RSA NETWITNESS® PLATFORM

Endpoint Insights Configuration Guide

for Version 11.2

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

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 2019

Contents

NetWitness Endpoint Insights Overview

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

RSA NetWitness Endpoint collects endpoint data from Windows, Mac, or Linux hosts, which can be used to investigate, report, alert, and perform analysis. Analysts can perform instant scans for detailed insights of the host behavior at any point in time. In addition, Endpoint can collect logs from Windows hosts. The NetWitness Endpoint Insights introduces two host types - Endpoint Hybrid and Endpoint Log Hybrid. You can only install one instance of the host type in your deployment. This means, you can deploy either one instance of Endpoint Hybrid or Endpoint Log Hybrid. You cannot change the type once deployed.

Endpoint Hybrid - collects and manages endpoint (host) data. It generates metadata for investigation, analysis, alerting, and reporting. It is configured and managed similar to a Log or Packet Decoder. The Endpoint Hybrid runs an Nginx server (in a reverse proxy mode) that receives data from the Endpoint agent. The following services run on the Endpoint Hybrid:

- Endpoint Server - Manages data received through Nginx, stores it in the Mongo database, and sends metadata to the Log Decoder.
- Log Decoder - Captures data from the Endpoint Server and processes the metadata.
- Concentrator - Aggregates metadata from the Log Decoder and makes it available for all upstream components like Investigate, Reporting Engine, and Event Stream Analysis similar to other NetWitness Decoder and Concentrator setup.

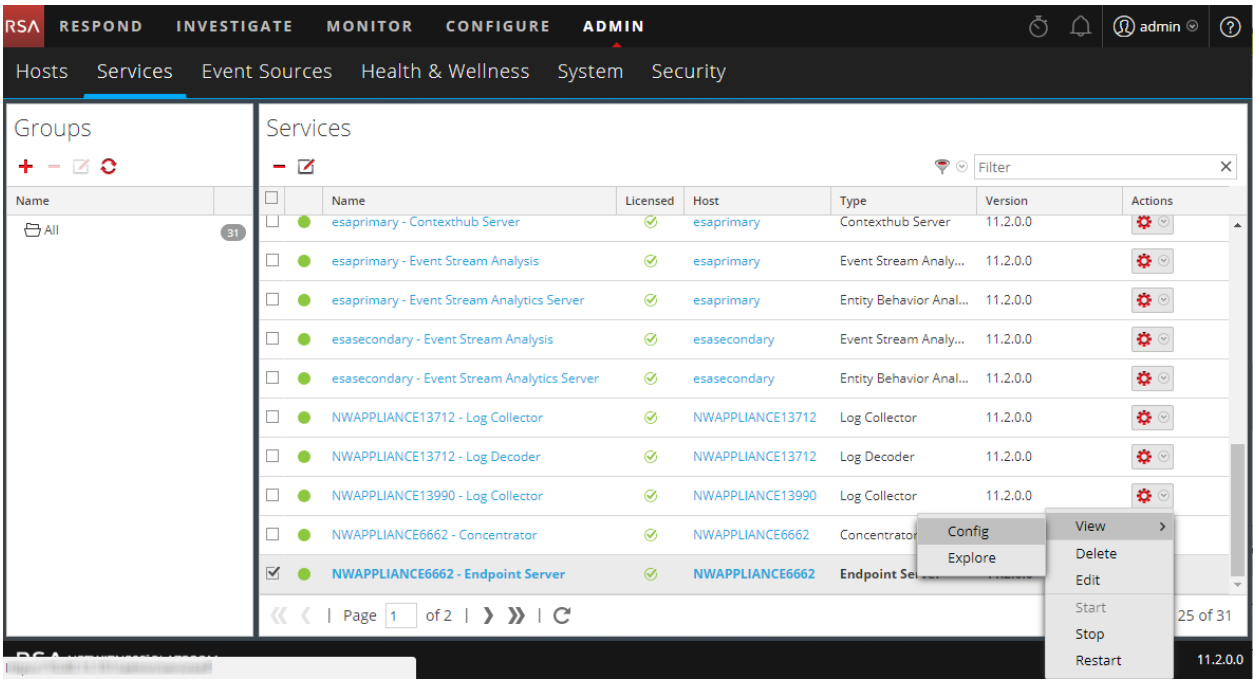
Endpoint Log Hybrid - captures endpoint and log data. In addition to the services running on the Endpoint Hybrid, a Log Collector service runs on the Endpoint Log Hybrid. It collects logs from Windows hosts, and all other event sources that are supported for the Log collection in the NetWitness Platform.

The *Hosts and Services Getting Started Guide* provides the information you need to understand and install all the NetWitness Platform services.

Basic configuration involves:

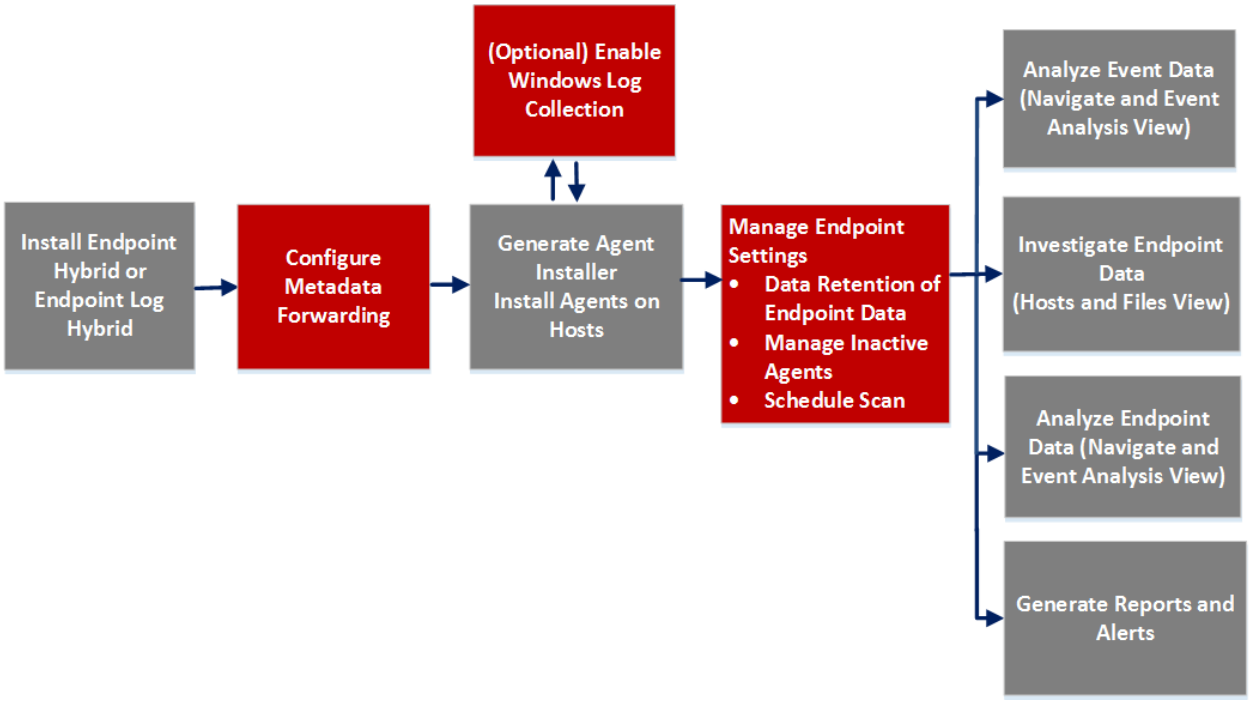
- Installing agents on hosts
- Configuring Endpoint meta forwarding, schedule scan, and retention policies
- Defining health and wellness policies to monitor Endpoint Server.

You can configure the required settings using the options in the NetWitness Platform user interface under Administration Services Config view (**ADMIN > Services > Endpoint Server > Config**).


RSA
RESPOND
INVESTIGATE
MONITOR
CONFIGURE
ADMIN
admin
Hosts
Services
Event Sources
Health & Wellness
System
Security
Groups
Name
All
31
Services
Filter
Name
Licensed
Host
Type
Version
Actions
esaprimary - Contexthub Server
esaprimary
Contexthub Server
11.2.0.0
esaprimary - Event Stream Analysis
esaprimary
Event Stream Analy...
11.2.0.0
esaprimary - Event Stream Analytics Server
esaprimary
Entity Behavior Anal...
11.2.0.0
esasecondary - Event Stream Analysis
esasecondary
Event Stream Analy...
11.2.0.0
esasecondary - Event Stream Analytics Server
esasecondary
Entity Behavior Anal...
11.2.0.0
NWAPPLIANCE13712 - Log Collector
NWAPPLIANCE13712
Log Collector
11.2.0.0
NWAPPLIANCE13712 - Log Decoder
NWAPPLIANCE13712
Log Decoder
11.2.0.0
NWAPPLIANCE13990 - Log Collector
NWAPPLIANCE13990
Log Collector
11.2.0.0
NWAPPLIANCE6662 - Concentrator
NWAPPLIANCE6662
Concentrator
NWAPPLIANCE6662 - Endpoint Server
NWAPPLIANCE6662
Page 1 of 2
25 of 31
Config
Explore
View
Delete
Edit
Start
Stop
Restart
11.2.0.0

Endpoint Server Configuration

This topic provides the high-level tasks required to configure the Endpoint Server service.



Tasks	Description
Install the Endpoint Hybrid or Endpoint Log Hybrid	See *Physical Host Installation Guide* and *Virtual Host Setup Guide*.
Configure Metadata Forwarding for the NetWitness Endpoint 11.1 Agents	Similar to Logs and Packets, you can view Endpoint metadata in the Navigate and Event Analysis view. You can also generate reports and alerts for the Endpoint data. By default, the Endpoint Meta option is disabled. The agent must be installed with the Endpoint Meta option enabled to forward metadata.

Tasks	Description
Install Agents on Hosts	The Endpoint agent installer is generated using the Packager tab under **ADMIN > Services > Config > Endpoint Server** from the NetWitness Platform user interface. The Packager is a zip file that contains executables and configuration files for generating agent installer for Linux, Mac, and Windows operating systems. You can install only one version of the agent on a host. If you have a previous version of an agent installed (for example, 4.4), uninstall this agent to install the 11.1 agent. After the agent is installed, it appears on the **Investigate > Hosts** view. By default, the Endpoint data is posted for the first time. To collect subsequent Endpoint data, you have to either schedule a scan or perform ad hoc scan. It retrieves data, such as drivers, processes, DLLs, files (executables), services, autoruns, security information, system configurations, and scripts found on the host. If the agent is configured for Log collection, it collects logs from Windows hosts, and forwards them to a Log Decoder or Remote Log Collector. For more information on Endpoint agent installation, see *Endpoint Insights Agent Installation Guide*.
Investigate Endpoint data	You can investigate the Endpoint data in the **Investigate > Hosts** and **Investigate > Files** views. For more information, see *NetWitness Investigate User Guide*.
Configure Scan Schedule	Schedule a scan either to run daily or weekly.
Configure Data Retention Policy	Define data retention policies to optimally store and manage the Endpoint data based on the age of the Endpoint data or the storage size. By default, 30 days of agent data is retained.
Manage Inactive Agents	By default, agents (including all the collected Endpoint data) that have not communicated with the Endpoint Server for 90 days will be automatically deleted.

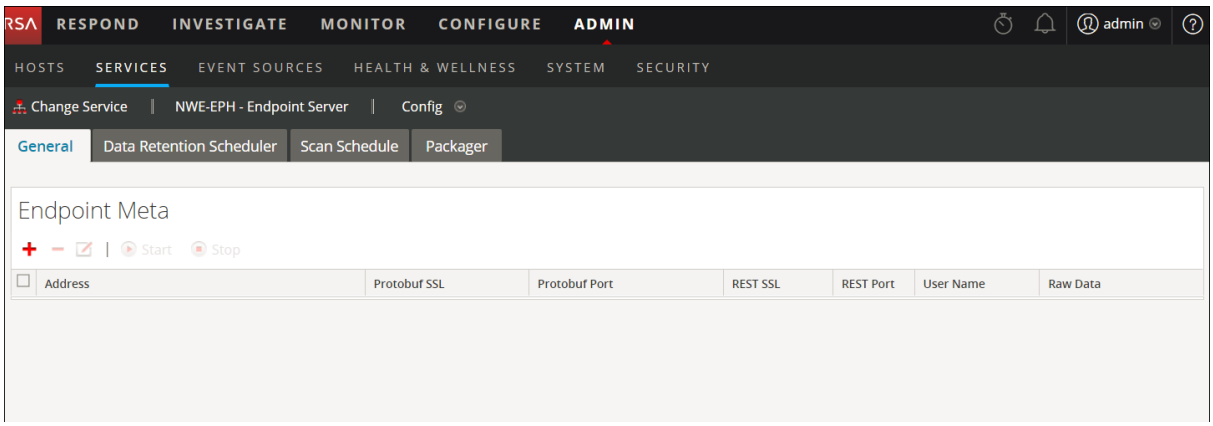
Configure Metadata Forwarding for the NetWitness Endpoint 11.1 Agents

You can view the Endpoint metadata in the NetWitness Platform Investigate (**Navigate** and **Event Analysis** views) similar to Logs and Packets. You must enable the metadata forwarding to forward the following categories:

Operating System	Categories
Windows	File, Service, DLL, Process, Task, Autorun, and Machine
Linux	File, Autrorun, Loaded Library, Systemd, Process, Cron, Initd, Machine
Mac	File, Daemon, Process, Task, Loaded Library, Autorun, Machine

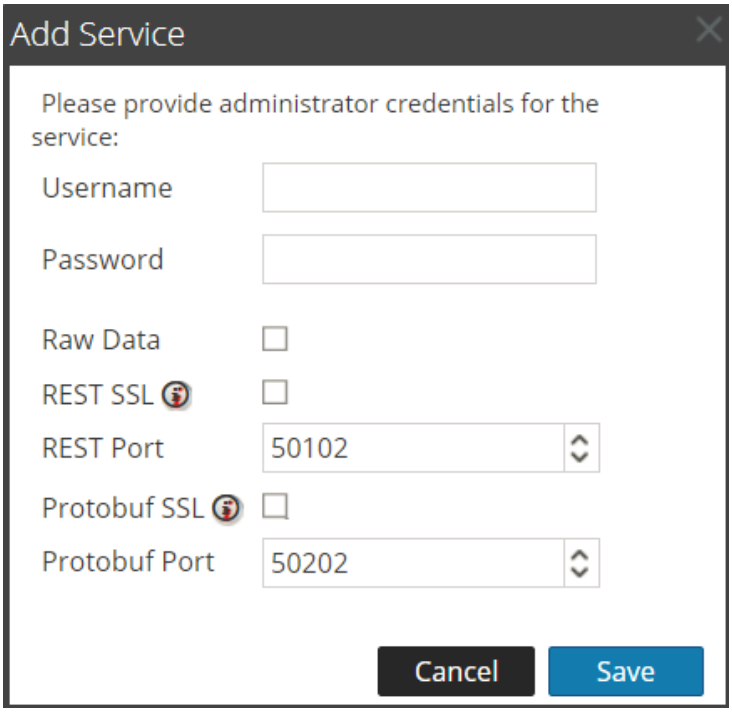
Configuring Metadata Forwarding

1. Go to **ADMIN** > **Services**.
2. In the Services view, select the **Endpoint Server** service.
3. Click  and select > **View** > **Config**.
4. Click the **General** tab.



5. Click  in the toolbar.
   The Available Services dialog is displayed.

6. Select the Log Decoder service and click **OK**.
   The Add Service dialog is displayed. You can add only one Log Decoder service.



7. Enter the administrator credentials for authentication.
8. (Optional) If you enable Raw Data, a brief summary of the session along with the metadata is sent.
9. (Optional) If you have enabled SSL on the REST port in the Log Decoder, select the **REST SSL** option. By default, the REST port for non-SSL is 50102 and SSL is 56102.
10. Select the **Protobuf SSL** option to enable SSL on Protobuf. By default, the Protobuf port is 50202.
11. Click **Save**.

After configuring the metadata forwarding, make sure to:

- Start the capture on the Log Decoder
- Start the aggregation on the Concentrator
- Add the Log Decoder as a service in the **Concentrator**

Starting Metadata Forwarding to the Log Decoder

1. In the Endpoint Meta config view, select the service.
2. Click Start
   The Endpoint Server starts forwarding the metadata to the Log Decoder.

Stopping Metadata Forwarding to the Log Decoder

1. In the Endpoint Meta config view, select the service.
2. Click Stop.
   The Endpoint Server stops forwarding the metadata to the Log Decoder.

Removing Metadata Forwarding

Note: Make sure you stop the service, before removing the metadata forwarding.

1. In the Endpoint Meta config view, select the service.
2. Click  .
3. Click **Apply**.

Endpoint Metadata Mappings

You can view the default metadata mappings or modify the metadata mappings for endpoints.

JSON Schema for Metadata Mappings

All metadata mappings is configured using the JSON schema. The following is a sample JSON schema:

```
{
"metaKeyPairs" : [
     {
     "metaKeyPairsCategory" : "",
     "keyPairs" : [
          {
          "endpointJpath" : "",
          "metaName" : "",
          "type" : "",
          "enabled" : true
          },
          {
          "endpointJpath" : "",
          "metaName" : "",
          "type" : "",
          "enabled" : true
          }
      ]
      }
```

```
]
}
```

The following APIs are used to view or modify the metadata mappings:

- `get-default` - Returns the default configurations for the endpoint metadata mappings.
- `get-custom` - Returns the custom configurations for the endpoint metadata mappings.
- `set-custom` – Helps customize the endpoint metadata mappings.

Viewing the Metadata Mappings

To view the endpoint metadata mappings:

1. On the NW server, run the `nw-shell` command from the command line.
2. Run the `login` command and enter the credentials.
3. Connect to the Endpoint Server using the following command:
   `connect --host <IP address> --port <number>`

Note: The default port is 7050.

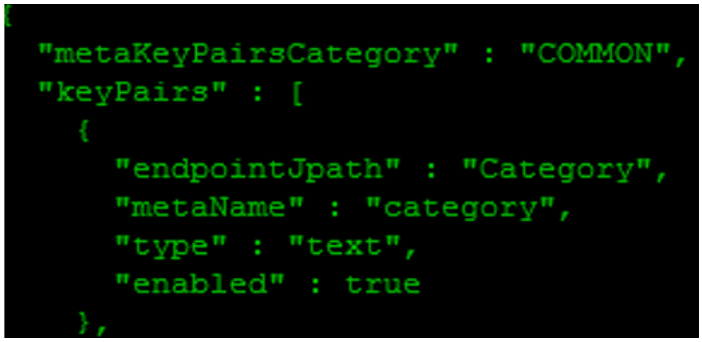
4. Run the following commands:
   ```
   cd endpoint/meta
   cd get-default
   invoke
   ```

The following screen shows the default metadata mappings:

To disable a default metadata mapping:

Enter the same endpointJpath value and set the enabled parameter to `false`.

For example, if the endpointJpath is `Category` and enabled parameter is `true`, enter the same endpointJpath and set the enable parameter to `false`.



Note: Do not modify the metaKeyPairsCategory in the schema; “COMMON”, “COMMON_MACHINE”, “COMMON_MACHINE_FOR_EVENTS”.

To change the metadata name or metadata type:

Enter the same endpointJpath value and specify values for the metaName and type.

Note: The metaName must exist in the table-map.xml of the Log Decoder, index-concentrator.xml or index-concentrator-custom.xml file of the Concentrator, for the metaName to appear on the Investigate view.

Adding or Modifying Metadata Mappings

To add or modify the metadata mappings, run the `set-custom` API. The metaKeyPairs configuration provided in the JSON file should match the JSON schema of the default configuration received through the `get-default` API.

1. On the NW server, run the `nw-shell` command from the command line.
2. Run the `login` command and enter the credentials.
3. Connect to the Endpoint Server using the following commands:

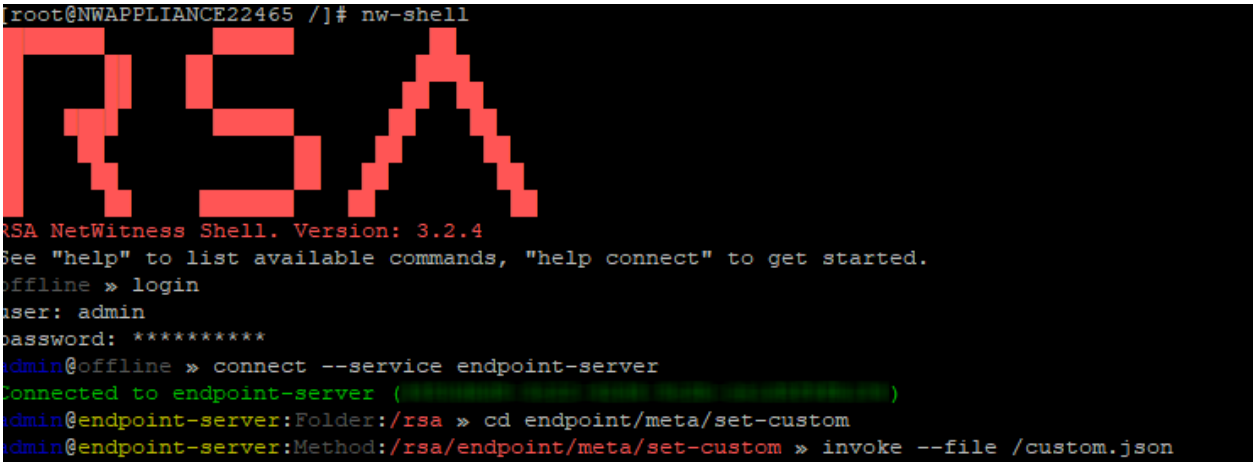
   ```
   connect --service endpoint-server
   ```

   Note: The default port number is 7050.

4. Run the following commands:

   ```
   cd endpoint/meta
   cd set-custom
   invoke --file <json file>
   ```

You can add new meta keys by adding entries to the file that will be uploaded using the `set-custom` API. The following example shows how to add a new metadata mapping:



Viewing the Custom Metadata Mappings

To view the custom metadata mappings, run the `get-custom` API, and then invoke commands.

Note: The `get-custom` API will return values only if the metadata mappings are modified using the `set-custom` API.

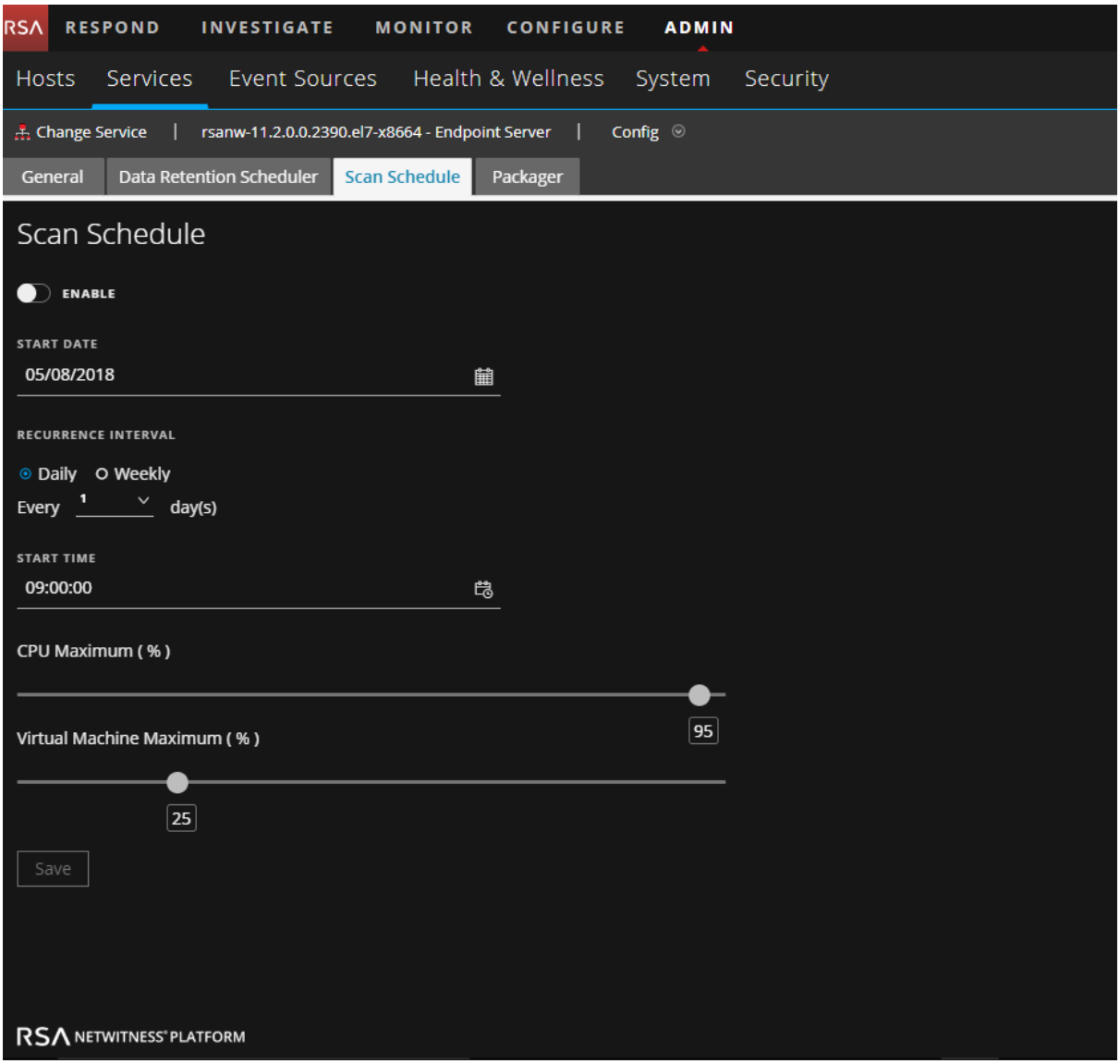
Configure Scan Schedule

You can schedule a scan to run daily or weekly.

Note: Only one schedule can be configured and is applicable to all the agents.

To configure a scan schedule:

1. Go to **ADMIN** > **Services**.
2. In the Services view, select the **Endpoint Server** service.
3. Click  and select > **View** > **Config**.
4. Click the **Scan Schedule** tab.



5. Click the **Enable** toggle switch to configure the scan.
6. Select the **Start Date**.
7. Select the recurrence interval - Daily or Weekly.

   Note: The values entered are specific to the agent time zone.

8. For a daily scan:
   - Select recurrence interval as **Daily**.
   - Specify the frequency of scan in days.
9. For a weekly scan:
   - Select recurrence interval as **Weekly**.
   - Specify the frequency of scan in weeks.
   - Select the day of the week.
10. Enter the start time of the scan.
11. Set the CPU Maximum value using the slider. This ensures the CPU limit of the NetWitness Endpoint Agent. If the agents are running on the virtual machines, set the Virtual Machine Maximum value using the slider.
12. Click **Save** to save the configuration.

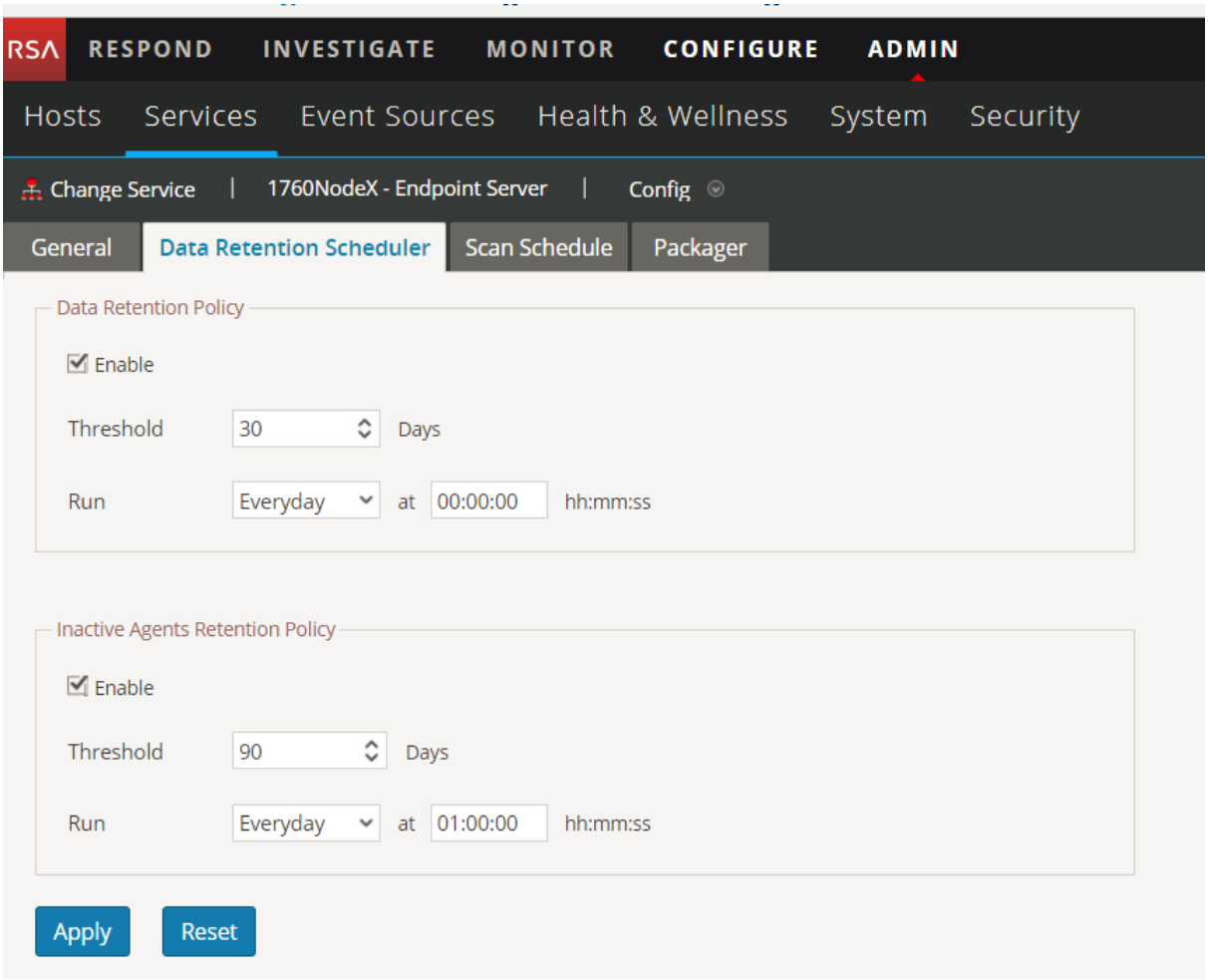
Note: If an agent is not able to perform the scan at the scheduled time because the machine is powered off or agent service is stopped, the next scan is based on the time difference between the current time and the next scheduled scan time.
For example, if a scan is scheduled to run every Wednesday at 6 PM and the agent service has stopped before the scan start time, and if the service is up on Thursday 10 AM, the agent will wait for the system to be fully up and running and immediately run a scan.
But if the service is up on the following Monday at 1 PM, the scan will run on the following Wednesday at 6 PM.

Configure Data Retention Policy

An administrator can configure the retention policies to retain the Endpoint data based on the age or the storage size. By default, days and size-based retention policies are enabled.

To change the configuration for age-based retention:

1. Go to **ADMIN** > **Services**
2. In the Services view, select the **Endpoint Server** service.
3. Click  and select > **View** > **Config**.
4. Click the **Data Retention Scheduler** tab.

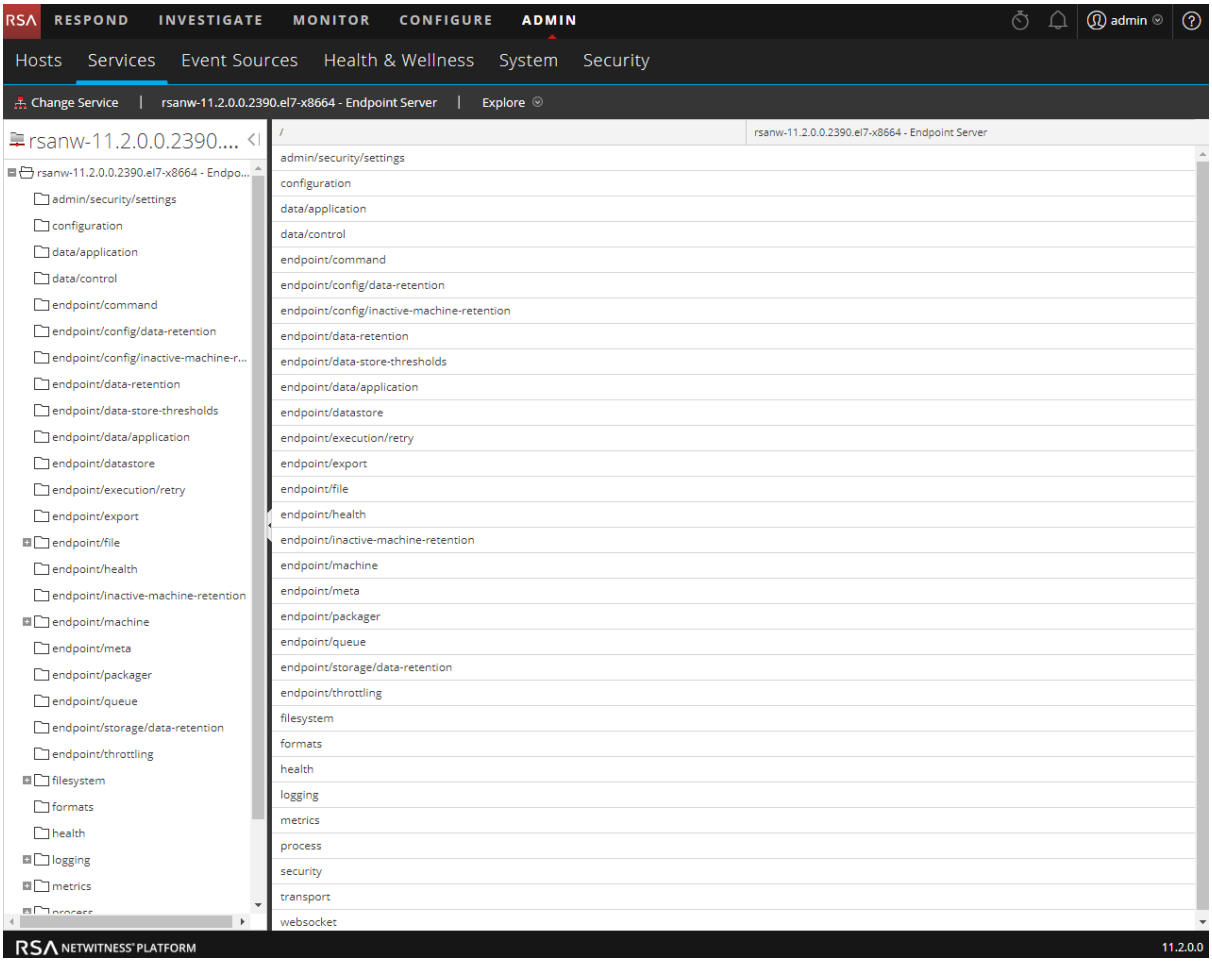


5. In the **Data Retention Policy** panel, by default, the **Threshold** is set to 30 days, and **Run** to Everyday. This means only 30 days of Endpoint data is retained and the older data is deleted from the database.
6. Click **Apply**.

To change the configuration for size-based retention:

By default, for the size-based retention, the `rollover-after` value is set to 80 and `rollover-chunk-size` is set to 10. This means that when the storage size exceeds 80 percent of the space allocated for the disk partition, 10 percent of the older Endpoint data is deleted from the database. However, you can change these values as follows:

1. Go to **ADMIN** > **Services**.
2. In the Services view, select the **Endpoint Server** service.
3. Click  and select > **View** > **Explore**. The Explore view is displayed:



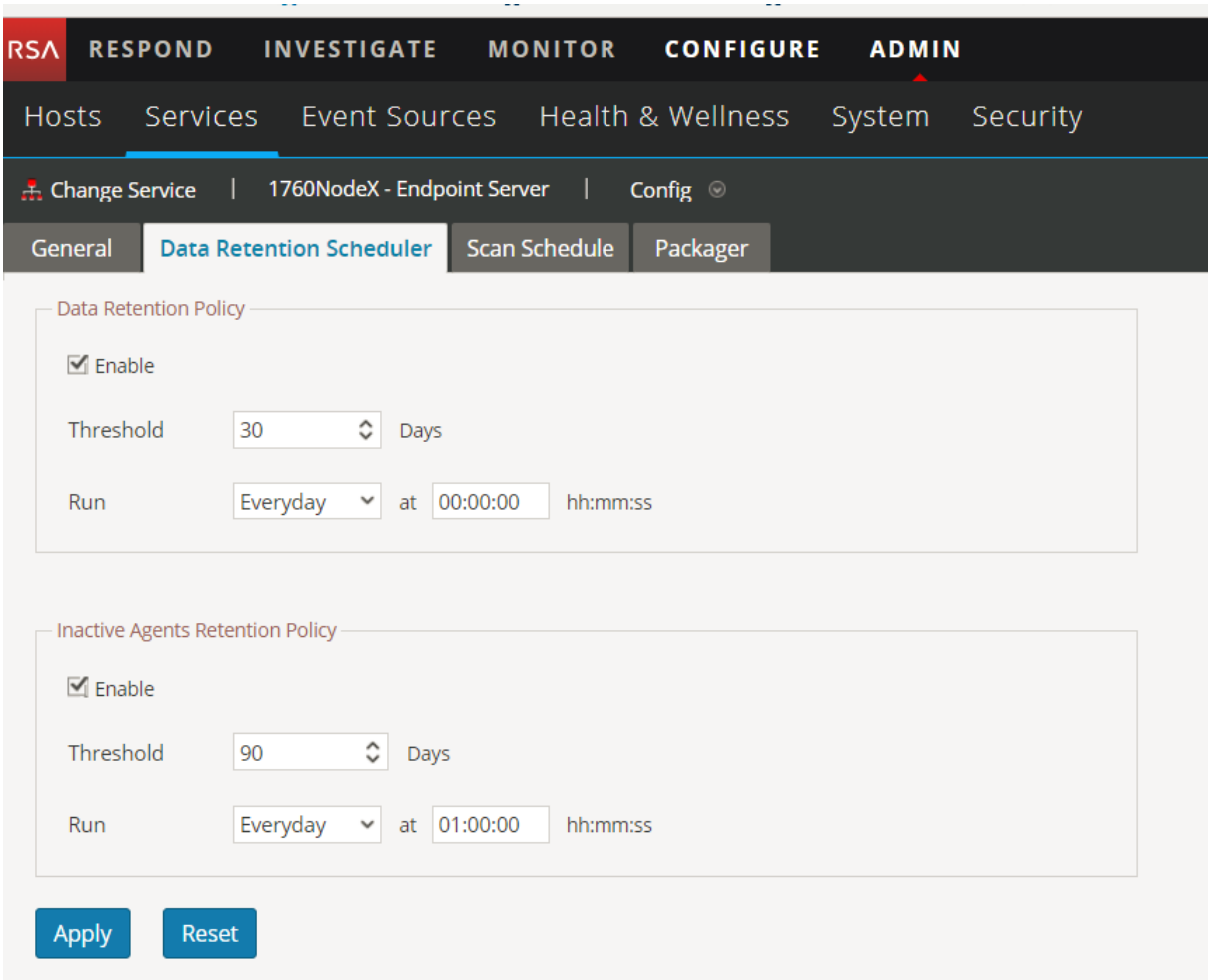
4. In the left panel, select **endpoint/config/data-retention**.
5. Edit the configurations based on your requirements.

Manage Inactive Agents

An administrator can configure the inactive agent retention policy to delete data of agents that are inactive, from the Endpoint Server. On deletion, the Endpoint Server stops collecting data from these agents. By default, this option is enabled.

To configure the inactive agent retention policy:

1. Go to **ADMIN** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click  and select > **View** > **Config**.
4. Click the **Data Retention Scheduler** tab.



5. In the **Inactive Agents Retention Policy** panel, by default, the **Threshold** is set to 90 days and **Run** to Everyday. This means that the data of agents that have not communicated with the Endpoint server for 90 days is deleted from the database.
6. Click **Apply**.

Note: The Inactive Agents Retention Policy is not applicable for NetWitness Endpoint 4.4.0.2 or later agents.

Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Endpoint 11.1

You can configure the Endpoint Metadata for the NetWitness Endpoint 4.4.0.2 in one of the following ways:

- **(Option 1) Integrate the NetWitness Endpoint 4.4.0.2 Console Server to an Endpoint Hybrid or Endpoint Log Hybrid** - The NetWitness Endpoint 4.4.0.2 or later agents data will be available in the **Investigate > Hosts** and **Files** view, and you can view the Endpoint metadata in the **Investigate > Navigate** and **Event Analysis** view. For this option, make sure the Endpoint sever is configured for meta forwarding. This integration includes the following steps:
  - Configuring the Client Certificate on the NetWitness Endpoint 4.4.0.2 Console Server
  - Enabling the Metadata Forwarding in the NetWitness Endpoint 4.4.0.2
  - Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server
- **(Option 2) Integrate the Meta Integrator service in the NetWitness Endpoint 4.4.0.2 directly to a Log Decoder** - You can view the Endpoint metadata in the **Investigate > Navigate** and **Event Analysis** view. The NetWitness Endpoint 4.4 agents data will not be available in the **Investigate > Hosts** and **Files** view. This integration includes the following steps:
  - Enabling the NetWitness Endpoint 4.4.0.2 Meta Forwarding to the Log Decoder
  - Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server

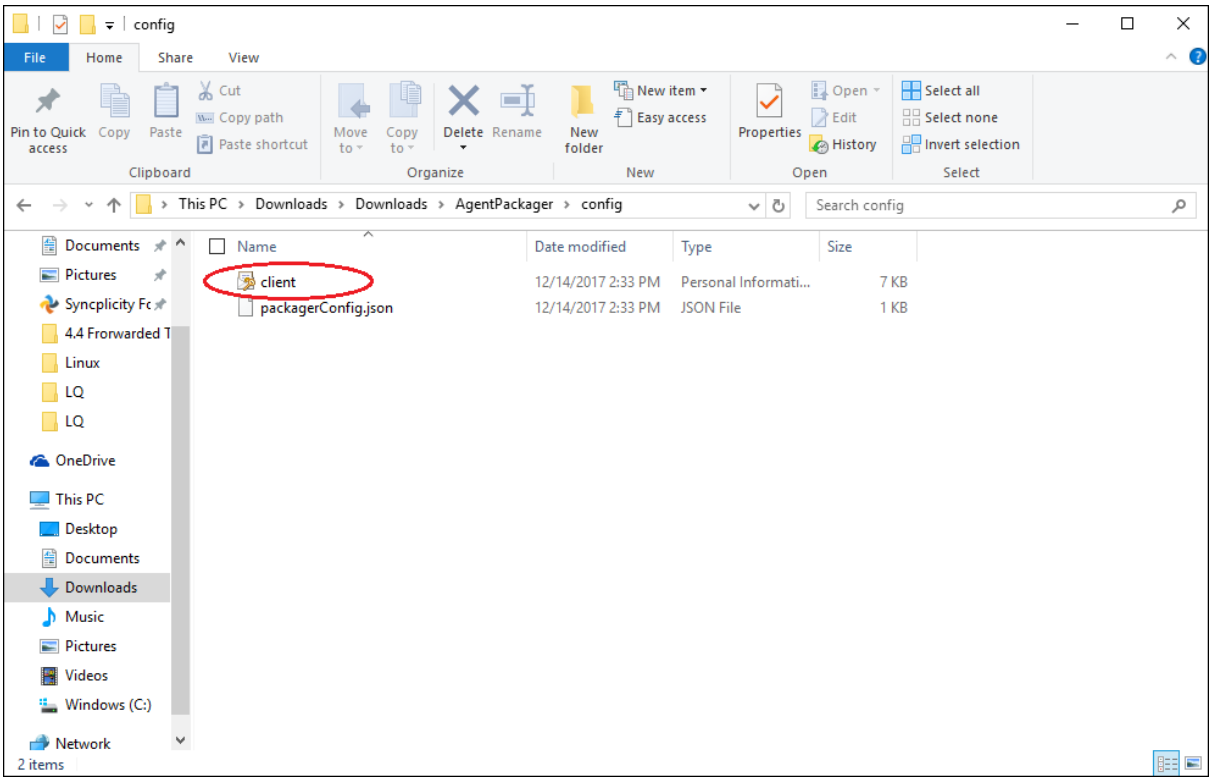
In addition to the categories mentioned for the NetWitness Endpoint 11.1 agents, the following categories are also forwarded for the NetWitness Endpoint 4.4.0.2 or later agents - File event, Network event, Registry event, and Process event.

(Option 1) Configuring the NetWitness Endpoint 4.4.0.2 Console Server

Configuring the Client Certificate on the NetWitness Endpoint 4.4.0.2 Console Server

The NetWitness Endpoint 4.4.0.2 Console Server must use the same client certificate that the NetWitness Endpoint 11.1 agents use to forward the metadata to the Endpoint Server.

1. Download the agent packager. For more information, see *Endpoint Insights Agent Installation Guide*.
2. Extract **AgentPackager.zip** and from the Config folder, obtain the client certificate.
3. Copy the client certificate to the NetWitness Endpoint 4.4 Console Server.

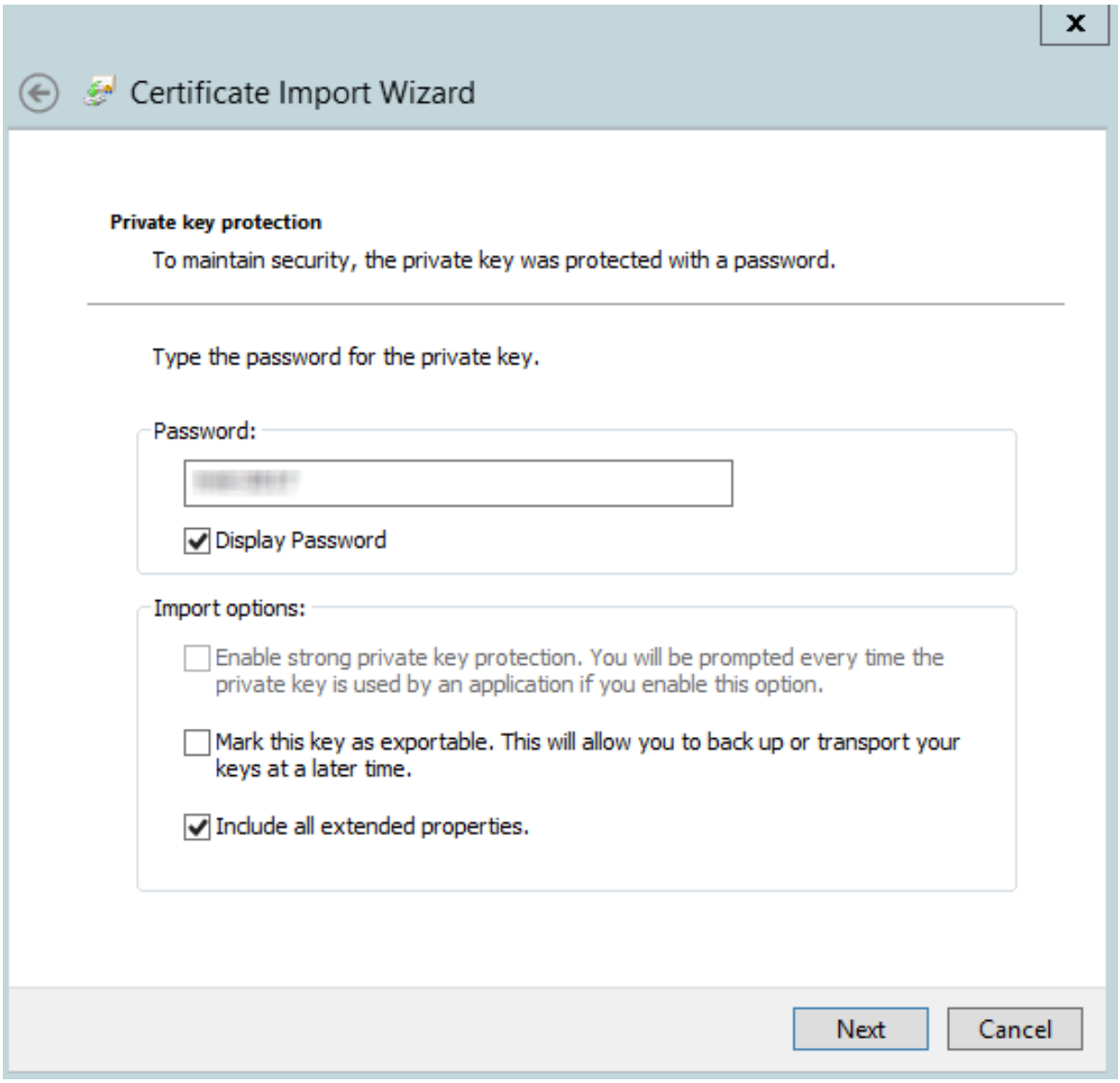


4. Double-click on the **client** file.

   The **Certificate Import Wizard** dialog is displayed.

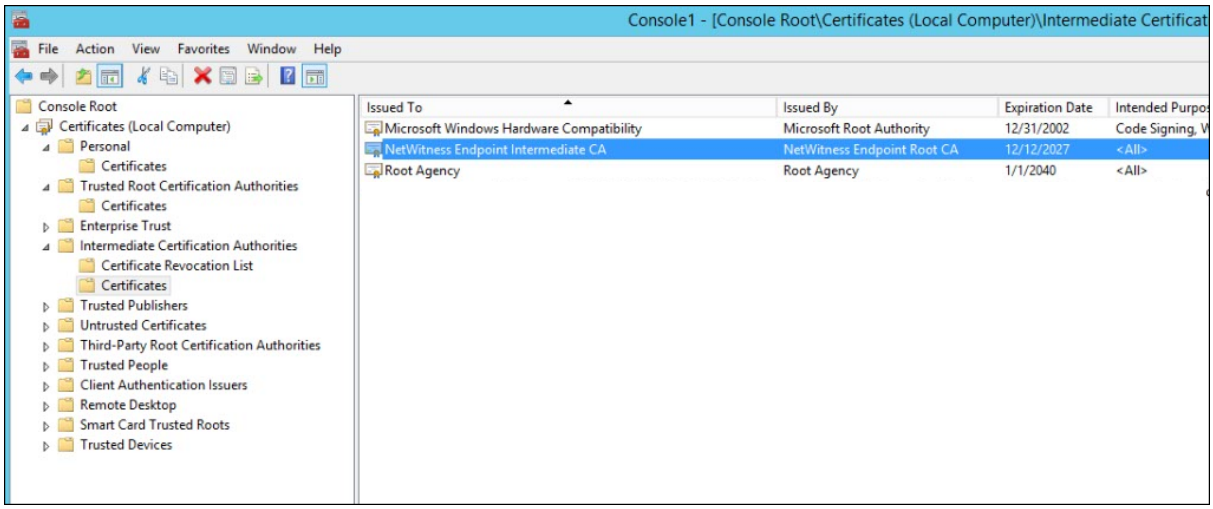
5. Select the store location as **Local Machine** and click **Next**.

6. Browse the file you want to import and click **Next**.
7. Enter the same password used while generating the agent packager.



8. Click **Next** and **Finish**.

   The certificate is listed under **Personal**, **Intermediate Certificate Authorities** > **Certificate** and **Trusted Root Certification Authorities** in the Console Server.



Enabling the Metadata Forwarding in the NetWitness Endpoint 4.4.0.2

To enable the metadata forwarding for the selected NetWitness Endpoint 4.4.0.2 agents, run the following command:

```
ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri <ENDPOINT LOG HYBRID> certificate <CERTIFICATE DISPLAY NAME>
```

For example, `ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://10.20.10.40 certificate rsa-nw-endpoint-agent`

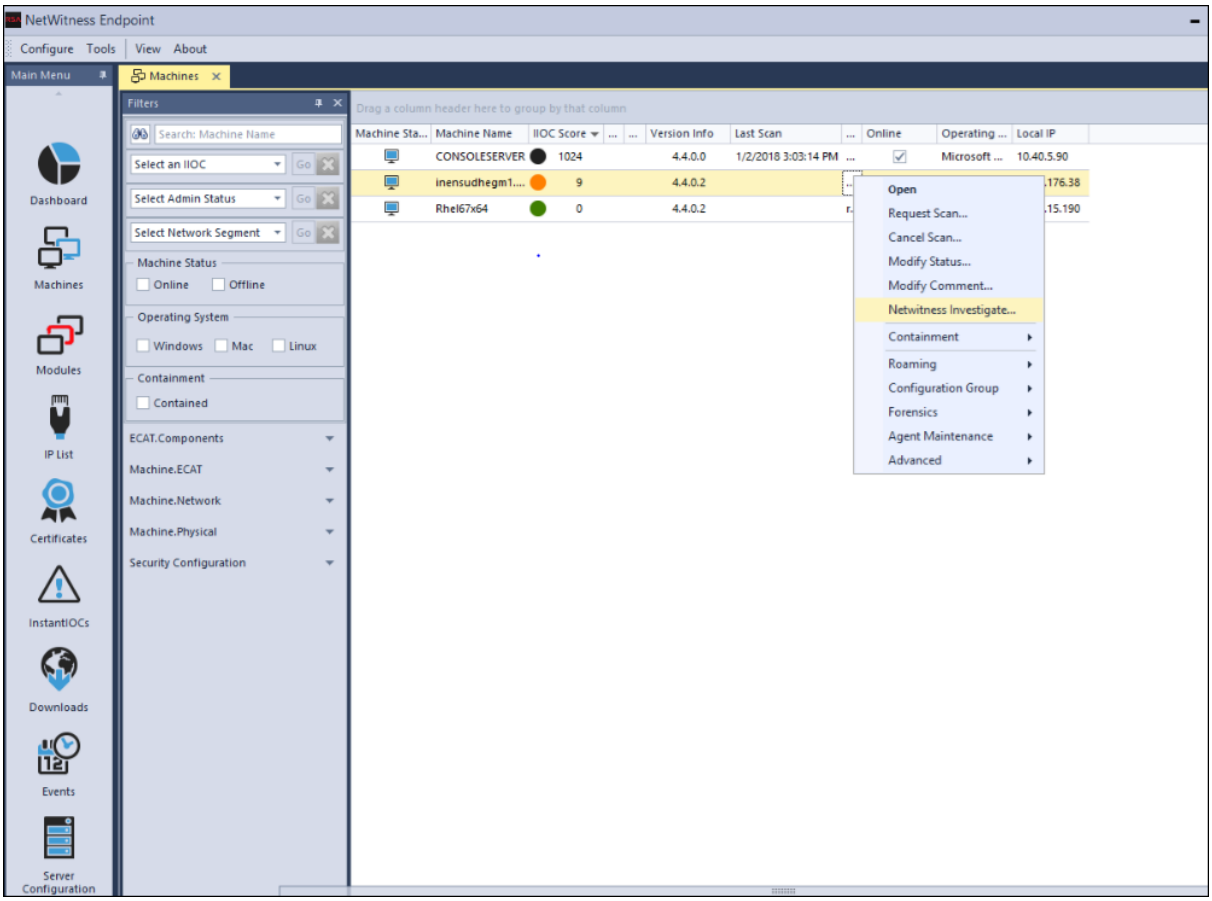
To debug, create a folder (for example, c:\JSON), and extract the converted JSON that are forwarded to NetWitness Platform, and provide this path in the command.

For example, `ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://10.20.10.40 certificate rsa-nw-endpoint-agent filepath c:\Json`

Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server

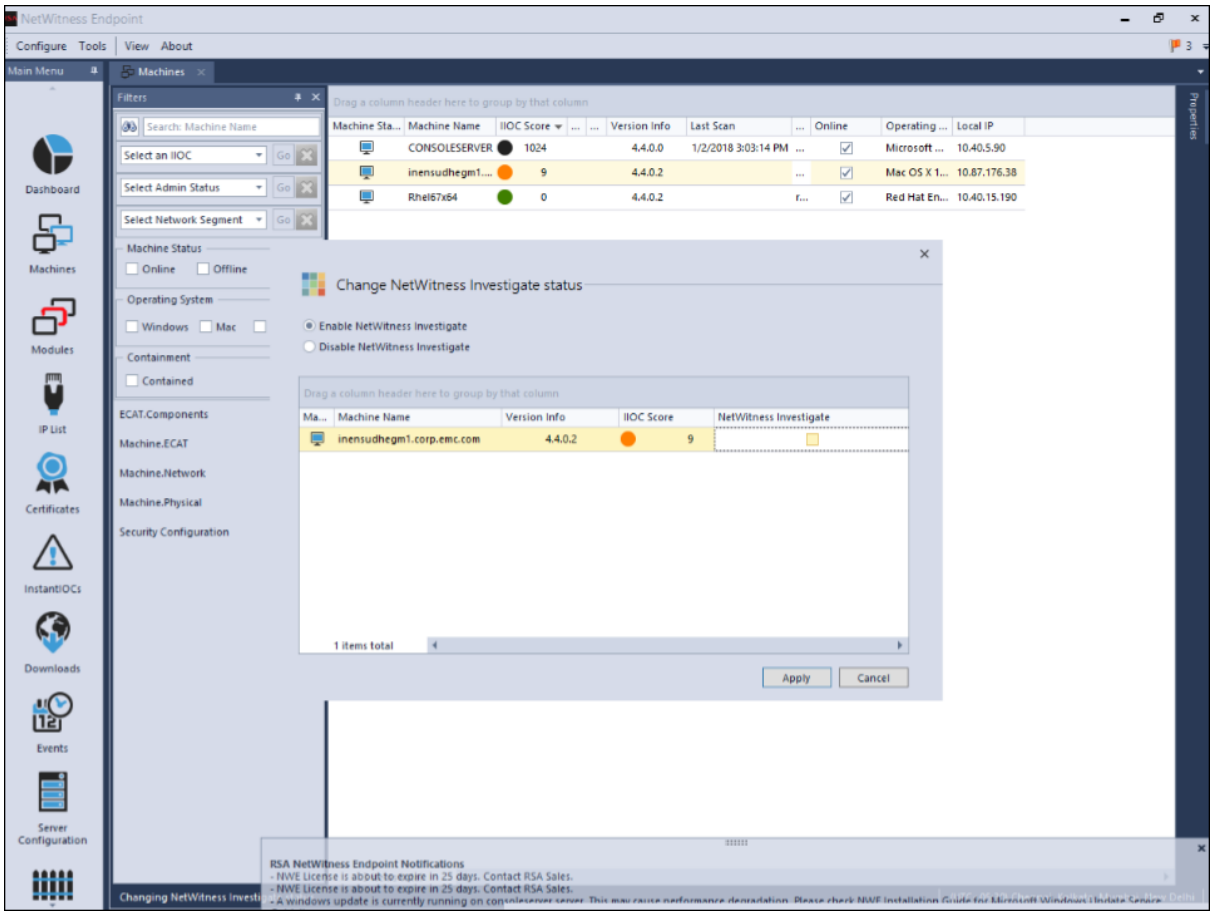
After you enable the Metadata Forwarding using any one of the above options, perform the following to enable the machines to forward metadata.

1. Open the NetWitness Endpoint 4.4.0.2 user interface.
2. Click **Machines** from the left panel. The list of available machines are displayed.



3. Select machines for which you want to forward metadata to the NetWitness Endpoint Server.
4. Right-click and select the **NetWitness Investigate** option.

   The Change NetWitness Investigate Status dialog is displayed.



5. Select the **Enable NetWitness Investigate** option.
6. Click **Apply**.
7. To verify if the **Enable NetWitness Investigate** option is enabled, repeat step 4.

(Option 2) Configuring the NetWitness Endpoint 4.4.0.2 Console Server

Enabling the NetWitness Endpoint 4.4.0.2 Meta Forwarding to the Log Decoder

To enable the Metadata Integrator service for the selected NetWitness Endpoint 4.4.0.2 agents, run the following command:

```
ConsoleServer.exe /nw-investigate enable
```

Note: When prompted for the Log Decoder Rest user name and password, enter the credentials that you used to configure the Log Decoder.

Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server

For more information, see Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server.

Disabling the Configuration

To disable the configuration, run the following command:

```
ConsoleServer.exe /nw-investigate disable
```

Endpoint References

This section is intended to help you understand the purpose of the Services Config View for the Endpoint Server. For each configuration, there is a brief introduction and a What Do You Want To Do table with links to related procedures. In addition, it includes workflow and Quick Look sections to highlight important features in the user interface.

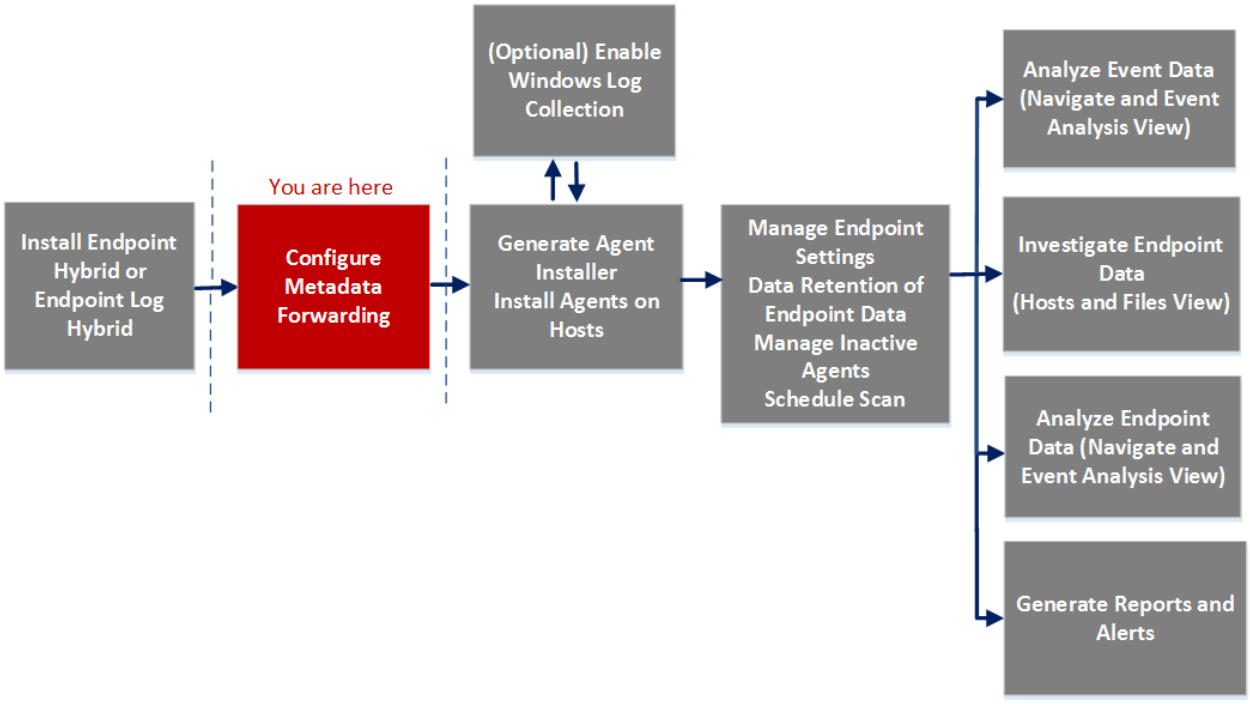
You can view the complete service nodes in tree form in the Services Explore view. For more information, see the "Services Explore View" topic in the *Hosts and Services Getting Started Guide*.

General Tab

In the **General** tab, you can configure the Endpoint metadata forwarding. To access this view:

1. Go to **ADMIN** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click  and select > **View** > **Config**.
4. Click the **General** tab.

Workflow



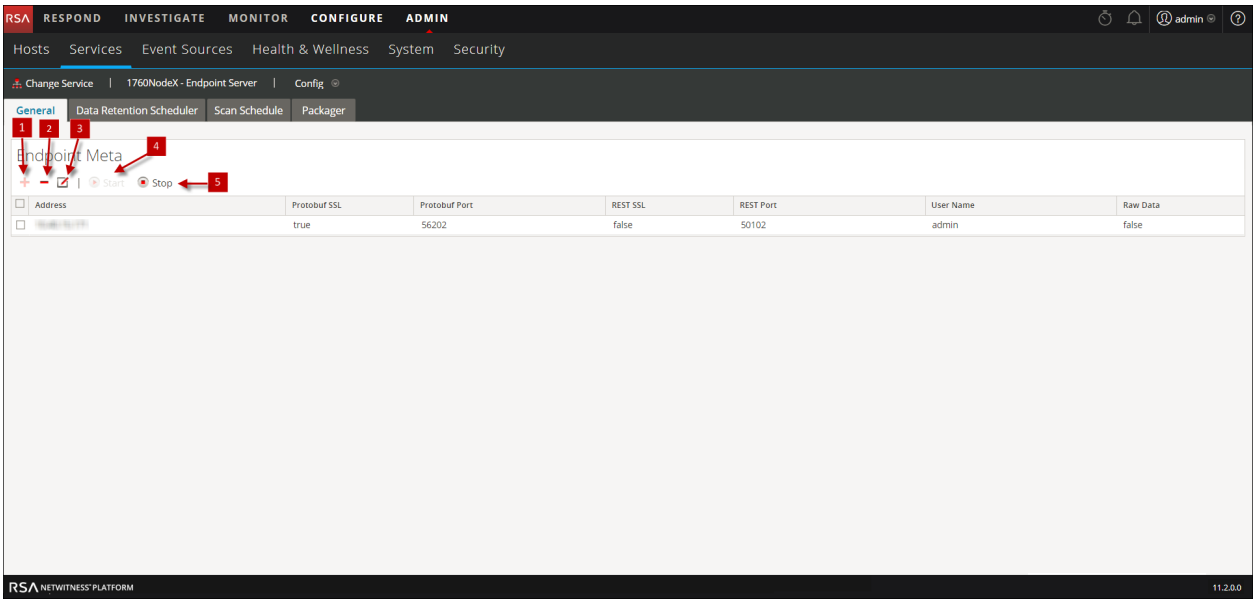
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Endpoint Metadata Forwarding for the NetWitness Endpoint 11.1 Agents	Configuring Metadata Forwarding
Administrator	Configure Endpoint Metadata Forwarding for the NetWitness Endpoint 4.4.0.2 or later Agents	Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Endpoint 11.1

*You can perform this task in the current view.

Quick Look

The following figure is an example of the General tab.



1. Click + to view the Available Services dialog.
2. Click − to delete the added service.
3. Click to edit the information for the added service.
4. Click Start to start the Endpoint metadata forwarding.
5. Click Stop to stop the Endpoint metadata forwarding.

The following table describes the fields in the General tab.

Field	Description
Address	Displays the IP address of the Log Decoder.
Protobuf SSL	Indicates if SSL is enabled on Protobuf. By default, this option is disabled.
Protobuf Port	Displays the port used for Protobuf. By default, the port is 50202.
REST SSL	Indicates if SSL is enabled on the REST port in the Log Decoder. By default, this option is disabled.
REST Port	Displays the port used for REST communication. The default value is 50102 (for non-SSL) and value 56102 (for SSL).

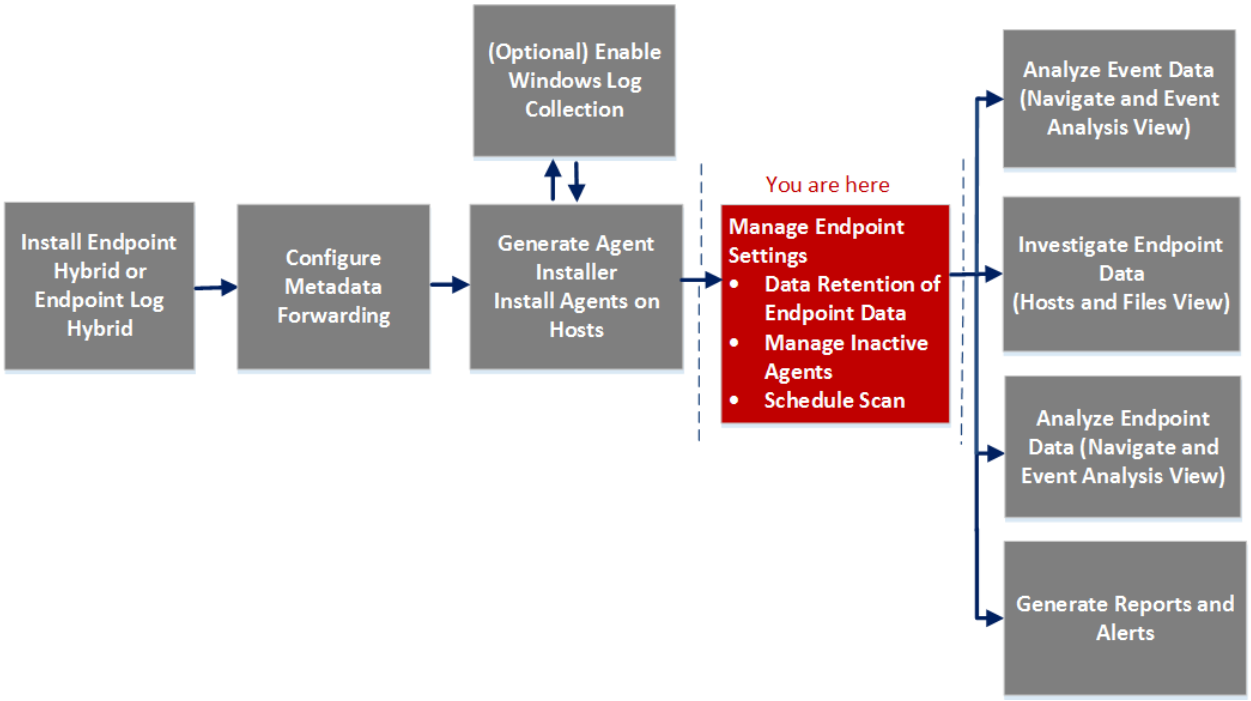
Field	Description
User Name	Displays the user name.
Raw Data	Sends a brief summary of the session along with the metadata if enabled. By default, this option is disabled.

Data Retention Scheduler Tab

In the **Data Retention Scheduler** tab, you can configure data retention and inactive agents policies. To access this view:

1. Go to **ADMIN** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click  and select > **View** > **Config**.
4. Click the **Data Retention Scheduler** tab.

Workflow



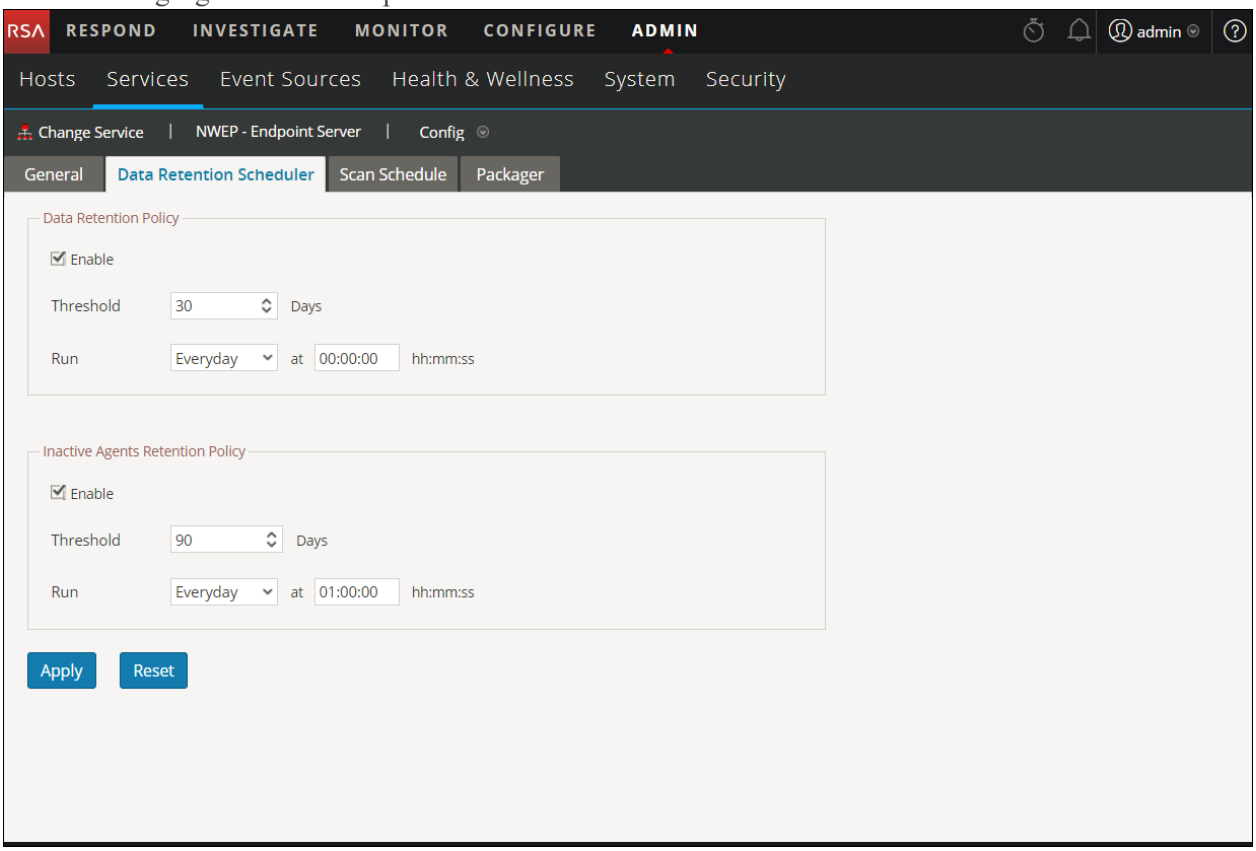
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Data Retention Policy*	Configure Data Retention Policy
Administrator	Configure Inactive Agents Policy*	Manage Inactive Agents

*You can perform this task in the current view.

Quick Look

The following figure is an example of the Data Retention Scheduler tab.



Features

The following table lists the fields for data retention policy.

Field	Description
Enable	Enables the configuration for the data retention policy. By default, this option is enabled.
Threshold	Displays the number of days the Endpoint data is retained in the database. By default, the Threshold is set to 30 days. The data older than 30 days is deleted from the database.
Run	Displays the schedule for running the data retention job. By default, the database check occurs everyday at 00:00:00 AM. You can select the frequency from the drop-down list (Everyday, Weekdays, Weekends, or Custom, where Custom allows you to select one or more specific days of the week) and time to run the job.
Apply	Overwrites any previous schedule for the data retention policy and applies the new schedule immediately.
Reset	Resets the schedule to the default settings.

The following table lists the fields for inactive agents retention policy.

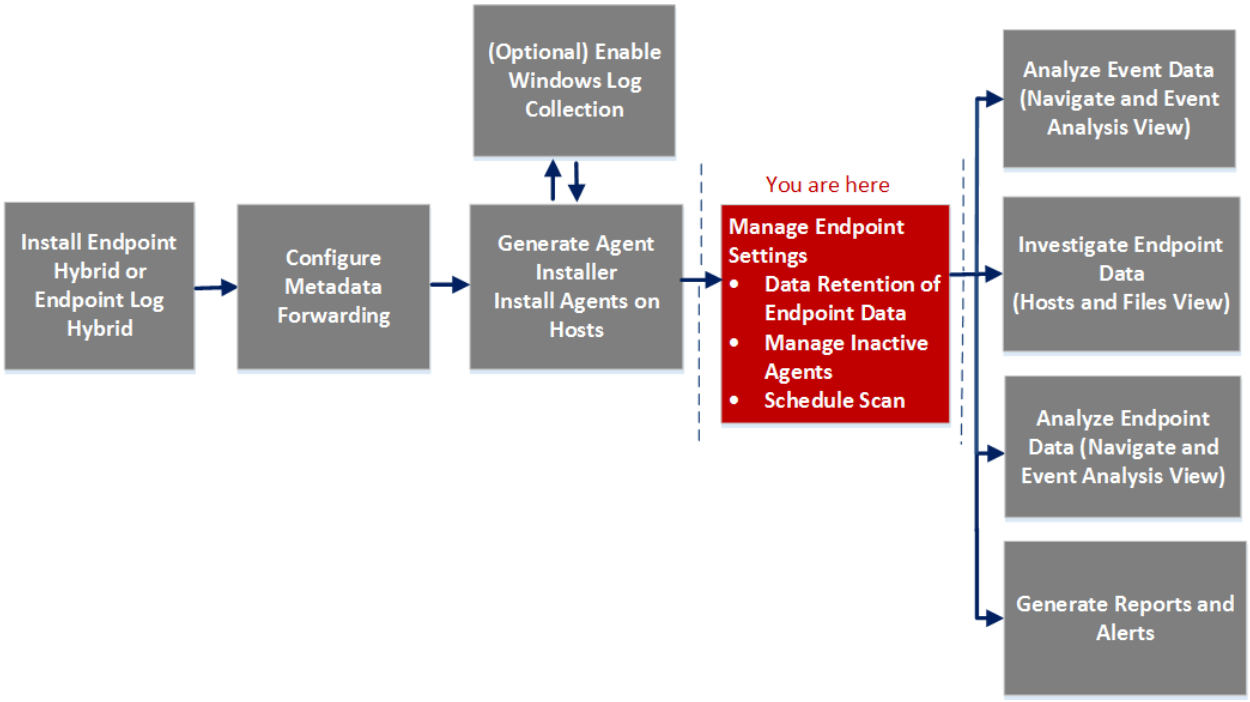
Fields	Description
Enable	Enables the configuration for the inactive agents policy. By default, this option is enabled.
Threshold	Displays the number of days the inactive agents are retained in the Endpoint Server. By default, the threshold value is 90 days.
Run	Displays the schedule for running the inactive agents retention job. By default, the database check occurs everyday at 00:00:00 AM. You can select the frequency from the drop-down list (Everyday, Weekdays, Weekends, or Custom, where Custom allows you to select one or more specific days of the week) and time to run the job.
Apply	Overwrites any previous schedule for the inactive agents retention policy and applies the new settings immediately.
Reset	Resets the schedule to the default settings.

Scan Schedule Tab

In the **Scan Schedule** tab, you can configure the schedule scan. To access this view:

1. Go to **ADMIN** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click  and select > **View** > **Config**.
4. Click the **Scan Schedule** tab.

Workflow



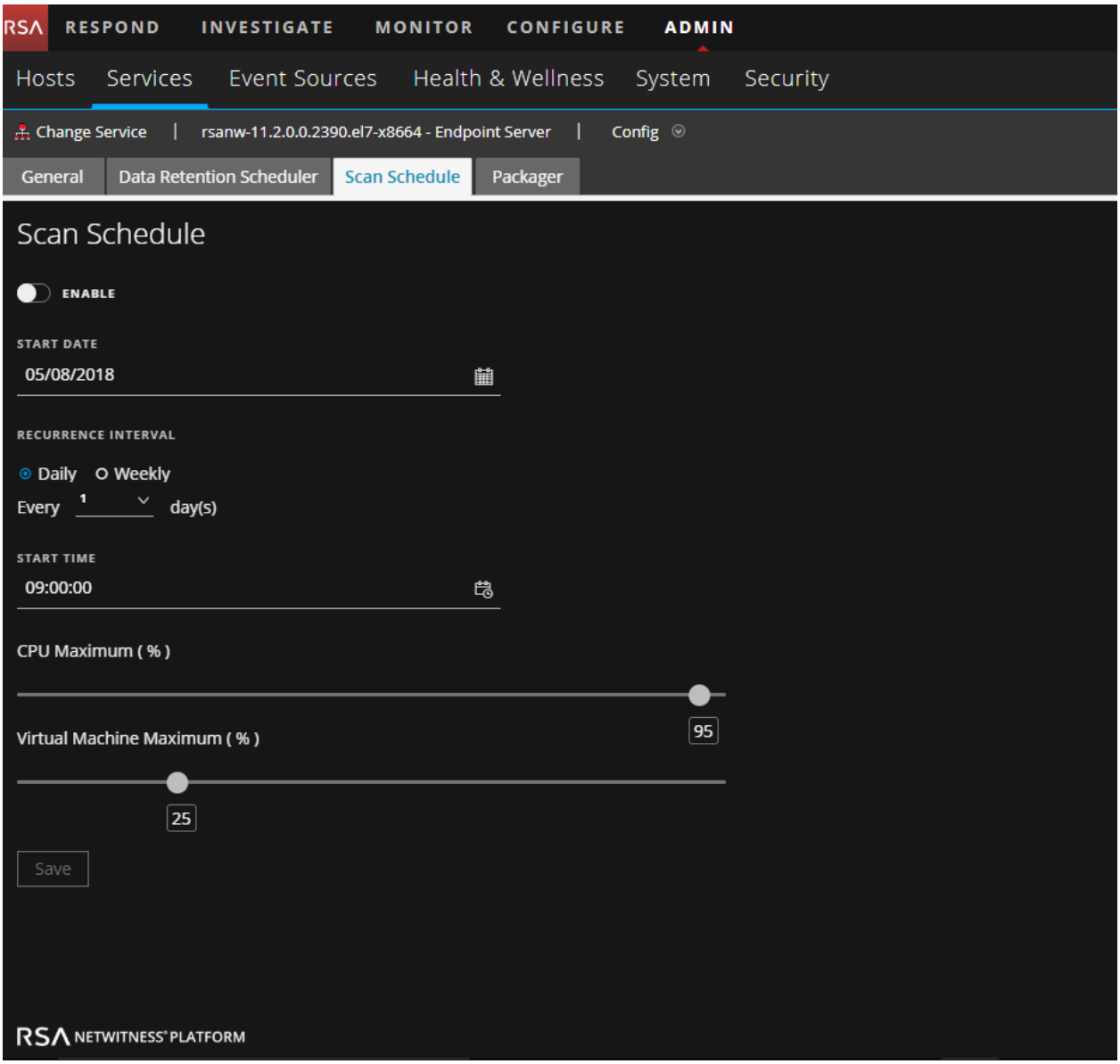
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Scan Schedule*	Configure Scan Schedule

*You can perform this task in the current view.

Quick Look

The following figure is an example of the Scan Schedule tab.



The following table describes the fields in the Scan Schedule tab. The values entered are specific to the agent time zone.

Field	Description
Enable	Select this option to configure the scan. By default, this option is disabled.
Start Date	Specify the date to start the scan.
Recurrence Interval	Select the recurrence interval to Daily or Weekly and set the frequency in days.
Start Time	Specify the time to start the scan.

Field	Description
CPU Max	Set the value using the slider. This ensures the CPU limit of the NetWitness Endpoint Agent.
VM Max	Set the value using the slider. **Note:** Use this option if agents are running on virtual machines. This is applicable only for Windows agents.

Packager Tab

In the **Packager** tab, you can generate an agent packager and agent installer. To access this view:

1. Go to **ADMIN** > **Services**.
2. In the Services view, select **Endpoint Server**.
3. Click  and select > **View** > **Config**.
4. Click the **Packager** tab.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Generate an Agent Packager for Endpoint Data Collection*	*Endpoint Insights Agent Installation Guide*
Administrator	Generating an Agent Packager for Windows Log Collection*	
Administrator	Generate an Agent Installer*	

*You can perform this task in the current view.

For more information on how to generate an agent, see *Endpoint Insights Agent Installation Guide*.

Troubleshooting

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

Agent Communication Issues

Issue	Agent is unable to communicate with the Endpoint server.

Explanation	This could be due to one of the following reasons:
	• In the agent packager:
	  • Server IP is incorrect
	  • Port specified is not available for communication with the Endpoint server
	• Endpoint Server or Nginx Server is not running
	• Firewall or IP table rules are blocking the connection between the host and Endpoint Server
	• Agent is inactive or manually deleted from the UI

Resolution	• Check if the Endpoint Server and Nginx Server are reachable • Uninstall the agent, reboot the host, and reinstall the agent • Update Firewall or IP table rules, if required

Issue	Agent takes a long time to scan.
Explanation	Sometimes, the NetWitness Endpoint scan takes a long time to complete. This is because of the CPU usage by other antivirus programs (such as Windows Defender, Mcafee, Norton, and so on) that may be installed on the agent machines.
Resolution	It is recommended to whitelist the NWEAgent.exe file in the antivirus Windows Suite.

Packager Issues

Message	`Failed to load the client certificate.`
Issue	Incorrect certificate password.
Explanation	While generating the agent installer, the certificate password does not match with the one provided while downloading the agent packager from the UI.
Resolution	Specify the correct certificate password.

Message	`An unexpected error has occurred attempting to retrieve this data.`
Issue	When attempting to access the Packager tab, it opens with the message.
Explanation	Endpoint Server might be down or not reachable.
Resolution	Check the status of the Endpoint Server under **Admin > Service**. If the service is not running, start the Endpoint Server.

Scan Schedule Issues

Message	`An unexpected error has occurred attempting to retrieve this data.`
Issue	When attempting to access the Scan Schedule tab, it opens with the message.
Explanation	Endpoint Server might be down or not reachable.
Resolution	Check the status of the Endpoint Server under **Admin > Service**. If the service is not running, start the Endpoint Server.

Health and Wellness Issues

Behavior	Endpoint metadata is not available in the **Investigate > Navigate** or **Event Analysis** view.
Issue	The health check of the Meta-Ld-Buffer shows **Unhealthy** in the Health and Wellness with the following exceptions: `dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder`
Resolution	Make sure that: • Capture is enabled on the Log Decoder • Metadata is configured properly

Behavior	For the NetWitness Endpoint 4.4.0.2 or later, metadata is not reaching the Endpoint Server.
Issue	The health of the Meta-Ld-Buffer shows **Unhealthy** in the Health and Wellness with the following exceptions: `dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder`
Explanation	Make sure that: • Certificate is obtained and imported to the NetWitness 4.4.0.2 or later Console Server • NetWitness Investigate option is enabled in the NetWitness Endpoint UI

	• Metadata forwarding is configured in the NetWitness 4.4.0.2 or later Console server

Behavior	The health check of the Data.Application.Connection-Health for Endpoint Server shows **Unhealthy**.
Issue	Either Mongo or Endpoint Server service is down.
Explanation	For error details, check the Endpoint Server logs in /var/log/netwitness/endpoint-server/endpoint-server.log.
Resolution	Restart the Mongo or Endpoint Server service.

Behavior	The health check of the Endpoint.Health.Overall-Health statistic shows **Unhealthy**.
Issue	Either Mongo or Endpoint Server service is down.
Explanation	Check the other Endpoint Server health statistics (such as, Data.Application.Connection-Health, Endpoint.Health.Ld-Buffer-Health) to identify which stats shows Unhealthy. If one of them is Unhealthy, the overall health of the Endpoint Server shows Unhealthy.
Resolution	See the resolution for these statistics in the Health and Wellness Issues section.

Issue	Agent rejection count is more than the alarm threshold.
Explanation	The agent rejected count is more than a specific limit and your custom policy is triggered. For example, agent rejected count for the last 5 hours is 10 percent of the deployed agents.
Resolution	Check the overall health of the Endpoint Server and the sizing guidelines.

Issue	Storage size of the Data application statistic has exceeded the alarm threshold.
Explanation	The storage size of the Data application has exceeded the threshold (for example, 75%), and the custom policy is triggered. **Note:** By default, the server automatically deletes the older data when it reaches 80% of the disk space.
Resolution	Check the threshold set in the data retention policy.

Issue	The health check of the Data.Application.Connection-Health shows Unhealthy or Fatal.
Explanation	The Mongo service is down.
Resolution	Check if the Mongo service is running and the Endpoint Server logs for error details.

Issue	The agent request count shows 0 for a alarm threshold.

Explanation	The agent request count shows 0 for the entire day or week. This could be due to one of the following reasons:
	• In the agent packager:
	  • Server IP is incorrect
	  • Port specified is not available for communication with the Endpoint server
	• Endpoint Server or Nginx Server is not running
	• Firewall or IP table rules are blocking the connection between the host and Endpoint Server
	• Agent is inactive or manually deleted from the UI

Resolution	• Check if the Endpoint Server and Nginx Server are reachable • Uninstall the agent, reboot the host, and reinstall the agent • Update Firewall or IP table rules, if required

Installation Issue

Behavior	NetWitness Platform allows multiple instances of Endpoint Hybrid or Endpoint Log Hybrid to be installed.
Issue	Only one instance of the Endpoint Hybrid or Endpoint Log Hybrid can be used for endpoint data.
Explanation	While the installation of Endpoint Hybrid or Endpoint Log Hybrid is in-progress, you can install another instance and the installation will be successful.
Resolution	You must delete all instances of Endpoint Hybrid or Endpoint Log Hybrid except the one that you want to use for endpoint data.

Finding Inactive Agents Issue

Issue	Agent might be inactive or has not communicated with the Endpoint Server for a long time.
Explanation	A list of inactive agents is available in the Mongo database with the agent ID. Using this information, you can search for further details of the inactive agents.
Resolution	To find inactive agents in your deployment, perform the following: 1. Open the Endpoint Server log file from `/var/log/netwitness/endpoint-server/endpoint-server.log` and search for Agent <ID> does not exist string. 2. Copy the agent ID displayed in the log file.

	3. Search for the agent ID in the NGINX access log file (`/var/log/nginx/access.log`) to retrieve the following details of an inactive agent: • IP Address • Date and time that the agent became inactive • Location