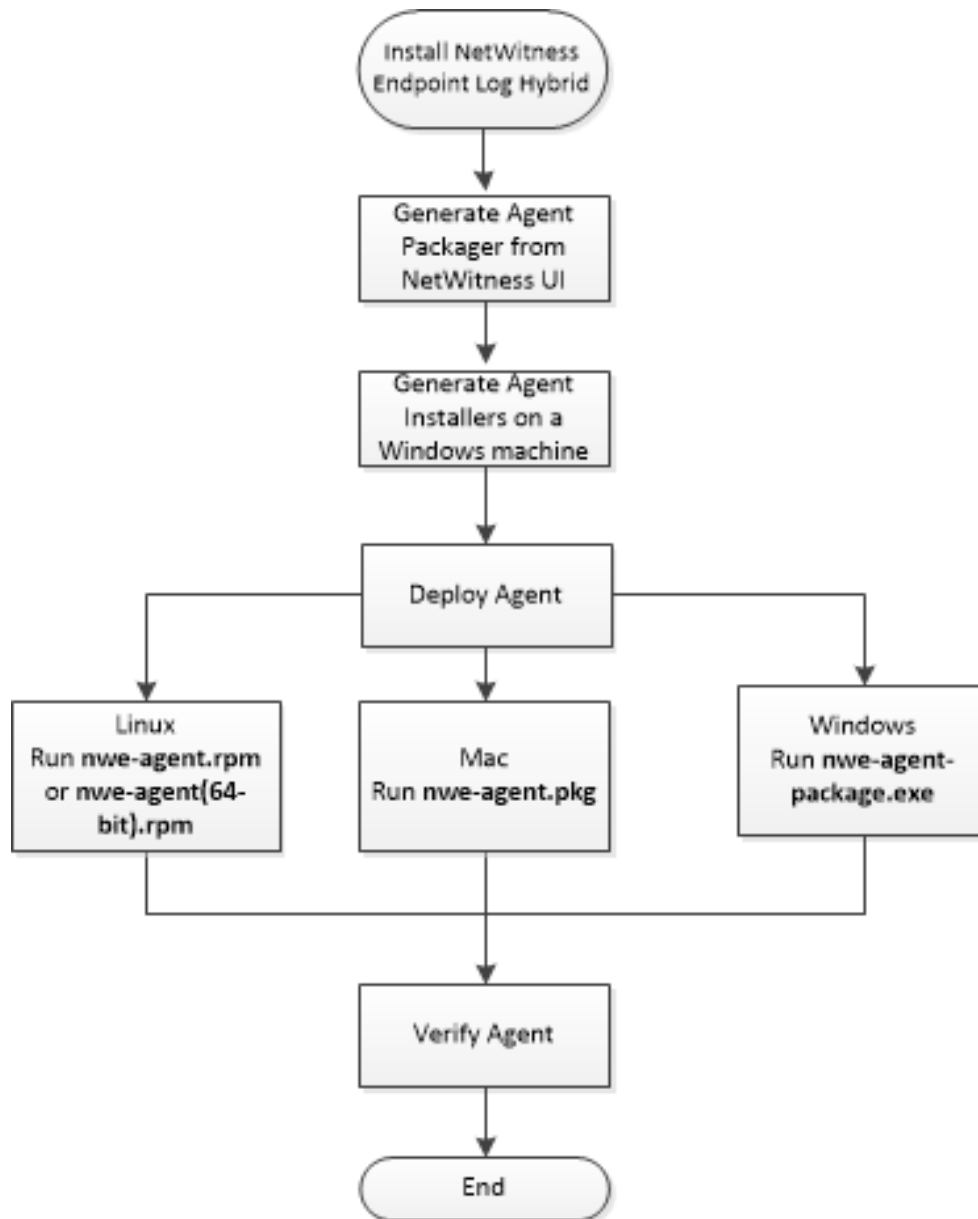
Prerequisites

- 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*.

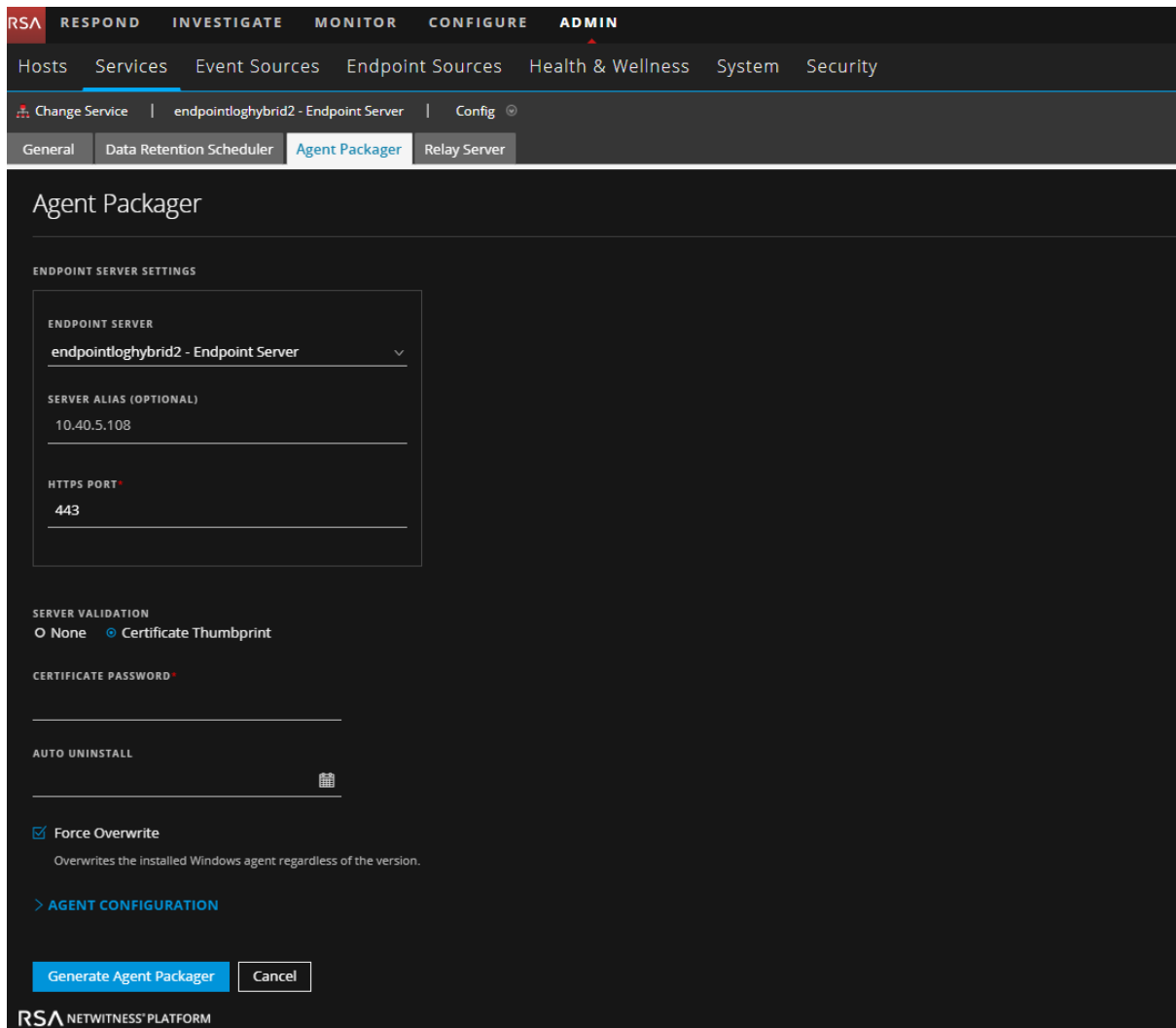# Generate an Agent Packager

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 deployment.
(Optional) Server Alias	Displays the alternate name of the Host name or IP on which the server can be reachable.
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>`
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, NWE.
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.

Field	Description
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 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.rpm (for Linux 32-bit)

   - nwe-agent(64-bit).rpm (for Linux 64-bit)

> **Note:** The MSI files should not be renamed.

Deploy and Verify 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 Investigate > 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 **Investigate** > **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 NWEAgent.

Deploying Agent (Linux)

To deploy the agent, run the **nwe-agent.rpm** (for 32-bit) or **nwe-agent(64-bit).rpm** (for 64-bit) file on the hosts you want to monitor.

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 could 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)

(Enter the administrator password when prompted.)

> **Note:** To upgrade Linux agents, run `rpm -U nwe-agent.i686.rpm` or `rpm -U nwe-agent.x86_64.rpm`.

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

  > **Note:** Click **Investigate > 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 Investigate > Hosts view contains the list of all hosts with an agent.

  > **Note:** Click **Investigate > 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
  ```

Configuring the Communication Between Endpoint Server and Endpoint Agents on Windows Vista, and 2008 Server

By default, the FIPS mode is enabled on the Endpoint Server, which means that agents installed on Windows Vista, and 2008 Server cannot communicate with the Endpoint server.

To resolve this, perform the following steps on the Endpoint Log Hybrid to disable the FIPS mode:

1. Go to `/etc/pki/tls/owb.cnf` and edit the file to disable the FIPS mode.

```
# FIPS Mode
#   Configures the BSAFE Libraries to be in FIPS Mode.
#
#   Values: "on", "off".
#   Default: "off"
fips mode = off
```

2. Go to `/etc/nginx/conf.d/nginx.conf` and edit the file to comment the following lines:

```
#    ssl_ciphers AES256+EECDH:AES256+EDH:!aNULL;
#    ssl_prefer_server_ciphers on;
```

3. Restart the Nginx server using the following command:

    ```
    systemctl restart nginx
    ```

Uninstall Agents

This section provides the commands to uninstall the agent.

Uninstalling Windows Agent

Run the following command:

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

Uninstalling Linux Agent

Run the following command:

```
rpm -ev 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 following versions of Endpoint agent to 11.3 and later:

- 4.4.0.0, 4.4.0.8, and 4.4.0.9

- 11.1.x and later

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

To upgrade from 11.1.x and later, download the 11.3 and later agent packager, and deploy the agent. For more information, see Generate an Agent Packager. After upgrading, the same host can be listed twice under **Investigate > Hosts** due to a change in the agent ID. To delete hosts with older agent version, see *NetWitness Endpoint User Guide*.

> **Note:** This is only applicable for Windows hosts. The agent ID remains the same for Linux and Mac.

To upgrade from 4.4.0.x, see *NetWitness Endpoint 4.4.0.x to NetWitness Platform 11.3 Migration Guide*.

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.

When you clone a VDI image, make sure that the SMBIOS UUID changes on the following VDIs to avoid duplication of agent IDs:

- Citrix XenServer

- VMWare Workstation

  > **Note:** In the .vmx file, make sure the `uuid.action = keep` is not set. For more information, see Configure a Virtual Machine to Keep the Same UUID.

- VMware vCloud Director

  For more information, see VMware Knowledge Base.

- vCenter hosted ESXi Server

To get the SMBIOS UUID on a 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.