



Endpoint Insights Agent Installation Guide

for Version 11.2



Copyright © 1994-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

Contact Information

RSA Link at <https://community.rsa.com> contains a knowledgebase 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 www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to Dell, 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 Dell.

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 RSA Link. 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

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

December 2018

Contents

- Introduction 4**
 - Supported Operating Systems 4
 - Windows 4
 - Linux 4
 - Mac 5
 - Hardware Requirements 5
 - Installation Flowchart 5
- Prerequisites 7**
- Generate an Endpoint Agent Packager 8**
 - Generating an Agent Packager for Endpoint Data Collection 8
 - Generating an Agent Packager with Windows Log Collection 10
- Generate Endpoint Agent Installers 15**
- Deploy and Verify Endpoint Agents 16**
 - Deploying Agents (Windows) 16
 - Verifying Windows Agents 16
 - Deploying Agent (Linux) 16
 - Verifying Linux Agents 16
 - Deploying Agent (Mac) 17
 - Verifying Mac Agents 17
 - Configuring the Communication Between Endpoint Server and Endpoint Agents on Windows Vista, 2008 Server, Mac OS X 10.9 and 10.10 17
- Uninstall Agents 19**
 - Uninstalling Windows Agent 19
 - Uninstalling Linux Agent 19
 - Uninstalling Mac Agent 19

Introduction

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

Hosts can be laptops, workstations, servers, tablets, routers, or any system, physical or virtual, where a supported operating system is installed. An Endpoint Insights 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 to collect only endpoint data or to collect both endpoint and log data (Windows only)
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 Windows logs (if enabled) from these hosts. It monitors activities and reports data and scan results to the Endpoint Hybrid or Endpoint Log Hybrid over HTTPs.

Supported Operating Systems

Windows

The agent software runs on the following Windows operating systems:

- Windows Vista (32 and 64-bit)
- 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)
- Windows 2008 Server (32 and 64-bit)
- Windows 2008 R2 (32 and 64-bit)
- Windows 2012 Server
- Windows 2012 Server R2
- Windows 2016 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:

- OS X 10.9 (Mavericks)
- OS X 10.10 (Yosemite)
- OS X 10.11 (El Capitan)
- macOS 10.12 (Sierra)
- macOS 10.13 (High Sierra)
- macOS 10.14 (Mojave)

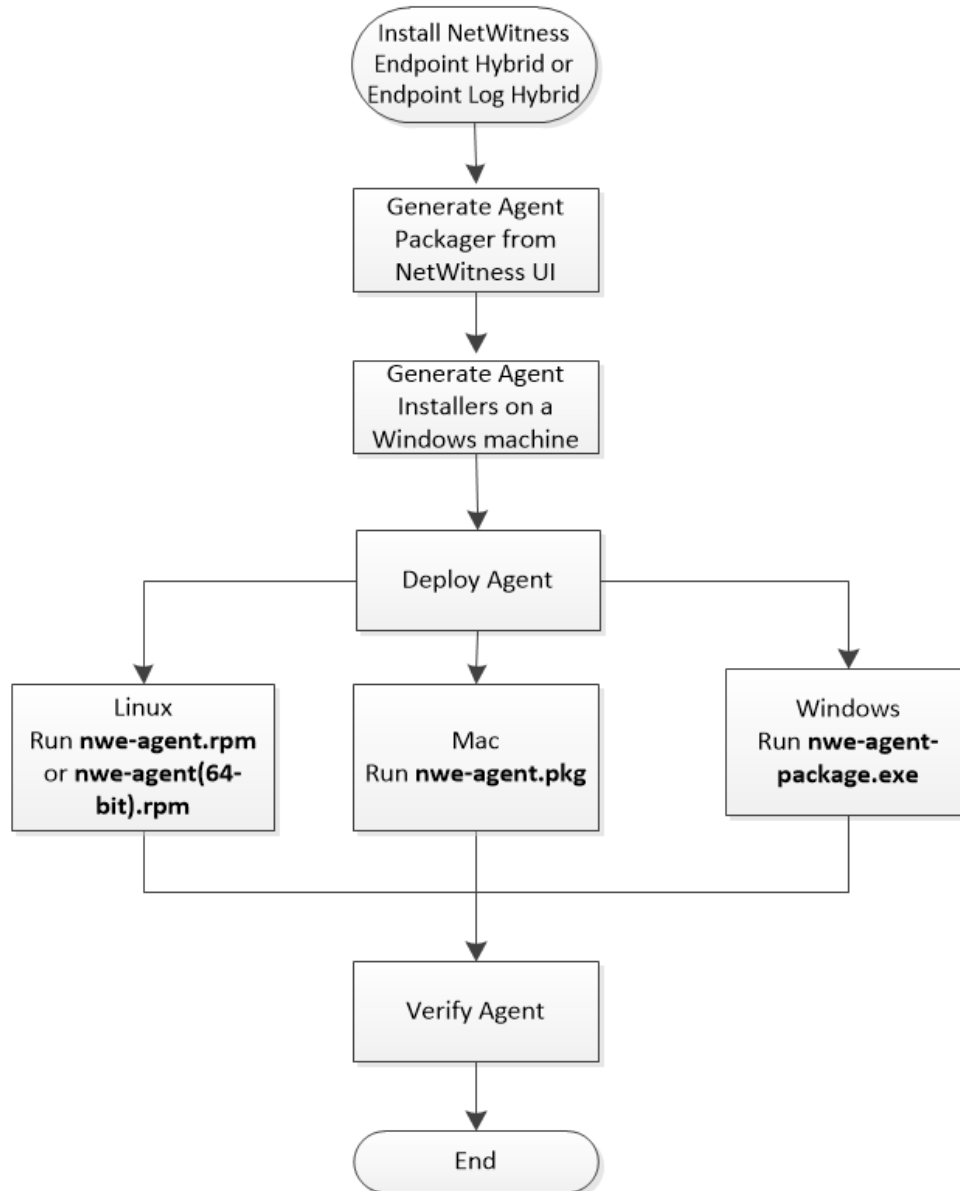
Hardware Requirements

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

- 256 MB RAM
- 100 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*.
- Configure NetWitness Endpoint Hybrid or Endpoint Log Hybrid. For more information, see the *Endpoint Insights Configuration Guide*.
- Configure Metadata Forwarding for the NetWitness Endpoint 11.1 Agents. For more information, see the *Endpoint Insights Configuration Guide*.

Generate an Endpoint Agent Packager

Generating an Agent Packager for Endpoint Data Collection

To generate an agent packager for collecting only 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 > Packager** tab. The

Packager tab is displayed.

The screenshot shows the 'Packager' configuration page in the RSA Endpoint Insights console. The navigation bar at the top includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this, there are tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Services' tab is active, and the 'Packager' sub-tab is selected. The breadcrumb trail shows 'Change Service' | 'rsanw-11.1.0.0.1850.e17-x8664 - Endpoint Server' | 'Config'. The configuration fields are as follows:

- ENDPOINT SERVER***: [Redacted]
- HTTPS PORT***: 443
- SERVER VALIDATION**: None, Certificate Thumbprint
- CERTIFICATE PASSWORD***: [Redacted]
- AUTO UNINSTALL**: [Redacted]
- Force Overwrite
- SERVICE NAME***: NWEAgent
- DISPLAY NAME***: RSA NWE Agent
- DESCRIPTION**: RSA Netwitness Endpoint
- Enable Windows Log Collection

At the bottom, there are three buttons: 'Reset', 'Generate Agent' (highlighted in blue), and 'Generate Log Configuration Only'.

4. Enter the values in the following fields:

Field	Description
Endpoint Server	Host name or IP address of the Endpoint Server. For example, 10.10.10.3.
HTTPS Port	Port number. For example, 443.
Server Validation	Determines how the agent validates the Endpoint Server certificate: <ul style="list-style-type: none"> • 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 as the previously installed agent, while creating a new agent. Note: If you want to force overwrite with MSI, run the following command: <code>msiexec /fvam <msifilename.msi></code>
Service Name	Name of the agent. This field is applicable only for Windows. For example, NWEAgent.
Display Name	Display name of the agent. This field is applicable only for Windows. For example, NWE.
Description	Description of the agent. This field is applicable only for Windows. For example, RSA NetWitness Endpoint.
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.

Generating an Agent Packager with Windows Log Collection



You can enable the Windows Log Collection feature in the agent while generating the agent packager. By enabling this option, a Log Configuration file is generated, and the agent can collect and forward Windows logs. To enable the Windows Log Collection:

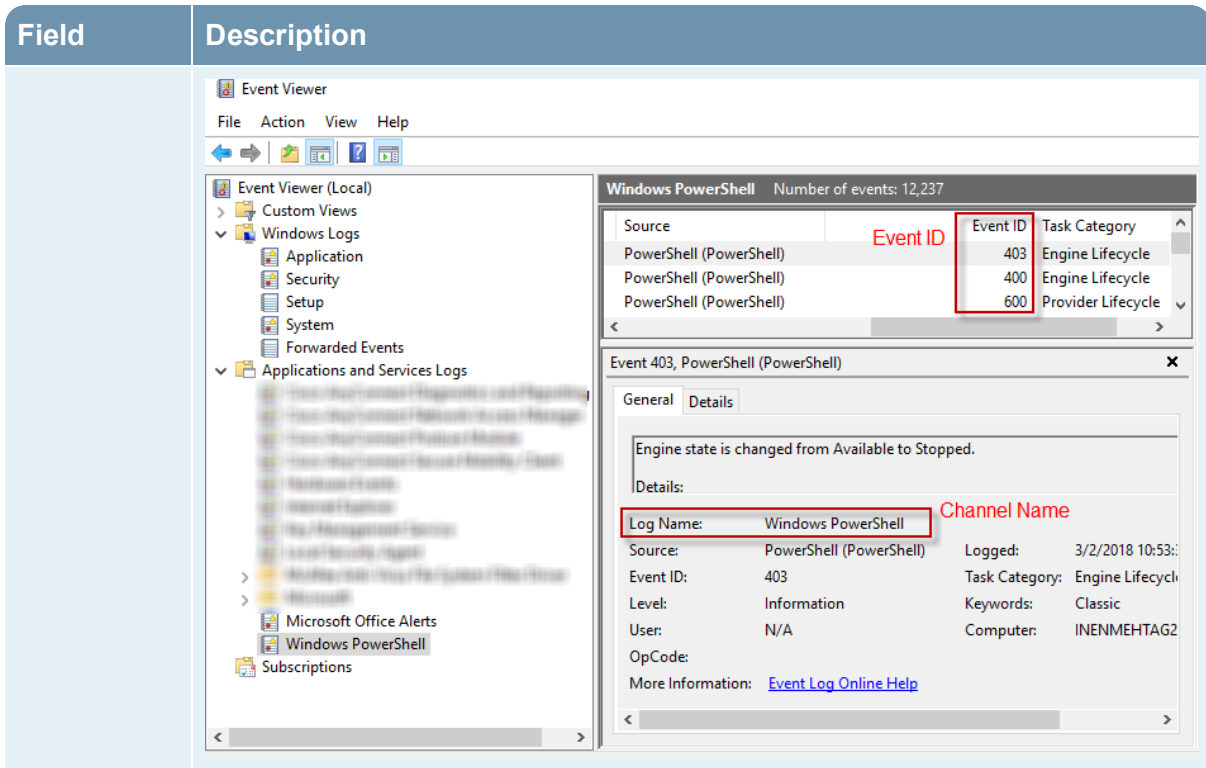
1. Perform steps 1 to 4 in [Generating an Agent Packager for Endpoint Data Collection](#).
2. Select **Enable Windows Log Collection**.

3. Enter or select the values in the following fields:

Field	Description
Configuration Name	Name of the configuration. Configuration name can have special characters, alphanumeric values, hyphens, spaces, and underscores.
Load Existing Configuration	Loads an existing configuration from the user system. The Windows Log Collection fields get populated with the information on a successful upload. <div style="border: 1px solid green; padding: 5px; margin-top: 5px;">Note: Warning messages are displayed during upload if there are any errors or warning.</div>

Field	Description
Primary Log Decoder/Log Collector	Primary Log Decoder or Log Collector for forwarding logs. This displays the list of Log Decoders or Remote Log Collectors in the current deployment. This field is a combination of display name of service, host name, and service type.
(Optional) Secondary Log Decoder/Log Collector	Secondary Log Decoder or Log Collector for forwarding logs. The secondary Log Decoder or Log Collector receives the Windows events if the agent cannot reach the primary Log Decoder or Log Collector. Note: When the Endpoint Agent is configured to use the UDP protocol and the Primary Log Decoder/ Remote Log Collector is not reachable, the secondary Log Decoder or Log Collector is not functional. The logs are not forwarded to the secondary Log Decoder or Log Collector when the primary is down, thus resulting in the event loss.
Protocol	Select the protocol from the drop-down menu. The available options are UDP, TCP, and TLS. By default, the protocol is TCP.

Field	Description
Channel Filters	<p>Channels from which the logs are collected. You can add or remove a channel filter. There should be at least one channel filter to collect the logs.</p> <ul style="list-style-type: none"> • Channel Name: Select the channel from the drop-down menu. The available options are System, Security, Application, Setup, and Forwarded Events. You can also create a custom channel by entering a custom channel name path. This is added to the channel name list. To find custom channels, go to the Windows Event Viewer on your computer. • Filter: Click  to add a channel filter. Click the drop-down menu to Include or Exclude the event IDs from a particular channel when generating the agent packager or the Log Configuration file. By default, for the Include option, the Event ID is set to ALL. For the Exclude option, the Event ID is set to blank. Click  to remove a channel filter. • Event ID: Enter the Event IDs for this channel. These are specific to channels and are the IDs that need to be collected. The event IDs can be numeric or a range. For example, use it in a range, 15-32. But, a reverse range is not allowed, for example, 32-15. Event IDs can also be used as combinations, for example, list of event IDs separated by commas, such as 248, 903, 16384, and so on. <div style="border: 1px solid green; padding: 5px; margin: 10px 0;"> <p>Note: When you enter ALL, it implies all event IDs for that channel.</p> </div> <p>You can use Windows Event Viewer to identify event IDs and channel name to be configured in the UI. The following example displays the navigation to get event ID and channel name for Windows Powershell. To view the information, go to Run and type <code>Event Viewer</code>, go to Applications and Services Logs > Windows Powershell. The event IDs and channel name in Application and Services Logs for Windows Powershell are displayed.</p>



Send test log Sends a test log message. By default, this option is enabled. A test log message is sent on a new agent deployment or configuration change from the agent to the Log Decoder. It contains all the fields configured for the agent. These events can help understand agents' connectivity to the destination.

Generate Agent Generates an agent packager. The Log Configuration file is created in the **AgentPackager.zip** file.

Generate Log Configuration Only Generates the Log Configuration file as per the parameters specified above or if uploaded using the Load Existing Configuration option.

Note: The content of the generated Log Configuration file should not be tampered. If any changes are made, the agent does not read the information from the file.

Note: You can enable the Windows Log Collection feature later by downloading and deploying the Log Configuration file. For more information, see "Add/Update Windows Log Collection file using Endpoint Agent" in the *Log Collection Configuration Guide*.

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.
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)
 - nwe-agent.pkg (for Mac)
 - nwe-agent.rpm (for Linux 32-bit)
 - nwe-agent(64-bit).rpm (for Linux 64-bit)

Deploy and Verify Endpoint Agents

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

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.

- 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. Use the 32-bit rpm for i386 and 64-bit rpm for x84_64 machines.

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, 2008 Server, Mac OS X 10.9 and 10.10

By default, the FIPS mode is enabled on the Endpoint Server, which means that agents installed on Windows Vista, 2008 Server, Mac OS X 10.9 and 10.10 cannot communicate with the Endpoint server.

To resolve this, perform the following steps on the Endpoint Hybrid or 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`