



NetWitness Endpoint Configuration Guide

for RSA NetWitness® Platform 11.3



Copyright © 1994-2019 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.

May 2019

Contents

NetWitness Endpoint Overview	6
Endpoint Agent Data Flow	7
Agent Modes	9
Endpoint Log Hybrid Configuration	10
Deploying Endpoint Application Rules and ESA Correlation Rules	12
Custom Endpoint Rule for Risk Scoring	12
1. Add a custom Application Rule	13
2. Add a custom ESA Rule	14
3. Add the rule to RiskConfig	15
Configuring Metadata Forwarding	18
Start Metadata Forwarding to the Log Decoder	19
Stop Metadata Forwarding to the Log Decoder	20
Remove Metadata Forwarding	20
Endpoint Metadata Mappings	20
JSON Schema for Metadata Mappings	20
View the Metadata Mappings	21
Add or Modify Metadata Mappings	23
View the Custom Metadata Mappings	23
Endpoint Sources	24
Groups	24
Policies	24
Group Ranking	25
Example 1	25
Example 2	25
Example 3	27
Default Agent Endpoint (EDR) Policy	28
Default Windows Log Policy	29
Creating Groups and Policies	30
Create a Group	30
Create an EDR Policy	32
Create a Windows Log Policy	35
Managing Groups	37
View Group Details	37
Filter Endpoint Groups	37
Edit a Group	38

Change Policy Ordering for Groups	39
Delete a Group	40
Managing Policies	41
View Policy Details	41
Filter Policies	41
Edit a Policy	42
Delete a Policy	43
Configuring Data Retention Policy	44
Managing Inactive Agents	46
Configuring Location for File Download	47
Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Platform	48
Enabling the NetWitness Endpoint 4.4.0.2 Metadata Forwarding to the Log Decoder	48
Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server	48
Endpoint References	51
General Tab	52
Workflow	52
What do you want to do?	52
Quick Look	53
Data Retention Scheduler Tab	55
Workflow	55
What do you want to do?	55
Quick Look	56
Packager Tab	58
Workflow	58
What do you want to do?	58
Endpoint Sources - Groups	59
Workflow	59
What do you want to do?	59
Related Topics	60
Quick Look	60
Create Group	61
Ranking Groups	64
Endpoint Sources - Policies	66
Workflow	66
What do you want to do?	66
Related Topics	67
Quick Look	67
Create Policy	68

Troubleshooting	73
Agent Communication Issues	73
Packager Issues	73
Scan Schedule Issues	74
Health and Wellness Issues	74
Installation Issue	76
Finding Inactive Agents Issue	76
NGINX Issue	77

NetWitness Endpoint Overview

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.1 and later.

NetWitness Platform provides an endpoint detection and response solution that continuously monitors the behavior of all endpoints in the network to provide deep visibility and analysis of executables and processes. It helps to detect new, unknown, and targeted attacks, highlights suspicious activity for investigation, exposes anomalous behaviors, and determines the scope of compromise to help analysts respond to advanced threats faster. During investigation, the analyst can use the visual indication of threat level to assess the risk of endpoints.

As part of this solution, NetWitness Platform introduces **Endpoint Log Hybrid** that:

- Collects and manages endpoint (host) data from Windows, Mac, and Linux hosts.
- Collect logs from Windows hosts.
- Generates metadata to correlate endpoint data with sessions from other events sources, such as logs and network.

Analysts can:

- Perform instant scans for detailed insights of the host behavior at any point in time.
- Analyze the scope of the attack across hosts and network through integrated metadata.
- Quickly triage and focus their investigation by managing suspect and legitimate files.
- Perform multiple checks of file legitimacy to determine if a file is malicious, including checking file certificates and hashes.
- Blacklist malicious files and then block them across all hosts in the network to prevent future execution of this file on any host.

Endpoint Log Hybrid runs an Nginx server (in a reverse proxy mode) that receives data from the Endpoint Agent. The following services run on the Endpoint Log Hybrid:

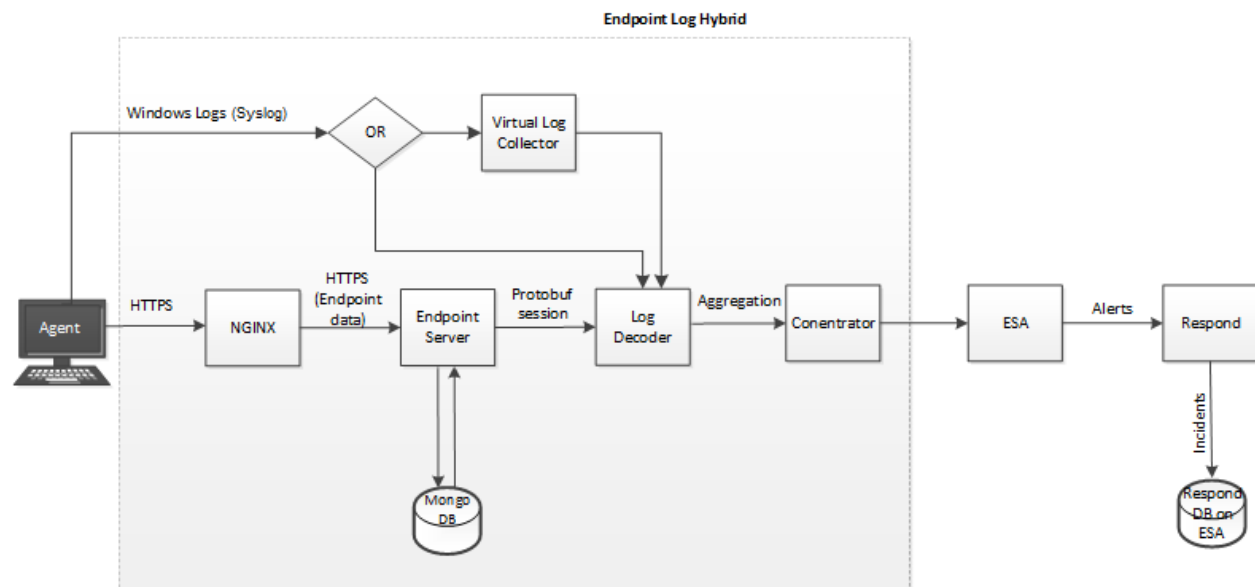
- **Endpoint Server:** Manages data received through Nginx, stores it in the Mongo database. It parses the events, generates metadata, and forwards it to the Log Decoder through protobuf.
- **Log Decoder:** Captures data from the Endpoint Server and processes the metadata.
- **Concentrator:** Aggregates metadata from the Log Decoder and makes it available for all upstream components like Investigate, Reporting Engine, Respond, and Event Stream Analysis similar to NetWitness Decoder and Concentrator.
- **Log Collector:** Collects logs from all event sources that are supported for the log collection in the NetWitness Platform.

In addition to the above services, the Endpoint Log Hybrid leverages the following services:

- **Event Stream Analysis (ESA):** Creates alerts from ESA rules for Endpoint data.
- **Endpoint Broker:** Provides a consolidated view of all Endpoint servers in a multiple Endpoint Log Hybrid deployment.

Endpoint Agent Data Flow

The following figure shows the endpoint data flow from the agent to 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
- Deploying the ESA rules from the Endpoint Rule Bundle
- Creating groups and policies
- Configuring Endpoint metadata forwarding and retention policies
- Defining health and wellness policies to monitor Endpoint Server

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

Agent Modes

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

In NetWitness Platform 11.3, the Endpoint agent can operate either in Insights or Advanced mode depending on the policy configuration. For more information on policy configuration, see the *NetWitness Endpoint Configuration Guide*. You can have both Insights and Advanced agents in a single deployment.

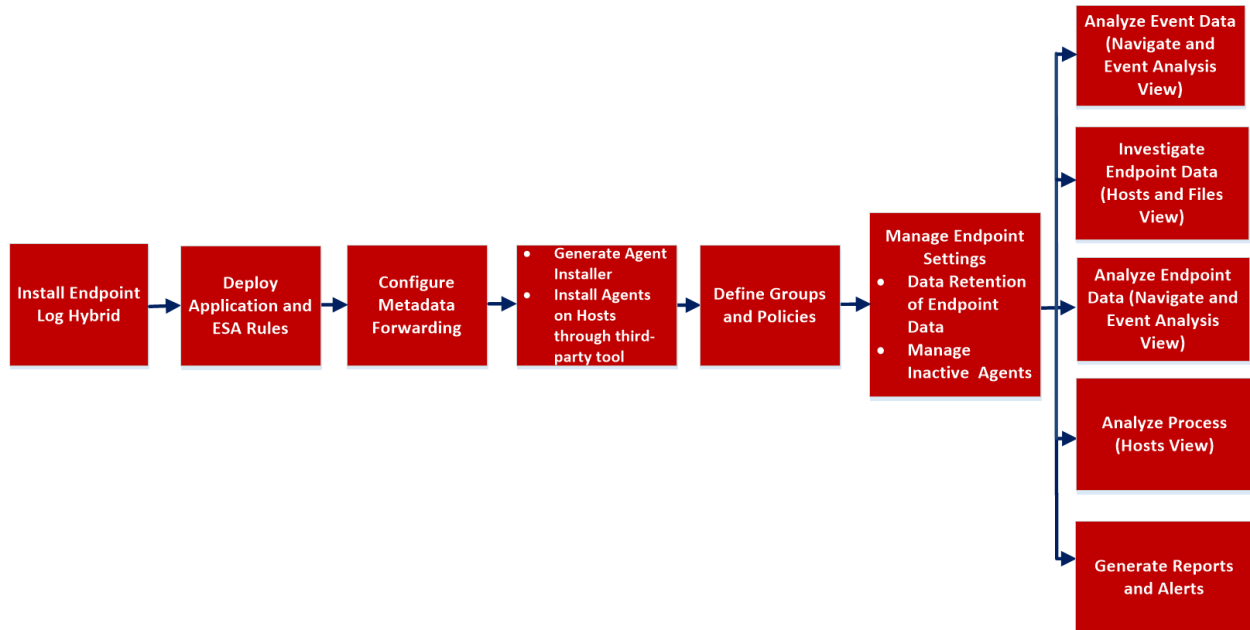
There is no license required for the Insights agent. However, you must procure a Throughput license for an Advanced agent. For more information on licensing, see the *Licensing Management Guide*.

The following table lists the features supported for Insights and Advanced agents:

Feature	Insights Agent	Advanced Agent
Scan data - Processes, Autroruns, Files, Drivers, Libraries, and System Information	Yes - Windows, Mac, and Linux	Yes - Windows, Mac, and Linux
Tracking data - Process, File, Registry, Network, and Console	No	Yes - Windows and Mac Registry and Console events are applicable only for Windows.
Anomaly detection - Image Hooks, Kernel Hooks, Registry Discrepancies, and Suspicious Threads	No	Yes - Windows
Windows log collection	Yes	Yes
Threat detection content - ESA, Application Rules	Yes	Yes
Analysis of downloaded file	No	Yes
File status - Whitelist, Blacklist, Graylist, and Neutral	Yes (View only)	Yes (View and modify)
File Remediate (Block)	No	Yes
Process visualization	No	Yes
Live connect	Yes	Yes
File reputation service (Third-party lookup)	Yes	Yes
Risk score for hosts	No	Yes

Endpoint Log Hybrid Configuration

This topic provides the high-level tasks required to configure the Endpoint Log Hybrid.



Tasks	Description
Install the Endpoint Log Hybrid	See the <i>Physical Host Installation Guide</i> and <i>Virtual Host Setup Guide</i> .
Deploy Application and ESA Rules	See Deploying Endpoint Application Rules and ESA Correlation Rules .
Configuring Metadata Forwarding	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	<p>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 11.3 agent.</p> <p>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, anomalies, system configurations, and scripts found on the host.</p>
Endpoint Sources	To efficiently manage and update endpoint agent configurations, you can group the agents, and manage their behavior using policies.
Enable Reputation Status	Reputation Status is enabled by default in an NetWitness Platform 11.3 deployment and displays information about the file. For troubleshooting, see the <i>Live Services Guide</i> .
Risk Score	Risk Score is calculated and obtained from NetWitness Respond for hosts and files. For more information, see the <i>NetWitness Respond Configuration Guide</i> .
Configuring Data Retention Policy	<p>Define data retention policies to optimally store and manage the Endpoint data based on the age of the Endpoint data or the storage size.</p> <p>By default, 30 days of agent data is retained.</p>
Managing 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.
Investigate Endpoint data	You can investigate the Endpoint data in the Investigate > Hosts and Investigate > Files views. For more information, see the <i>NetWitness Endpoint User Guide</i> .

Deploying Endpoint Application Rules and ESA

Correlation Rules

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The existing IIOCs from NetWitness Endpoint 4.4.0.x are now available as OOTB Endpoint Application rules tagged as Indicators of Compromise, Behaviors of Compromise, Enablers of Compromise, and Analysis.File. Application rules for Endpoint are automatically available on installation of NetWitness Platform 11.3.

For Endpoint risk score, every Application rule must have an ESA rule that generates alerts used for the risk score calculation. A set of OOTB ESA rules are available as Endpoint Rule Bundle. You must specify the Endpoint data sources (Concentrators) and deploy the ESA Rules from the Endpoint Rule Bundle. For more information, see "Deploy Endpoint Risk Scoring Rules on ESA" section in the *ESA Configuration Guide*.

If the Application rule key value matches with ESA rule then an alert is triggered which is used to compute the risk score and an incident is raised when risk score exceeds the defined threshold limit.

Note: If you are upgrading from an existing Endpoint Log Hybrid to 11.3, you must deploy the Application rules from RSA Live. During deployment, you must specify Endpoint Log Hybrid Log Decoder service. In case of multiple Endpoint servers, select all the Endpoint Log Hybrid Log Decoder services. For more information, see the *Live Services Management Guide*.

You can view the application rules that are deployed in **Admin > Endpoint Log Hybrid - Log Decoder > Config > App Rules** and application rules that were triggered in **Investigate > Navigate > Endpoint Log Hybrid - Concentrator > App rules**.

The Endpoint ESA rules generate alerts with the severity; Critical, High, and Medium. You can view the alerts on:

- Risk Details tab - You can view Critical, High and Medium alerts for a host or file on **Investigate > Hosts > Risk Details** or **Investigate > Files > Risk Details**.
- Respond view : You can view only critical and high severity alerts on **NetWitness Respond > Alerts**.

Custom Endpoint Rule for Risk Scoring

If you have custom IIOCs in NetWitness Endpoint 4.4.0.x, you need to create these custom Endpoint rules. Once you have created your custom Application rule, you must create the custom ESA Rule for risk score calculation and update the RiskConfig file in MongoDB.

To create a custom Endpoint rule, perform the following:

1. Add a custom Application rule
2. Add a custom ESA rule
3. Update the risk configuration file

1. Add a custom Application Rule

To add a custom application rule:

1. Complete steps 1-11 in "Configure Application Rules" topic of *Decoder and Log Decoder Configuration Guide*.

Note: You must be familiar with the metakeys tagged as (Indicators of Compromise, Behaviors of Compromise, Enablers of Compromise, and Analysis.File) on which an alert will be generated. In the example below, the alert is generated on Analysis.File metakey for In Encrypted Directory rule.

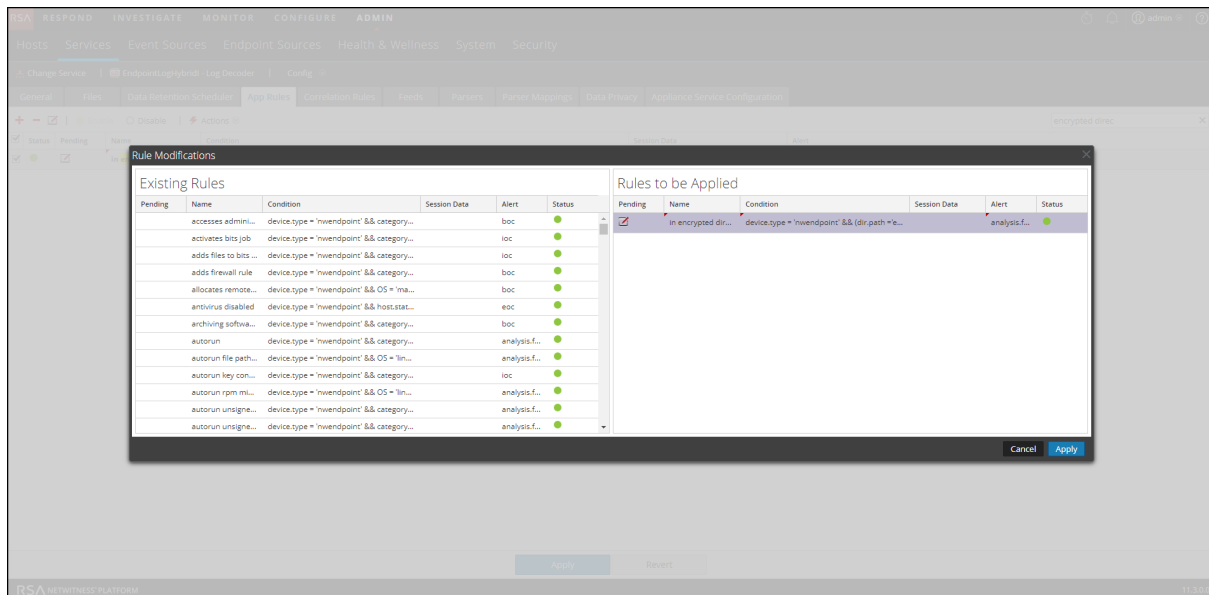
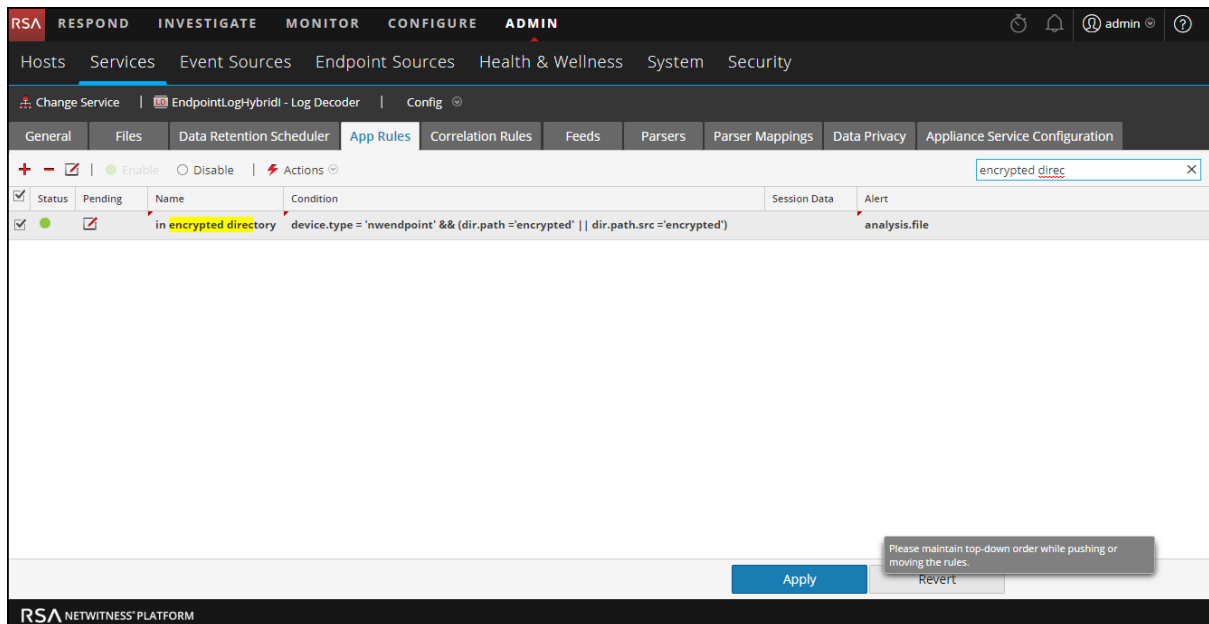
Following is an example of an Application Rule created for In Encrypted Directory alert.

The screenshot shows the 'Rule Editor' dialog box with the following configuration:

- Rule Definition**
 - Rule Name:** in encrypted directory
 - Condition:** device.type = 'nwendpoint' && (dir.path = 'encrypted' || dir.path.src = 'encrypted')
- Session Data**
 - ☐ Stop Rule Processing
 - ☐ Keep
 - ☐ Filter
 - ☐ Truncate
- Session Options**
 - ☒ Alert
 - ☐ Forward
 - ☐ Transient
 - Alert On:** analysis.file

At the bottom of the dialog are buttons for 'Reset', 'Cancel', and 'OK'.

2. After a custom application rule is added successfully, select the newly created rule (For example, In Encrypted Directory alert) and click **Apply**.



In case of multiple Endpoint servers, you must create this custom Application rule on every Endpoint Hybrid Log Decoder service.

2. Add a custom ESA Rule

To add a custom ESA rule, perform the following.

1. SSH to the Admin Server.
2. Create a new JSON file (for example, in `encrypted_directory.json`) with the custom ESA rule definition in the below format.

```
{
  "id": "In Encrypted Directory", "key": "analysis.file",
```

```

"value": "in encrypted directory",
"title": "In Encrypted Directory",
"type": "ENDPOINT",
"enabled": true,
"description": "End Point rule for In Encrypted Directory",
"severity": "MEDIUM"
}

```

The following table describes the fields that define a rule.

Fields	Description
id	The name of the ESA Rule. For example, In Encrypted Directory.
key	The metakey on which an alert would be generated. For example, alert is generated on analysis.file metakey for In Encrypted Directory rule.
value	Specify the value. The value must exactly match with the App rule name. For example, in encrypted directory.
title	The name of the alert. For example, In Encrypted Directory.
type	Specify the type of rule. For custom endpoint rule, the type must be ENDPOINT.
enabled	The status of the rule. Specify true, if the rule should be considered for risk scoring.
description	The description of the rule.
severity	The severity of the rule; critical, high or medium.

- To enter shell mode of nw-shell, execute the following command:
nw-shell
- Connect to ESA correlation-server using the following command:
connect --service correlation-server
- Login to the ESA correlation-server using the following command
login

Note: You must provide Administrator username and password.

- Navigate to the API xpath using the following command:
cd correlation/keyvalue/settings/set
- Execute the API using the following command:
invoke --file <absolute-path-to-rule-definition-file>

Note: You must specify the absolute path to the rule definition file. For example, invoke --file /root/rule.json

3. Add the rule to RiskConfig

After you create the custom Application rule and the ESA rule, you must update the RiskConfig in mongoDB.

To update the riskconfig file, perform the following:

1. SSH to Admin Server.
2. Create a JavaScript file (For example, `in-encrypteddirectory- rule.js`) with the custom ESA rule definition in the below format.

```
db.risk_rule.insertMany(
[ {
  "name" : "In Encrypted Directory",
  "enabled" : true,
  "handler" : "Default",
  "entities" : {

  },
  "metas" : {
    "File" : [
      {
        "meta" : "checksum_src",
        "name" : "filename_src",
        "weight" : NumberInt(100)
      }
    ],
    "Host" : [
      {
        "meta" : "agent_id",
        "name" : "alias_host",
        "weight" : NumberInt(100)
      }
    ]
  },
  "_class" : "com.rsa.asoc.respond.pipeline.risk.rules.AlertScoringRule"
} ]
)
```

The following table describes the fields that define a rule.

Field	Description
name	The name of the ESA rule.
enabled	The flag to enable or disable risk scoring. Specify true to enable risk scoring.

Field	Description
handler	The value of this should be Default.
entities	The value of this should be empty.
metas > Files > meta	The metakey for a file for which score should be calculated.
metas > Files > name	The name of the metakey of the file identity.
metas > Files > weight	By default the weight value is 100.
metas > Host > meta	The metakey for a host for which score should be calculated.
metas > Host > name >	The name of the metakey of the host identity.
metas > Host > weight	By default the weight value is 100.
_class	This is used for internal purpose, do not change.

3. Insert the new rule into the riskconfig file on mongoDB using following command:

```
mongo respond-server --authenticationDatabase admin -u deploy_admin
-p <deploy_admin-user-password> in-encrypted-directory-rule.js
```

4. Confirm if ESA rule is updated successfully in the riskconfig, using following command

```
mongo respond-server --authenticationDatabase admin -u deploy_admin -p
<deploy_admin-user-password> --eval "db.risk_rule.find({ 'name': /*.*In
Encrypted Directory.*/i })"
```

5. Restart the Respond server for the changes to take effect.


```
service rsa-nw-respond-server restart
```

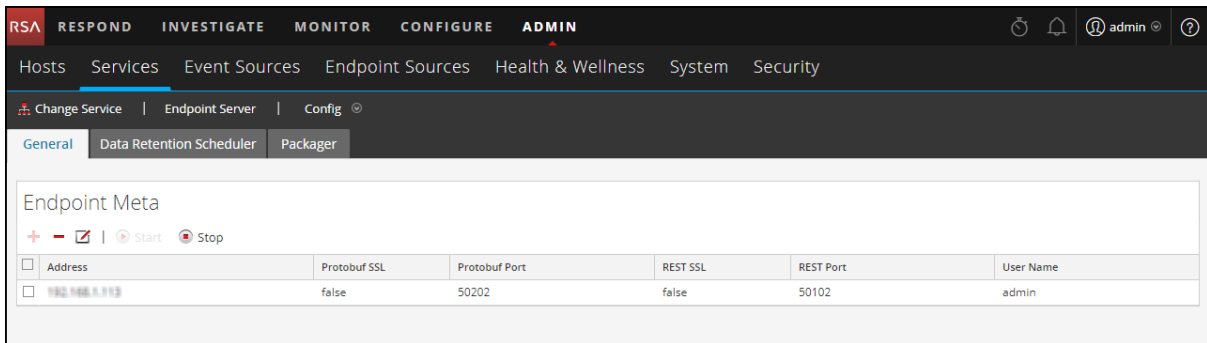
After you create a custom Endpoint rule and update the risk configuration file, whenever an event is generated for the new rule (For example, In Encrypted Directory) an alert will be generated and the risk score is calculated for the host and file.

Configuring Metadata Forwarding


To view the metadata, you must enable the metadata forwarding while installing the Endpoint Log Hybrid. The Endpoint metadata is displayed in the NetWitness Platform Investigate (**Navigate** and **Event Analysis** views) similar to Logs and Packets. For information on metadata mappings, see [Endpoint Metadata Mappings](#).

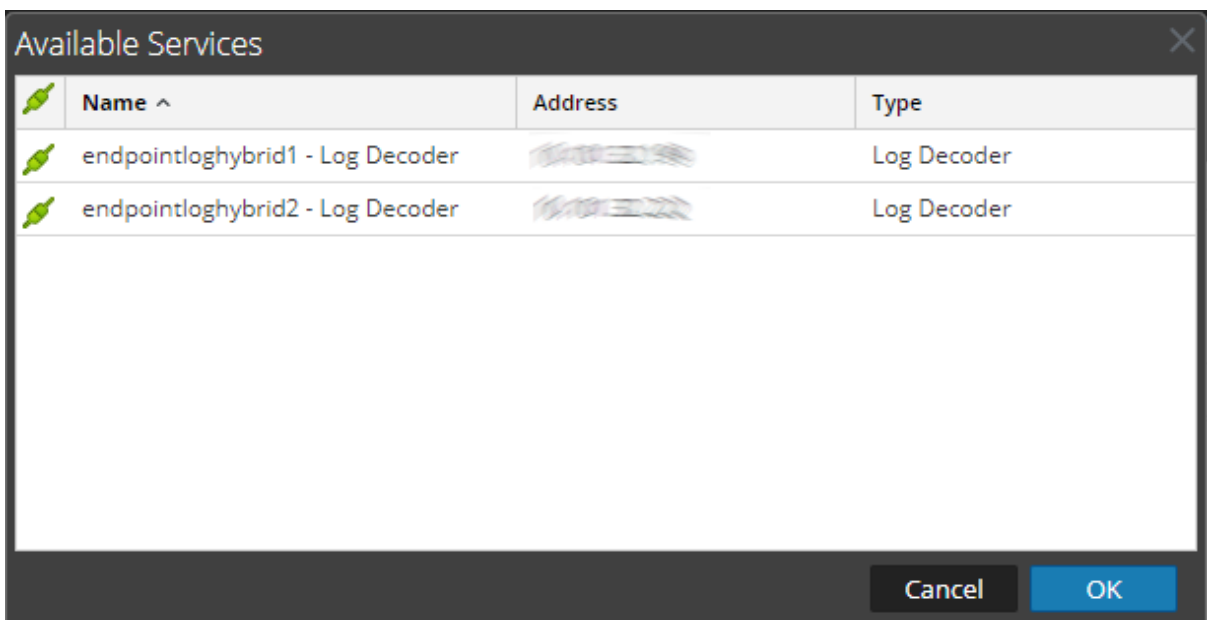
To configure metadata forwarding:

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.



Address	Protobuf SSL	Protobuf Port	REST SSL	REST Port	User Name
192.168.1.113	false	50202	false	50102	admin

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



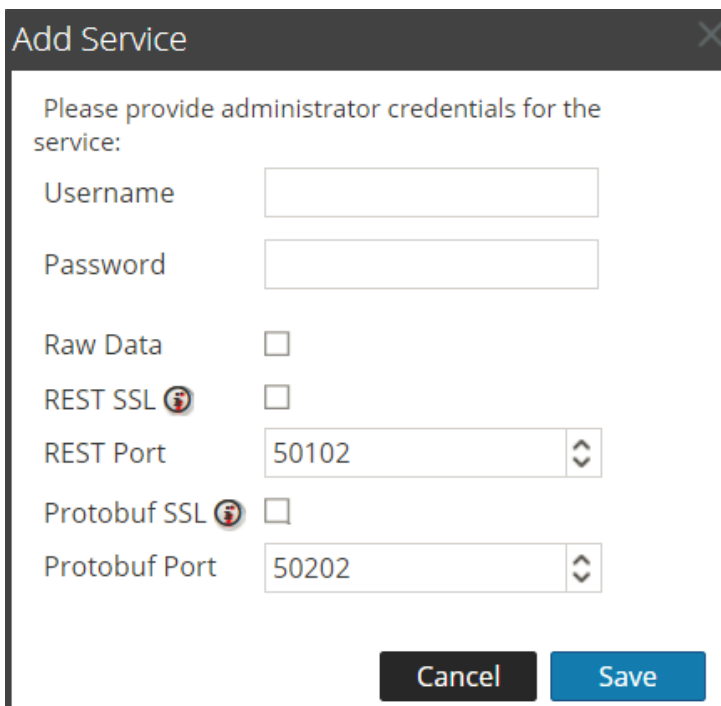
Name ^	Address	Type
endpointloghybrid1 - Log Decoder	192.168.1.113	Log Decoder
endpointloghybrid2 - Log Decoder	192.168.1.113	Log Decoder

Cancel OK

6. Select a Log Decoder service and click **OK**.

The Add Service dialog is displayed.

Note: You can add only one Log Decoder service.

The image shows a dialog box titled "Add Service" with a close button (X) in the top right corner. Inside the dialog, there is a prompt: "Please provide administrator credentials for the service:". Below this, there are two text input fields: "Username" and "Password". Underneath these are four options, each with a checkbox and a red information icon: "Raw Data", "REST SSL", "Protobuf SSL", and "Protobuf Port". The "REST Port" and "Protobuf Port" fields are accompanied by spinners showing the values "50102" and "50202" respectively. At the bottom of the dialog are two buttons: "Cancel" and "Save".

Add Service

Please provide administrator credentials for the service:

Username

Password

Raw Data ☐

REST SSL ⓘ ☐

REST Port

Protobuf SSL ⓘ ☐

Protobuf Port


Cancel Save

7. Enter the administrator credentials for authentication.
8. (Optional) If you enable Raw Data, a brief summary of the session is forwarded along with the metadata.
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 50202 and SSL is 56202.
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**

Start Metadata Forwarding to the Log Decoder


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

Stop Metadata Forwarding to the Log Decoder

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

Remove 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.

View 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:

```

    {
      "endpointJpath" : "users/sessionType",
      "metaName" : "logon_type",
      "type" : "text",
      "enabled" : true
    },
    {
      "endpointJpath" : "hostFileEntries/hosts",
      "metaName" : "dhost",
      "type" : "text",
      "enabled" : true
    },
    {
      "endpointJpath" : "securityConfigurations",
      "metaName" : "event_state",
      "type" : "text",
      "enabled" : true
    }
  ]
},
{
  "metaKeyPairsCategory" : "MACHINE_IDENTITY",
  "keyPairs" : [
    {
      "endpointJpath" : "_id",
      "metaName" : "agent.id",
      "type" : "text",
      "enabled" : true
    },
  ],
}

```

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`.

```

{
  "metaKeyPairsCategory" : "COMMON",
  "keyPairs" : [
    {
      "endpointJpath" : "Category",
      "metaName" : "category",
      "type" : "text",
      "enabled" : true
    },
  ],
}

```

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.

Add or Modify 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 metaKeys 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:

```
root@NWAPPLIANCE22465 /]# nw-shell
RSA
RSA NetWitness Shell. Version: 3.2.4
See "help" to list available commands, "help connect" to get started.
offline » login
user: admin
password: *****
admin@offline » connect --service endpoint-server
Connected to endpoint-server (10.10.10.10:7050)
admin@endpoint-server:Folder:/rsa » cd endpoint/meta/set-custom
admin@endpoint-server:Method:/rsa/endpoint/meta/set-custom » invoke --file /custom.json
```

View 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.

Endpoint Sources

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The Endpoint agents deployed in your environment may be large in number and geographically distributed. To efficiently manage and update configurations automatically, agents can be organized into smaller subsets called **Groups**.

Groups

Groups can be created based on IP address (IPv4 and IPv6), host names, operating system type, and operating system description. You can create groups based on your requirements. For example, you can group all agents running on Windows 2016 Server and IP ranging from 10.40.10.1 to 10.40.10.200. For more information on creating groups, see [Creating Groups and Policies](#).

Note: All agents that are not part of any group use the default policy settings.

Policies

To manage the behavior of agents in a group, you can apply a set of rules called **Policies**. The RSA NetWitness Platform supports two types of policies for endpoints: **Agent Endpoint** and **Agent Windows Logs** policies. The following default policies are available on installation.

Note: RSA recommends that you review these default policies before deploying agents.

- [Default Agent Endpoint \(EDR\) Policy](#)
- [Default Windows Log Policy](#)

You can either assign the default policies to a group, modify the default EDR policy, or create custom policies based on your organization requirements.

Note: You cannot edit the default Windows Logs policy.

You can do the following through a policy:

- Define the agent mode - Insights or Advanced
- Configure scan schedule and settings
- Configure endpoint settings, such as which Endpoint server the agents should communicate, port details, and beacon intervals
- Configure response actions such as blocking
- Configure Windows Log collection

For example, you can create a policy to schedule scan and enable blocking. For more information on creating policies, see [Create an EDR Policy](#) or [Create a Windows Log Policy](#).

Group Ranking

When a group is created, a rank is associated with every group based on the creation order. If an agent belongs to multiple groups, to handle conflicting configurations, you can reorder the groups to change the ranking, and the policy associated with the highest ranked group takes precedence.

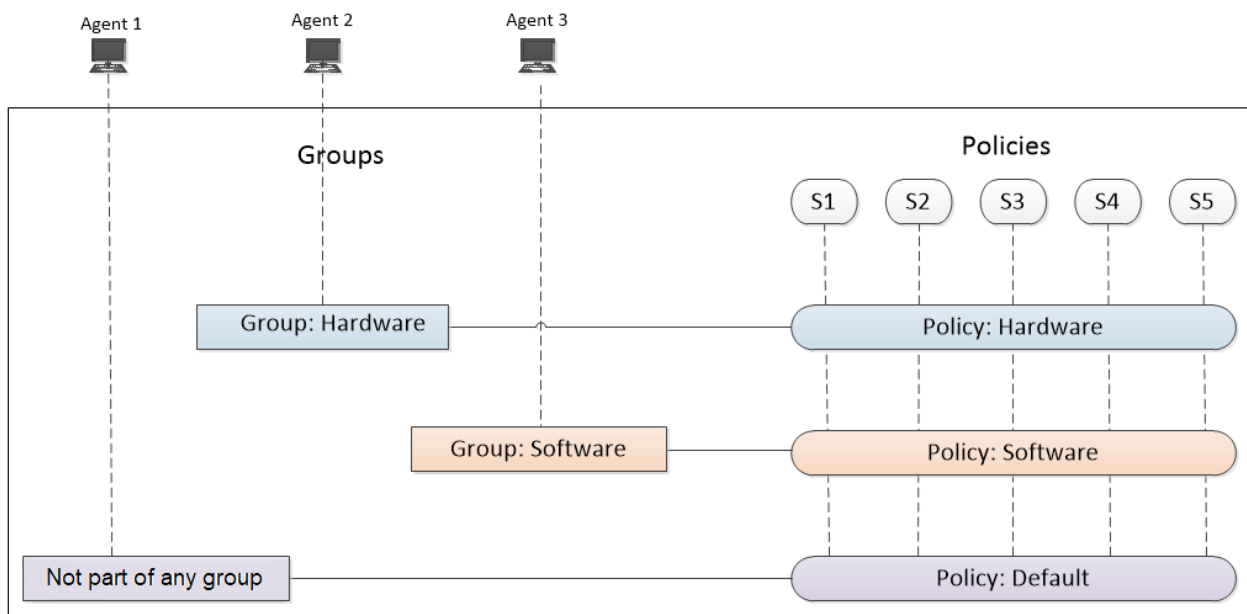
Example 1

A **Server** group contains 100 hosts with a default Agent Endpoint policy. Amongst these, if 20 hosts require further investigations, analyst can:

1. Create a temporary group with a static list of these 20 hosts.
2. Create or apply any policy to this group that will not impact any other hosts.
3. Edit the ranking for the new group, moving to the top of the Ranking list (making sure it is above the existing Server group).
4. After investigation is done, delete this group. The hosts are revalidated and assigned to the appropriate group based on the ranking.

Example 2

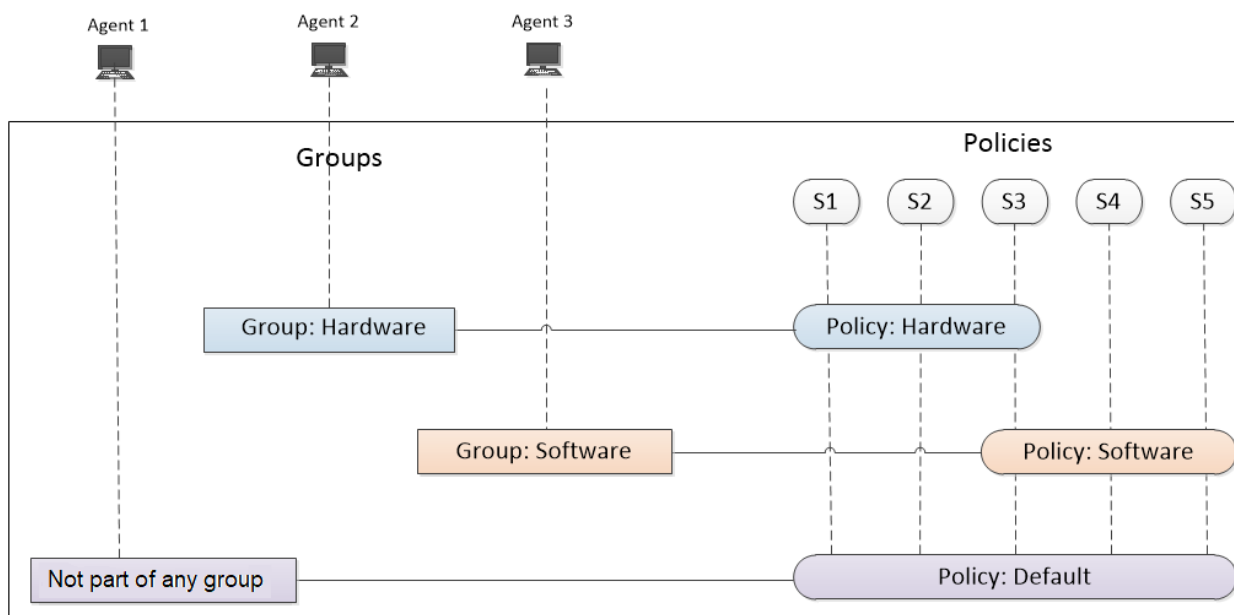
Case 1:



* S1, S2, S3, S4, and S5 represents policy settings, such as run scheduled scan, agent mode, scan settings, response actions, and so on.

Each agent is a part of a unique group that is associated with a policy, where each policy has all settings S1, S2, S3, S4, and S5 defined. For example, Agent 2 is a part of the group Hardware, where all settings in the policy Hardware are applicable.

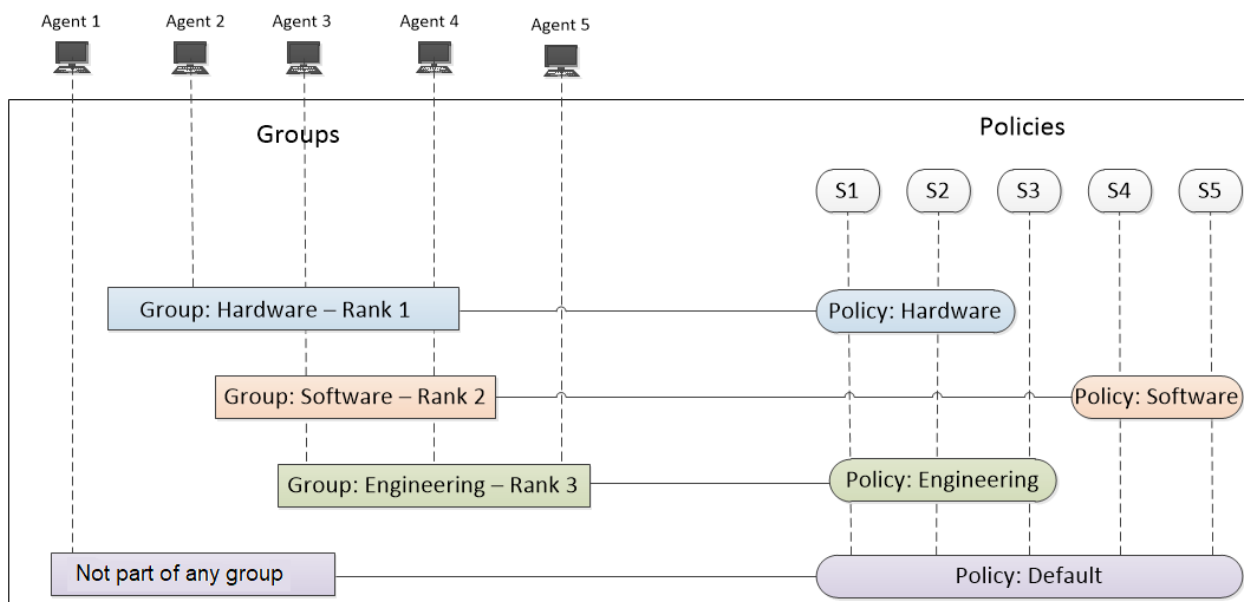
Case 2:



* S1, S2, S3, S4, and S5 represents policy settings, such as run scheduled scan, agent mode, scan settings, response actions, and so on.

In the policy Hardware, S4 and S5 settings are not defined, and hence the agent 2 inherits settings S4 and S5 from the default policy.

Case 3:



* S1, S2, S3, S4, and S5 represents policy settings, such as run scheduled scan, agent mode, scan settings, response actions, and so on.

- Agent 2 is a part of the highest ranked group Hardware, and with the policy Hardware. The agent 2 inherits settings S3, S4, and S5 from the default policy as they are not defined in the policy Hardware.
- Agent 3 is a part of Hardware, Software, and Engineering groups, and with the policy Software. The agent considers the settings S4 and S5 from the policy Software, and the remaining undefined settings are inherited as follows:

- S1 and S2 from the policy Hardware, which is associated with the highest ranked group.
- S3 from the policy Engineering, which is the next ranked group.
- Agent 4 is a part of Hardware, Software, and Engineering groups, and with the policy Engineering.
 - Though settings S1 and S2 are defined in policy Engineering, the agent 4 considers the settings S1 and S2 from the policy Hardware as it is associated with the highest ranked group.
- S4 and S5 from the policy Software, which is the associated with the next highest ranked group.
- S3 from the policy Engineering.

The following are some of the key points:

- If an agent is not assigned to any group, default policies are applied.
- A policy can be assigned to multiple groups. However, a group can only have one policy of each type (Agent Endpoint and Agent Windows Logs).
- An agent can belong to multiple groups. The policy is derived based on the ranking of the group as shown in the above example (case 3).
- If all settings are defined in a single policy, and it is the highest ranked policy for an agent, no policy settings from other ranked groups are inherited (case 1).
- If there are any undefined settings in the policy, the settings from the default policy is considered as shown in the example above (case 2 and 3).
- If an agent falls into more than one group, its complete set of policy attributes is determined as follows:
 - It takes all settings from the highest ranked policy that applies.
 - Any settings that are not set in the highest ranked policy are taken from the next highest ranked policy that applies.
 - If there are still unset attributes , they are taken from the default policy.
 - If there are any conflicts, the higher ranked policy wins.

Example 3

Assume the following:

- Agent A belongs to below two groups, **Production Servers** and **All Windows Hosts**.
- The Production Servers group has the **Schedule scan set and no blocking** policy assigned, and it has the following settings:
 - Schedule Scan : Enabled
 - Effective Date: 2019-03-08
 - Start Time: 09:00
 - Scan Frequency: Every 1 week
 - CPU Maximum: 45 %

- Virtual Machine Maximum: 20 %
- Blocking: Disabled
- The All Windows Hosts group has the **EDR for All Windows** policy applied, which has the following settings:
 - Scan Master Boot Record: Disabled
 - Blocking: Enabled
- The **Production Servers** group is ranked higher than the **All Windows Hosts** group for EDR policies. Keep in mind that ranking only applies to policies of the same source type: that is, all EDR policies are ranked, and all Windows Logs policies are ranked separately.

Agent A gets its final policy configuration as per the ranking of the groups (and associated policies) to which it belongs:

- The agent uses the schedule set in the **Schedule scan set and no blocking** policy.
- Scan Master Boot Record is disabled, because that is set in the **EDR for All Windows** policy.
- Blocking is disabled: since there is a conflict, the value in the higher ranked policy is used.
- All other attributes are set based on values in the Default EDR policy.
- Note that if you wanted Blocking to be enabled, you could change the group ranking so that All Windows Hosts is higher than Production Servers: in this case, Production Servers would win the conflict, and Blocking would be enabled for Agent A.

Default Agent Endpoint (EDR) Policy

When an agent is installed, it operates in an Insights mode until a policy is assigned. The following are the default EDR policy settings:

Settings	Fields	Default Value
Scan Schedule	Run Scheduled Scan	Disabled
	Effective Date	Current date
	Scan Frequency	Every 1 week
	Start Time	09:00 (this is 9 AM)
	CPU Maximum	25%
	Virtual Machine Maximum	10%
Agent Mode	Monitoring mode	Advanced

Settings	Fields	Default Value
Scan Settings	Scan Master Boot Record	Disabled
	Auto Scan New Systems When Added	Disabled
Response Action Settings	Blocking	Disabled
Endpoint Server Settings	Endpoint Server	The agent considers the default Endpoint Server that is configured during packager generation.
	Endpoint Server Forwarder (Optional)	
	HTTPS Port	443
	HTTPS Beacon Interval	15 Minutes
	UDP Port	444
	UDP Beacon Interval	30 Seconds

Default Windows Log Policy

The following are the default Windows Log policy settings:

Settings	Fields	Default Value
Windows Log Settings	Status	Disabled
	Protocol	TLS
	Send Test Log	Disabled

Creating Groups and Policies

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The following sections provide instructions on how to create groups and policies.

Create a Group

To create a group:

1. Go to **ADMIN > Endpoint Sources** view.
2. In the left panel, select the **Groups** tab.

GROUP NAME	SOURCE COUNT	POLICY(IES) APPLIED	GROUP DESCRIPTION	SOURCE TYPES APPLIED	PUBLICATION STATUS
Advanced Agents	0	Advanced Agents	Advanced agents group	Agent Endpoint	Published
Hardware	0	Advanced Agents	Hardware group	Agent Endpoint	Published
Migrated Agents	1	Migrate	Migrated agents group	Agent Endpoint	Published

3. In the toolbar, click **Create New**.
4. In the **New Group** panel, click **Identify Group**, and enter a group name and group description, and click **Next**.

NEW GROUP

Identify Group

GROUP NAME
Enter a unique group name

GROUP DESCRIPTION
Enter a description

Previous **Next** Save and Close Publish Now Cancel


5. Click **Define Group** and specify the logical statements that define the condition for an agent to be included in the group. Each logical statement consists of: parameter, operator, and values to match.

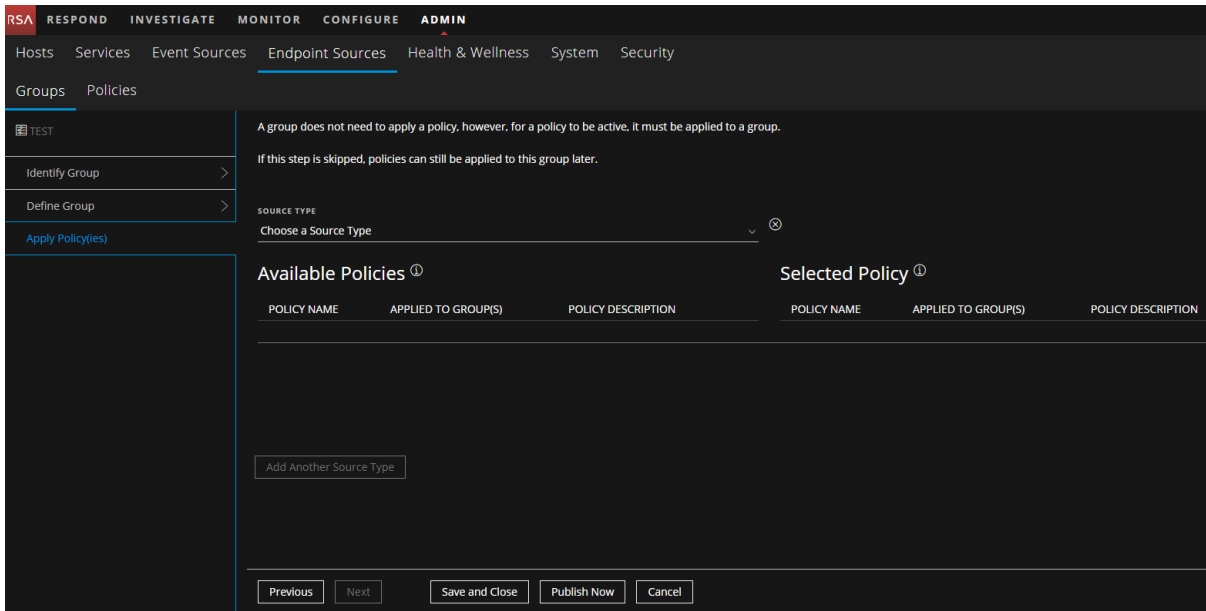
- In the **Include source if** ___ **of the conditions are met** field, select the appropriate conditions - all or any.
- For each logical statement, select the required options:

Item	Description
Parameter	<p>The parameter can be OS Type, OS Description, Host Name, IPv4, or IPv6.</p> <ul style="list-style-type: none"> • OS Type, OS Description, Host Name: The value you enter should reference hardware or virtual machines that are running endpoint agents. • IPv4 or IPv6: Enter valid IP addresses as either ranges or as a set of IP addresses to include or exclude. <p>Note: If you do not want to include certain IP addresses, use the Not in operator, and enter the IP address separated by a space or a comma.</p>
Operator	<p>The choice of values is dependent upon the parameter you chose. For example, if your parameter is OS Type, the only operator available is in.</p>
Value or values to match	<p>The value or values to match. For the OS Type parameter, you can choose one or more values from the drop-down list. For all other parameters, you can enter free-form text.</p> <p>Note: Although you can enter any text for values, the system validates your entries when you attempt to proceed to another screen, and will not allow you to proceed until values are valid.</p>

6. Click **Add Condition** to add another condition.
7. Click **Next** to proceed.
8. (Optional) Click **Apply Policy(ies)** and select the source type from the drop-down list. Policies with

the selected source type are displayed below **Available Policies**. You can either assign default policies or custom policies. For more information on creating policies, see [Create an EDR Policy](#) and [Create a Windows Log Policy](#).

Select a policy by clicking . Skip this step if you want to apply the policy later to the group.



Note: You can attach only one policy per source type to a group. That is, you cannot attach more than one Agent Endpoint policy to a single group, nor more than one Agent Windows Logs policy.

9. Do one of the following:


- Click **Save and Close** to save the settings and return to the Groups view. The publication status is displayed as **Unpublished** in the Groups view.

Note: You can select an unpublished group and click **Publish** to publish a group.

- Click **Publish Now** to publish the group.

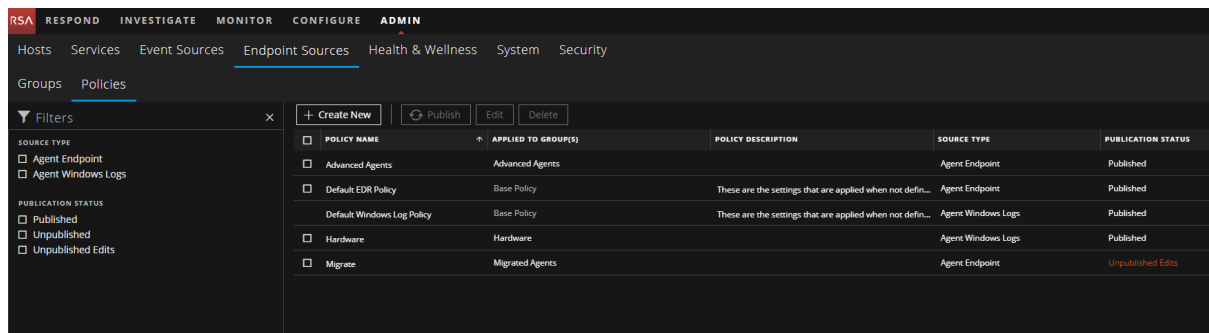
Create an EDR Policy

While creating a policy (either an EDR policy or a Windows Log policy), note the following:

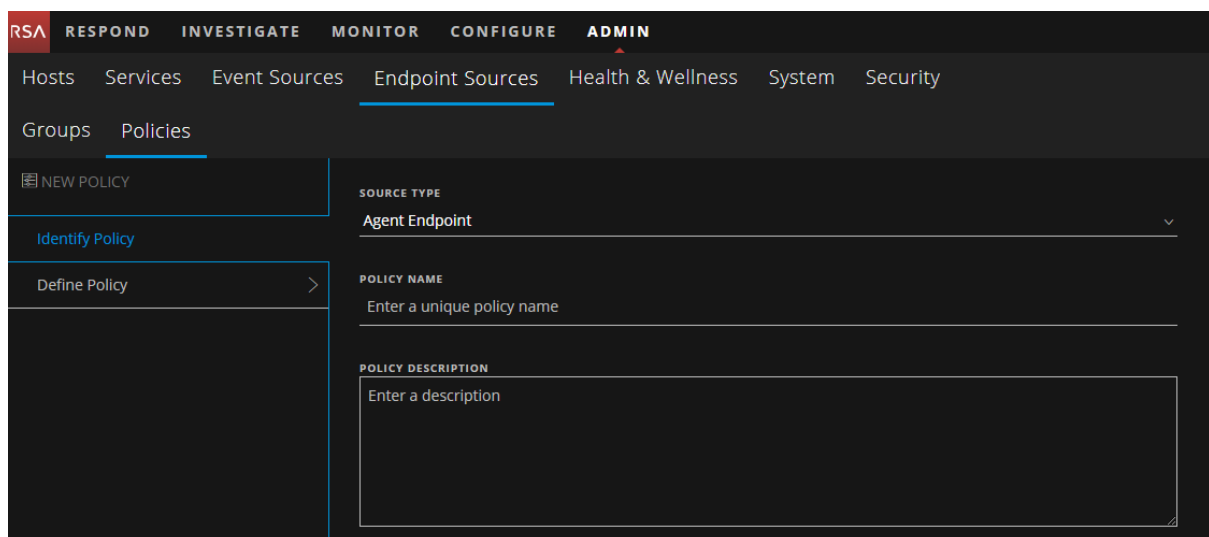
- Whenever you choose a setting, it is added to the **Selected Settings** panel.
- To clear any of your selected settings, click  to remove that setting.
- At any point in the wizard, you can choose **Save and Close**, so that you can return to complete the policy creation at a later time.


To create an EDR policy:

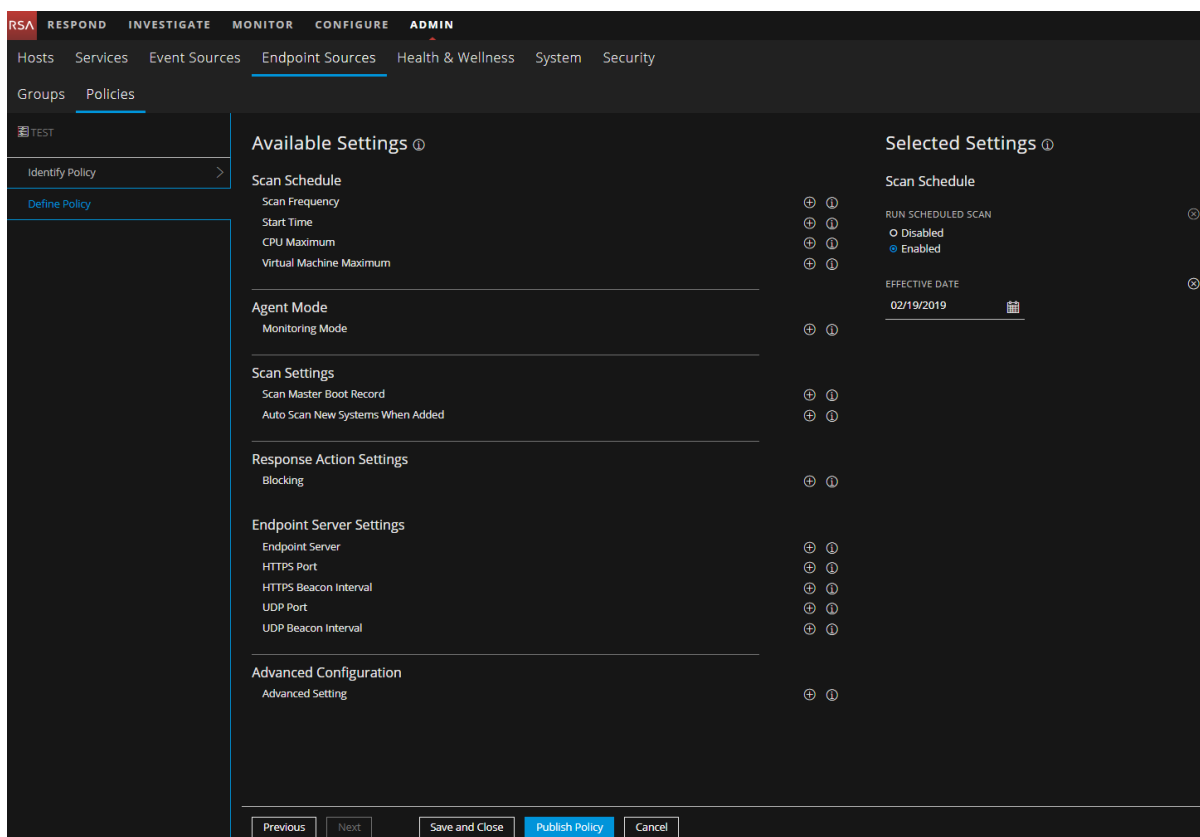
1. Go to **ADMIN > Endpoint Sources**.
2. Click **Policies**. The available policies are displayed.



3. Click **Create New** to add a new policy.
4. In the New Policy panel, select **Identify Policy**, and do the following:



- Select **Agent Endpoint** as the source type from the drop-down list.
 - Enter the policy name.
 - Enter a description for the policy.
5. Click **Next**.
 6. Click  to select a setting from list of **Available Settings**. Once clicked, the specific setting is moved under the **Selected Settings** panel. You need to enter the required values for the selected settings. For details, see [Define Policy Panel for Agent Endpoint Policy](#).



- In the Scan Schedule category:
 - Enable **Run Schedule Scan** to configure the scan.

Note: The following scan schedule options are available only when the scan schedule is enabled.

- Set the date when the scan schedule should be effective.
- Select the recurrence (days or weeks) and frequency of the scan.
- Select the start time of the scan.
- Set the CPU Maximum value using the slider.
- If the agents are running on virtual machines, set the Virtual Machine Maximum value using the slider.
- Add **Agent Mode** to select the monitoring mode of the agent - Insights or Advanced.
- In the Scan Settings category:
 - Enable **Scan Master Boot Record** to include Master Boot Record (MBR) details in scheduled scans.
 - Enable **Auto Scan New Systems When Added** to automatically queue a scan for any host that does not have any snapshot data.
- Enable **Response Action Settings** to prevent the execution of a malicious file on any host.
- In the Endpoint Server Settings:

- Add the Endpoint server that the agent will communicate from the drop-down list.

Note: If you do not select an Endpoint Server, the agent uses the default Endpoint Server that is configured during packager generation.

- (Optional) Enter an alternative hostname or IP address.
- Enter the HTTPS port used for communication.
- Specify the HTTPS beacon interval.
- Enter the UDP port used for communication.
- Specify the UDP beacon interval.
- **Advanced Configuration** - For RSA Support staff only.

IMPORTANT: It is strongly recommended not to use the Advanced Configuration unless advised to do so by RSA Support staff.

7. Do one of the following:


- Click **Save and Close** to save the settings and return to the Policies view. The policy will be listed under the **Unpublished** category.
- Click **Publish Policy** to publish the policy.

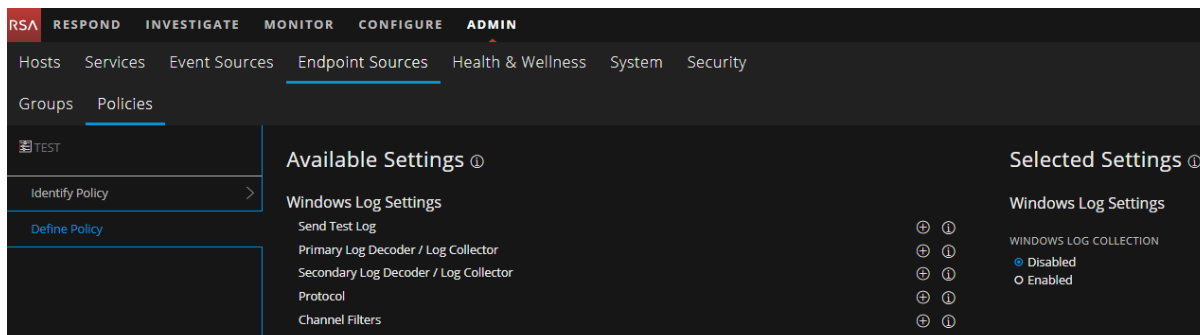
Create a Windows Log Policy

To create a Windows Log policy:

1. Go to **ADMIN > Endpoint Sources**.
2. Click **Policies**. The available policies are displayed.
3. Click **Create New** to add a new policy.
4. In the New Policy panel, select **Identify Policy**, and do the following:

The screenshot displays the RSA NetWitness Admin console interface. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The 'ADMIN' tab is active, and the 'Endpoint Sources' sub-tab is selected. On the left sidebar, the 'Policies' section is expanded, showing options for 'NEW POLICY', 'Identify Policy', and 'Define Policy'. The 'Identify Policy' option is selected. The main panel shows the 'SOURCE TYPE' dropdown set to 'Agent Windows Logs'. Below this, there are input fields for 'POLICY NAME' (with the placeholder 'Enter a unique policy name') and 'POLICY DESCRIPTION' (with the placeholder 'Enter a description').

- Select **Agent Windows Logs** as the source type from the drop-down list.
 - Enter the policy name.
 - Enter a description for the policy.
5. Click **Next**.
6. Click  to select a setting from list of **Available Settings**. Once clicked, the specific setting is moved under the **Selected Settings** panel. You need to enter the required values for the selected settings.



- Select **Windows Log Collection** to enable Windows Log collection. By default, this option is disabled.
- Enable **Send Test Log** to send a test log. By default, this option is disabled.
- Select **Primary Log Decoder / Log collector** to forward logs from the drop-down list.
- (Optional) Select **Secondary Log Decoder / Log collector** to forward logs from the drop-down list.

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.

- Select **Protocol** from the drop-down list. The available options are UDP, TCP, and TLS. By default, the protocol is TCP.
 - Add **Channel Filters** and select the channels from which the logs are collected from the drop-down list. You can add or remove a channel filter and specify individual Event IDs.
7. Do one of the following:
- Click **Save and Close** to save the settings and return to the Policies view. The policy will be listed under the **Unpublished** category.
 - Click **Publish Policy** to publish the policy.

Managing Groups

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

You can view group details, edit group details, filter endpoint groups, delete groups, and edit group ranking. For details on how to create groups, see [Create a Group](#).

View Group Details

To view properties of the selected group:

1. Go to **ADMIN > Endpoint Sources**.
2. In the left panel, select the **Groups** tab. The details, such as group name, source count, policies applied, group descriptions, source type applied, and publication status are displayed. For more details on these columns, see [Endpoint Sources - Groups](#).
3. Click the row to view the properties in the right-panel.

GROUP NAME	SOURCE COUNT	POLICY(IES) APPLIED	GROUP DESCRIPTION	SOURCE TYPES APPLIED	PUBLICATION STATUS
Advanced Agents	0	Advanced Agents	Advanced agents group	Agent Endpoint	Published
Hardware	0	Advanced Agents	Hardware group	Agent Endpoint	Published
Migrated Agents	1	Migrate	Migrated agents group	Agent Endpoint	Published

Hardware
Hardware group

Policy(ies) Applied
Agent Endpoint Advanced Agents

Source Count
0

Definition
Sources included if ALL of the following conditions are met:
Host Name contains: SA-Server
OS Type is: Windows
OS description is equal to: Microsoft Windows 10 Enterprise
OS Type in: Windows
IPV4 between: 10.40.15.100 and 10.40.15.200

History
Created On: 2019-02-05 03:36
Created By: admin
Last Updated On: 2019-02-20 10:30
Last Updated By: admin
Last Published On: 2019-02-20 10:30

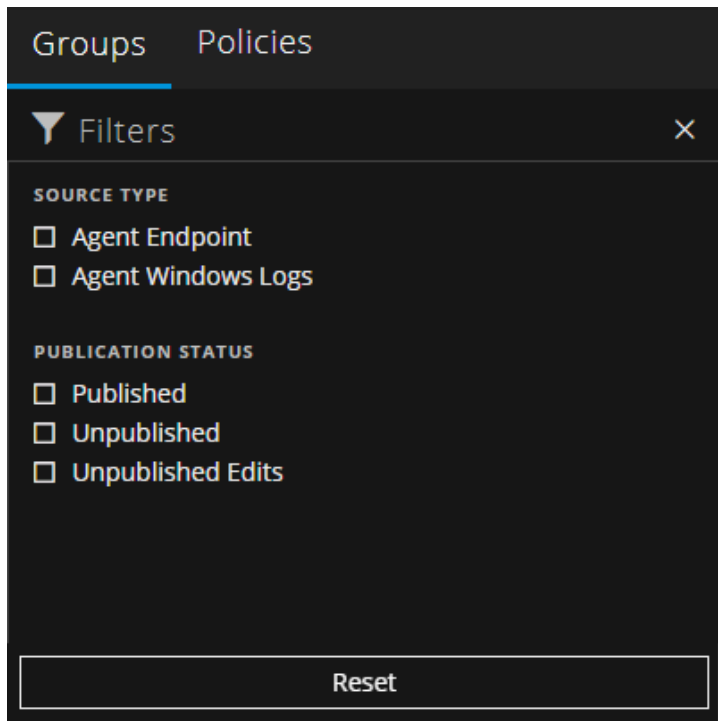
Filter Endpoint Groups

The Filters Panel allows you to filter the list of displayed groups, based on the one of the following source type:



- Agent Endpoint
- Agent Windows Logs

Additionally, you can sort based on publication status:

- Published - Groups that are published to use.
- Unpublished - Groups that are saved but not published.
- Unpublished Edits - Groups that are previously published and edited later and saved, but not published.



The Filters panel can be hidden or displayed:

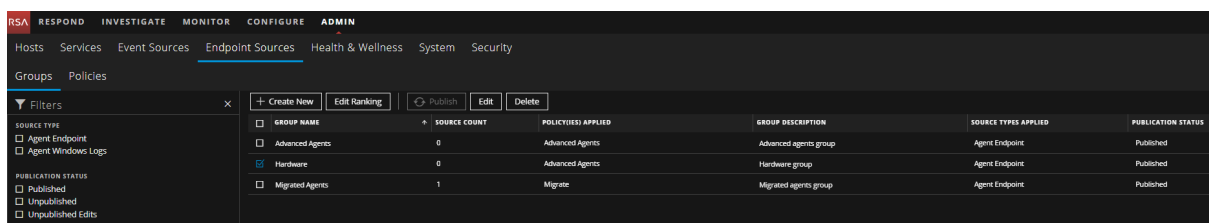
- To hide, click the  icon at the top-right of the panel.
- To display if hidden, click the  icon in the toolbar.

Click **Reset Filters** to remove the currently applied filter criteria.

Edit a Group

You can edit the properties of the group at any point in time. To edit properties of a group:

1. Go to **ADMIN > Endpoint Sources**.
2. Select a group and click **Edit**.



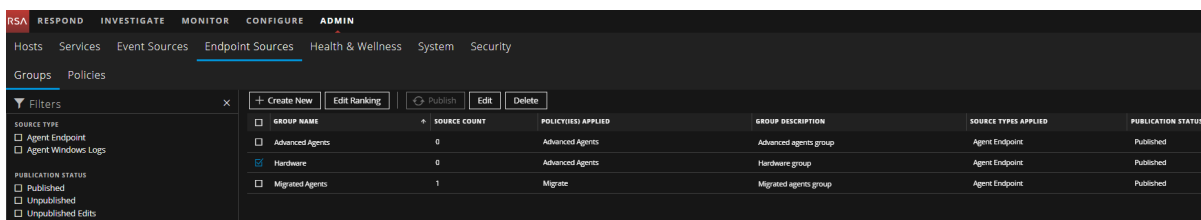
3. Edit the group details as required.
4. Do one of the following:
 - Click **Save and Close** to save the changes and return to the Groups view. The group will be listed under the **Unpublished Edits** category.

- Click **Publish Now** to publish the changes.

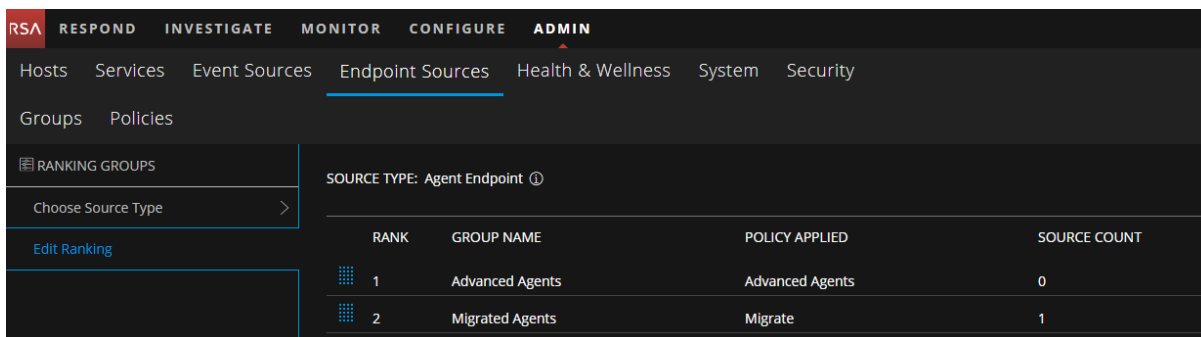
Change Policy Ordering for Groups


An endpoint agent can be included in multiple groups. And these groups can have different policies applied to them. In this case, you can edit the ordering or ranking of policies, to specify a hierarchy for your policies. To edit the ordering or ranking of a group:

1. Go to **ADMIN > Endpoint Sources**.
2. Select the Groups tab and click **Edit Ranking**.



3. Select one of the following source type for the drop-down list:
 - Agent Endpoint to rank the groups associated with Agent Endpoint type policies.
 - Agent Windows Logs to rank the groups associated with Agent Windows Log type policies
4. Click **Next**.
5. Reorder your groups as necessary.



- a. Select  next to a group.
- b. Drag the group up or down to change the priority. Priority decreases from top to bottom.
- c. Repeat moving groups until they are ordered as you prefer.

Note: To move any group to the top, select the group and click **Set Top Ranking**.

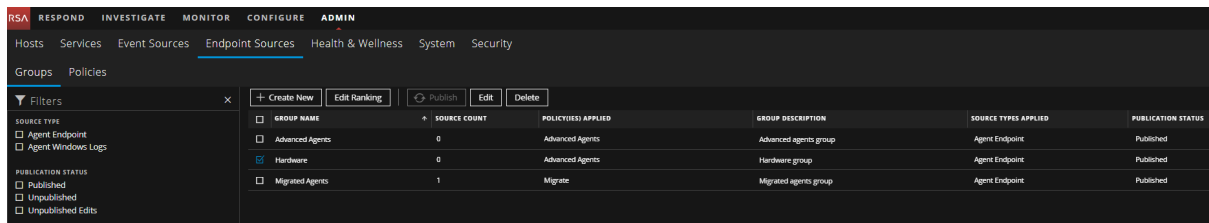
6. Once you have the preferred order, click the appropriate option:
 - **Publish Ranking** for the new ranking to take effect.

- **Reset Ranking** to reset the ranking to the last saved or published order.
- **Cancel** to exit without changing the rankings.

Delete a Group

To delete a group:

1. Go to **ADMIN > Endpoint Sources**.
2. The **Groups** tab and available groups are displayed.



GROUP NAME	SOURCE COUNT	POLICY(IES) APPLIED	GROUP DESCRIPTION	SOURCE TYPES APPLIED	PUBLICATION STATUS
<input type="checkbox"/> Advanced Agents	0	Advanced Agents	Advanced agents group	Agent Endpoint	Published
<input checked="" type="checkbox"/> Hardware	0	Advanced Agents	Hardware group	Agent Endpoint	Published
<input type="checkbox"/> Migrated Agents	1	Migrate	Migrated agents group	Agent Endpoint	Published

3. Select one or more groups and click **Delete**.
4. Click **Delete**. The confirmation message is displayed.
5. In the Delete Groups dialog, click **Delete Group(s)** to permanently delete the selected groups.

Managing Policies

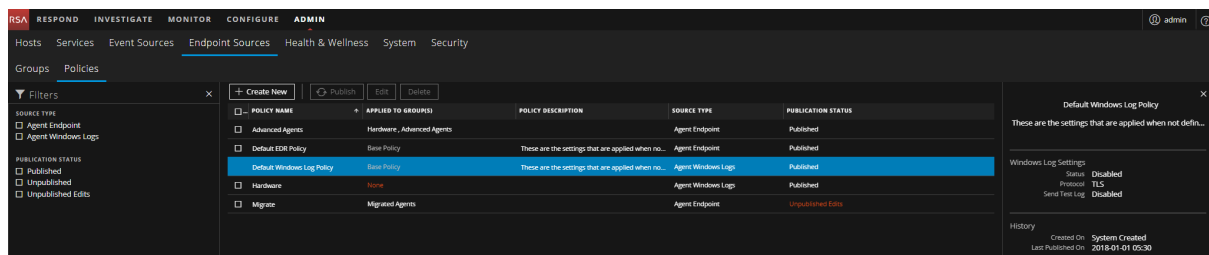
Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

You can view, edit, filter, and delete policies. For details on how to create policies, see [Create an EDR Policy](#) or [Create a Windows Log Policy](#).

View Policy Details

To view properties of the selected policy:

1. Go to **ADMIN > Endpoint Sources**.
2. In the left panel, select the **Policies** tab. The details, such as policy name, applied to groups, policy description, source type, and publication status are displayed. For more details on these columns, see [Endpoint Sources - Policies](#).
3. Click the row to view details about selected policy in right pane.



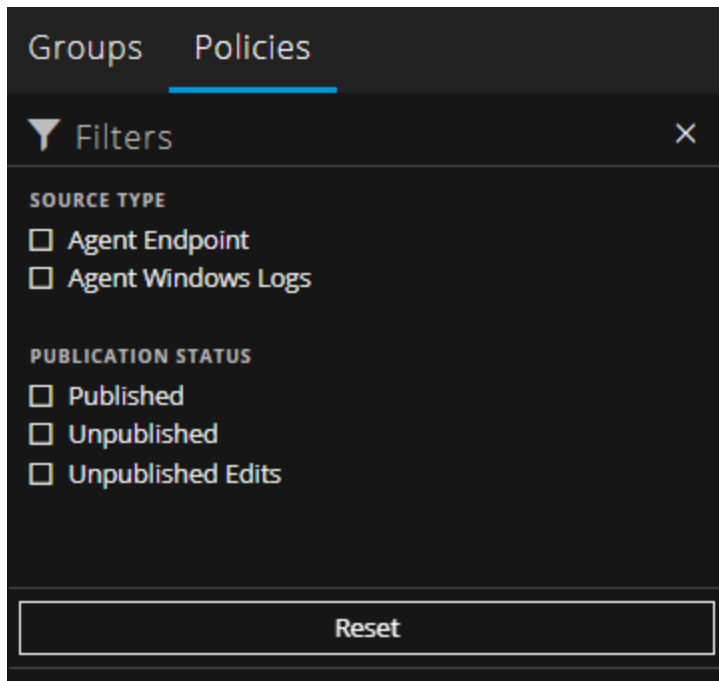
Filter Policies

The Filters Panel allows you to filter the list of displayed policies, based on the source type:



- Agent Endpoint, or
- Agent Windows Logs

Additionally, you can filter based on publication status:

- Published: Policies that are published to use.
- Unpublished: Policies that are saved but not published.
- Unpublished Edits: Policies that are previously published and edited later and saved, but not published.



The Filters panel can be hidden or displayed:

- To hide, click the  icon at the top-right of the panel.
- To display if hidden, click the  icon in the toolbar.

Click **Reset Filters** to remove the currently applied filtering criteria.

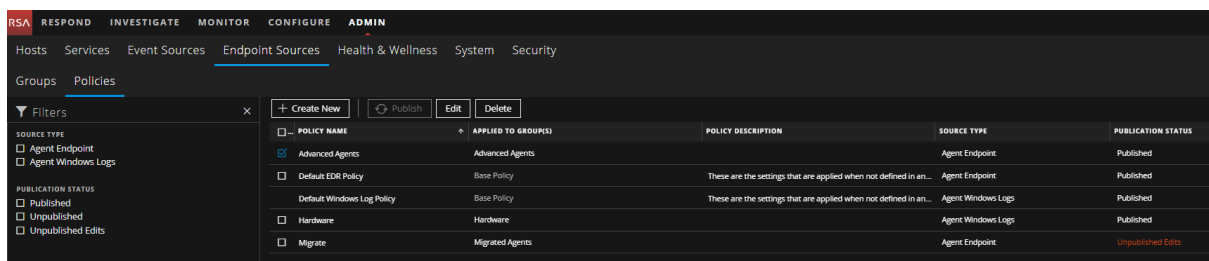
Edit a Policy

You can edit the settings of the default Agent Endpoint and custom policies. The default Agent Windows Log policy cannot be edited.

Note: For the default EDR policy, you cannot edit the source type, policy name, and policy description. However, you can edit the details in the Define Policy panel.

To edit a policy:

1. Go to **ADMIN > Endpoint Sources**, and select the **Policies** tab.
2. Select a policy and click **Edit**.



3. Edit the policy details as required.
4. Do one of the following:
 - Click **Save and Close** to save the changes and return to the Policies view. The policy will be listed under the **Unpublished Edits** category.
 - Click **Publish Policy** to publish the changes.

Delete a Policy

To delete a policy:

1. Go to **ADMIN > Endpoint Sources**.
2. Click the **Policy** tab. The available policies are displayed.


</

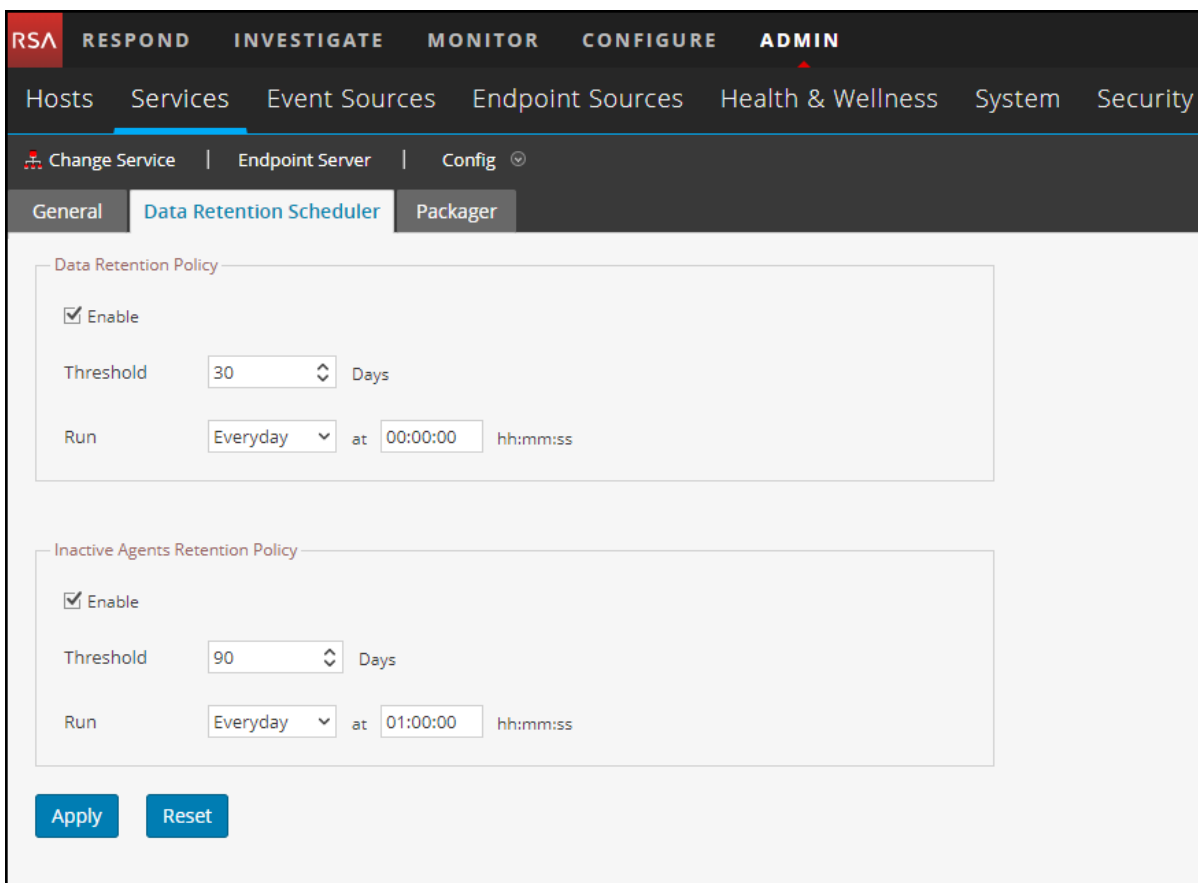
3. Select one or more policies and click **Delete**.
The confirmation message is displayed.
4. In the Delete Policies dialog, click **Delete Policy(ies)** to permanently delete the selected policies.

Configuring 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.




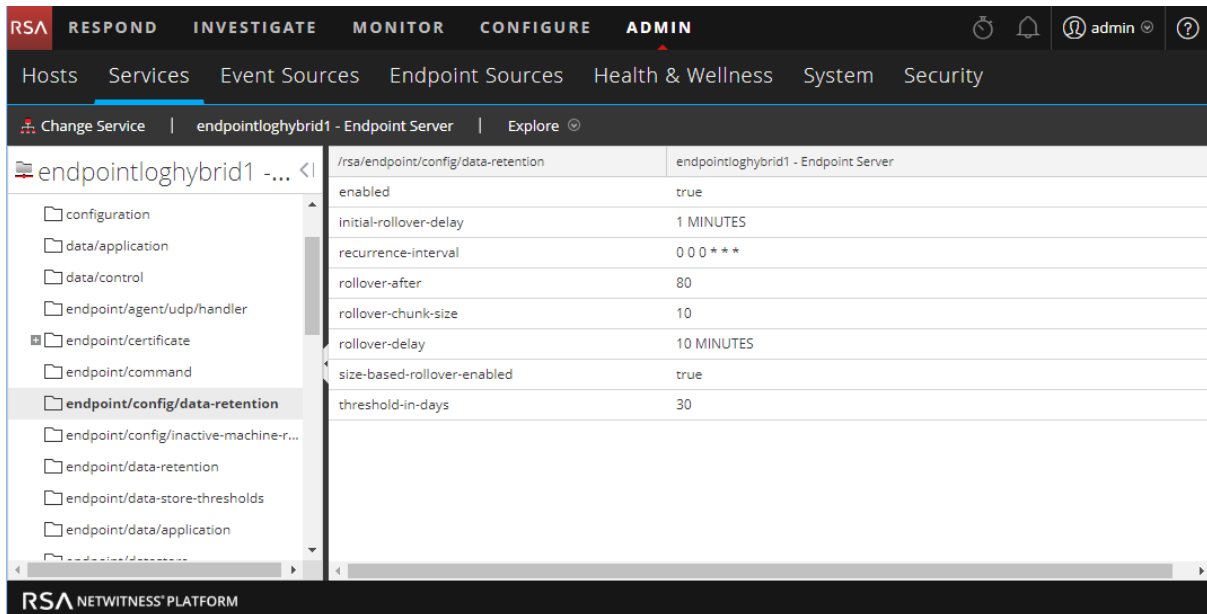
The screenshot shows the NetWitness Endpoint Configuration interface. The top navigation bar includes tabs for RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, there are sub-tabs for Hosts, Services, Event Sources, Endpoint Sources, Health & Wellness, System, and Security. The 'Services' tab is selected, and the 'Endpoint Server' service is chosen. The 'Config' button is visible. The 'Data Retention Scheduler' tab is active, showing two sections: 'Data Retention Policy' and 'Inactive Agents Retention Policy'. Both sections have an 'Enable' checkbox checked, a 'Threshold' field set to 30 and 90 respectively, and a 'Run' field set to 'Everyday' at '00:00:00' and '01:00:00' respectively. 'Apply' and 'Reset' buttons are at the bottom.

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:




Path	Value
enabled	true
initial-rollover-delay	1 MINUTES
recurrence-interval	0 0 0 * * *
rollover-after	80
rollover-chunk-size	10
rollover-delay	10 MINUTES
size-based-rollover-enabled	true
threshold-in-days	30

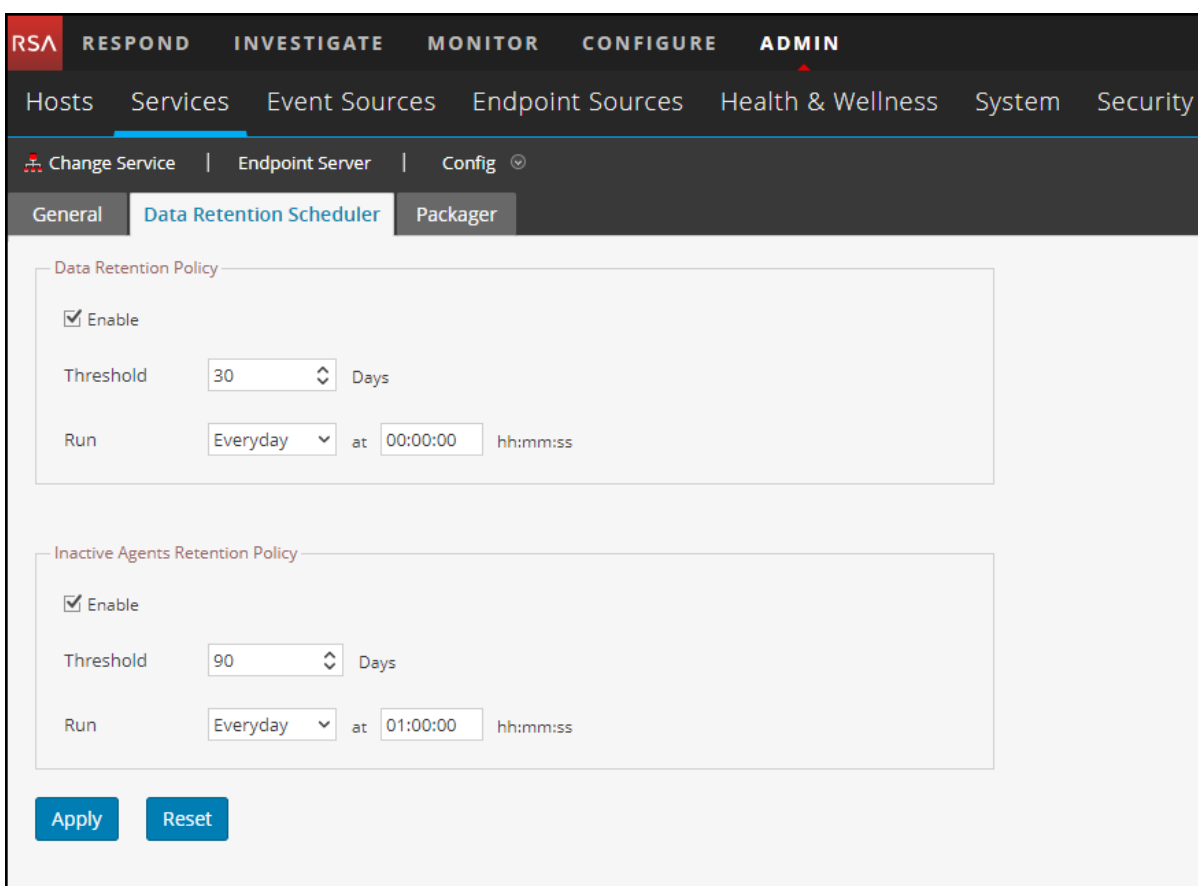
4. In the left panel, select **endpoint/config/data-retention**.
5. Edit the configurations based on your requirements.

Managing 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.



The screenshot shows the NetWitness Endpoint configuration interface. The top navigation bar includes tabs for RSA, RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Below this, there are sub-tabs for Hosts, Services, Event Sources, Endpoint Sources, Health & Wellness, System, and Security. The 'Services' tab is selected, and the 'Endpoint Server' is chosen. The 'Config' button is visible. The 'Data Retention Scheduler' tab is active, showing two policy sections: 'Data Retention Policy' and 'Inactive Agents Retention Policy'. Both sections have an 'Enable' checkbox checked, a 'Threshold' set to 30 and 90 days respectively, and a 'Run' frequency of 'Everyday' at '00:00:00' and '01:00:00' respectively. 'Apply' and 'Reset' buttons are at the bottom.

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.

Configuring Location for File Download

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

You must configure the location to download the files from hosts to the Endpoint server. To configure, make sure that you have `endpoint-server.configuration.manage` permissions.

1. Create a directory in the Endpoint server and provide write permissions for the user "netwitness".
2. In the Explore view, go to **endpoint/download**.
3. In the base-path, provide the location of the directory.

Integrating NetWitness Endpoint 4.4.0.2 or Later with NetWitness Platform

You can configure the Endpoint Metadata for the NetWitness Endpoint 4.4.0.2 by integrating 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. This integration includes the following steps:

- [Enabling the NetWitness Endpoint 4.4.0.2 Metadata Forwarding to the Log Decoder](#)
- [Enabling Machines to Forward Metadata from the NetWitness Endpoint 4.4.0.2 to the NetWitness Endpoint Server](#)

Enabling the NetWitness Endpoint 4.4.0.2 Metadata Forwarding to the Log Decoder

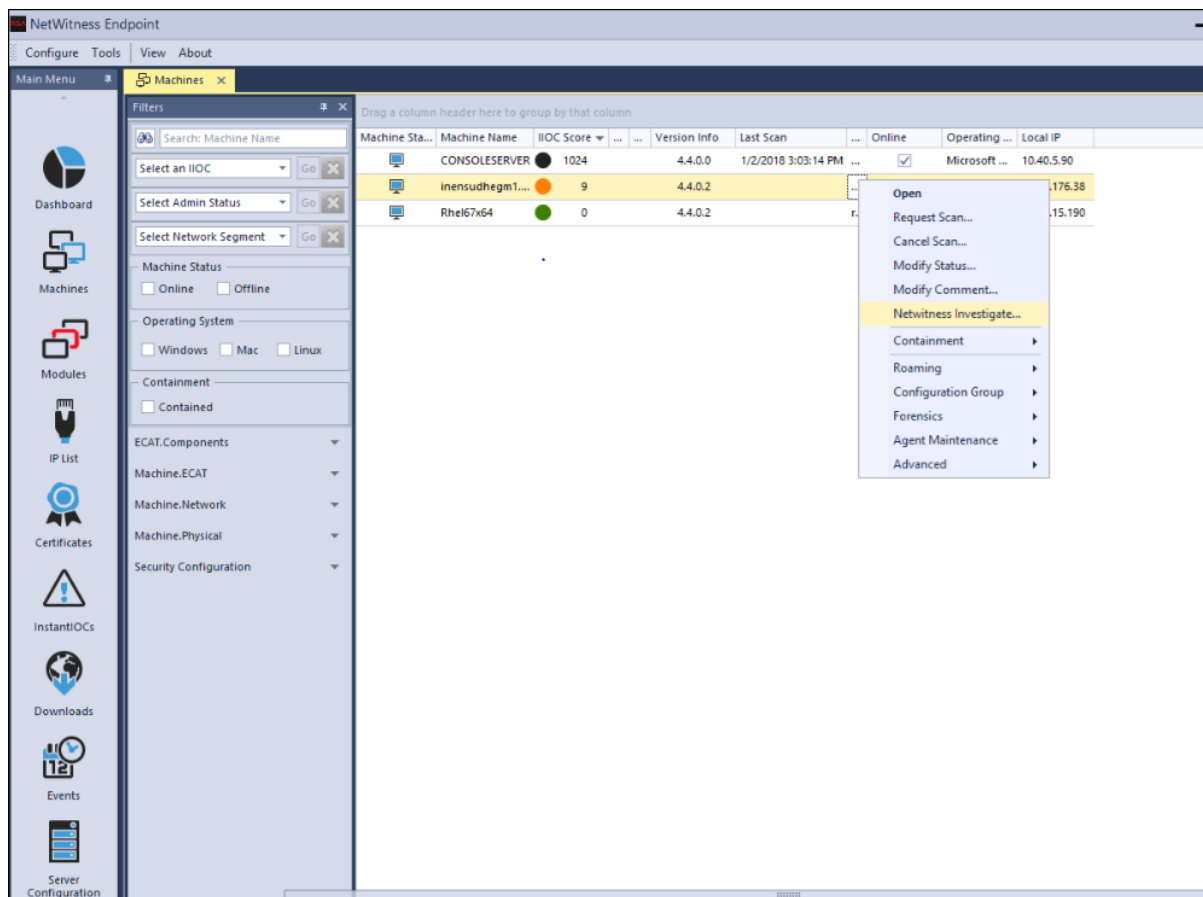
To enable the Metadata Integrator service for the selected NetWitness Endpoint 4.4.0.2 agents, run the following command:

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

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

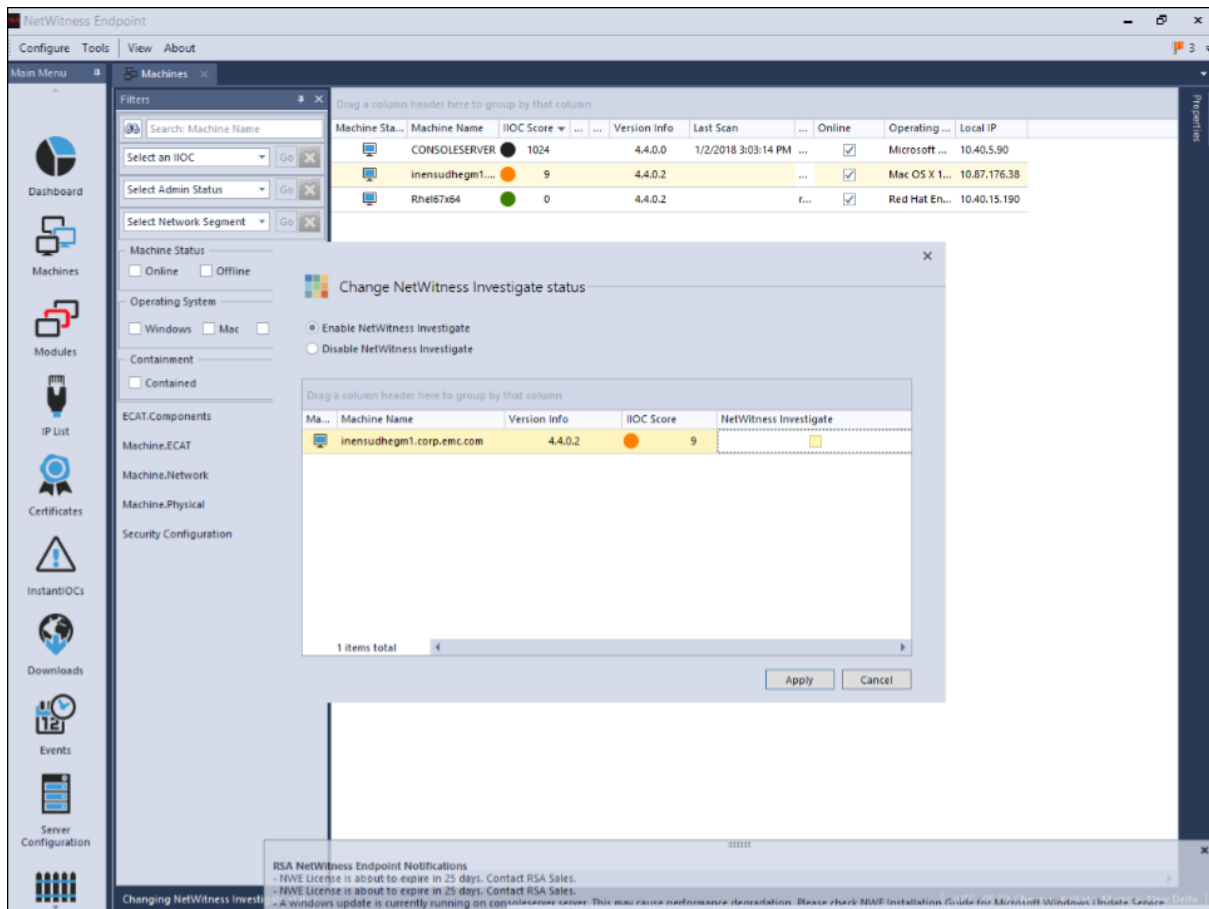
After you enable the Metadata Forwarding using any one of the above options, perform the following to enable the machines to forward metadata.

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.


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 for multiple endpoint servers. To access this view:

1. Go to **ADMIN > Services**.
2. In the Services view, select **Endpoint Server** for which you want to configure the metadata forwarding.
3. Click  and select **> View > Config**.
4. Click the **General** tab.

Workflow



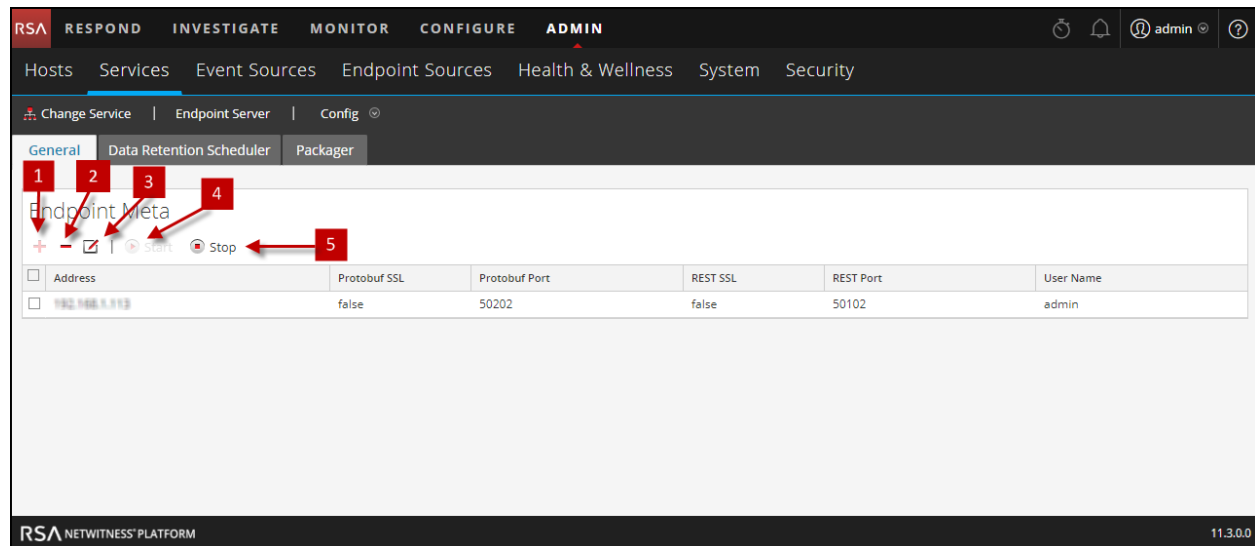
What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Endpoint Metadata Forwarding for the NetWitness Endpoint 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 Platform

*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 50202 (for non-SSL) and value 56202 (for SSL).
User Name	Displays the user name.

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

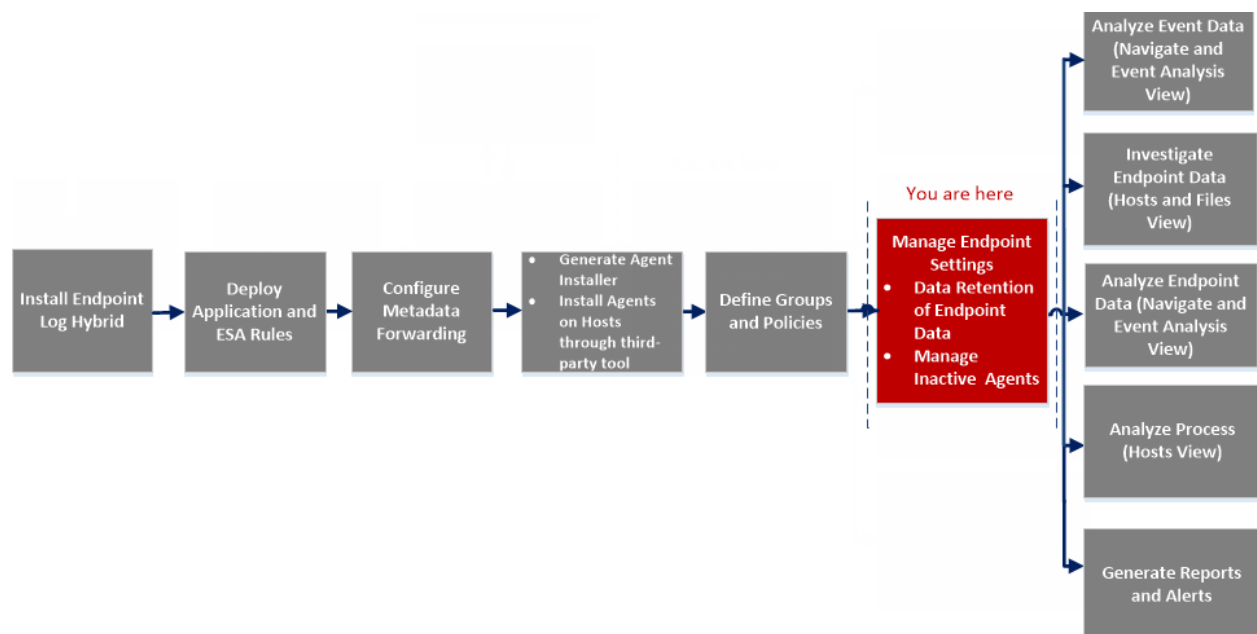
Data Retention Scheduler Tab

In the **Data Retention Scheduler** tab, you can configure data retention and inactive agents policies for multiple endpoint servers. 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.

Repeat the above steps to configure data retention settings for multiple endpoint servers.

Workflow



What do you want to do?

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

The screenshot displays the NetWitness Platform interface for configuring the Data Retention Scheduler. The top navigation bar includes tabs for Hosts, Services, Event Sources, Endpoint Sources, Health & Wellness, System, and Security. The 'ADMIN' section is active, and the 'Data Retention Scheduler' tab is selected. The configuration is divided into two main sections: 'Data Retention Policy' and 'Inactive Agents Retention Policy'. Each section has an 'Enable' checkbox (checked), a 'Threshold' dropdown (set to 30 and 90 days), and a 'Run' schedule (set to 'Everyday' at '00:00:00' and '01:00:00' respectively). At the bottom, there are 'Apply' and 'Reset' buttons. The footer shows 'RSA NETWITNESS PLATFORM' and version '11.3.0.0'.

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.

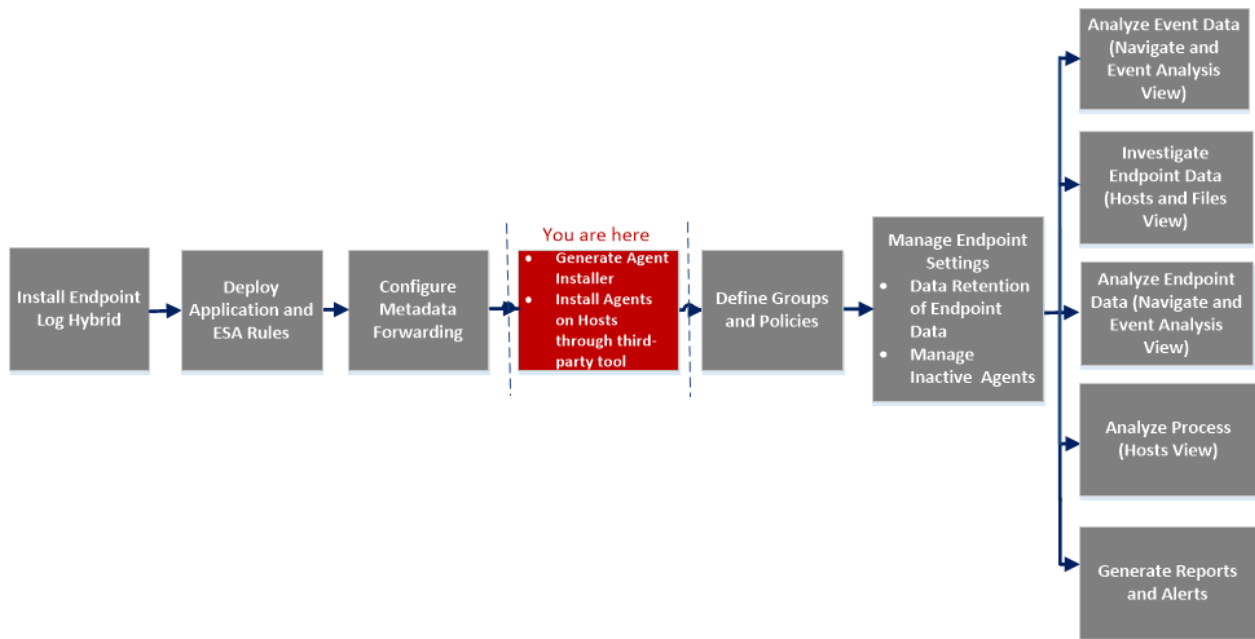
Fields	Description
Enable	Enables the configuration for the inactive agents policy. By default, this option is enabled.
Threshold	Displays the number of days the inactive agents are retained in the Endpoint Server. By default, the threshold value is 90 days.
Run	Displays the schedule for running the 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.

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.

Workflow



What do you want to do?

Role	I want to ...	Show me how
Administrator	Generate an Agent Packager for Endpoint Data Collection*	<i>NetWitness Endpoint Agent Installation Guide</i>
Administrator	Generate an Agent Installer*	

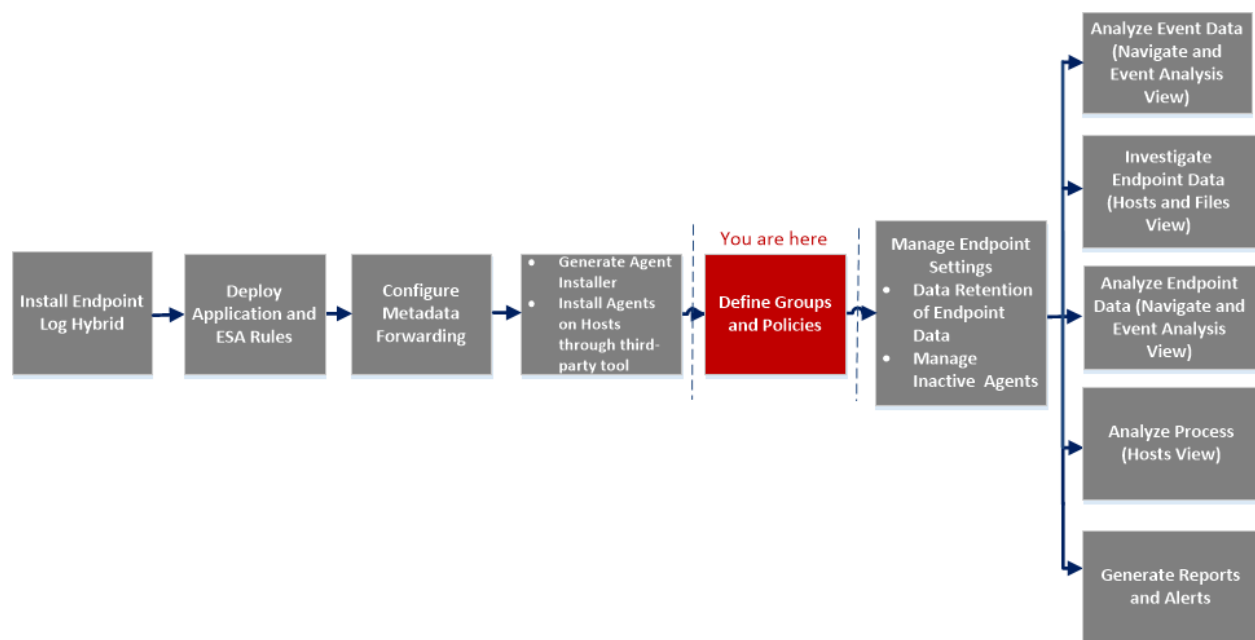
*You can perform this task in the current view.

Endpoint Sources - Groups

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The **ADMIN > Endpoint Sources** view contains two tabs: **Groups** and **Policies**.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Administrator	create new groups*	Create a Group
Administrator	edit groups*	Edit a Group
Administrator	edit ranking*	Change Policy Ordering for Groups
Administrator	delete groups*	Delete a Group
Administrator	view default policies	Default Agent Endpoint (EDR) Policy
Administrator	create an EDR policy	Create an EDR Policy
Administrator	create a Windows Log policy	Create a Windows Log Policy
Administrator	edit policies	Edit a Policy
Administrator	delete policies	Delete a Policy

*You can perform this task in the current view.

Related Topics

- [Endpoint Sources](#)
- [Managing Policies](#)

Quick Look

Below is an example of the Groups tab:

GROUP NAME	SOURCE COUNT	POLICIES APPLIED	GROUP DESCRIPTION	SOURCE TYPES APPLIED	PUBLICATION STATUS
Advanced Agents	0	Advanced Agents	Advanced agents group	Agent Endpoint	Published
Hardware	0	Advanced Agents	Hardware group	Agent Endpoint	Published
Migrated Agents	1	Migrate	Migrated agents group	Agent Endpoint	Published

1 Actions in the toolbar:

Create New - Lets you create a new group. For more information, see [Create a Group](#)

Edit Ranking - Lets you edit the ranking of groups. For more information, see [Change Policy Ordering for Groups](#)

Publish - Publishes the selected group or groups.

Edit - Lets you edit the details of an existing group. For more information, see [Edit a Group](#).

Delete - Deletes the selected group or groups permanently. For more information, see [Delete a Group](#).

2 Filters. You can filter groups based on Source Type and Publication Status.

To hide, click the  icon at the top-right of the panel. To display if hidden, click the  icon in the toolbar.

Reset - Removes the currently applied filter criteria.

For more information, see [Filter Endpoint Groups](#).

3 Table. Displays the group details:

- Group name - Name of the group.
- Source Count: Number of hosts that are currently members of the group.
- Policies applied: Lists the policies applied to this group.
- Group description - Description of the group.
- Source Types Applied: Type of policies applied to the group: Agent Endpoint, Agent Windows Logs, or both
- Publication Status: Status of the group - Published or Unpublished.

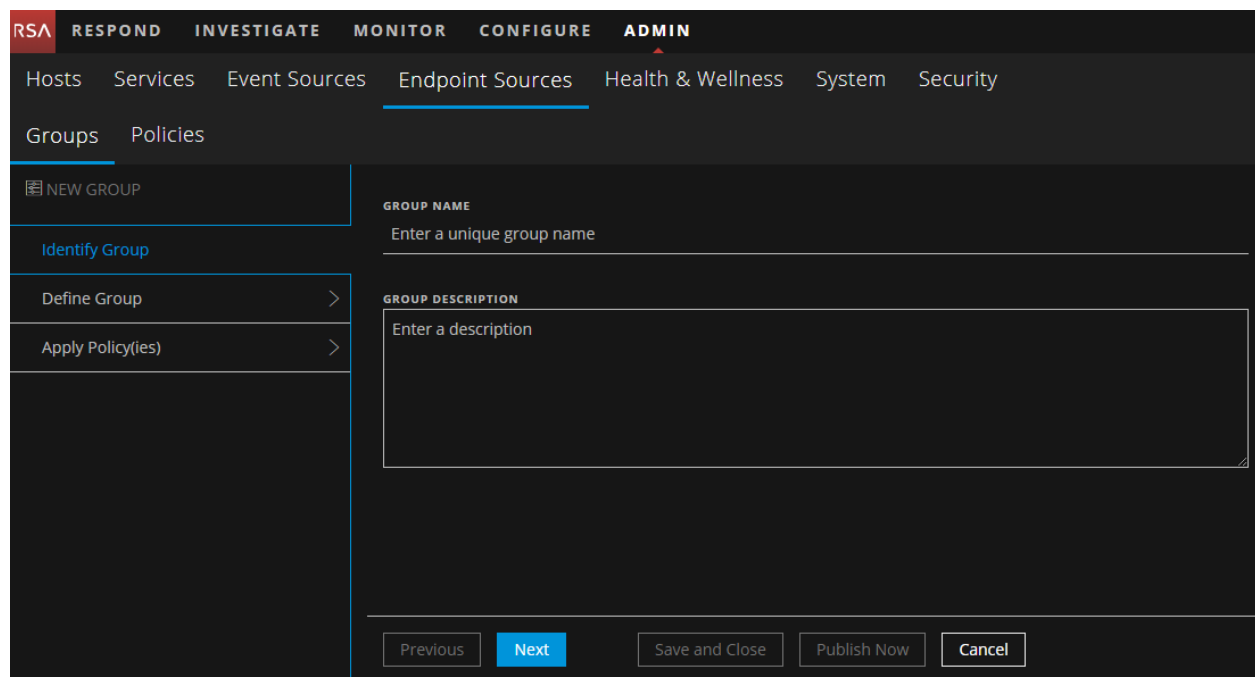
Sort Columns. If you mouse over a column header, a sort icon is displayed: . Click the icon to sort by the selected column.

4 Details panel. Displays the properties of the selected group.

Note: Click the row to view the Properties panel for a group.

Create Group

Below is an example of the Create Group dialog. The table describes the information and options in the Create Group dialog.



Field	Description
Group Name	Name of the group. The name should be unique.
Group Description	Description of the group and should not exceed 8000 characters.

Below is an example of Define Group panel. The table describes the information and options in the Define Group panel:

The screenshot shows the 'Define Group' panel in the NetWitness interface. The top navigation bar includes 'RSA', 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'CONFIGURE' tab is active, and the 'Endpoint Sources' sub-tab is selected. The left sidebar shows 'Groups' and 'Policies', with 'TEST' selected under 'Groups'. The main panel displays the 'Define Group' configuration for the 'TEST' group. It includes a section 'Include source if all of the following conditions are met:' with a dropdown for 'OS Type' set to 'in'. Below this is a button 'Add Condition'. At the bottom, there are buttons for 'Previous', 'Next', 'Save and Close', 'Publish Now', and 'Cancel'.

Field	Description
Include source if ...of the conditions are met	Defines the conditions for an agent to be included in the group. Available options are all or any.
Parameter	<p>The parameter can be OS Type, OS Description, Host Name, IPv4, or IPv6.</p> <ul style="list-style-type: none"> OS Type - Type of operating system. Available options are: Windows, Linux, and MacOS. OS Description - Description of the operating system. The description should not exceed 256 characters. Available operators are: is equal to, contains, start with, and ends with. For example, Microsoft Windows 10 Enterprise. Host name - Name of the host. The host name can contain only alphanumeric characters. Available operators are: is equal to, contains, start with, ends with, and in. For example, DESKTOP-QQPDNG3. IPv4 and IPv6 - IP address. Available operators are: between, in, not in, and between. For example, 10.40.15.220. <p>Note: If you do not want to include certain IP addresses, use the Not in operator, and enter the IP address separated by a space or a comma.</p>

Field	Description
Operator	The choice of values is dependent upon the parameter you chose. For example, if your parameter is OS Type, the only operator available is in .
Value or values to match	The value or values to match. For the OS Type parameter, you can choose one or more values from the drop-down list. For all other parameters, you can enter free-form text. <div> Note: Although you can enter any text for values, the system validates your entries when you attempt to proceed to another screen, and will not allow you to proceed until values are valid. </div>
Add condition	Lets you add another condition.

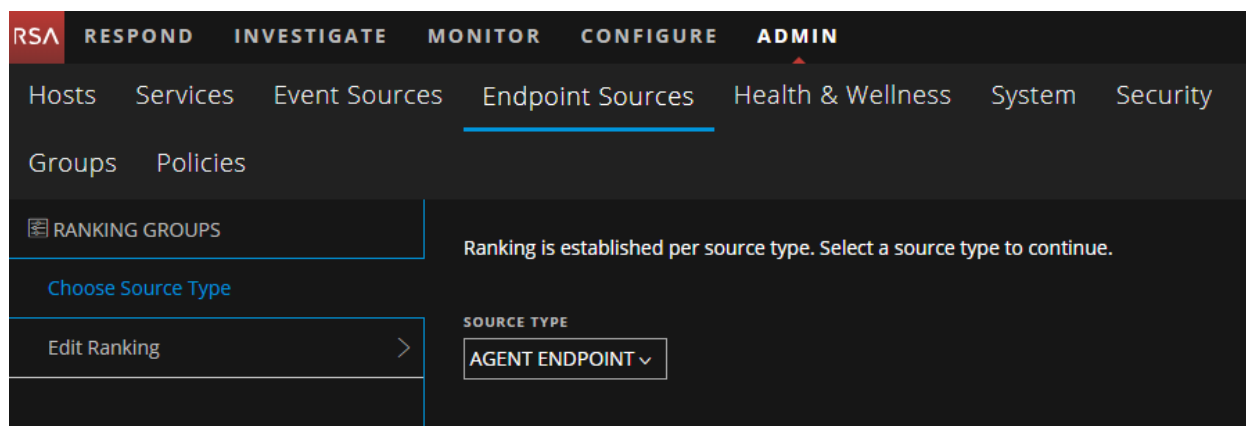
Below is an example of Apply Policies panel. The table describes the information and options in the Apply Policies panel:

Field	Description
Source Type	Defines the source type for the group. Available options are Agent Endpoint and Agent Windows Logs.
Available Policies	List the available policies associated with the source type.
Selected Policies	List the policies selected.
Add Another Source Type	Lets you add another source type.
Save and Close	Saves the settings and closes the Create Group dialog.

Field	Description
Publish Now	Publishes the created group.

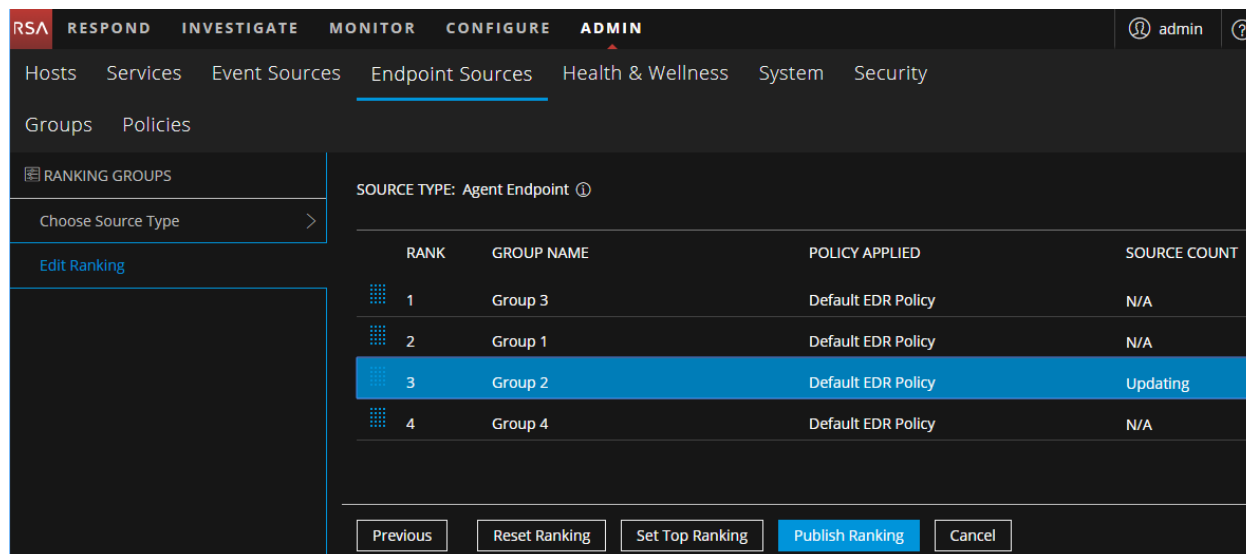
Ranking Groups

Below is an example of the Ranking Groups dialog. The table describes the information and options in the Ranking Groups dialog.



Field	Description
Source Type	Establishes ranking for the source type. Available options are Agent Endpoint and Agent Windows Logs.

Below is an example of the Edit Ranking panel.



- 1 Drag the group up or down to change the priority. Priority decreases from top to bottom.

2

Actions in the toolbar:

Previous - Navigates to the Choose Source Type panel.

Reset Ranking - Resets the ranking to the original order.

Set Top Ranking - Moves the selected group to the top.

Publish Ranking - Lets you edit the details of an existing group. For more information, see [Edit a Group](#).

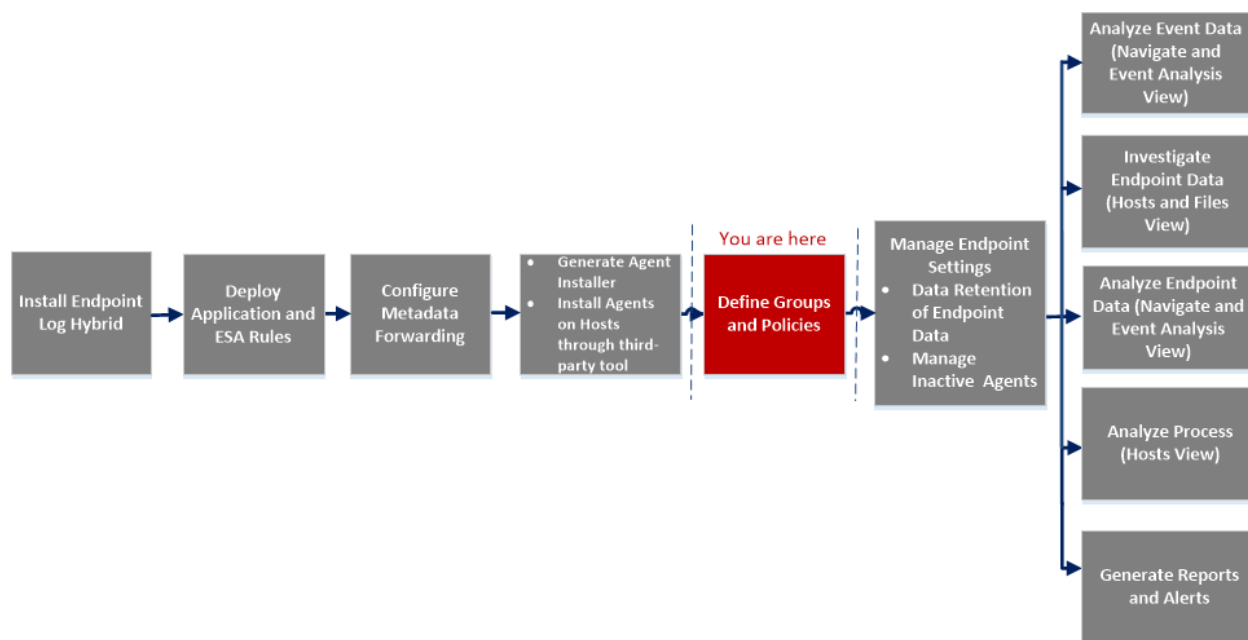
Cancel - Discards the changes and returns to the Groups tab.

Endpoint Sources - Policies

Note: The information in this topic applies to RSA NetWitness® Platform Version 11.3 and later.

The **ADMIN > Endpoint Sources** view contains two tabs: **Groups** and **Policies**.

Workflow



What do you want to do?

User Role	I want to ...	Show me how
Administrator	create new groups	Create a Group
Administrator	edit groups	Edit a Group
Administrator	edit ranking	Change Policy Ordering for Groups
Administrator	delete groups	Delete a Group
Administrator	view default policies*	Default Agent Endpoint (EDR) Policy
Administrator	create an EDR policy*	Create an EDR Policy
Administrator	create a Windows Log policy*	Create a Windows Log Policy
Administrator	edit policies*	Edit a Policy
Administrator	delete policies*	Delete a Policy

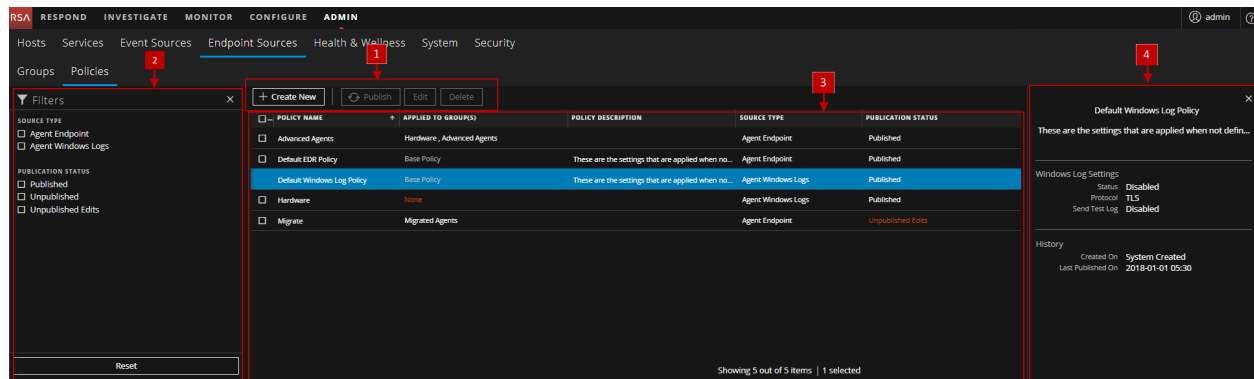
*You can perform this task in the current view.



Related Topics


- [Endpoint Sources](#)
- [Managing Groups](#)

Quick Look

Below is an example of the Policies tab:



- Actions in the toolbar:**
 - **Create New:** Lets you create a new policy. For more information, see [Managing Policies](#).
 - **Publish:** Publishes the selected policy.
 - **Edit:** Lets you edit the details of an existing policy. For more information, see [Edit a Policy](#).
 - **Delete:** Deletes the selected policies permanently. For more information, see [Delete a Policy](#).
- Filters:** You can filter groups based on Source Type and Publication Status. To hide, click the  icon at the top-right of the panel. To display if hidden, click the  icon in the toolbar.
Reset: Removes the currently applied filter criteria.
 For more information, see [Filter Policies](#).
- Policy View.** Displays the policy details:
 - Policy name: Name of the policy.
 - Applied to groups: Lists the group to which this policy is applied.
 - Policy description: Description of the policy.
 - Source type: Defines the source type: Agent Endpoint or Agent Windows Logs.
 - Publication Status: Status of the policy: Published or Unpublished.

Sort Columns. If you mouse over a column header, a sort icon is displayed: . Click the icon to sort by the selected column.

4 **Properties Panel.** Displays the properties of the selected policy.

Note: To view the Properties panel for a policy, click the Policy Name.

Create Policy

Below is an example of the Create Policy dialog. The table describes the information and options in the Create Policy dialog.

Field	Description
Source Type	Displays the source type for the policy. Available options are Agent Endpoint and Agent Windows Logs.
Policy Name	Name of the policy. The name should be unique.
Policy Description	Description of the policy. Description should not exceed 8000 characters.

Define Policy Panel for Agent Endpoint Policy

Below is an example of Define policy panel. The table describes the information and options for Agent Endpoint policy:

RSA

RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN

Hosts Services Event Sources Endpoint Sources Health & Wellness System Security

Groups Policies

TEST

Identify Policy

Define Policy

Available Settings ⓘ

Scan Schedule

Scan Frequency

Start Time

CPU Maximum

Virtual Machine Maximum

Agent Mode

Monitoring Mode

Scan Settings

Scan Master Boot Record

Auto Scan New Systems When Added

Response Action Settings

Blocking

Endpoint Server Settings

Endpoint Server

HTTPS Port

HTTPS Beacon Interval

UDP Port

UDP Beacon Interval

Advanced Configuration

Advanced Setting

Selected Settings ⓘ

Scan Schedule

RUN SCHEDULED SCAN

Disabled

Enabled

EFFECTIVE DATE

02/19/2019

Previous

Next

Save and Close

Publish Policy

Cancel

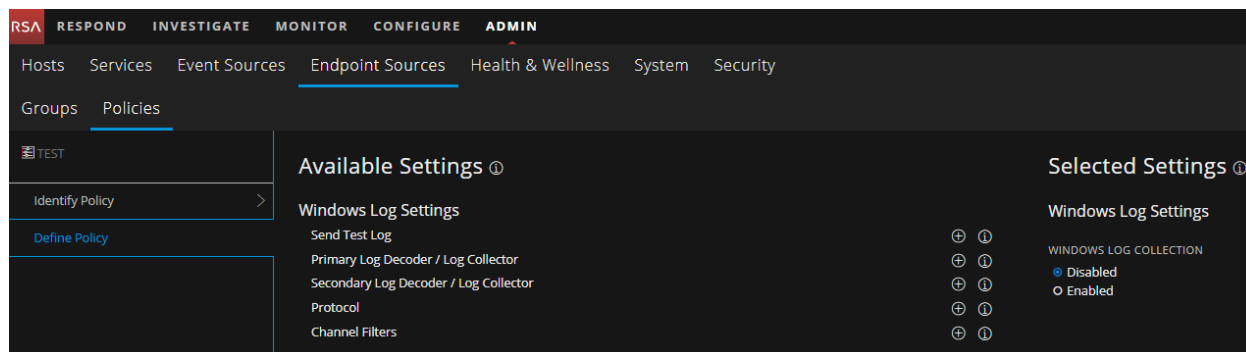
Settings	Description
Scan Schedule	
Run Scheduled Scan	<p>Run a scheduled scan if you want to receive regular snapshots from a host. Scan snapshots provide detailed information about processes and files loaded on the memory. By default, this option is disabled. You can also run a manual scan from the INVESTIGATE > Hosts view.</p> <p>Note: The following scan schedule options are available only when the scan schedule is enabled. The values entered are specific to the agent time zone.</p>
Effective Date	Date when the policy takes effect. If you do not want this policy to take effect as soon as it is applied to a group and published, set an effective date that is in the future. By default, this is set to the current date.

Settings	Description
Scan Frequency	<p>Determines how often the scheduled scan runs on a host. By default, this is set to every 1 week. Every network is different and the frequency should balance the needs of the analysts for current data, availability to review the data, and how systems deal with the load of the generated data.</p> <p>Select Days or Weeks:</p> <ul style="list-style-type: none"> Days: Select the number of days of the scan frequency. You can set a schedule to scan every n days, where n is 1, 2, 3, 4, 5, 6, 10, 15, or 20. For example, to scan every third day, select 3. Weeks: Select after how many weeks the policy scan should be initiated and on which day of the week the policy scan should initiate. For example, to scan every other Wednesday, choose 2 and W.
Start Time	<p>Time when the scheduled scan starts to run on a host. By default, this is set to 9:00. This is the local host time, meaning that scans across a global network will not run all at once. Note that the time is in 24 hour format. To set a time of 7:30 PM, select 19:30.</p>
CPU Maximum	<p>Amount of CPU the agent can use to run scheduled scans on physical hosts. By default, the value is set at 25%. Increasing the CPU maximum increases the speed of scan snapshot retrieval.</p> <p>Drag the slider to specify the maximum CPU usage by the created policy. Minimum value is 5%. Use the slider to select the maximum CPU processing power to use for the scan. Note that the higher the percentage, the less CPU is available for other tasks on the host.</p>
Virtual Machine Maximum	<p>Amount of CPU the agent can use to run scheduled scans on virtual machines. By default, the value is set at 10%. Increasing the virtual machine maximum value increases the speed of scan snapshot retrieval.</p> <p>Drag the slider to specify the maximum Virtual Machine usage by the policy. Minimum value is 5%. Use the slider to select the maximum CPU processing power to use for the scan. Keep in mind that the higher the percentage, the less CPU is available for other tasks running on the virtual machine.</p>
Agent Mode	
Monitoring mode	<p>Allows you to specify whether an agent should operate in Insights (free) or Advanced mode (license). By default, it is set to Advanced.</p>
Scan Settings	
Scan Master Boot Record	<p>Includes Master Boot Record (MBR) details in scheduled scans. By default, this option is disabled. This can help to identify when an operating system boot sequence is compromised. However, not all modifications to the MBR are malicious, as they could be made to provide encryption or enforce licensing of certain legitimate software.</p>

Settings	Description
Auto Scan New Systems When Added	<p>Automatically scans when a new host is added. By default, this option is disabled. If this option is disabled, no snapshot data is displayed in the INVESTIGATE > Hosts view until a manual or scheduled scan is run on these hosts. Existing hosts will not be affected.</p> <p>Note: Enabling this option on a new deployment when this policy is applied to a large number of hosts may result in a large number of simultaneous scans that cause performance degradation.</p>
Response Action Settings	
Blocking	<p>Allows an analyst to prevent the execution of a malicious file on any host running an Advanced mode agent. By default, this option is disabled. File blocking will not be enforced if it is disabled by policy, which might be desirable to ensure that there are no performance side effects on systems where CPU or IO performance is critical.</p> <p>Note: Blocking is not supported for an Insights agent.</p>
Endpoint Server Setting	
Endpoint Server	<p>Displays all available Endpoint servers in the deployed.</p> <p>Note: If you do not select an Endpoint Server, the agent uses the default Endpoint Server that is configured during packager generation.</p>
Endpoint Server Forwarder (Optional)	The optional server alias allows you to enter an alternative hostname or IP address on which the server can be reached in the case that agents need to go through a NAT or similar in order to reach the Endpoint Server.
HTTPS Port	<p>Port number used for HTTPS communication. By default, the port is set to 443.</p> <p>If you want to change this port, make sure that it matches the server configuration. If you enter the wrong port, the agents can no longer communicate with the Endpoint server and the system will be non-functional.</p>
HTTPS Beacon Interval	<p>Determines how often an agent can communicate with the Endpoint server over HTTPS. By default, the value is set to 15 minutes. The default method of beaconing is UDP. Beaconing is used as a method of keep-alive to know if a host is online and to allow hosts to respond faster than the fallback HTTPS beacon time.</p>
UDP Port	<p>Port number used for UDP communication. By default, the port is set to 444.</p> <p>If you want to change this port, make sure that it matches the server configuration. Entering the wrong port results in loss of functionality and effects performance.</p>
UDP Beacon Interval	Determines how often an agent can communicate with the Endpoint server over UDP. By default, the value is set to 30 seconds.

Define Policy Panel for Windows Logs Policy

The table describes the information and options for Agent Windows Logs policy:



Settings	Description
Windows Log Collection	If enabled, logs from the Windows hosts are collected and forwarded to the NetWitness Platform. By default, this option is disabled.
Send Test Log	If enabled, a sample log is sent to the configured server when the policy is loaded to test connectivity. This allows to test the configuration before standard logs are available. By default, this option is disabled.
Primary Log Decoder / Log collector	Primary NetWitness Platform Log Decoder or Log Collector to which the collected Windows logs are forwarded.
(Optional) Secondary Log Decoder / Log collector	If the primary Log Decoder or Log Collector is not reachable, the collected Windows logs are forwarded to the secondary Log Decoder or Log Collector. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> Note: NetWitness Platform cannot detect failures when UDP protocol is used. </div>
Protocol	Select whether TLS, TCP, or UDP transport protocol is used to forward the collected Windows logs to the NetWitness Platform servers. By default, the protocol is TCP.
Channel Filters	<p>Configure which Windows Log events to collect by selecting a channel, filter condition, and the relevant event IDs. You can either select common channels, such as Security or System from the drop-down list, or create custom channels by entering the channel name. By default, all events are collected from a selected channel.</p> <p>To collect a subset of events from that channel replace 'ALL' with the relevant Event IDs. Select INCLUDE if only events with the listed Event IDs should be collected or select EXCLUDE to collect all events except for these events.</p>

Troubleshooting

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

Agent Communication Issues

Issue	Agent is unable to communicate with the Endpoint server.
Explanation	<p>This could be due to one of the following reasons:</p> <ul style="list-style-type: none">• In the agent packager:<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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 <code>NWEAgent.exe</code> file in the antivirus Windows Suite.

Issue	You want to change the responsiveness of the Agent.
Explanation	Depending on your installation, you can adjust Beaconsing intervals to change how responsive your agents are.
Resolution	If resources are not a concern, you can lower the HTTPS Beacon Interval and UDP Beacon Intervals. If resources are a concern and responsiveness of the agent is not, you can increase these intervals.

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: <ul style="list-style-type: none"> • 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

Explanation	<p>following exceptions:</p> <pre>dataprocessor-5] WARN MetaManagement Meta Forwarding waiting for free buffer in Log decoder</pre>
	<p>Make sure that:</p> <ul style="list-style-type: none"> • 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 <code>/var/log/netwitness/endpoint-server/endpoint-server.log</code> .
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	<p>The storage size of the Data application has exceeded the threshold (for example, 75%), and the custom policy is triggered.</p> <div style="border: 1px solid green; padding: 5px;"> <p>Note: By default, the server automatically deletes the older data when it reaches 80% of the disk space.</p> </div>

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	<p>The agent request count shows 0 for the entire day or week. This could be due to one of the following reasons:</p> <ul style="list-style-type: none"> In the agent packager: <ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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
-------	--

Explanation	long time.
	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:
	<ol style="list-style-type: none">1. Open the Endpoint Server log file from <code>/var/log/netwitness/endpoint-server/endpoint-server.log</code> 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 (<code>/var/log/nginx/access.log</code>) to retrieve the following details of an inactive agent:<ul style="list-style-type: none">• IP Address• Date and time that the agent became inactive• Location

NGINX Issue

Issue	Nginx rejects post requests exceeding request size 100 GB.
Explanation	By default, the payload size in the NGINX server is set to 100 GB. This causes any data post request exceeding 100 GB to fail.
Resolution	Add the following setting to the Nginx configuration file (<code>/etc/nginx/conf.d/nginx.conf</code>) and restart the Nginx server. <code>client_max_body_size xx</code> where, xx is the size that you want to set.