NetWitness® Platform

Version 12.4.1.0

NetWitness Endpoint Configuration Guide

NETWITNESS

Platform

Contact Information

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

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates 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 RSA.

It is advised not to deploy third-party repos or perform any change to the underlying NetWitness Operating System that is not part of the supported NetWitness version. Any such change outside of the NetWitness approved image may result in a service or functionality conflict and require a reimage of the NetWitness system to bring NetWitness back to an optimized functional state. In the event a third-party repo is deployed, or other non-supported change is made by the customer without NetWitness approval, the customer takes full responsibility for any system malfunction until the issue can be remediated through troubleshooting efforts or a reimage of the service.

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 NetWitness Community. 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

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

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

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at https://www.netwitness.com/standard-form-agreements/.

June, 2024

Contents

NetWitness Endpoint

About NetWitness Endpoint

NetWitness Platform provides an endpoint detection and response solution that continuously monitors the behavior of all endpoints in and outside 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 introduces **Endpoint Log Hybrid** that:

- Collects and manages endpoint (host) data from Windows, Mac, and Linux hosts.
- Collect log files and Windows 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.
- Download Files, Master File Table (MFT), system dump, and process dump for forensic investigation.
- Isolate host from the network to safely investigate possible threats within the host.

Endpoint Log Hybrid receives data from the Endpoint Agents. The following services run on the Endpoint Log Hybrid:

- **Endpoint Server**: Manages data received and stores it in a database. It parses the events, generates metadata, and forwards it to the Log Decoder through protobuf. You can deploy up to 6 Endpoint Log Hybrid hosts. For a consolidated view of all endpoint data from multiple Endpoint Log Hybrid hosts, install the Endpoint Broker. You can add only one broker in a NetWitness platform deployment which serves up to 6 Endpoint Log Hybrid hosts. Multiple Endpoint Log Hybrids are required to share certificates by copying them from the primary Endpoint Log Hybrid to the secondary Endpoint Log Hybrid using the `SCP` command.

  Note: You may need to install your Endpoint Server on separate hardware from your Log Decoder. If you are only using NW Platform for collecting and analysing logs, you can co-locate your Endpoint Server on the same physical hardware as your Log Decoder. For more information, see the Prepare Virtual or Cloud Storage topic in the *Storage Guide for NetWitness Platform*.

  If you exceed these guidelines, the amount of disk space usage and CPU might become so high as to create alarms for your Endpoint Server in Health and Wellness. If you notice this, and are running both log collection and EDR scans, you can use Throttling to control the amount of data coming into the Log Decoder.

  If that doesn't help, NetWitness recommends that you move your Endpoint Server onto separate hardware from that used by your Log Decoder.

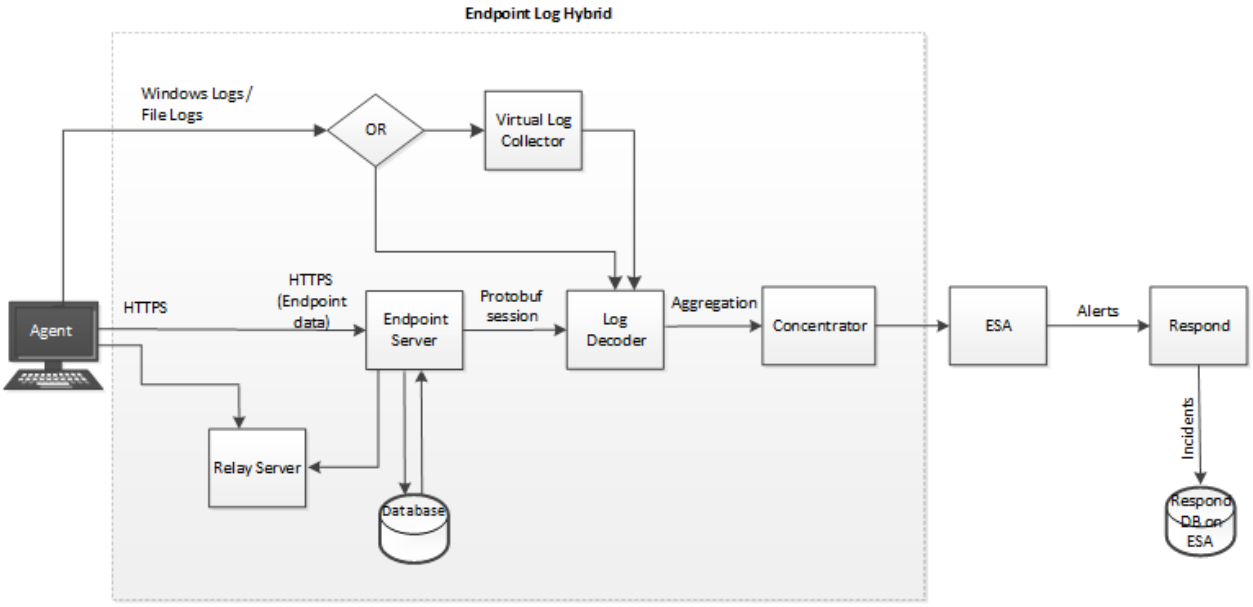
- **Log Decoder**: Captures data from the Endpoint Server and processes the metadata.
- **Concentrator**: Aggregates metadata from the Log Decoder and makes it available for all upstream components like Investigate, Reporting Engine, Respond, and Event Stream Analysis similar to NetWitness Decoder and 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:

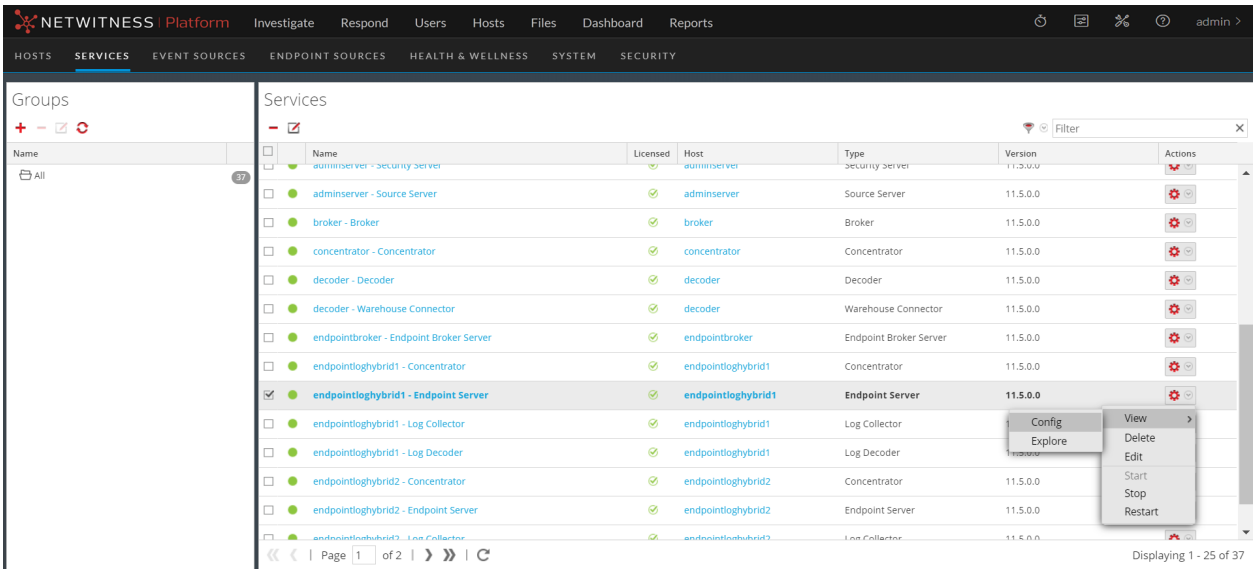


The *Hosts and Services Getting Started Guide* provides the information you need to understand and install all the NetWitness services.

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
- Installing and configuring Relay Server

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


NETWITNESS | Platform
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
HOSTS
SERVICES
EVENT SOURCES
ENDPOINT SOURCES
HEALTH & WELLNESS
SYSTEM
SECURITY
Groups
Name
All
37
Services
Filter
Name
Licensed
Host
Type
Version
Actions
adminserver - Source Server
adminserver
Source Server
11.5.0.0
broker - Broker
broker
Broker
11.5.0.0
concentrator - Concentrator
concentrator
Concentrator
11.5.0.0
decoder - Decoder
decoder
Decoder
11.5.0.0
decoder - Warehouse Connector
decoder
Warehouse Connector
11.5.0.0
endpointbroker - Endpoint Broker Server
endpointbroker
Endpoint Broker Server
11.5.0.0
endpointloghybrid1 - Concentrator
endpointloghybrid1
Concentrator
11.5.0.0
endpointloghybrid1 - Endpoint Server
endpointloghybrid1
Endpoint Server
11.5.0.0
endpointloghybrid1 - Log Collector
endpointloghybrid1
Log Collector
endpointloghybrid1 - Log Decoder
endpointloghybrid1
Log Decoder
endpointloghybrid2 - Concentrator
endpointloghybrid2
Concentrator
11.5.0.0
endpointloghybrid2 - Endpoint Server
endpointloghybrid2
Endpoint Server
11.5.0.0
Config
Explore
View
Delete
Edit
Start
Stop
Restart
Page 1 of 2
Displaying 1 - 25 of 37

Agent Modes

In NetWitness latest versions, 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 license for an Advanced agent. For more information on licensing, see the *Licensing Management Guide*.

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

Feature	Insights Agent	Advanced Agent
Full System Scan	No	Yes
Scan data - Processes, Autoruns, 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.
Expanded network visibility	Yes - Windows	Yes - Windows
Anomaly detection - Image Hooks, Kernel Hooks, Registry Discrepancies, and Suspicious Threads	No	Yes - Windows
Windows log collection	Yes	Yes
File log collection	Yes - Windows	Yes - Windows
Threat detection content - ESA, Application Rules	Yes	Yes
Analysis of downloaded file	Yes	Yes
File status - Whitelist, Blacklist, Graylist, and Neutral	Yes	Yes
File remediate (Block)	No	Yes - Windows
Process visualization	No	Yes
Live connect	Yes	Yes
File reputation service (Third-party lookup)	Yes	Yes
Risk score for hosts	No	Yes

Feature	Insights Agent	Advanced Agent
MFT, process dump, and system dump download	No	Yes - Windows
Automatic file download	Yes	Yes
Automatic Memory DLL Download	No	Yes
Manual file download	No	Yes
Network isolation	No	Yes - Windows
Relay server	Yes	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	For a physical host: See *Install Endpoint Log Hybrid* topic under Post Installation Tasks on *Physical Host Installation Guide* For a virtual host: See *Install Endpoint Log Hybrid* topic under Step 5. Post Installation Tasks on *Virtual Host Setup Guide*.
Configure one or more Endpoint Log Hybrids	For a physical host: See *Configuring Multiple Endpoint Log Hybrids* topic under Post Installation Tasks on *Physical Host Installation Guide* For a virtual host: See *Configuring Multiple Endpoint Log Hybrids* topic under Step 5. Post Installation Tasks on *Virtual Host Setup Guide*.
Add hosts to the Endpoint Log Hybrid	For a physical host: See *Add Hosts to the Endpoint Log Hybrid* topic under Post Installation Tasks on *Physical Host Installation Guide* For a virtual host: See *Add Hosts to the Endpoint Log Hybrid* topic under Step 5. Post Installation Tasks on *Virtual Host Setup Guide*.
Deploy Application and ESA Rules	See Deploying Endpoint Application Rules and ESA Correlation Rules.

Tasks	Description
Configuring Metadata Forwarding	Similar to logs and packets, you can view Endpoint metadata in the Navigate and Events 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.
Install Agents on Hosts	The Endpoint agent installer is generated using the Packager tab under **(Admin) > Services > Config > Endpoint Server** from the NetWitness 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. After the agent is installed, it appears on the **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. **Note:** If a Windows host has proxy setup enabled and configured, the Endpoint agent communicates to the Endpoint server through proxy. If a host has both Automatic (Auto detect and Setup Script) and Manual proxy settings enabled and configured, the order of precedence is as follows: 1. Manual proxy setup 2. Automatic proxy setup - Use setup script 3. Automatic proxy setup - Automatically detect settings
Install and Configure the Relay Server	See (Optional) Installing and Configuring Relay Server.

Tasks	Description
3rd Party Scan	Configure 3rd party scans like YARA and OPSWAT. See Configure YARA and Configure OPSWAT
Permissions	Grant or Revoke role permissions for the selected Endpoint Server. See Manage Role Permissions at Endpoint Server Level
Manage Groups and Policies	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 deployment and displays information about the file. For troubleshooting, see the *Live Services Guide*.
Risk Score	Risk Score is calculated and obtained from NetWitness Respond for hosts and files. For more information, see the *NetWitness Respond Configuration Guide*.
Configuring Data Retention Policy	Define data retention policies to optimally store and manage the Endpoint data based on the age of the Endpoint data or the storage size. By default, 30 days of agent data is retained.
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.
Configure Retention Policy for Downloaded Files	Define retention policy to optimally store and manage the downloaded data such as system dump, process dump, files, and MFT. By default, 90 days of data is retained.
Investigate Endpoint data	You can investigate the Endpoint data in the **Hosts** and **Files** views. For more information, see the *NetWitness Endpoint User Guide*.

Deploying Endpoint Application Rules and ESA Correlation Rules

The existing IIOCs from NetWitness Endpoint 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 .

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, 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) >Services > 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 **Hosts** > **Risk Details** or **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, 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 tasks:

1. Add a custom Application Rule: For more information on creating a custom Application Rule, see *Create an Application Rule* topic in the **Live Services Management Guide**.
2. Add a custom ESA Rule: For more information on creating a custom ESA Rule, see *Create an ESA Rule* topic in the **Live Services Management Guide**.
3. Add the rule to RiskConfig

ESA Rule Parameters

The following table describes the fields that define an ESA 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.

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.
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
```

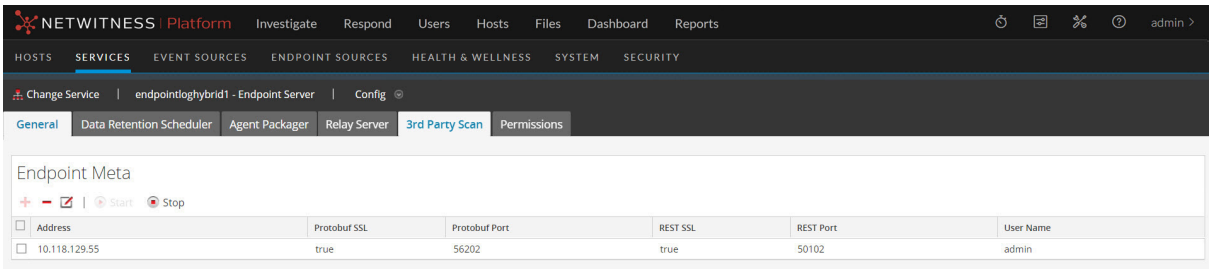
After you create a custom Endpoint rule and update the risk configuration file, whenever an event is generated for the new rule (For example, In Encrypted Directory) an alert will be generated and the risk score is calculated for the host and file.

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 Investigate (**Navigate** and **Events** views) similar to Logs and Packets. For information on metadata mappings, see Endpoint Metadata Mappings.

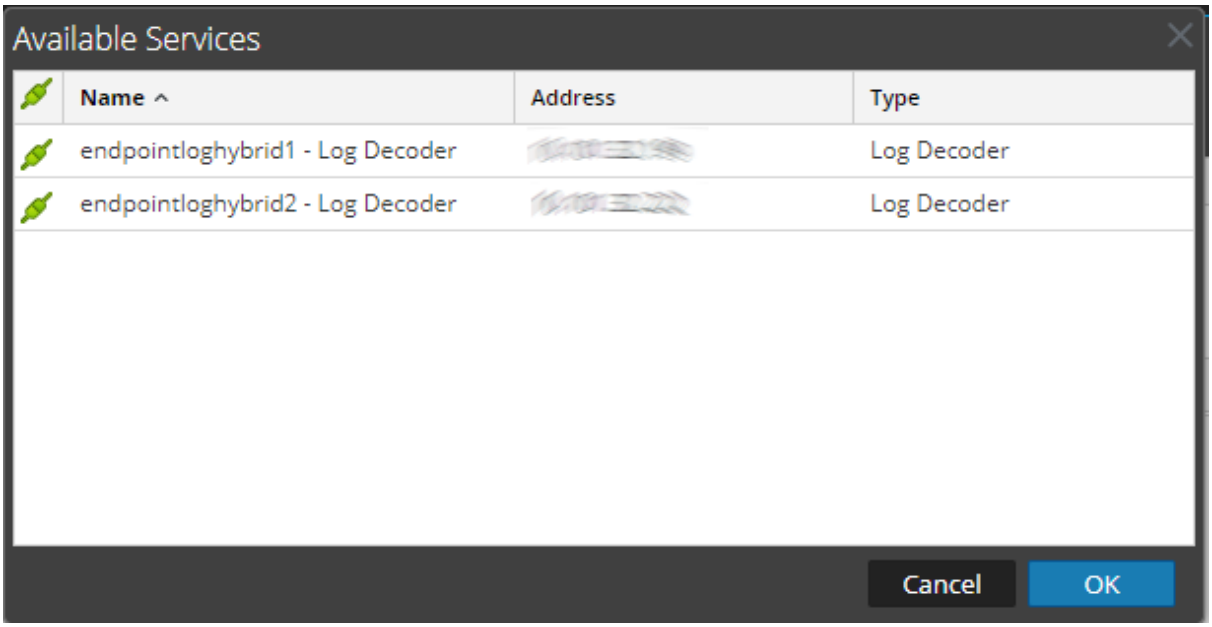
To configure metadata forwarding:

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.



5. Click in the toolbar.

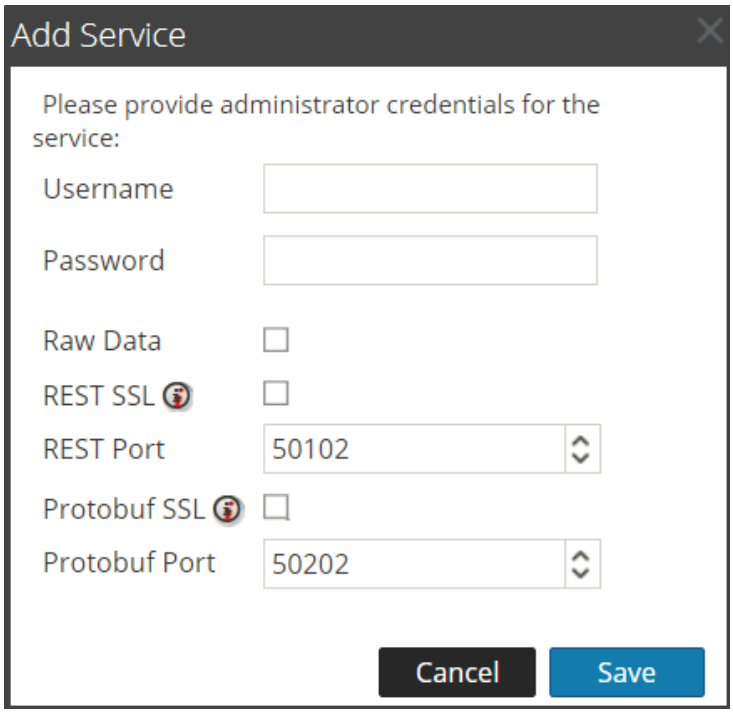
   The Available Services dialog is displayed.



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

   The Add Service dialog is displayed.

Note: You can add only one Log Decoder service.



7. Enter the administrator credentials for authentication.
8. (Optional) If you enable Raw Data, a brief summary of the session 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 50102.
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:

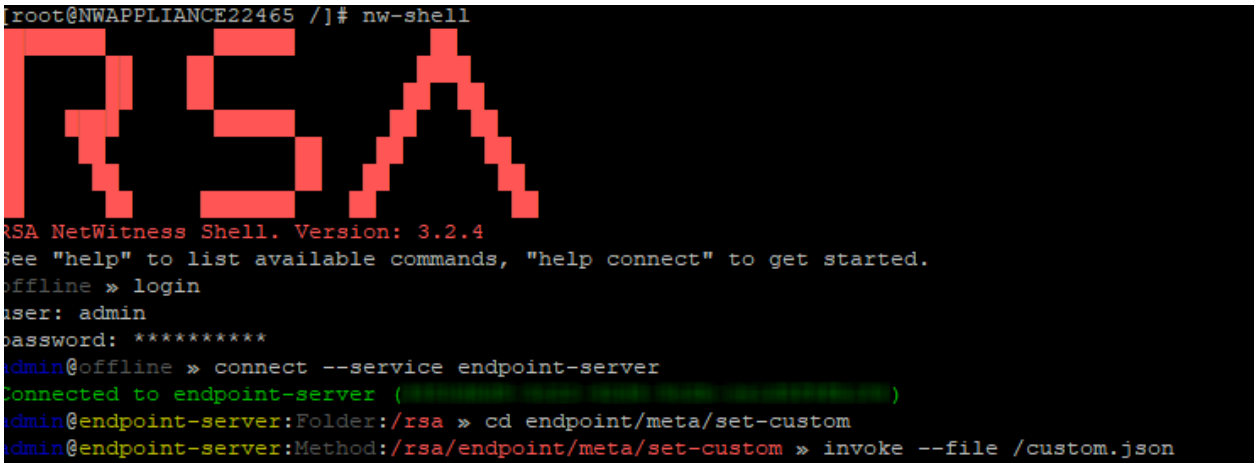
   ```
   connect --service endpoint-server
   ```

   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:



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

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 Machine OU, 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 NetWitness supports three types of policies for endpoints: **Agent Endpoint**, **Agent File Logs**, and **Agent Windows Logs** policies. The following default policies are available on installation.

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

- Default Agent Endpoint (EDR) Policy
- Default Windows Log Policy
- Default File Log Policy

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

Note: You cannot edit the default policy for Windows Logs nor for File Logs.

You can do the following through a policy:

- Define the agent mode - Insights or Advanced
- Configure scan schedule and settings
- Configure automatic file download
- 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 and File 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, Create a File Log 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.

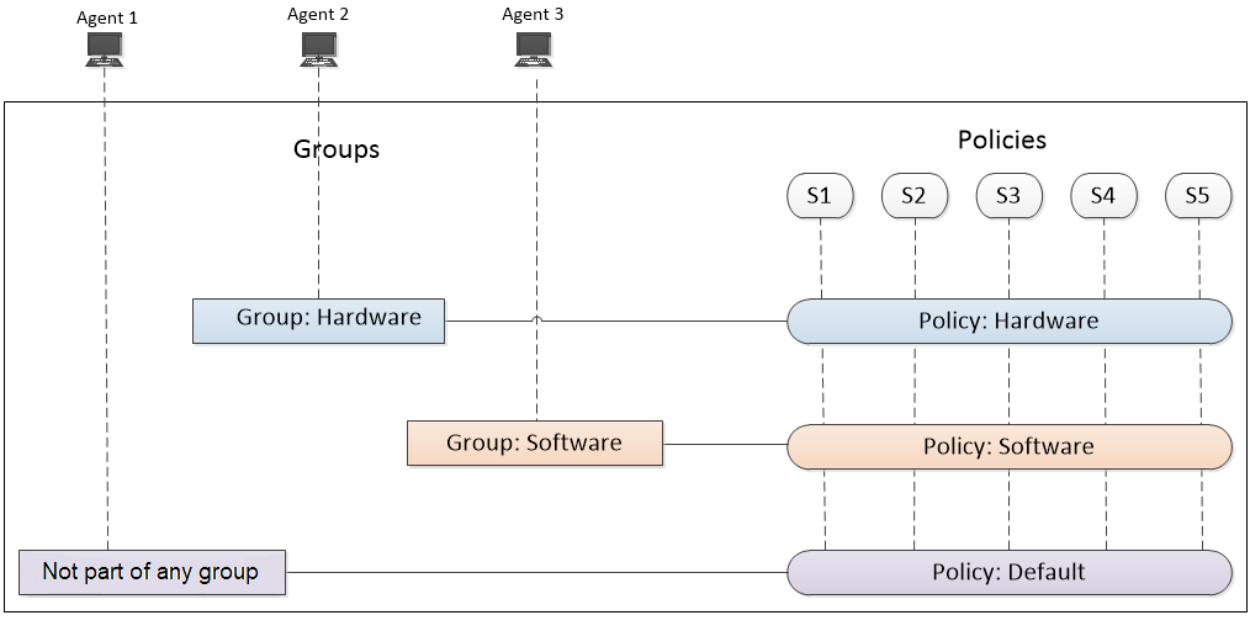
Example 1

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

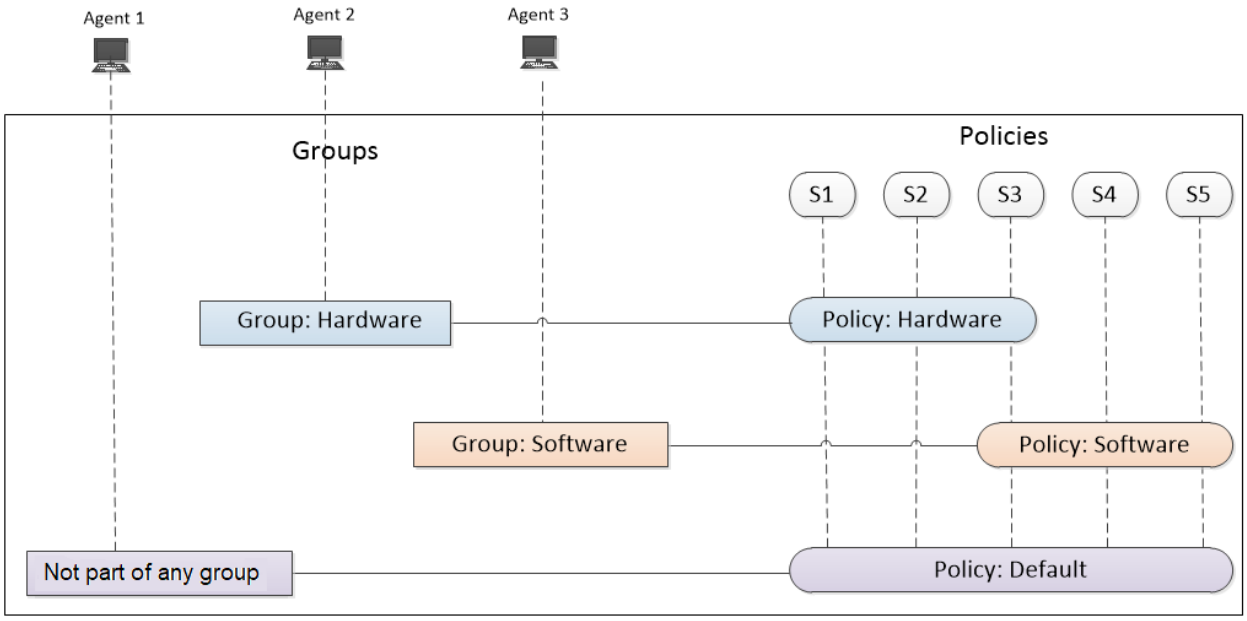
Case 1:



* 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.

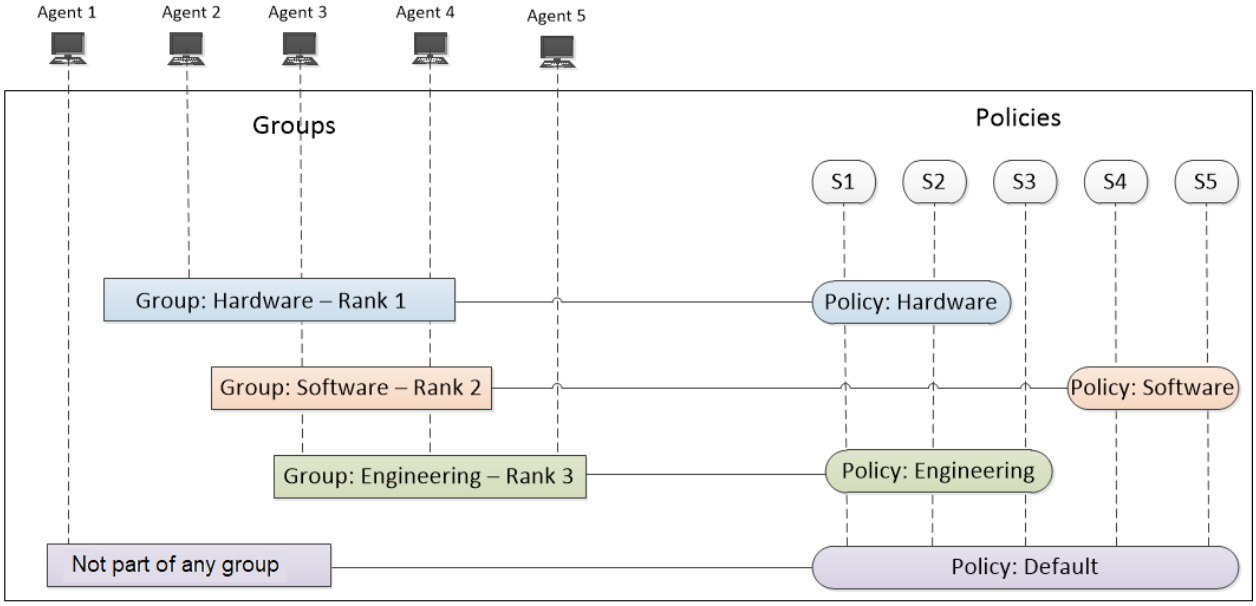
Case 2:



* 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 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
File Download Settings	Automatic File Download	Enabled
	Automatic Memory DLL Download	Enabled
	Signature	Exclude All Signed
	File Size Limit	1 MB
Response Action Settings	Blocking	Disabled
	Network Isolation	Disabled
Endpoint Server Settings	Endpoint Server	The agent considers the default Endpoint Server that is configured during packager generation.
	Server Alias (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

Default File Log Policy

The following are the default File Log policy settings:

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

Creating Groups and Policies

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

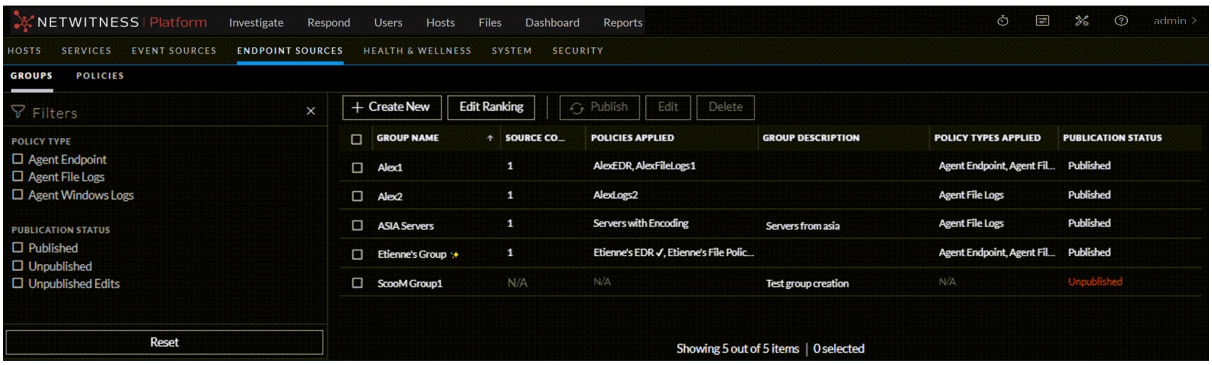
The following sections provide instructions on how to create groups and policies.

- Groups: Create a Group
- Policies:
  - Construct a Policy
  - Create an EDR Policy
  - Create a Windows Log Policy
  - Create a File Log Policy
  - Replace Windows SFTP Agents

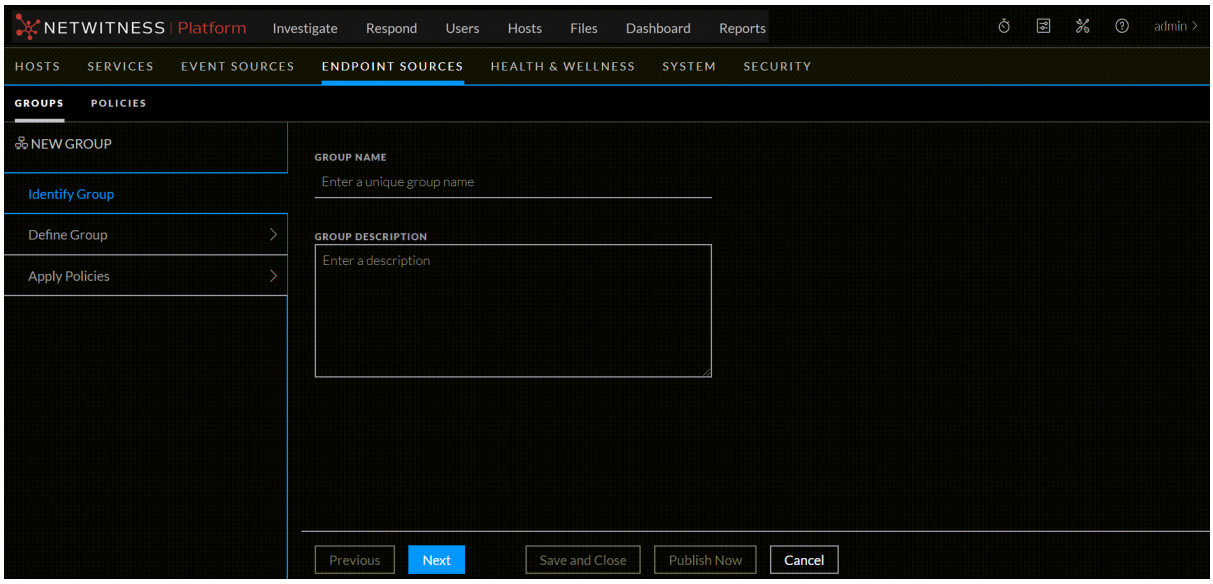
Create a Group

To create a group:

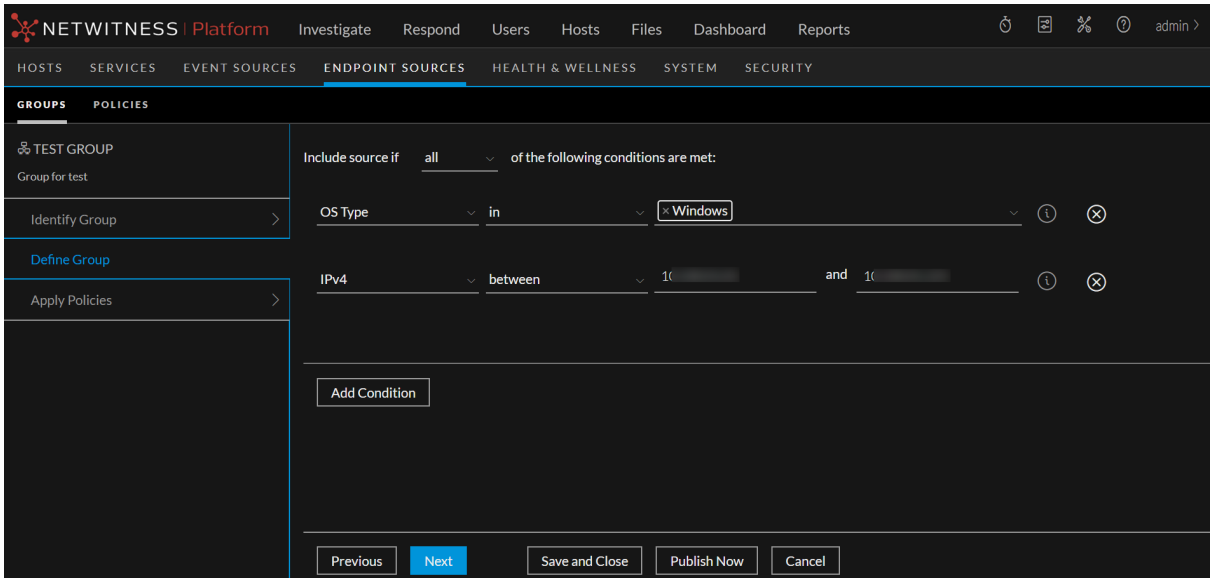
1. Go to **(Admin) > Endpoint Sources** view.
2. In the left panel, select the **Groups** tab.



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



5. 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.



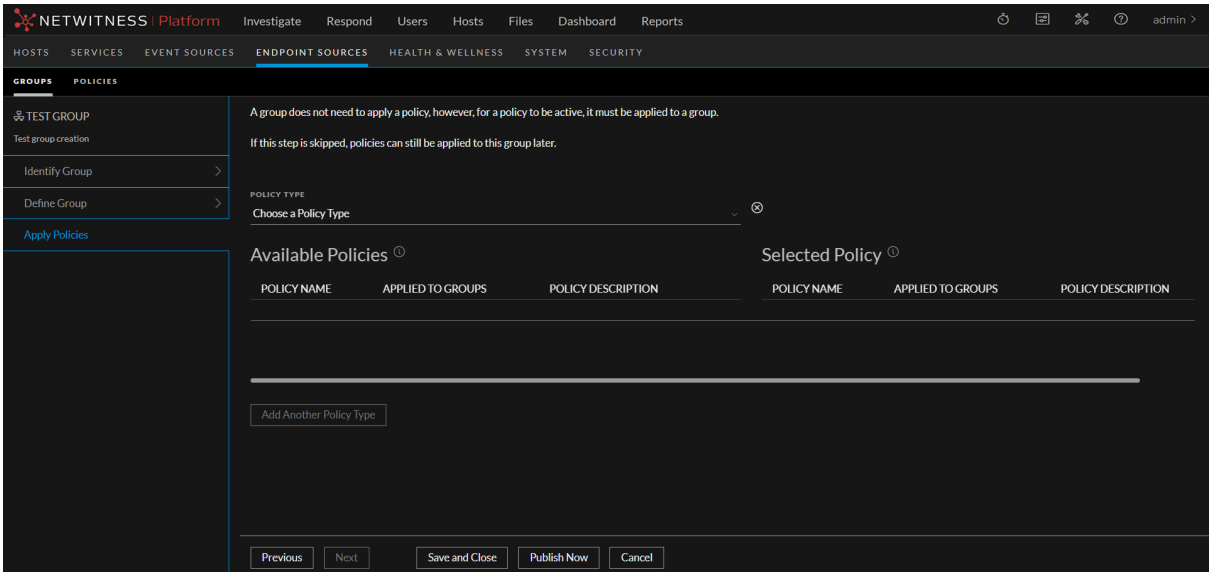
- In the **Include source if ___ of the conditions are met** field, select either **all** or **any**.
- For each logical statement, select the required options:

Item	Description
Parameter	The parameter can be OS Type, OS Description, Host Name, IPv4, IPv6, Machine OU, Tag, and Subnet. • 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. • Machine OU: Enter a valid Machine OU(Organizational Unit) name. • Tag: Enter a valid tag that already exists. • Subnet: Enter a valid Subnet mask. **Note:** If you do not want to include certain IP addresses, use the **Not in** operator, and enter the IP addresses separated by a space or a comma.
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. **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.

6. Continue adding conditions until you have completely specified the new group. After you have added all conditions, click **Next** to proceed.
7. (Optional) Click **Apply Policies** and select the source type from the drop-down list.

   Policies with the selected source type are displayed below **Available Policies**.

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



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.

For more information on creating policies, see Create an EDR Policy, Create a Windows Log Policy, or Create a File Log Policy.

8. 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.

Construct a Policy

When you create a policy, you should keep in mind the way groups and Agents can inherit values from other policies. The simplest way to construct a policy is to set values for all of the available settings for that policy type. If you do this, you can assign the policy to one or more groups, and all of the agents in those groups can receive the settings defined in the policy itself.

However, you do not need to set all possible available settings within a single policy. In the Group Ranking section, there are examples that show where values can come from, based on the ranking order.

Note: Remember that a group can have no more than one of each policy type assigned to it: it can be assigned 0 or 1 Agent Endpoint, Agent File Logs, and Agent Windows Logs policies.

If an agent is only a member of one group, that agent's settings are as follows:

- If a value is set in the policy assigned to the group, that value is used.
- If a value is not set in the policy assigned to the group, the value set in the default policy is used.

For agents that are members of multiple groups, it is a bit more complicated. For these agents, the settings are evaluated from highest priority member group (as set on the Edit Rankings page) to the lowest priority member group. If a parameter is set in a higher group, it is not overwritten, event if the same parameter is also set in a lower group. For example, assume an Agent is part of three groups:

- If a value is set in the highest ranked policy, the agent uses that value.
- If a value is not set in the highest ranked policy, but is set in the second-highest-ranked policy, the agent uses the value from the second-highest-ranked policy.
- If a value is not set in either the first- or second-highest ranked policy, but is set in the third-highest-ranked policy, the agent uses the value from the third-highest-ranked policy.
- If a value is set in the highest-ranked policy and either or both of the other policies, the value is taken from the highest-ranked policy.
- If a value is not set in any of the three policies assigned to the agent, the agent uses the value set in the default policy.

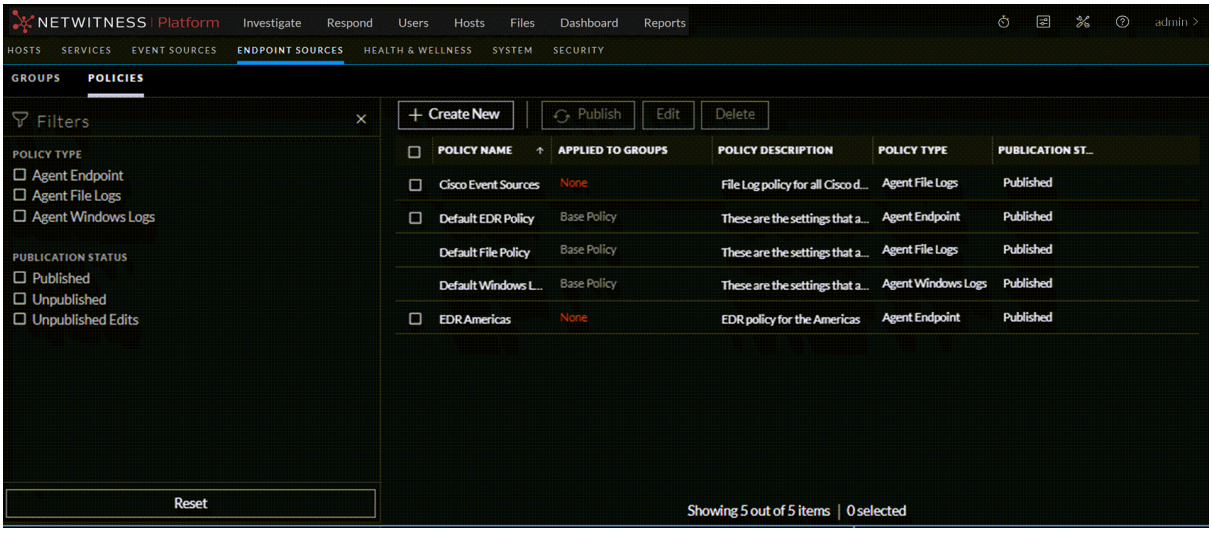
Create an EDR Policy

While creating a policy, note the following:

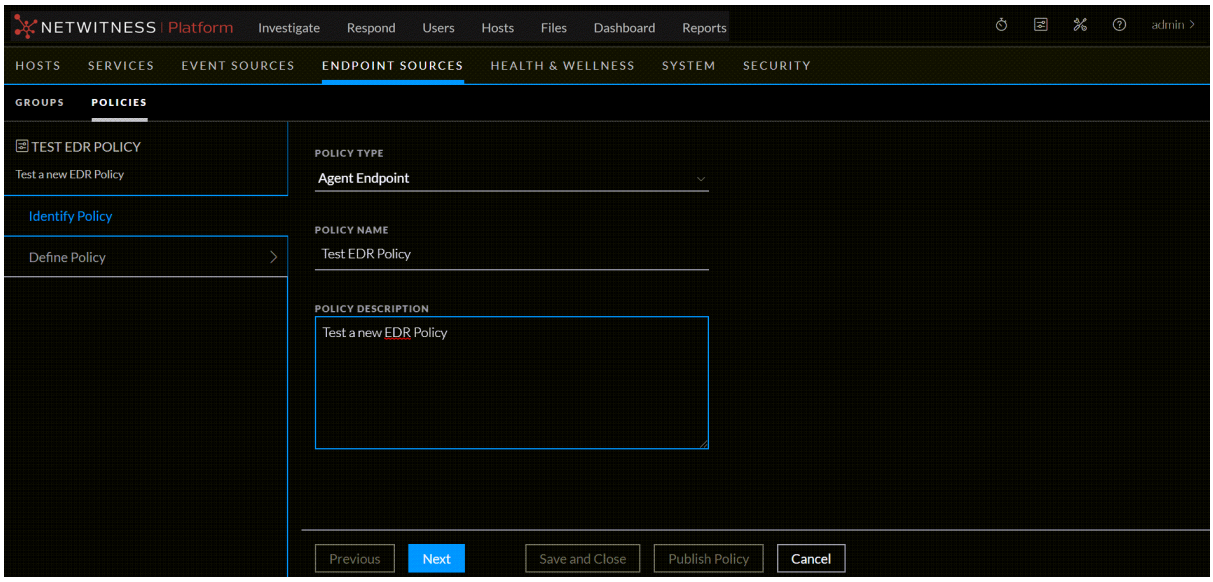
- Whenever you choose a setting, it is added to the **Selected Settings** panel.
- To clear any of your selected settings, click  to remove that setting.
- At any point in the wizard, you can choose **Save and Close**, so that you can return to complete the policy at a later time.

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, do the following:

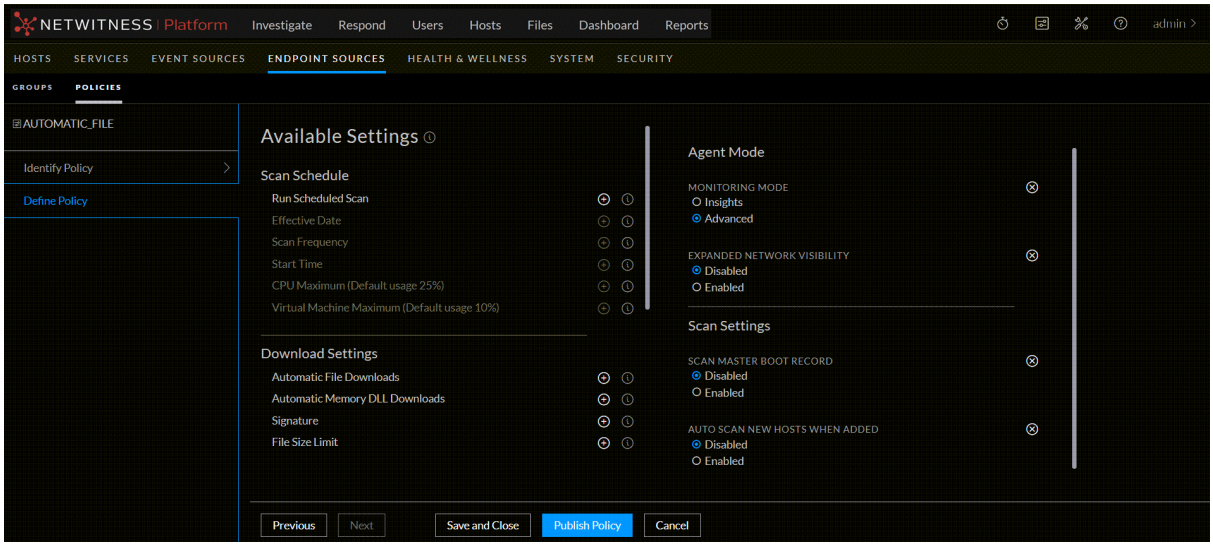


- Select **Agent Endpoint** as the source type from the drop-down list.
- Enter the policy name.
- Enter a description for the policy.

5. Click **Next**.

6. Click  to select a setting from list of **Available Settings**. After you click, 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.

Note: You do not need to set all possible available settings within a single policy. The complete list of settings for an agent is derived from one or more groups to which that agent belongs. This is described in more detail in Construct a Policy.



- In the Scan Schedule category, enable **Run Scheduled Scan** to configure the scan, and set any of the available parameters based on your needs. For more details, see Define Policy Panel for Agent Endpoint Policy.
- In the **Agent Mode** category, you can set the following:
  - Select the monitoring mode of the agent - Insights or Advanced.
  - Select **Expanded Network Visibility**:

    ### Prerequisite

    Note: For Expanded Network Visibility to work, ensure the service user account used for aggregating Endpoint Log Decoder data to Endpoint Concentrator is assigned with the `decoder.manage` permission. For more information on how to assign roles and permissions, see "Services Security View - Aggregation Role" in the *Hosts and Services Getting Started Guide for NetWitness Platform*.

    - To enable network tracking and monitoring on Windows hosts in Insights mode.

    Note: Reports UDP connections for Windows 10 version 1803 in Insights mode.

    - To optimize the frequency of agents sending network events for both Insights and Advanced modes.
    - The endpoint agents should have the **Expanded Network Visibility** option enabled for enriched network events from NetWitness Platform packet deployment with endpoint data. In the **Events** View > **Hosts** tab, the endpoint data related to the network event selected will be automatically displayed if it exists. For more information, see "Host Information" in the *Investigate User Guide*.

    Note: For network tracking in Insights mode, verify that the Windows Management Instrumentation (WMI) service is enabled.
- In the Scan Settings category, you can enable either or both of the following actions:
  - 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
- In the Download Settings category, you can set the following:
  - Enable **Automatic File Downloads** to automatically download files based on the Signature and file size. By default this option is enabled.
  - Enable **Automatic Memory DLL Downloads** to automatically download all the memory DLLs that are detected during a scan. By default this option is enabled.
  - Select the **Signature** type to limit the download of files based on the signature (not available for Linux systems).

- Specify the **File Size Limit** to limit the download of files based on the file size. The file size limit should be between 1 KB - 10 MB.

- In the Response Action Settings category you can enable or disable the following actions:
  - Enable **Blocking** to prevent the execution of a malicious file on any host.
  - Enable **Network Isolation** to provide an option to isolate a compromised host during investigation.
- In the Endpoint Server Settings, configure your server:
  - 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 Setting** - For NetWitness Support staff only.

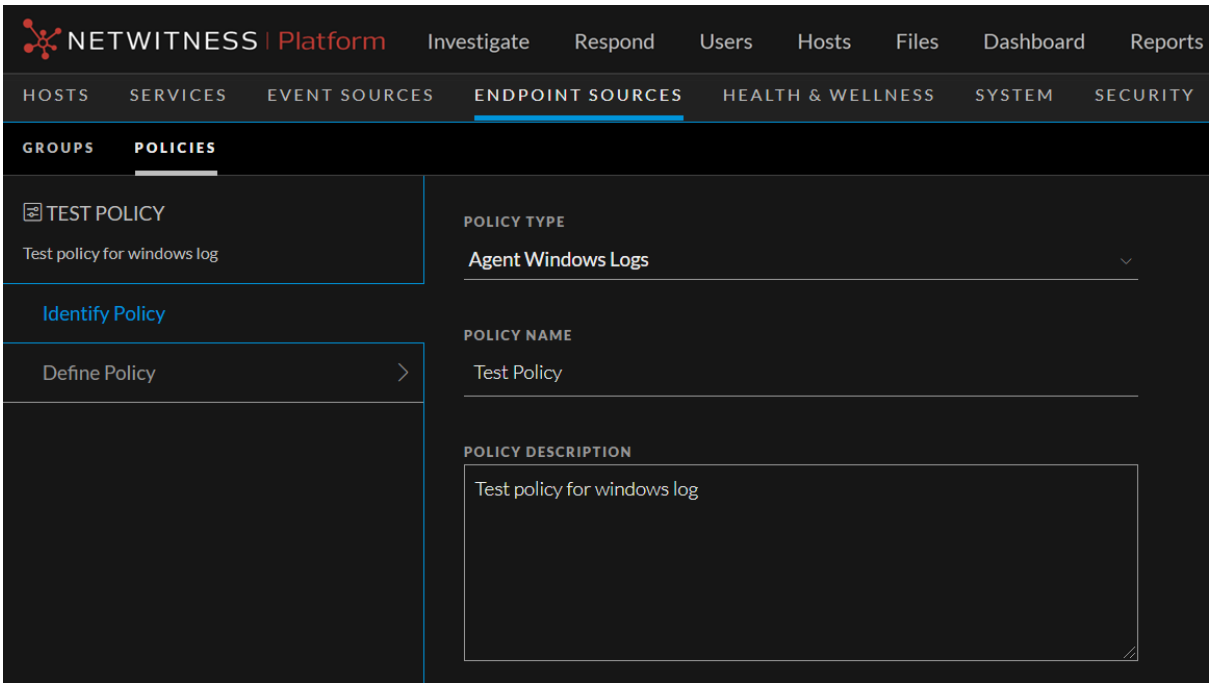
    IMPORTANT: It is strongly recommended not to use the Advanced Configuration unless advised to do so by NetWitness.

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, do the following:

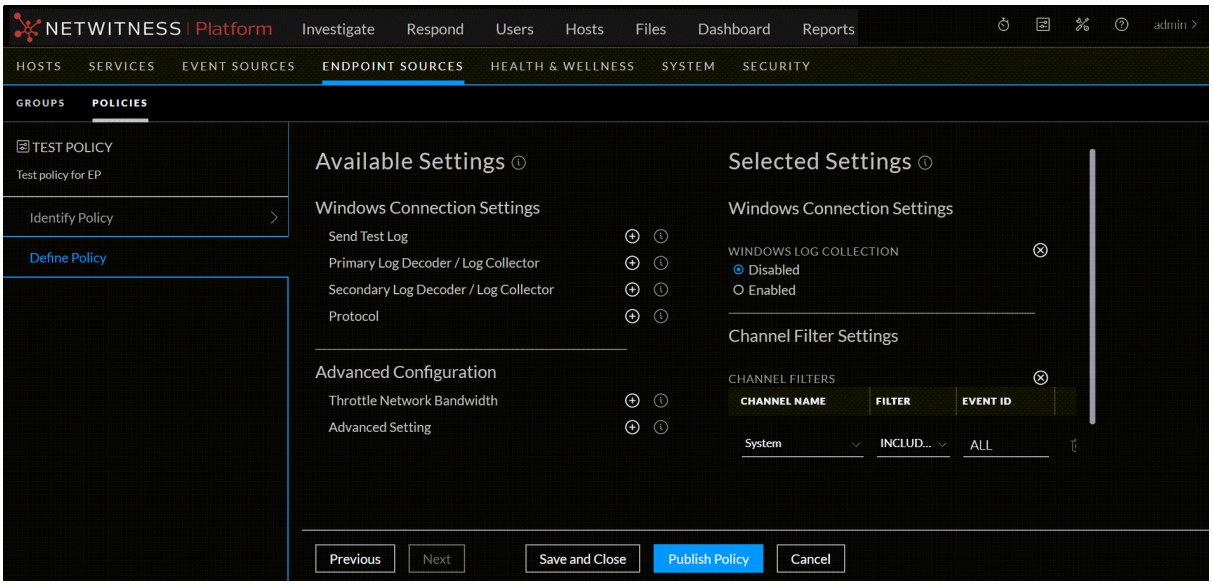


- Select **Agent Windows Logs** as the source type from the drop-down list.
- Enter the policy name.
- Enter a description for the policy.

5. Click **Next**.

6. Click  to select a setting from list of **Available Settings**. After you click a setting it is moved under the **Selected Settings** panel. You need to enter the required values for the selected settings.

Note: You do not need to set all possible available settings within a single policy. The complete list of settings for an agent is derived from one or more groups to which that agent belongs. This is described in more detail in Construct a Policy.



- 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 TLS.
- 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.

- **Advanced Configuration**
  - **Throttle Network Bandwidth:** use this setting to limit network bandwidth that the Agent uses to connect to NetWitness. This setting is disabled by default: click **Enabled** to turn it on, and then enter a value in kilobits per second.
    - If not set, Agent does not do any network throttling.
    - If set to a positive value ***x***, agent limits network bandwidth to ***x*** kbps.
  - **Advanced Setting** - For NetWitness Support staff only.

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

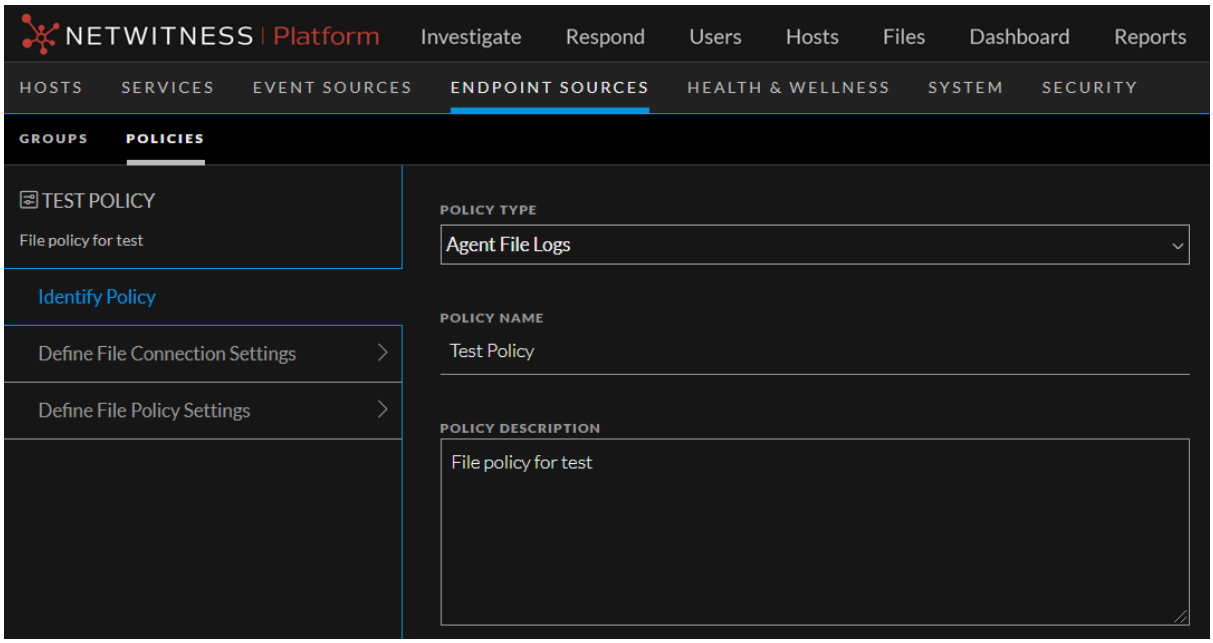
7. Do one of the following:
   - Click **Save and Close** to save the settings and return to the Policies view. The policy will be listed under the **Unpublished** category.
   - Click **Publish Policy** to publish the policy.

Create a File Log Policy

Note: You cannot create File Log policies while the system is in mixed mode. Until all Endpoint servers are updated to latest version, the Agent File Logs options on the policy create, assign policy, and edit ranking pages are disabled.

To create a File 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, do the following:

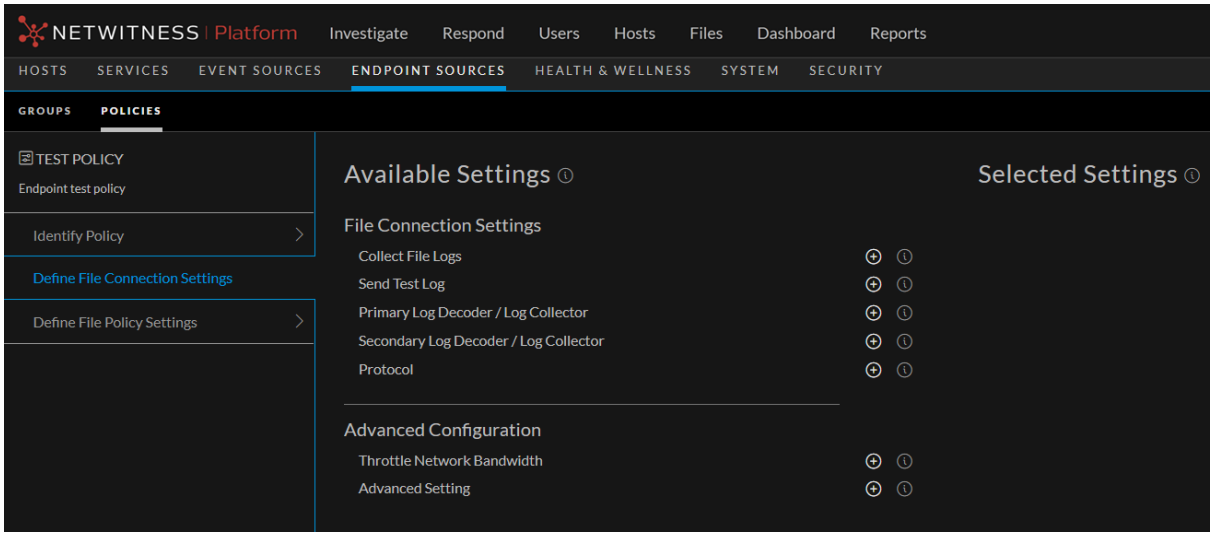


- Select **Agent File Logs** as the source type from the drop-down list.
- Enter the policy name.
- Enter a description for the policy.

5. Click **Next**.

6. Click  to select a setting from list of **Available Settings**. After you click a setting, the specific setting is moved under the **Selected Settings** panel. You need to enter the required values for the selected settings.

Note: You do not need to set all possible available settings within a single policy. The complete list of settings for an agent is derived from one or more groups to which that agent belongs. This is described in more detail in Construct a Policy.



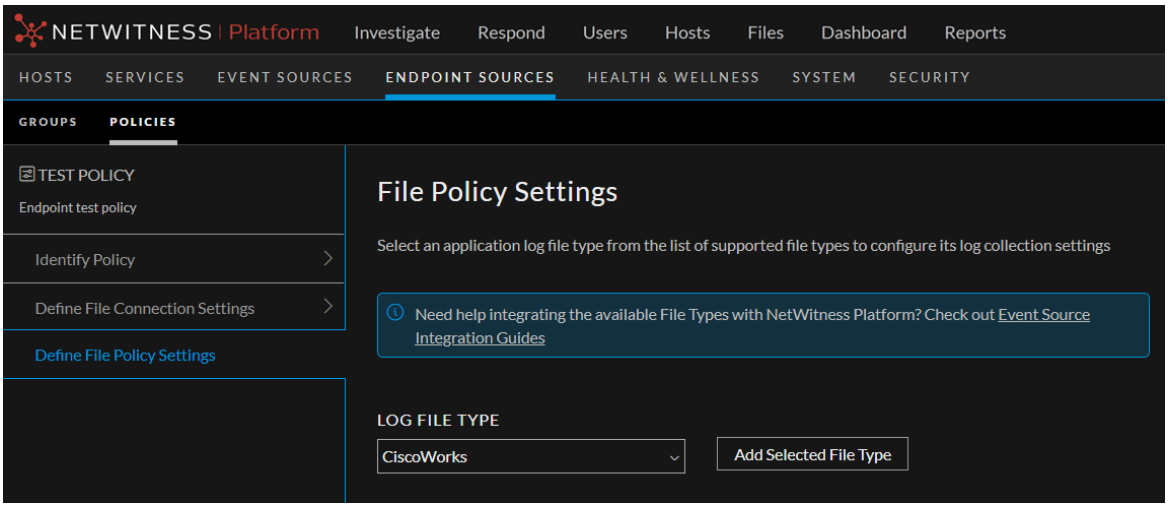
- Enable **Collect File Logs** to collect file logs on endpoints assigned to this policy. By default, this option is disabled.
- Enable **Send Test Log** to send a test log. By default, this option is disabled.
- Select **Primary Log Decoder / Log collector** to forward file logs from the drop-down list.
- (Optional) Select **Secondary Log Decoder / Log collector** to forward file 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.
- **Advanced Configuration**
  - **Throttle Network Bandwidth:** use this setting to limit network bandwidth that the Agent uses to connect to NetWitness. This setting is disabled by default: click **Enabled** to turn it on, and then enter a value in kilobits per second.
    - If not set, Agent does not do any network throttling.
    - If set to a positive value ***x***, agent limits network bandwidth to ***x*** kbps.
  - **Advanced Setting** - For NetWitness Support staff only.

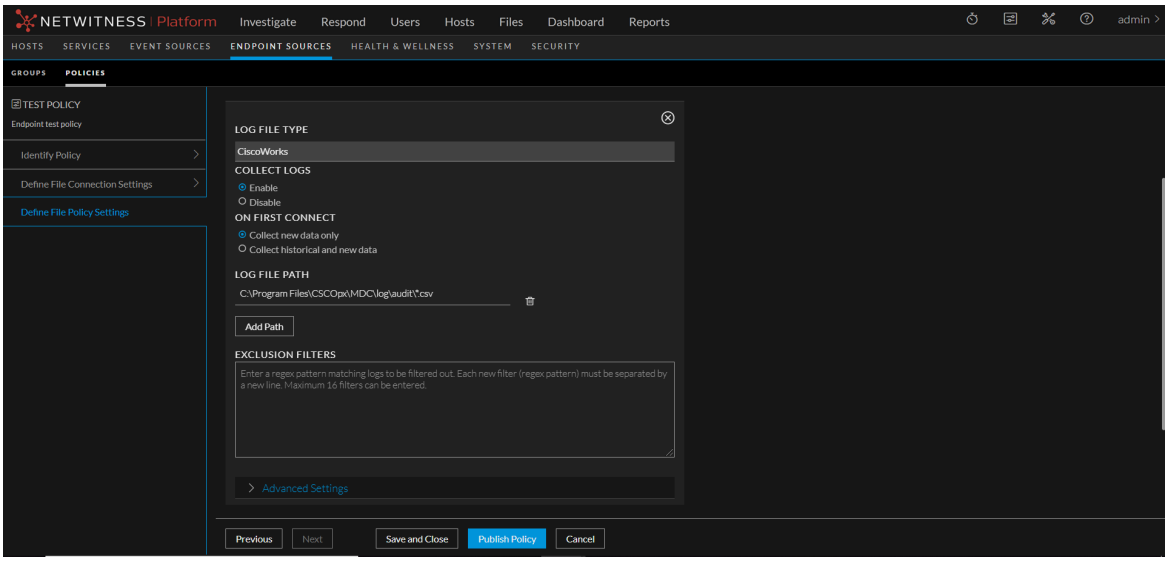
    IMPORTANT: It is strongly recommended not to use the Advanced Configuration unless advised to do so by NetWitness.

7. Click **Next**, and add the file type or types for the policy.
   a. Select a log file type from the list, then click **Add Selected File Type** to configure its log collection settings.



   For a list of currently supported event source types, see Endpoint Sources - Policies.

   b. Choose values for the available parameters.



- **Collect Logs**: Select **Enable** or **Disable**.
- **On First Connect**: Choose whether or not to collect older, historical data, or just new data. The default setting is to collect new data only.

  Note: New data is data that is collected starting from when you configure log collection for the specified event source.

- (Optional) **Log File Path**: Add a path for where the log files are stored. This is only necessary if the log files are not stored in the standard directory for the selected event source type. To add a path, click **Add Path** and enter a pathname.

  Note: This can be a Universal Naming Convention (UNC) pathname. (`\\host-name\share-name\file-path`).

  Click **Add Path** again to add another path. You can add as many paths as you like.

- **Exclusion Filters**: You can enter a newline-separated list of exclusion filters, which specify log files from which NetWitness should not be collecting data.

  Note: The filter needs to be entered as a valid regex string, or the system will not allow you to save it.

- Advanced Settings: note that most users do not need to set these parameters.
  - **Source Alias**: For most installations, this value is not needed. Use this to specify a unique event source name, in the case you have multiple event sources of the same type, for example two IBM WebSphere MQ event sources in the same NetWitness installation.
  - **File Encoding**: Select a type of file encoding. You can choose from a wide variety of encodings. The default value is **UTF-8/ASCII**.

For more details on the available parameters, see Panels for Log File Policy.

c. You can add more file types to the policy. After you have added all your file types, proceed to the next step.

8. 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.

Replace Windows SFTP Agents

Note that you might want to replace the SFTP Agent for Windows with the NetWitness Endpoint Agent for collection from file event sources. If so, perform the following procedure:

1. Using the File Collection Policy wizard (as described below), configure file collection for your event sources.
2. Verify that collection is working.
3. On each of your event sources, stop the SFTP service.

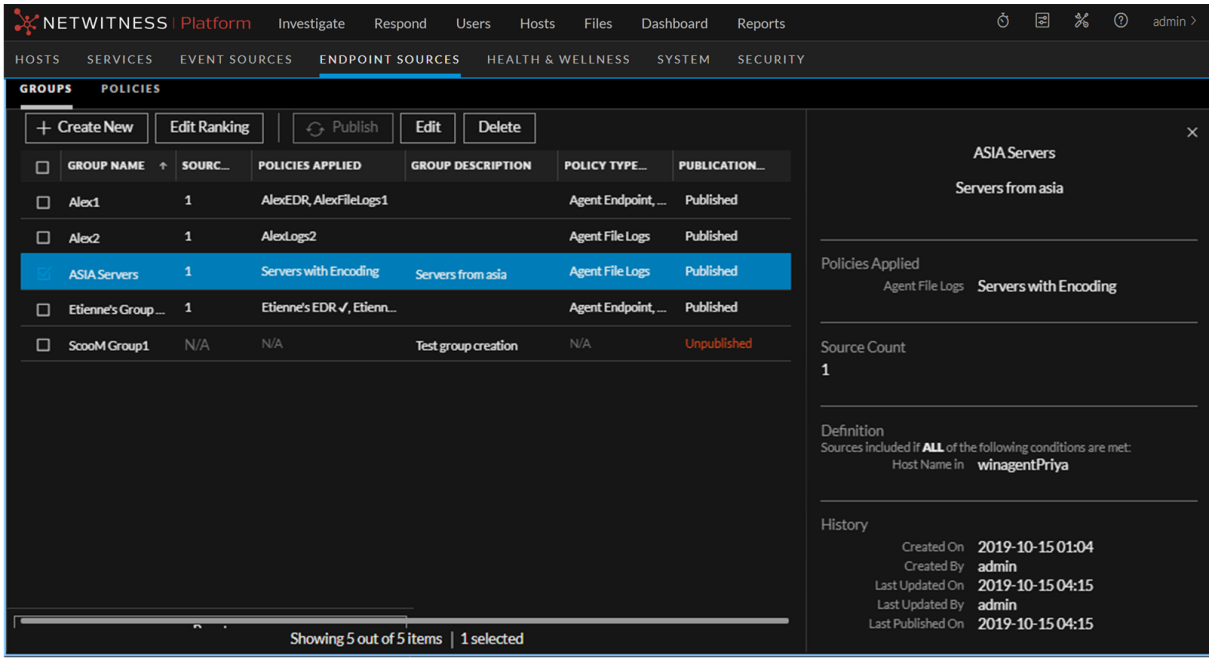
Managing Groups

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.



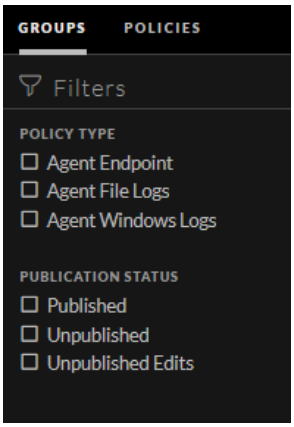
Filter Endpoint Groups

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

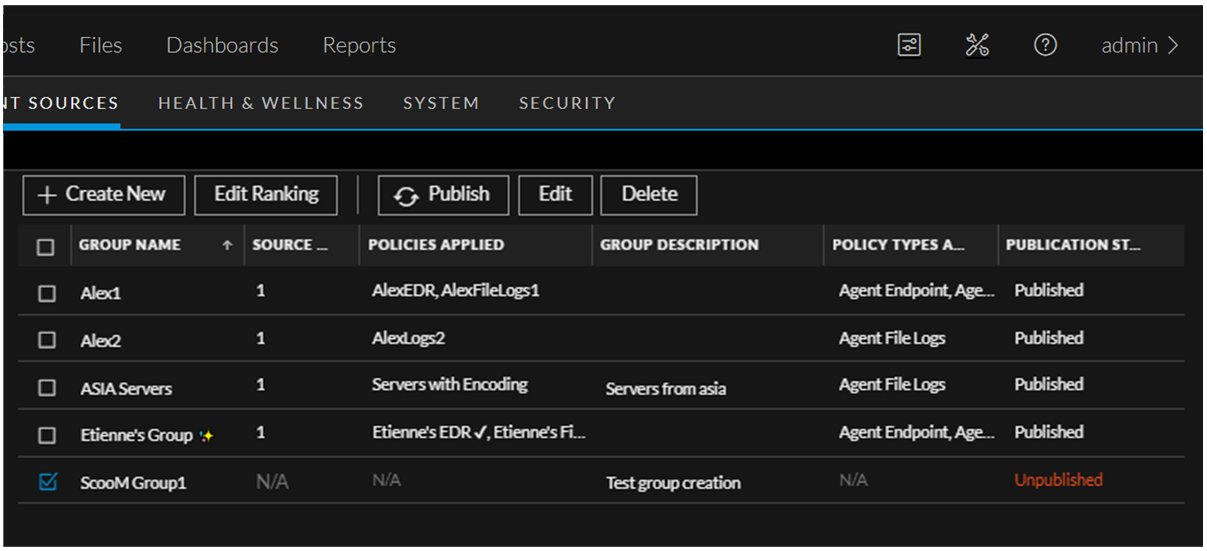
You can edit the properties of the group at any point in time. To edit properties of a group:

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.

Delete a Group

To delete a group:

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



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

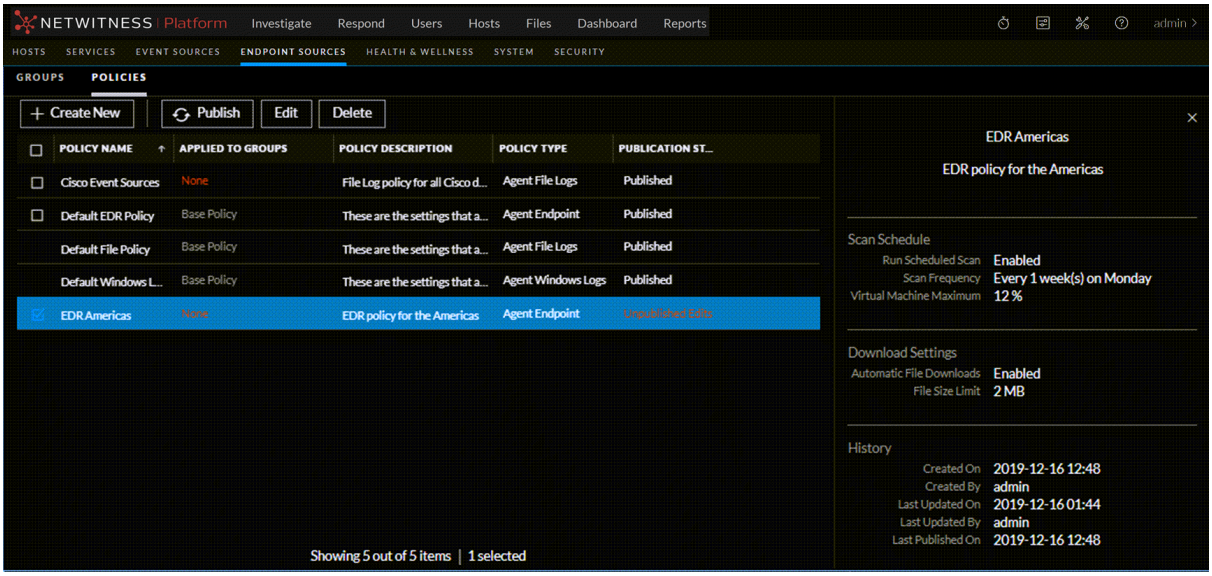
You can view, edit, filter, and delete policies, as detailed in the following sections:

- View Policy Details
- Filter Policies
- Edit a Policy
- Delete a Policy
- Conflict Resolution

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.



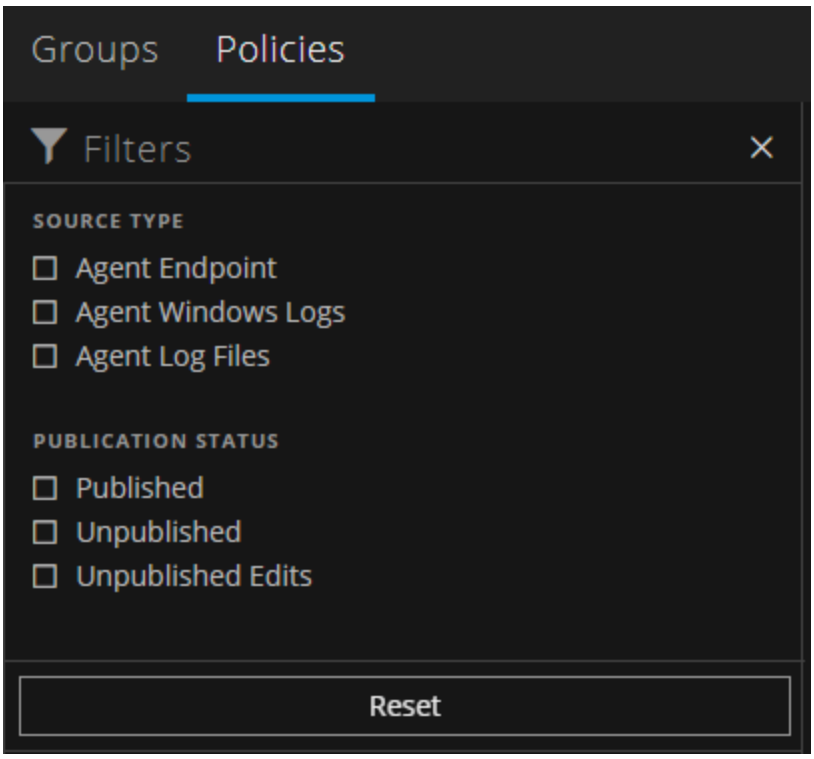
Filter Policies

The Filters Panel allows you to filter the list of displayed policies, based on the source type. You can filter on any combination of the following:

- Agent Endpoint
- Agent File Logs
- 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.

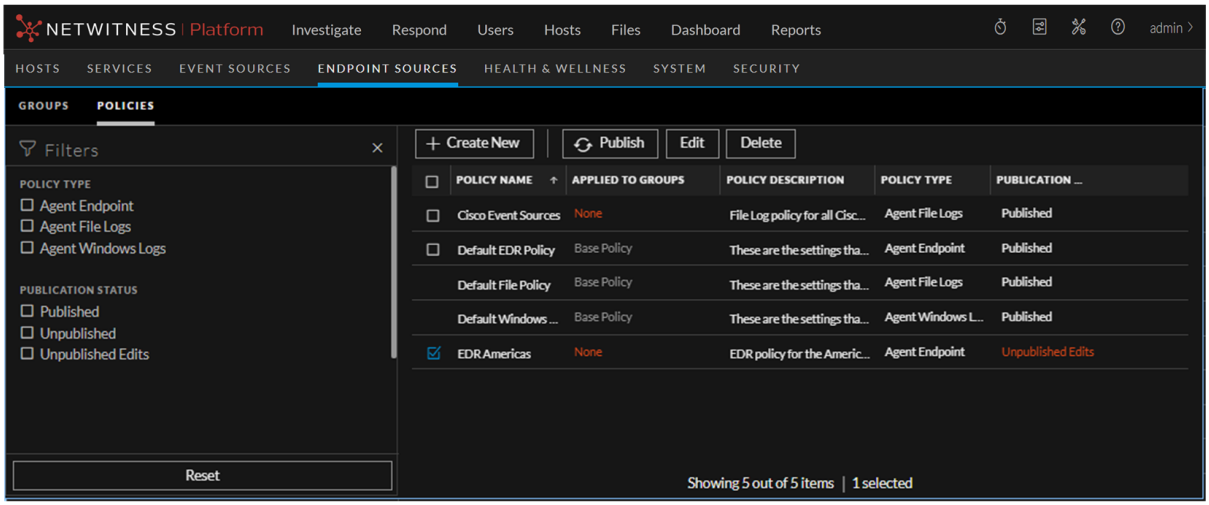
Edit a Policy

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**.

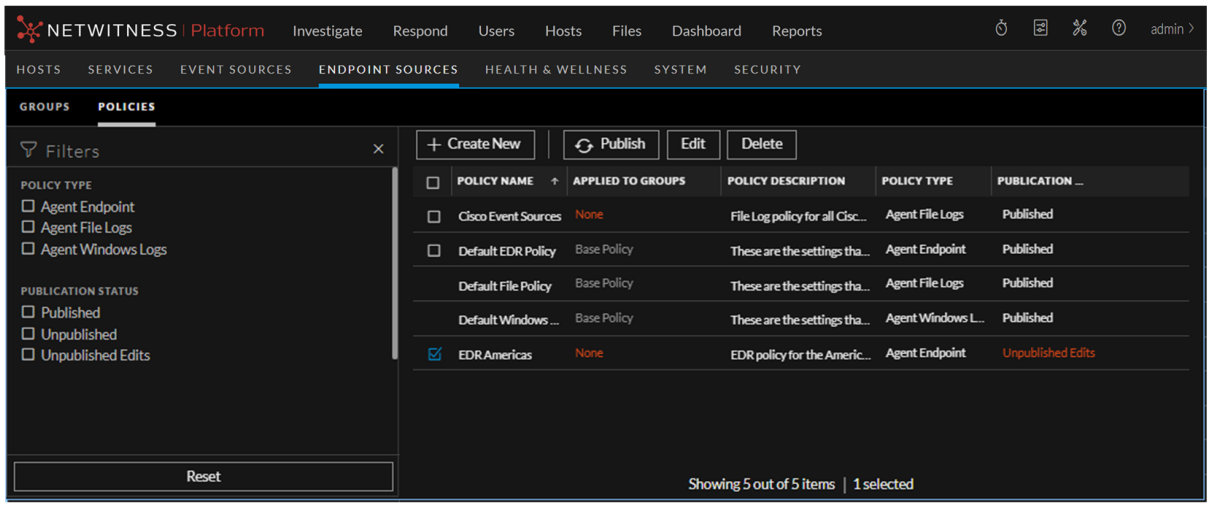


3. Edit the policy details as required.
4. Do one of the following:
   - Click **Save and Close** to save the changes and return to the Policies view. The policy will be listed under the **Unpublished Edits** category.
   - Click **Publish Policy** to publish the changes.

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.

Conflict Resolution

An endpoint can be in more than one group, and can thus have more than one Agent Endpoint, Agent File Logs, or Windows Logs policy applied to it. In this case, there may be conflicting settings that could be applied to the endpoint.

For example, an endpoint that is in two Groups could have two, different File Log policies applied to it. In this case, some of the settings could have conflicting values. The value that is actually applied to the endpoint is determined by the highest-ranked policy that contains a value for that setting.

For example, assume there is an endpoint that has 2 Agent File Log policies applied to it:

- LF Policy One: Log File Type is webgateway, and **File Encoding** is set to UTF-8
- LF Policy Two: Log File Type is webgateway, and **File Encoding** is set to Local Encoding

How NetWitness assumes the webgateway logs are encoded is dependent upon which policy is ranked higher:

- If Policy One is ranked higher than Policy Two, NetWitness treats the logs as having UTF-8 encoding.
- If Policy Two is ranked higher than Policy One, NetWitness treats the logs as having Local Encoding.

For an example using EDR policies, see Simulation Examples, which shows how you can preview the settings that would be applied before actually changing any policy rankings.

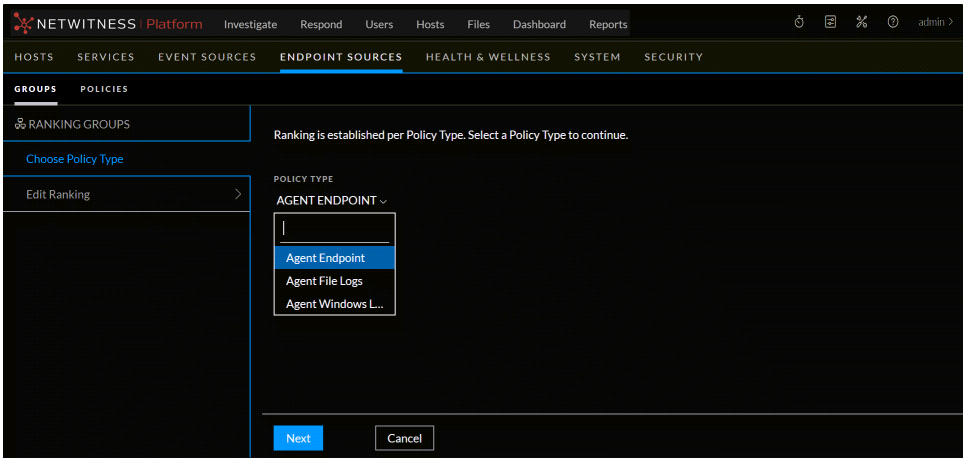
Change Policy Ordering for Groups

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.

Edit Ranking

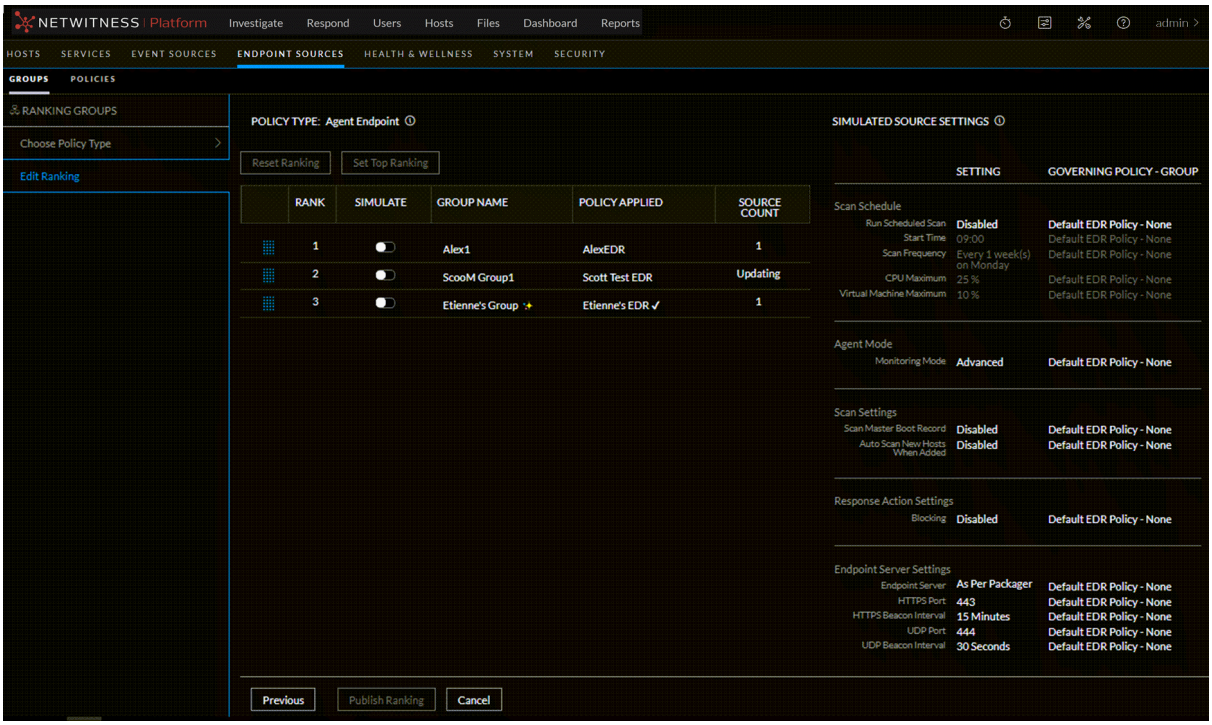
To edit the ordering or ranking of a group:

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
   - **Agent Log Files** to rank the groups associated with agents that are using File Collection.



4. Click **Next**.

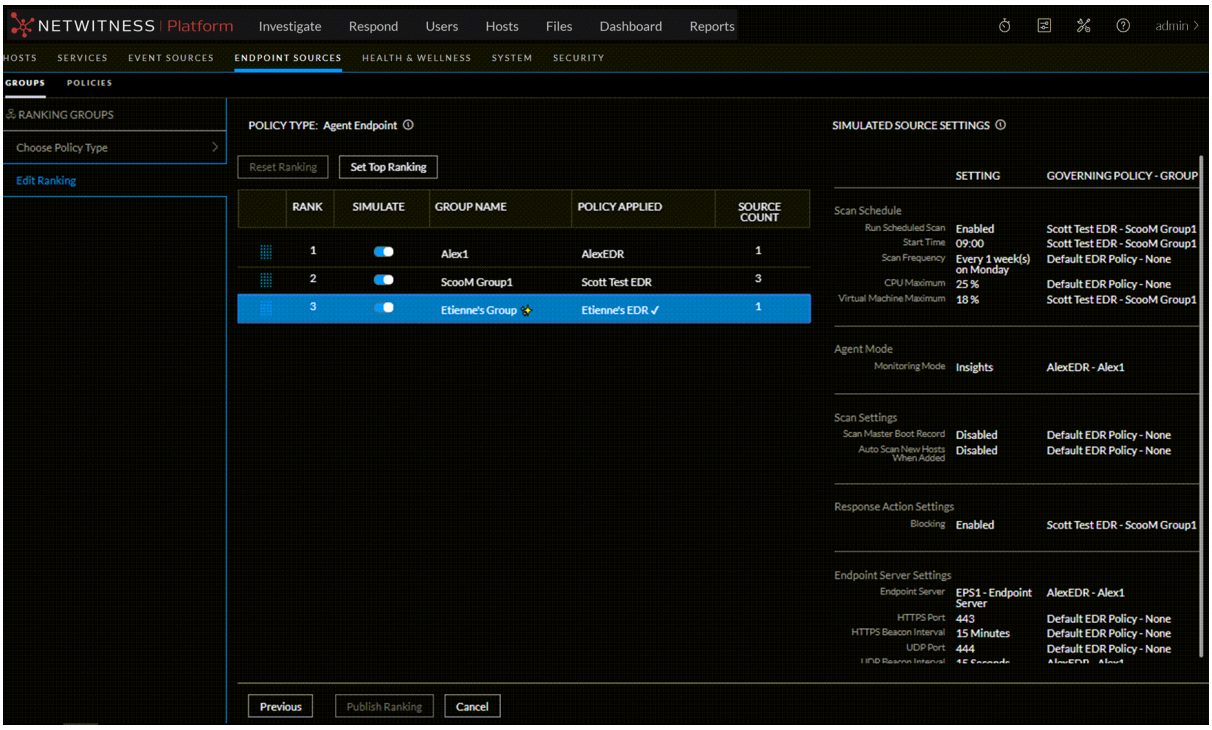
   The Ranking view is displayed:



You can simulate your policy settings and how they affect the endpoints within their groups. This gives you the ability to preview how your changes to the ranking will affect the policy settings applied to each hypothetical agent.

5. You can manipulate the sliders to simulate different options. You can select the slider in the **Simulate** column for each group into which a hypothetical agent would fall, and drag it to the right to simulate turning on that policy.

   This image shows all policies being simulated:



6. Reorder your groups as necessary.
   a. Select anywhere within a group's row.
   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**.

7. As you change the rankings for your groups, you can preview how the policy settings would change based on your new rankings. For example, assume each of the following scenarios:
   - If you have a hypothetical agent that belongs in group 1, simulate only group 1 to see which policies would affect that agent.
   - If you have a hypothetical agent that belongs in group 1 and group 2, simulate both group 1 and group 2 to see how policies would be applied for that agent.
8. After you have specified the optimal ranking order, you can publish the new ranking.

Simulation Examples

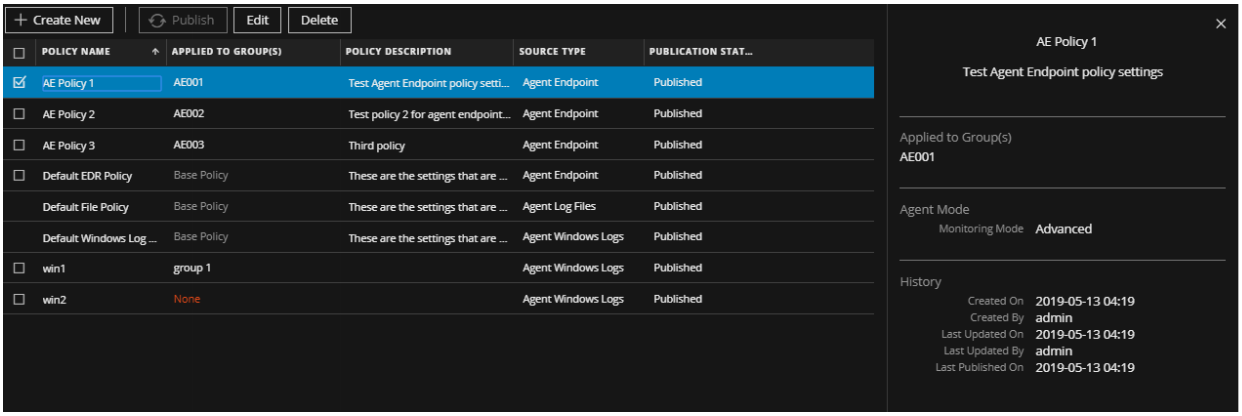
This section contains simulation examples for Agent Endpoint policies and Agent Log policies. Note that Windows policies have the same behavior as Agent Endpoint policies.

Agent Endpoint Policies Examples

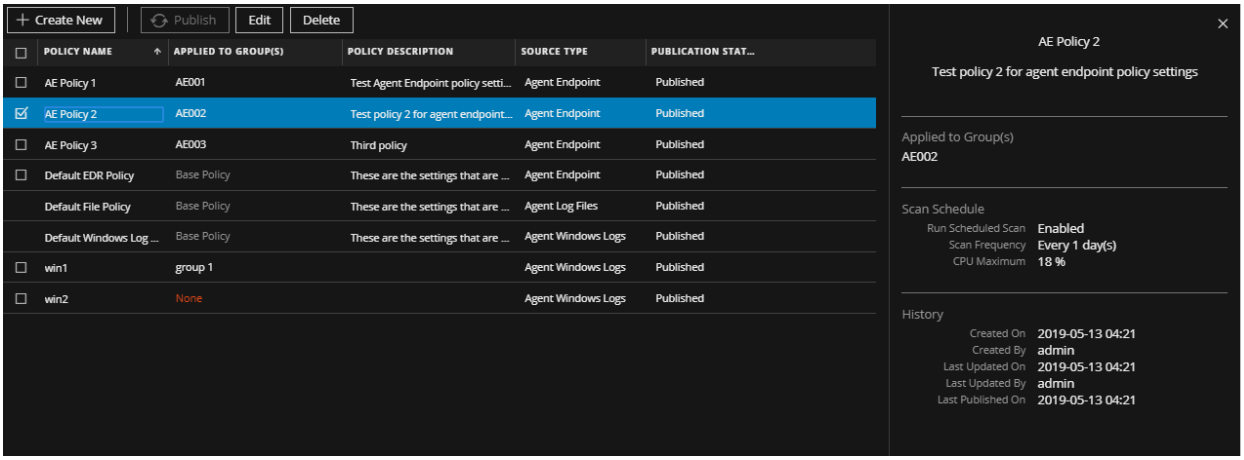
The **Simulated Source Settings** panel shows each individual policy setting, along with the governing policy for each setting.

Examine **AE Policy 1**, **AE Policy 2** and **AE Policy 3** to see which values are set in those policies.

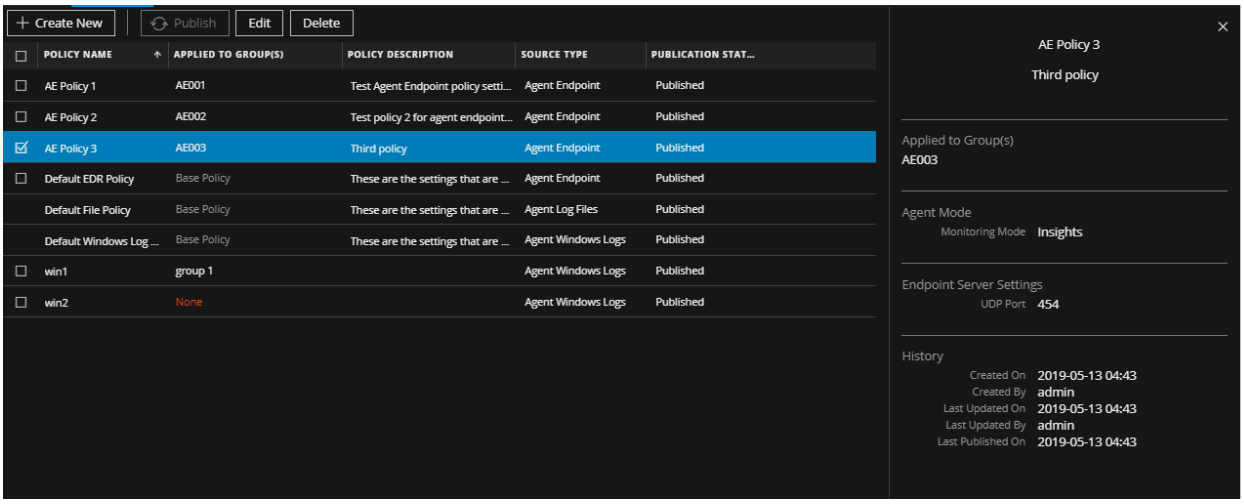
AE Policy 1 has Agent Mode set:



AE Policy 2 has a scan schedule set, as well as limiting the CPU maximum to 18%:

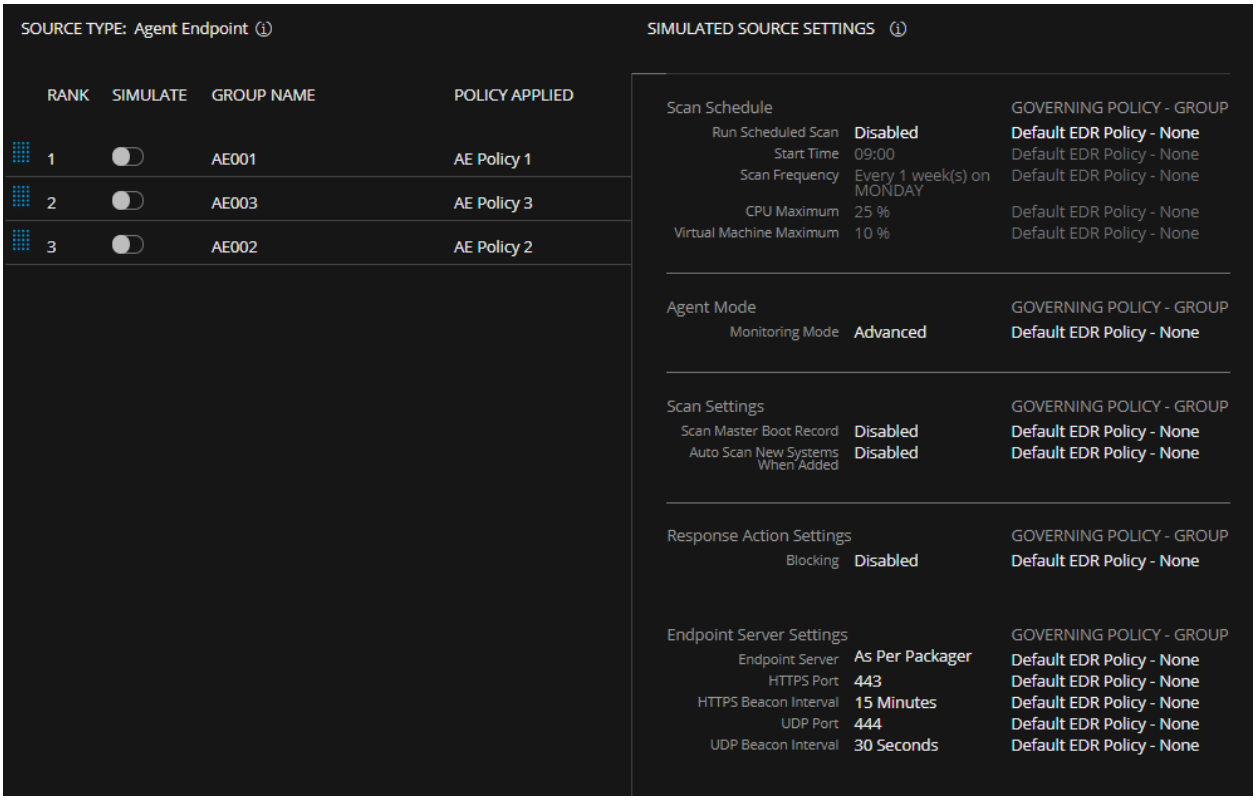


AE Policy 3 has Agent Mode set (to **Insights**), and sets the UDP Port to **454**:



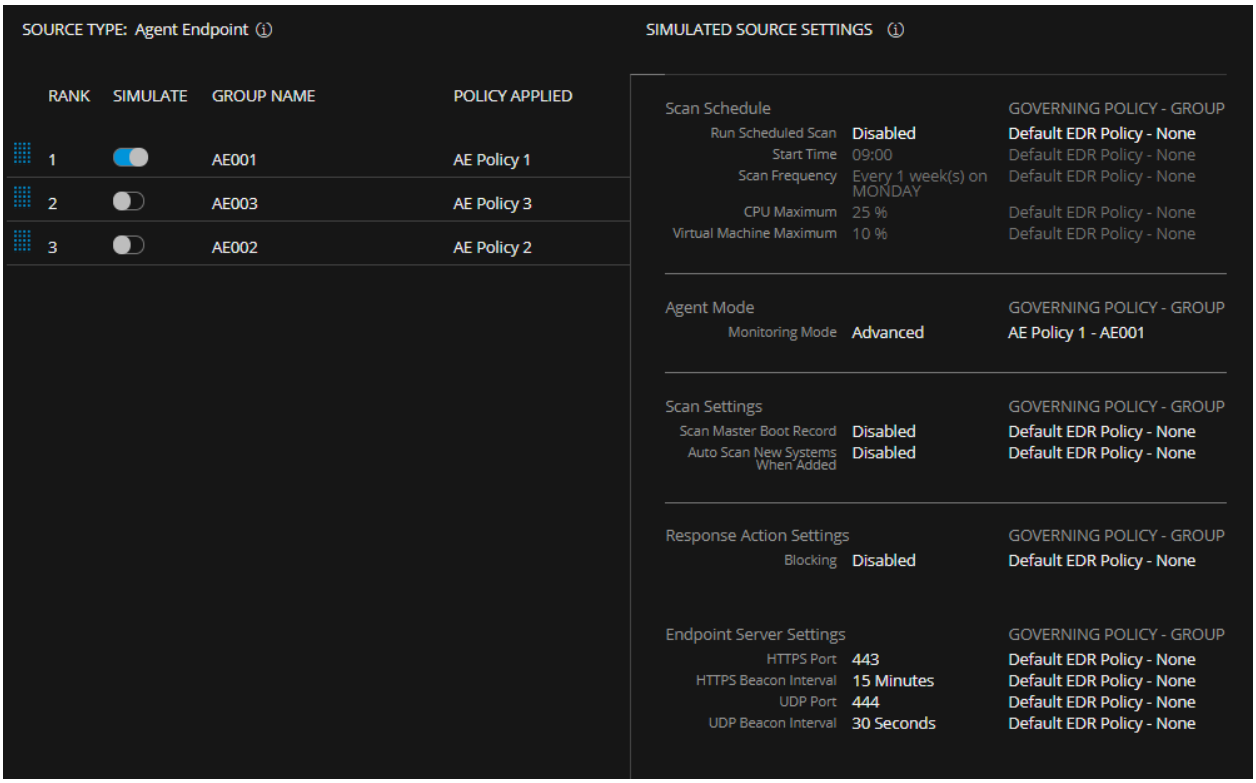
No Settings Applied

When none of the policies are simulated, you can see that the Default EDR Policy governs all behavior.



Simulate a Single Policy

When you select the AE001 Group, you can see that the values set in AE Policy 1 govern the behavior Agent Mode, as well as the Default EDR Policy being used for all unset parameters.



Simulate Multiple Policies

When you select multiple groups and policies, you can see the effects of each policy, based on the current ranking.

You can see that Agent Mode is set to **Insights**: this is because **AE Policy 3** is ranked above **AE Policy 1**, so the higher ranked policy's setting is used. None of the other parameters are set in more than a single policy, so for those, each policy's setting is used. Since **AE Policy 1** only has Agent Mode set—and **AE Policy 3** ranks higher and sets a different value—**AE Policy 1** does not govern any of the EDR settings. And finally, for parameters not set in any of the simulated policies, the Default EDR Policy settings are used.

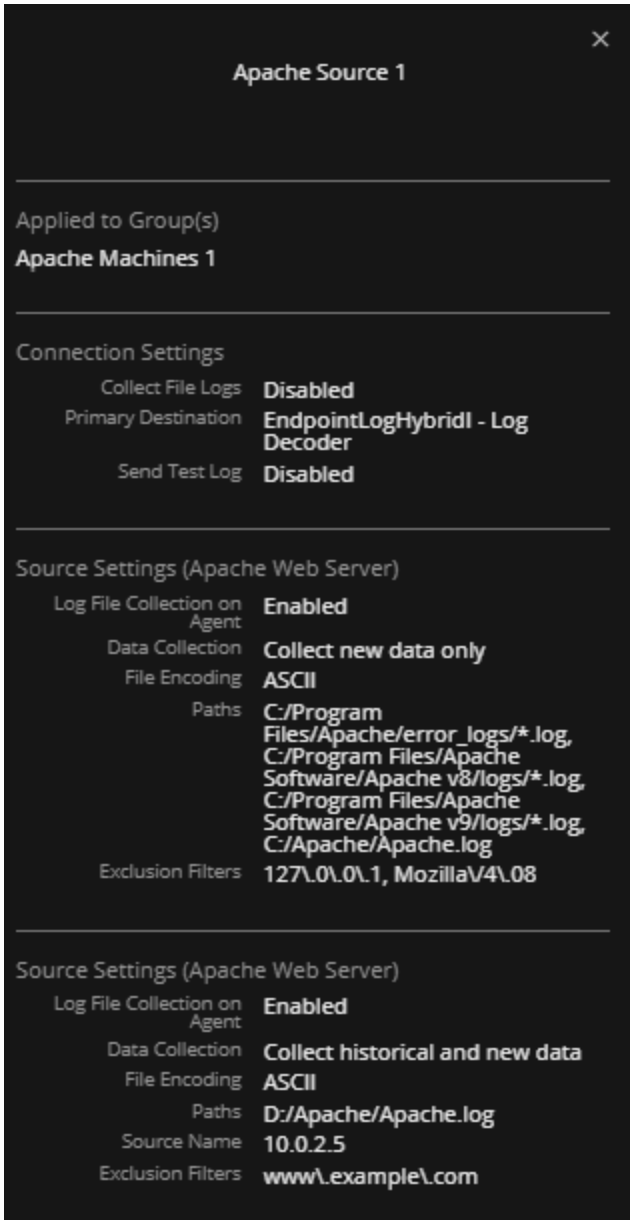
File Log Policies Simulation Example

The collection of parameter values into a complete policy works a bit differently for File Log policies than for EDR or Windows policies. To determine which values are applied from which policies, note the following:

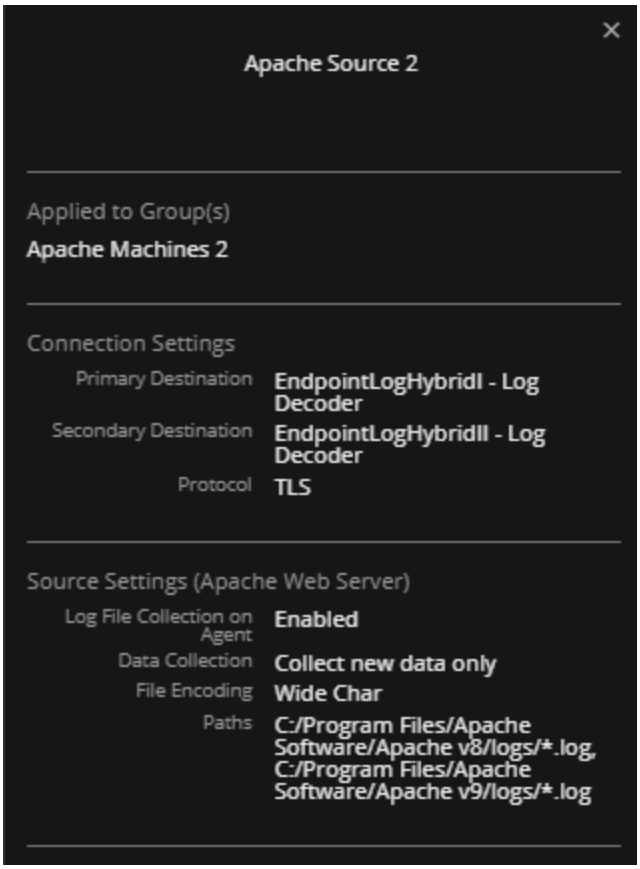
- Each event source type acts as a separate setting. That is, if a policy has values for both Apache and Access Manager, for example, each of those event source types is treated as a separate set of values.
- When an endpoint inherits values, it might not only get values from the highest ranked policy that has a value set. It might, for example, inherit Apache values from one policy, and Access Manager settings from another.
- If you consider a set of File Log policies that all include settings for the same event sources, then they behave the same as EDR and Windows policies.

Consider the following example, where there are three log file policies—two with Apache source types and one with MS SQL event source type.

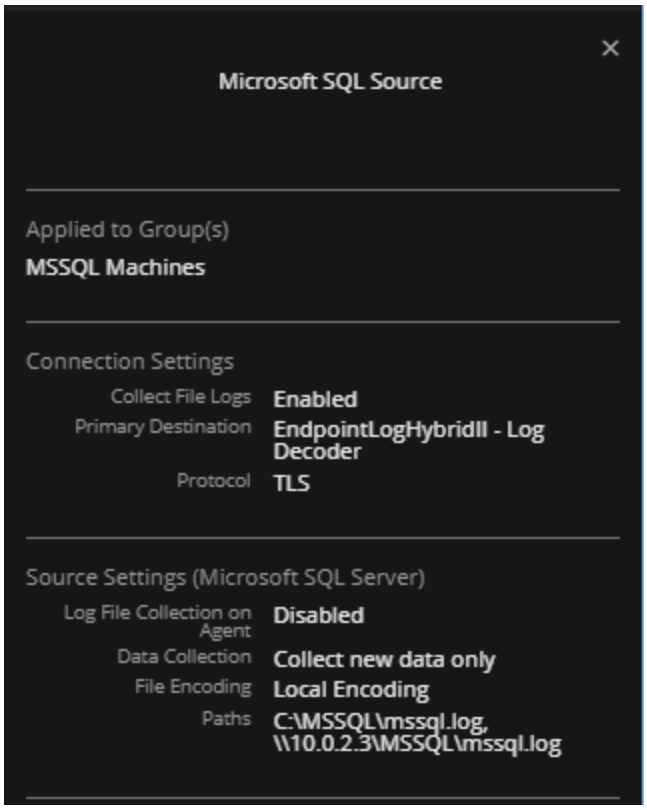
- File policy **Apache Source 1**:



- File policy **Apache Source 2**:

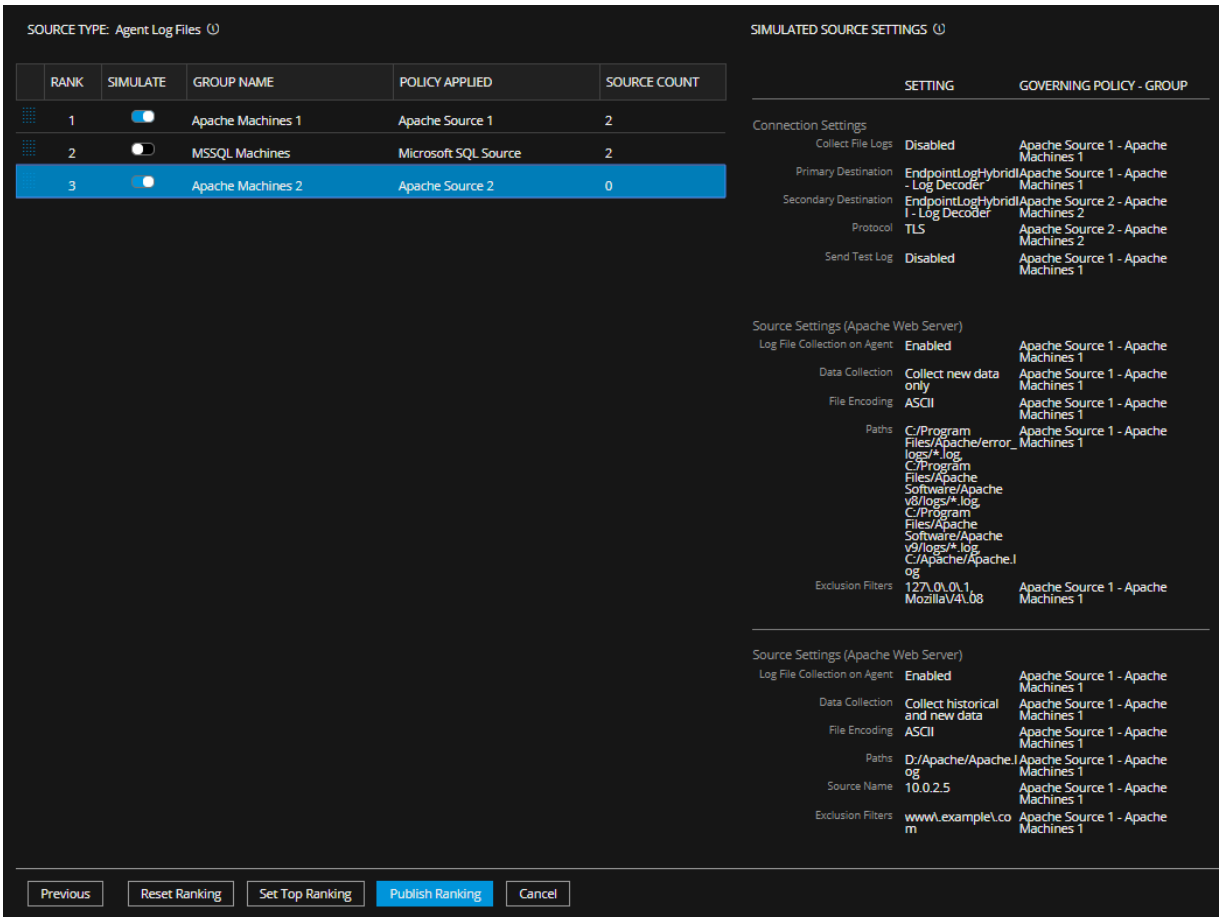


- File policy **Microsoft SQL Source**:



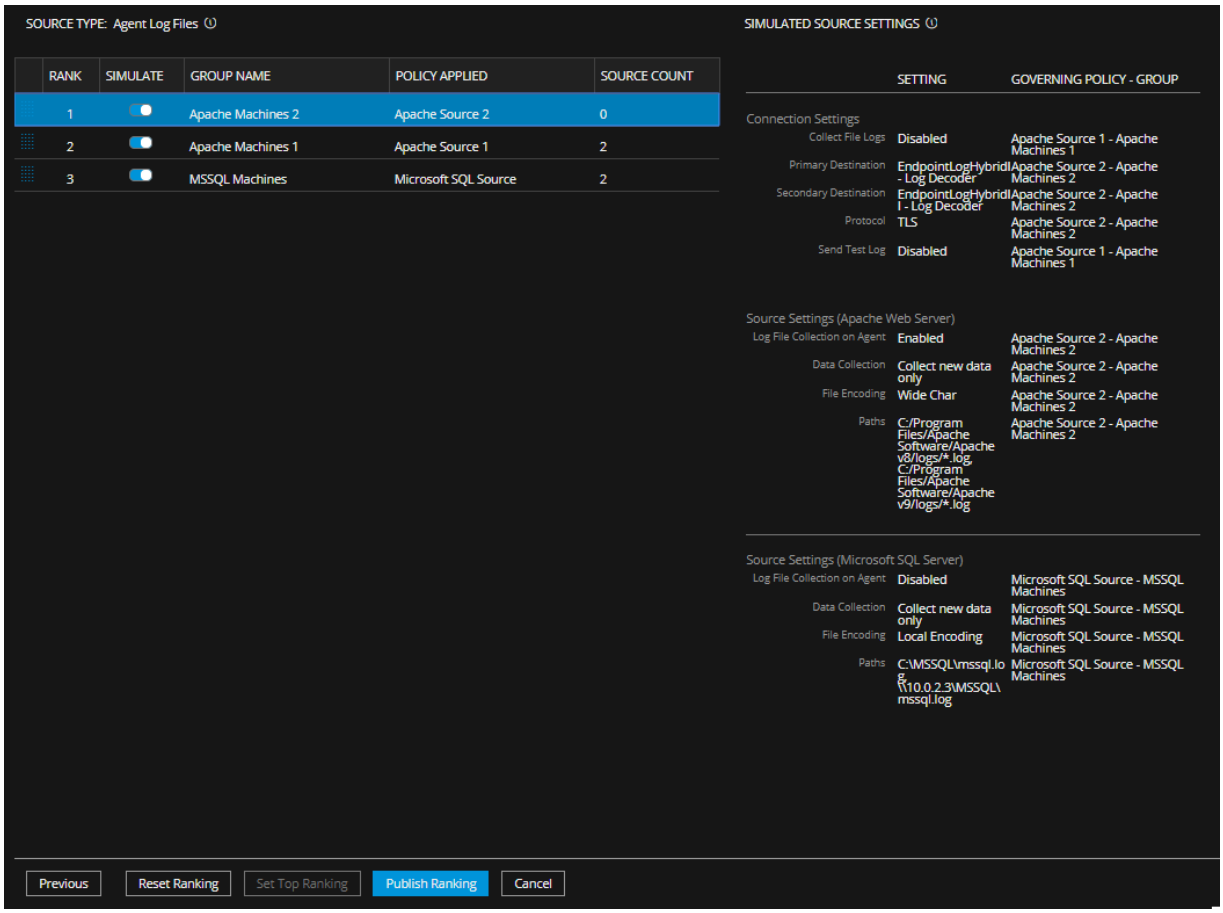
Examine two of the possible ranking orders:

- Simulate policies 1: **Apache Source 1**, 2: **Apache Source 2**. Note that in this case, the MS SQL policy is not simulated.



In this case, all Apache settings for the group are inherited from the **Apache Source 1** policy.

- Move the **Apache Source 2** policy higher than **Apache Source 1** policy, and add the **Microsoft SQL Source** policy. Simulate policies 1: **Apache Source 2**, 2: **Microsoft SQL Source**, 3: **Apache Source 1**.



In this case, all Apache settings for the group are inherited from the **Apache Source 2** policy, and groups also get the MS SQL settings.

So, the Apache settings are inherited from the highest ranked Apache policy **only**, but the source settings as a whole are **combined** to include settings from each event source type.

The SIMULATE Slider

The slider has two positions:

- On: 
- Off: 

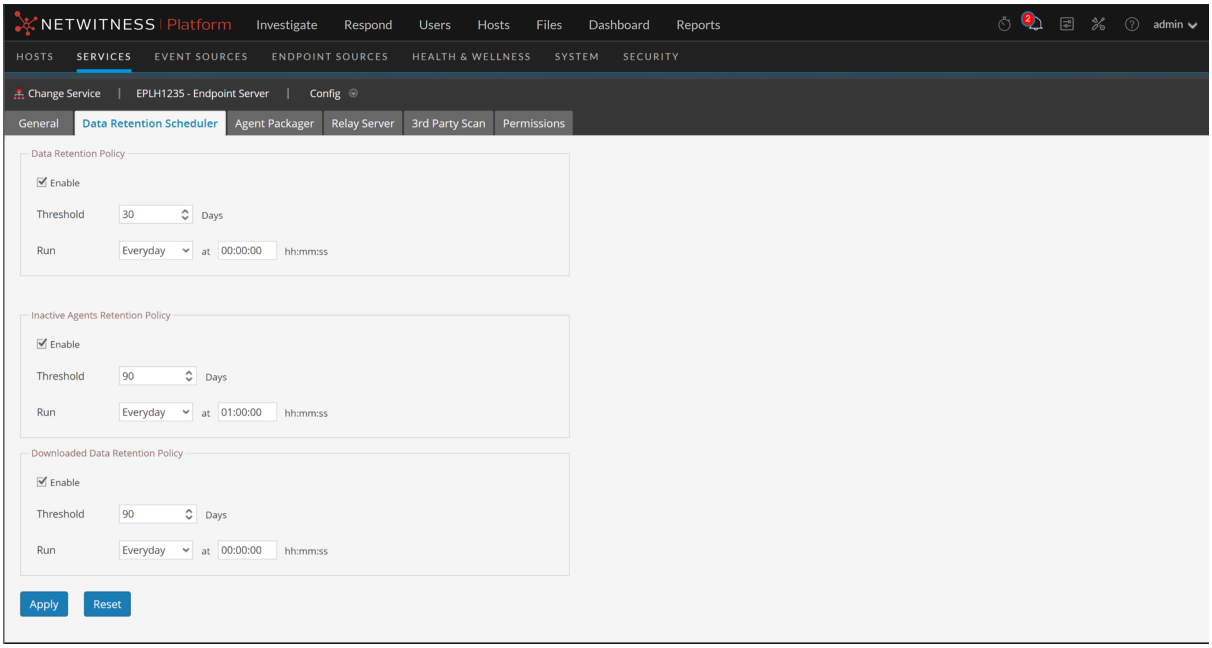
If the simulate slider is ON for a policy, that policy's values are factored into the complete set of governing settings. If the slider is OFF for a policy, the setting for that policy have no effect on the list of the governing settings.

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.

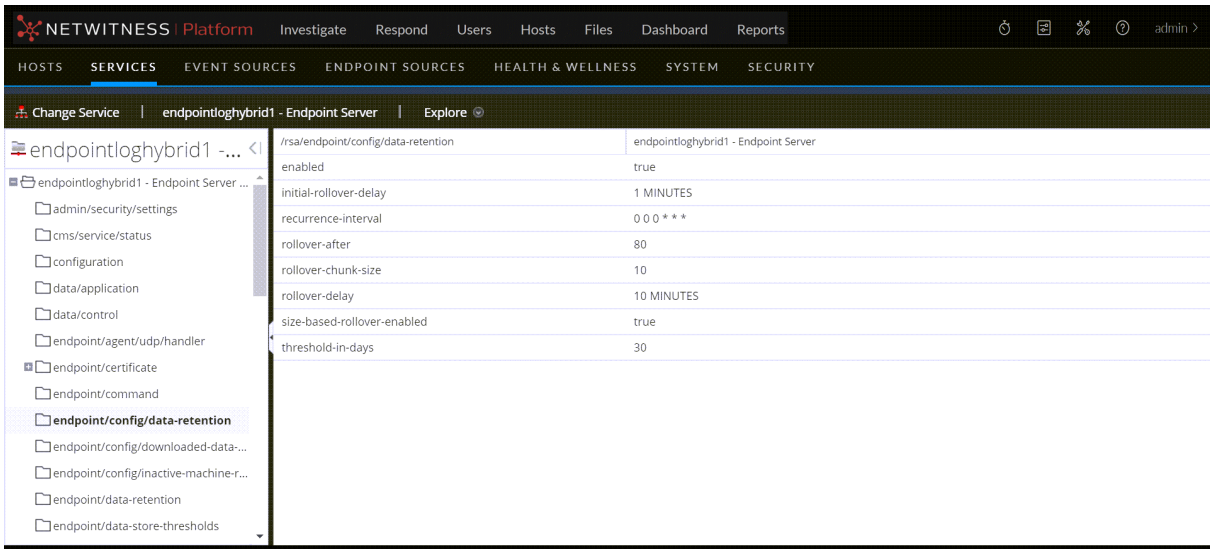


5. In the **Data Retention Policy** panel, by default, the **Threshold** is set to 30 days, and **Run** to Everyday. This means only 30 days of Endpoint data is retained and the older data is deleted from the database.
6. Click **Apply**.

To change the configuration for size-based retention:

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

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

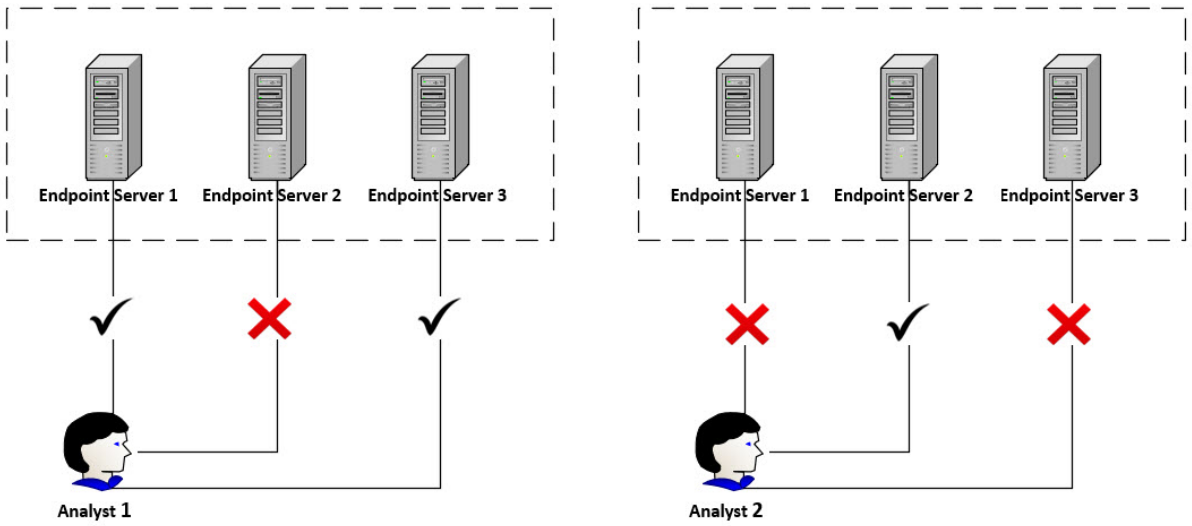


4. In the left panel, select **endpoint/config/data-retention**.
5. Edit the configurations based on your requirements.

Manage Role Permissions at Endpoint Server Level

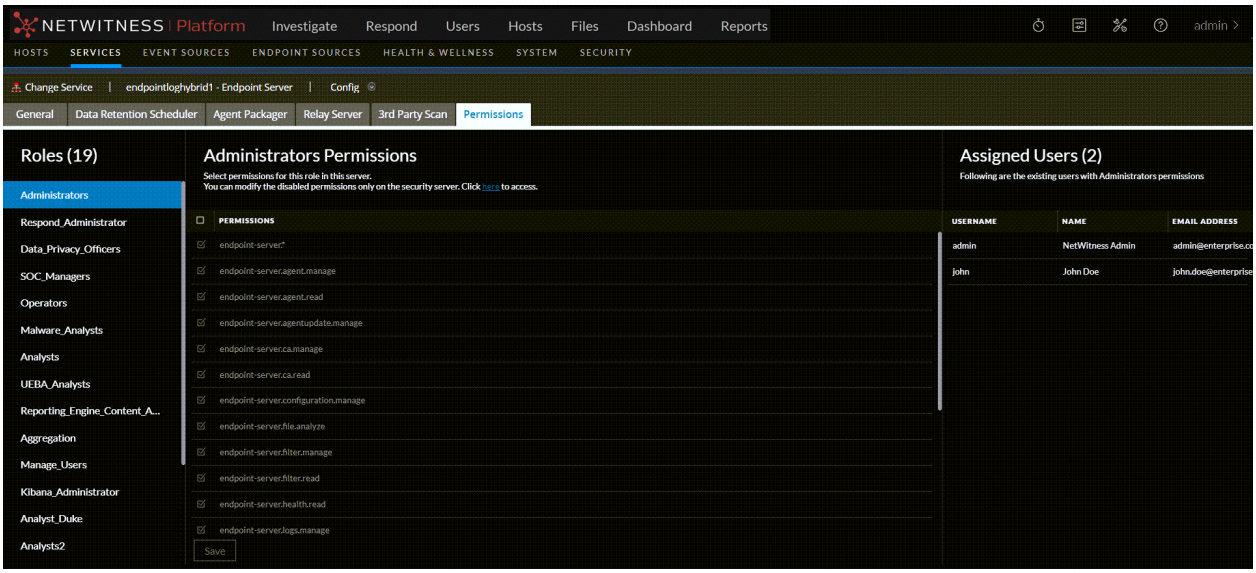
NetWitness Platform provides more flexibility for managing RBAC (Role-Based Access Control). This enhancement enables you to grant/revoke access for any role at individual endpoint server levels in an environment rather than all. On the **admin > Config** view for any endpoint server, you can navigate to the **Permissions** tab and manage a significant number of permissions for the selected endpoint server. A new permission called **endpoint-server.file.analyze** lets the user perform file analysis activities(Analyze Files, Save a Local Copy and Initiate OPSWAT Scans), allowing more flexible options to manage user permissions. Refer to Manage Users with Roles and Permissions on the *System Security and User Management Guide* for more information.

The following illustrations show how you can set permissions at the endpoint server level for an analyst.



To configure permissions at the endpoint server level:

1. Go to **(Admin) > Services**.
2. In the Services view, select the Endpoint Server service.
3. Click  and select **View > Config**.
4. Navigate to **Permissions** tab.
5. Select a role from the **Roles** pane on the left. (For more information on managing roles, refer (Optional) Add a Role and Assign Permissions in *System Security and User Management Guide*.)
6. Select the permissions from the **PERMISSIONS** section (Center pane).
7. Click **Save**. The **Assigned Users** pane on the right shows the list of users assigned with the selected role and permissions.
8. Repeat steps **5 – 7** if you want to modify permissions to any role. Make sure you save the changes before navigating out of the current role.



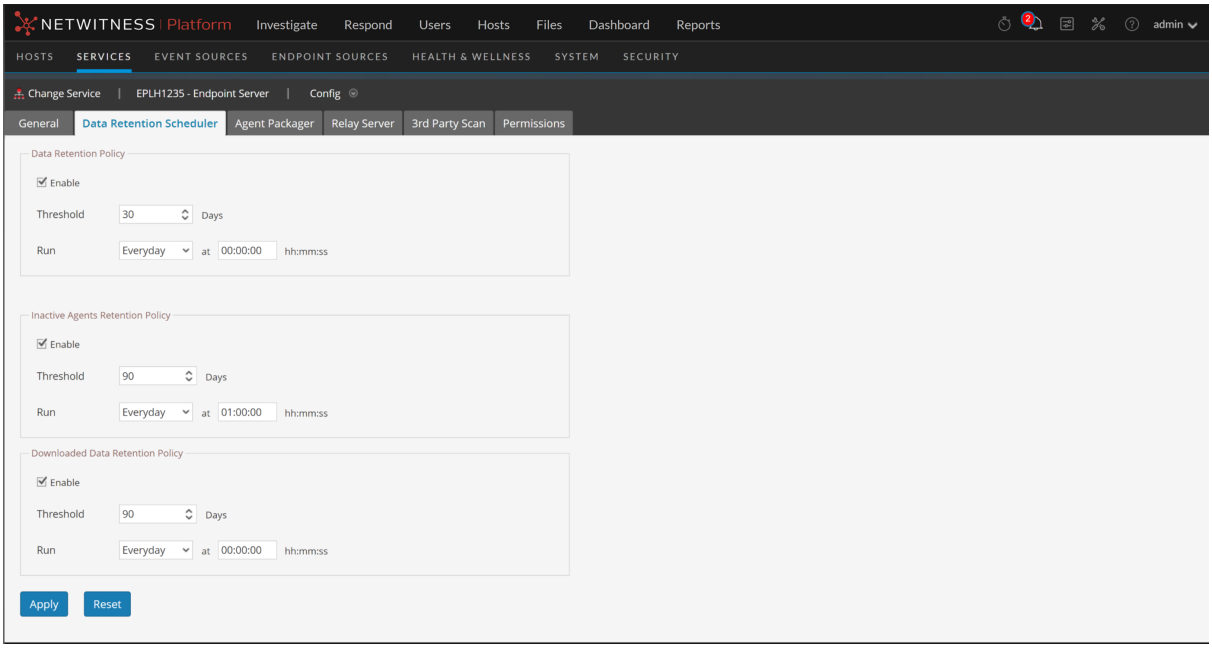
Note: Some of the permissions on the Permissions tab are disabled, and you can modify them only on the Security server (Admin > Security). All other permissions listed here are editable on both the Security server and the Permissions tab. For more information on managing permissions and on the NetWitness Platform, see *System Security and User Management Guide*.

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.



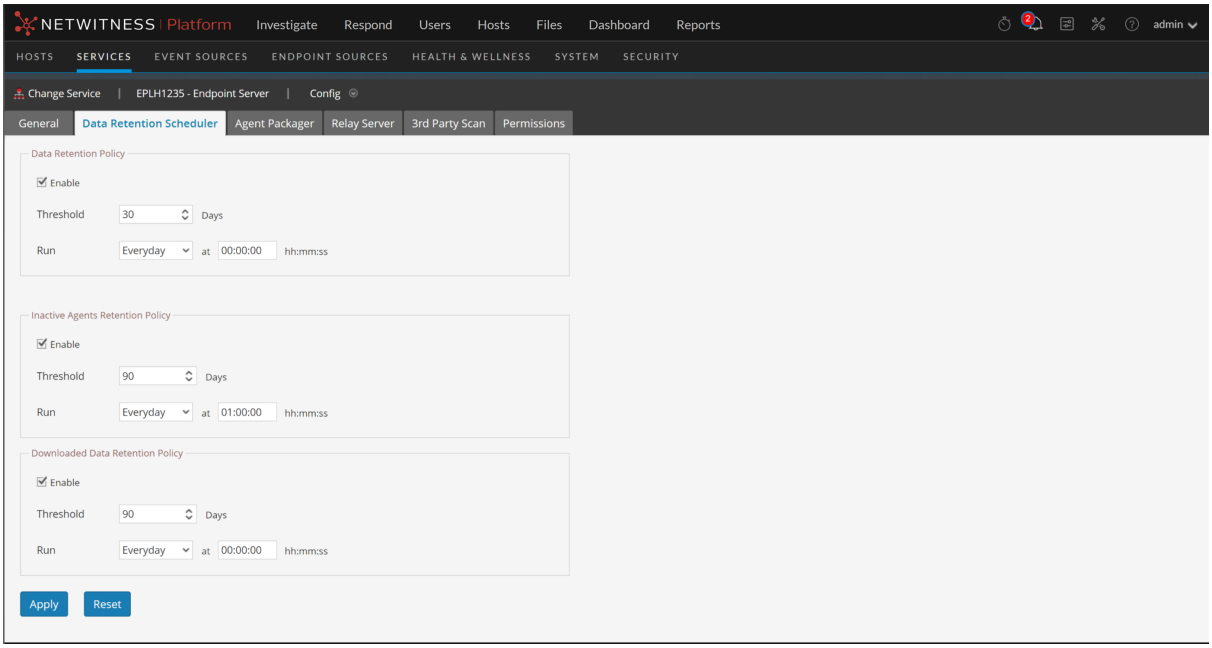
5. In the **Inactive Agents Retention Policy** panel, by default, the **Threshold** is set to 90 days and **Run** to Everyday. This means that the data of agents that have not communicated with the Endpoint server for 90 days is deleted from the database.
6. Click **Apply**.

Configure Retention Policy for Downloaded Files

An administrator can configure the retention policy to delete the downloaded files from the Endpoint server based on the number of days. By default, this option is enabled.

To configure the retention policy:

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



5. In the **Downloaded Data Retention Policy** panel, by default, the **Threshold** is set to 90 days and **Run** to every day. This means only 90 days of data is retained and the older data is deleted from the Endpoint server.
6. Click **Apply**.

(Optional) Installing and Configuring Relay Server

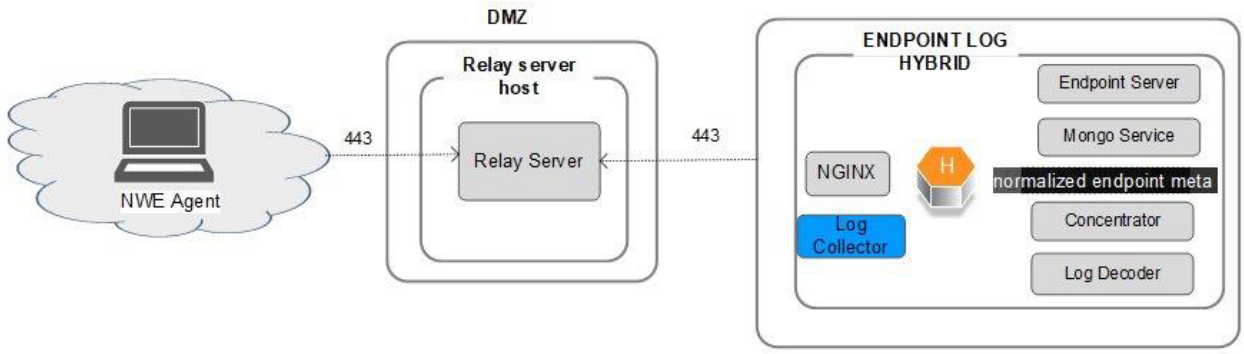
Relay Server (referred to as RAR in NetWitness Endpoints) extends NetWitness Platform's visibility into endpoints when they are outside the corporate network. The Relay Server deployed in a cloud or DMZ relays the endpoint data between the hosts and the Endpoint Server. The hosts that are outside the corporate network send the endpoint data to the configured Relay Server and the corresponding Endpoint server pulls the data.

Note: If you have Windows hosts that are outside the corporate network, the log data is not sent to the Relay Server.

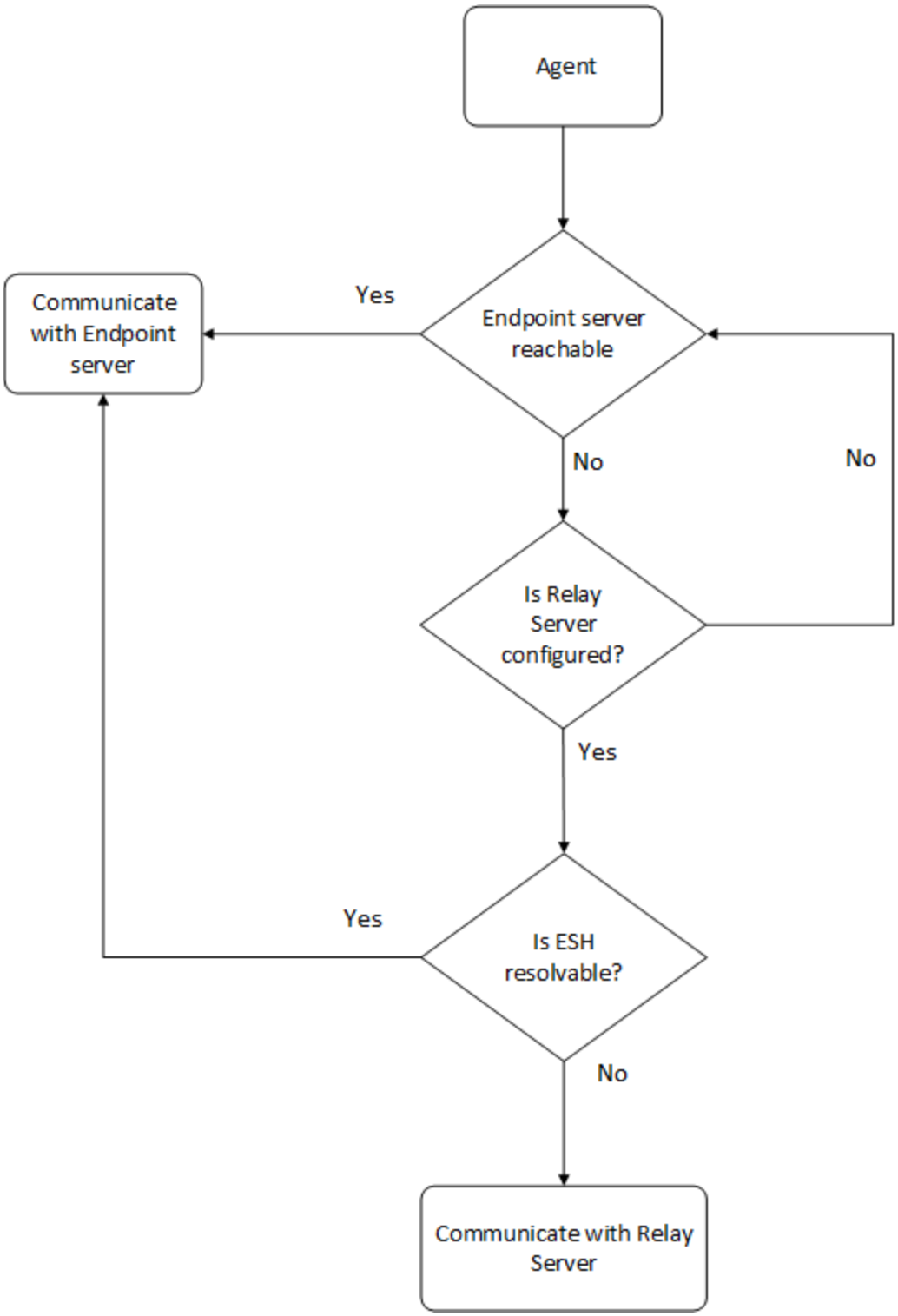
You can configure a Relay Server on the Endpoint Server Config view. Once the Relay Server is configured, the policy for the host is automatically updated and you can view the Relay Server settings on the **Host Details** view > **Policy Details** panel.

You can configure a single Relay Server with one or more Endpoint servers. In this case, the Relay Server ensures that the endpoint data reaches the Endpoint Server configured in the policy.

The following describes the architecture of the Relay Server.



The following flowchart explains how the host switches to the Relay Server.


Agent
Endpoint server reachable
Yes
Communicate with Endpoint server
No
No
Is Relay Server configured?
Yes
Yes
Is ESH resolvable?
No
Communicate with Relay Server

Installing the Relay Server

The Relay Server installer contains binaries, certificates, configuration files, and the installation script required to install the Relay Server.

IMPORTANT:
- The Relay Server version must match with the corresponding NetWitness Endpoint Server version. If you plan to upgrade a Relay Server to a newer version, first upgrade the Endpoint Server, then download the Relay Server installer, and run the installer script.
- Operating System updates and general system hardening on the Relay Server must be managed by the customer according to standard best practices. The Relay server package does not contain OS updates and the operating system will not be updated as part of the standard NetWitness update process.
- Do NOT run the nwsetup-tui script to install the Relay Server. Follow the instructions in this document only as Relay Server is an independent server and not part of NetWitness UI (Admin > Hosts).

Installation Media

The Relay Server can be installed only on EL 8 or NetWitness Platform 12.4.0.0 base image which is available for download from Downloads page (https://community.netwitness.com/t5/netwitness-platform-downloads/tkb-p/netwitness-downloads). Also, make sure that the Relay server host is connected to internet to download the required dependencies.
For more information on deploying Relay Server host on a:

- DMZ - see "Step 1a. Deploy the Virtual Host to create VM" in the *Virtual Host Installation Guide*.
- Cloud
  - see "Step 1. Deploy NW Server Host" in the *Azure Installation Guide*.
  - see "AWS Deployment" in the *AWS Installation Guide*.

Relay Server Host System Requirements

Agents	RAM	CPU Cores	Disk	Ideal Beacon Interval
20000	32 GB	4 cores	200GB	5 min

To install the Relay Server:

1. Log in to NetWitness Platform.
2. Click  **(Admin) > Services**.
3. Select the **Endpoint Server** service and click  > **View** > **Config** > **Relay Server** tab.
4. In the **Download Installer** section, enter the installer password and click **Download** to download the Relay Server installer file (**RelayInstaller.zip**).

5. Copy the Relay Server installer file (**RelayInstaller.zip**) to the Relay Server host.
6. Unzip the **RelayInstaller.zip** file on the Relay Server host. For example:

   ```
   /home/RelayInstaller.zip
   unzip <installer path>
   ```

7. Set up the execution permission using the following command:

   ```
   chmod +x install.sh
   ```

8. Run the installer script using the following command:

   ```
   ./install.sh
   ```

   The **All necessary RPMs will be installed without further** prompts is displayed.
9. Enter **Y** to continue the installation.

   The password prompt is displayed.
10. Enter the password.

    Note: Make sure you enter the same password you set while downloading the Relay Server installer.

    Note: In case if you are re-installing the Relay Server host. **Do you wish to update the list** prompt is displayed.
    - Enter **Y** to update the Endpoint server IPs.

    Enter the Endpoint Server IPs prompt is displayed.
11. Enter all the Endpoint server IPs you plan to configure with the Relay server with comma separated.

If the Relay Server installation is successful, you can check the status of the services:

- Check if the Relay Server is up and running:

  ```
  systemctl status rsa-nw-relay-server
  ```

- Check if Ngnix is running:

  ```
  systemctl status ngnix
  ```

You can also update Endpoint Server IPs without installing the Relay Server.

To update Endpoint Server IPs without installing the Relay Server:

1. Run the following command:

   ```
   bash /var/netwitness/relay-configure-allowed-hosts.sh
   ```

   The list of all the configured Endpoint server IPs is displayed and **Do you wish to update the list** prompt is displayed.
2. Enter **Y** to update the list of Endpoint server IPs.

   Enter the Endpoint Server IPs prompt is displayed.
3. Enter a comma-separated list of all the Endpoint Server IPs to update.

   The list of updated IPs is displayed.

Configuring the Relay Server

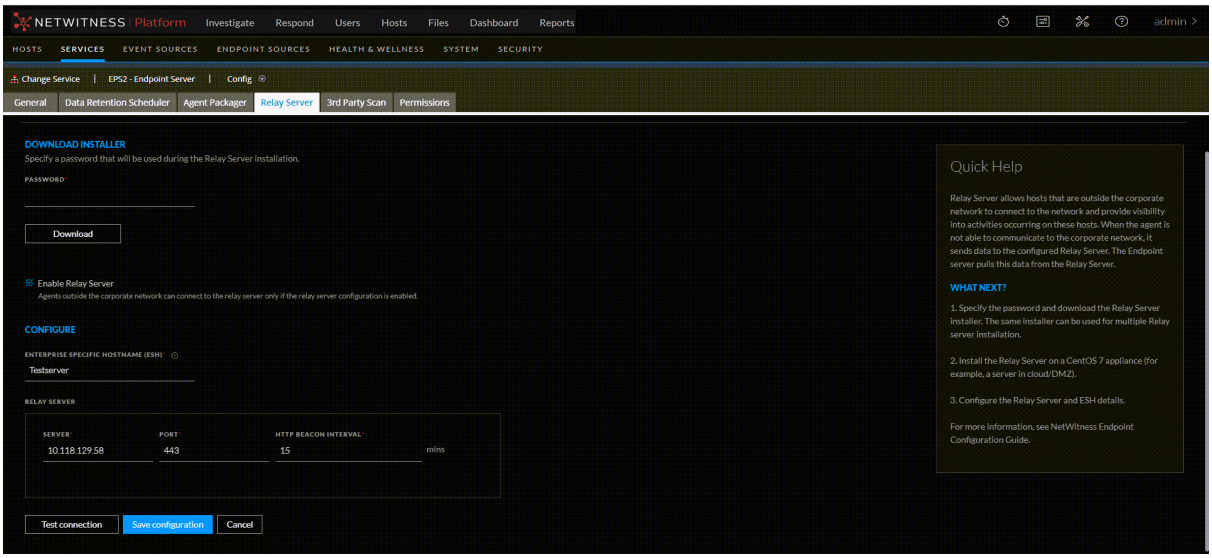
Make sure you have installed the Relay Server.

Note: During Relay Server host installation, firewalld is configured to allow incoming connections only on TCP ports 443 and 22.

To configure the Relay Server:

1. Log in to NetWitness Platform.
2. Click **(Admin) > Services**.
3. Select the **Endpoint Server** service and click > **View** > **Config** > **Relay Server** tab.

   The Relay Server tab is displayed.



4. Select the **Enable Relay Server** check box to enable the Relay Server configuration.

   Note: To disable the Relay Server, clear the **Enable Relay Server** check box.

   Caution: Before you disable the Relay Server configuration, if the hosts will be always roaming make sure to migrate these hosts to an alternate Endpoint server configured with a different Relay server. Else these hosts will not be able to connect back to the corporate network. When you disable the configuration, the Relay Server settings are removed from the EDR policy.

5. In the **Configure** section:

a. Enter the ESH.

IMPORTANT: This should a hostname that can only be resolved on the corporate internal DNS and not on public internet DNS (ex: 1.1.1.1 or 8.8.8.8). It is used to determine if the host running the Endpoint agent client is connected to the internal network (physically on premise or through VPN).

b. Specify the Relay **Server**, **Port** and **HTTP Beacon Interval**.

IMPORTANT: The Relay Server needs to be a hostname that can be resolved correctly on both internal DNS (with the internal IP) and public DNS (with the public IP)

6. Click **Test Connection** to check if the Relay Server is reachable.
7. Click **Save Configuration** to save the configuration.

Note: Before you modify the Relay Server configuration, perform any one of the following:
- Make sure that the hosts are inside the corporate network so that the policy with the Relay Server configuration is applied.
- If hosts will always be roaming, then migrate these hosts to an alternate Endpoint server configured with a different Relay Server.

IMPORTANT: You must change the root password after you deploy the Relay Server host.

Note: If you encounter test connection failure between Endpoint server and relay server, see **Relay Server Issues** section in the Troubleshooting topic.

Configure YARA

YARA helps analysts in identifying and classifying malware in a simple and effective manner. By default YARA is disabled, administrators can configure and enable YARA. You are required to provide YARA rule files and specify the path where these rule files are stored. Ensure that the Endpoint server and YARA rules directory are in the same appliance.

Note: The YARA rules directory should have the permission as 'netwitness'.

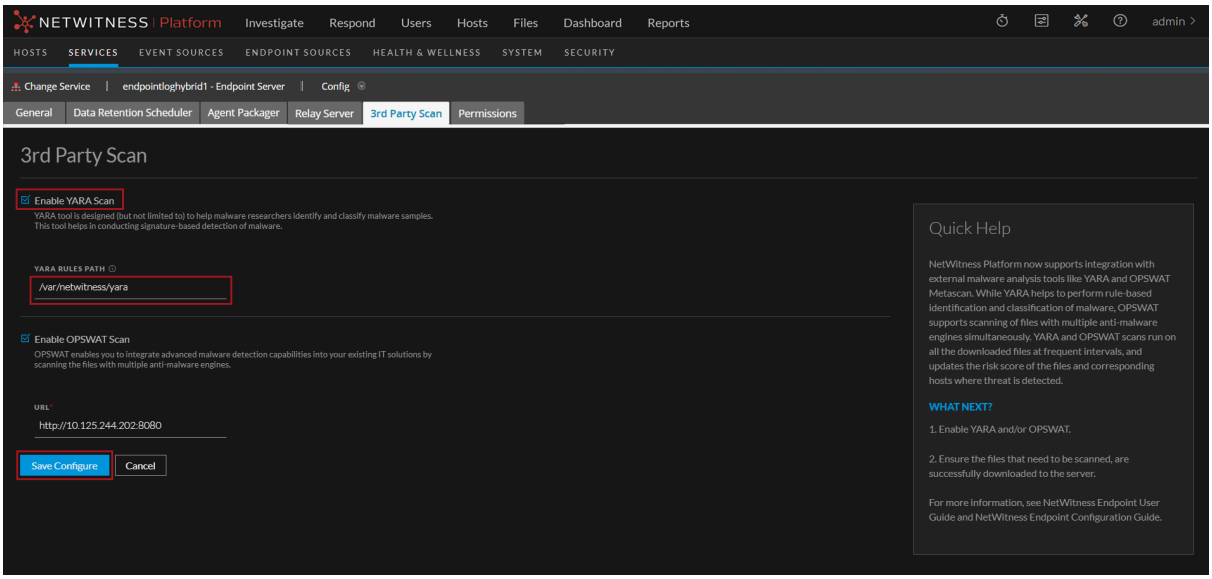
Note: For new installations, YARA will be included as part of the orchestration. If you are upgrading to NetWitness Platform, YARA is included automatically. In case of an upgrade, deploy the following Yara App rules from Live-

- Yara Rule Matched
- Process with Matched Yara Rule

IMPORTANT: Ensure that YARA is configured and YARA RULES PATH is same across all the Endpoint servers.

To change the configuration for YARA:

1. Go to **(Admin) > Services**.
2. In the Services view, select the **Endpoint Server** service.
3. Click and select **View** > **Config**.
4. Click the **3rd Party Scan** tab.



5. Select **Enable YARA Scan.**

6. In **YARA RULES PATH**, specify the directory path where the YARA rule files are stored.

   Note: You can add any number of YARA rule files in this directory. Each rule file can have more than one rule. All downloaded files are scanned by all the YARA rule files.

7. Click **Save Configure**.

Configure OPSWAT

OPSWAT (MetaDefender Core) provides advanced malware detection capabilities by scanning files with multiple anti-malware engines simultaneously. OPSWAT is disabled by default. As an administrator, you can enable and configure OPSWAT on the endpoint servers.

Note: You need to deploy the following OPSWAT app rules from Live services to log decoder for successful configuration of OPSWAT on endpoint servers:

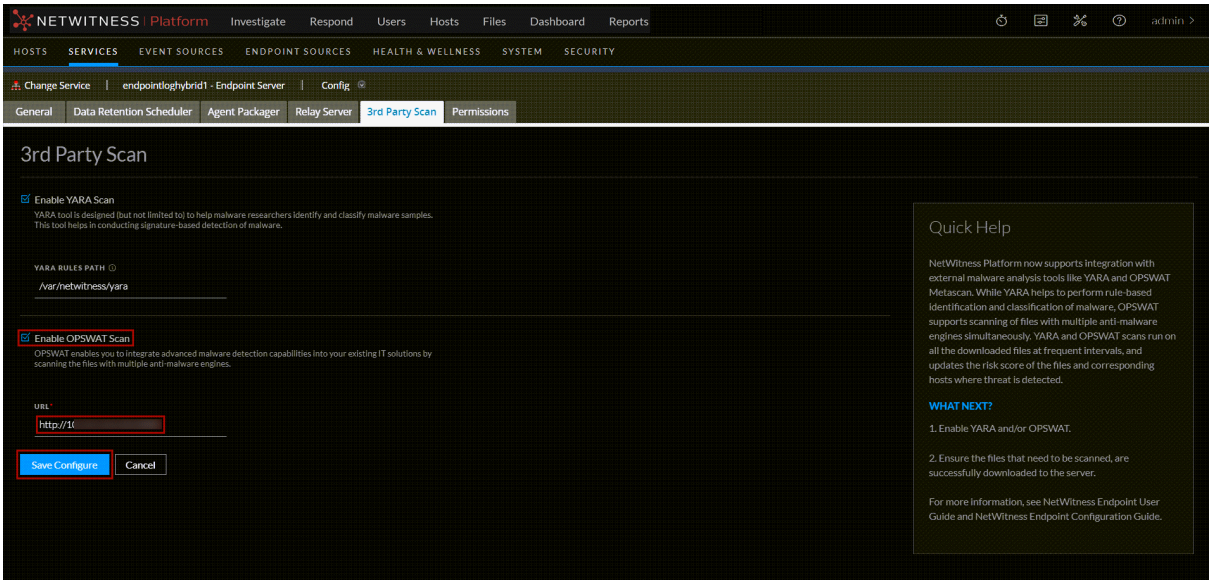
- opswat reported infected
- opswat reported suspicious
- process with opswat reported suspicious
- process with opswat reported infected

IMPORTANT: Ensure that OPSWAT is configured in all endpoint servers and the configuration parameters are consistent across all endpoint servers.

To enable and configure OPSWAT:

1. Go to **(Admin) > Services**.
2. In the Services view, select the Endpoint Server service.
3. Click  and select **View > Config**.
4. Click the **3rd Party Scan** tab.
5. Select **Enable OPSWAT Scan**.
6. Enter the URL.

7. Click **Save Configure.**



Integrating NW Endpoint with NW Platform

You can configure the Endpoint Metadata for the NetWitness Endpoint by integrating the Meta Integrator service in the NetWitness Endpoint directly to a Log Decoder. You can view the Endpoint metadata in the **Investigate > Navigate** and **Events** views. This integration includes the following steps:

- Enable Metadata Forwarding
- Enable Machines to Forward Metadata

Enable Metadata Forwarding

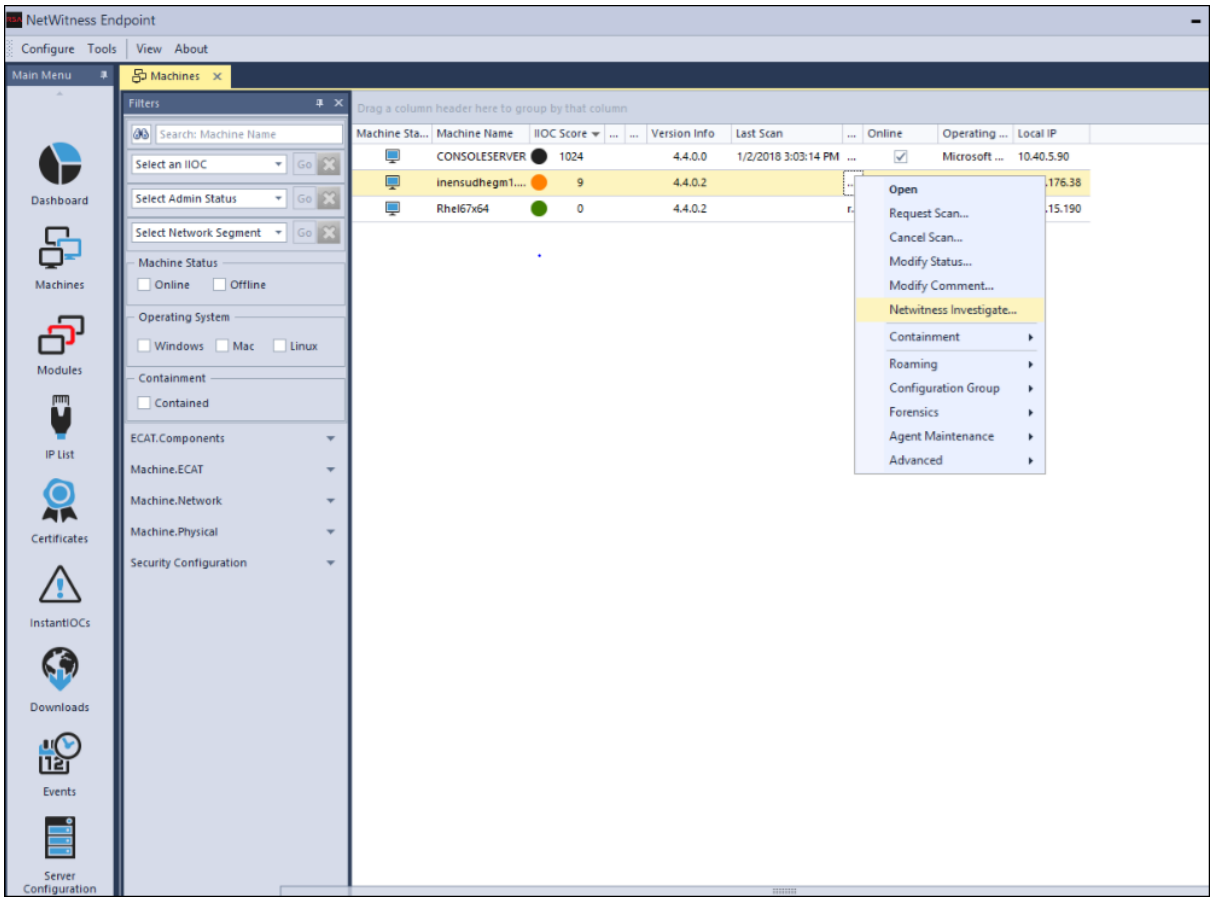
To enable the Metadata Integrator service for the selected NetWitness Endpoint agents, run the following command:

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

Enable Machines to Forward Metadata

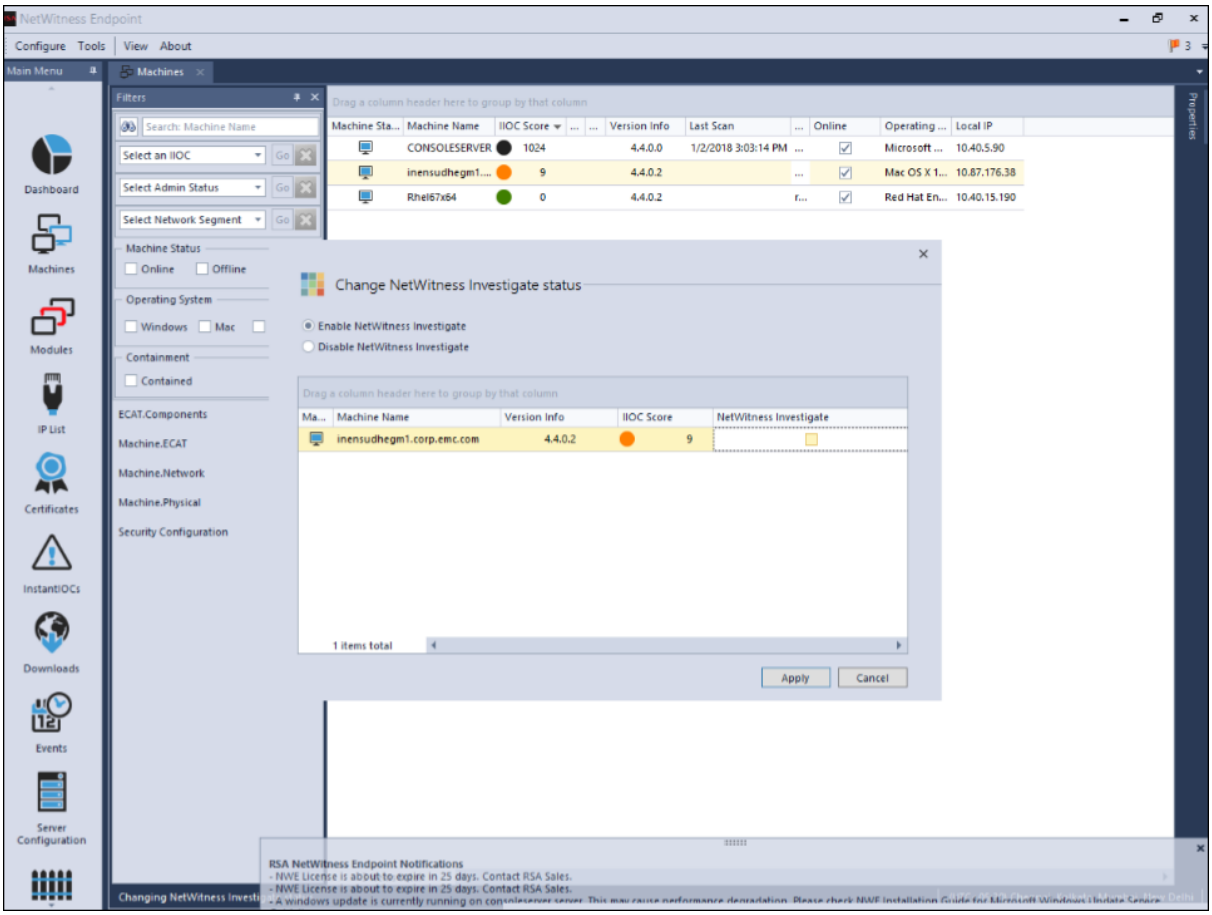
After you enable the Metadata Forwarding using any one of the above options, perform the following to enable the machines to forward metadata to the Log Decoder.

1. Open the NetWitness Endpoint 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.

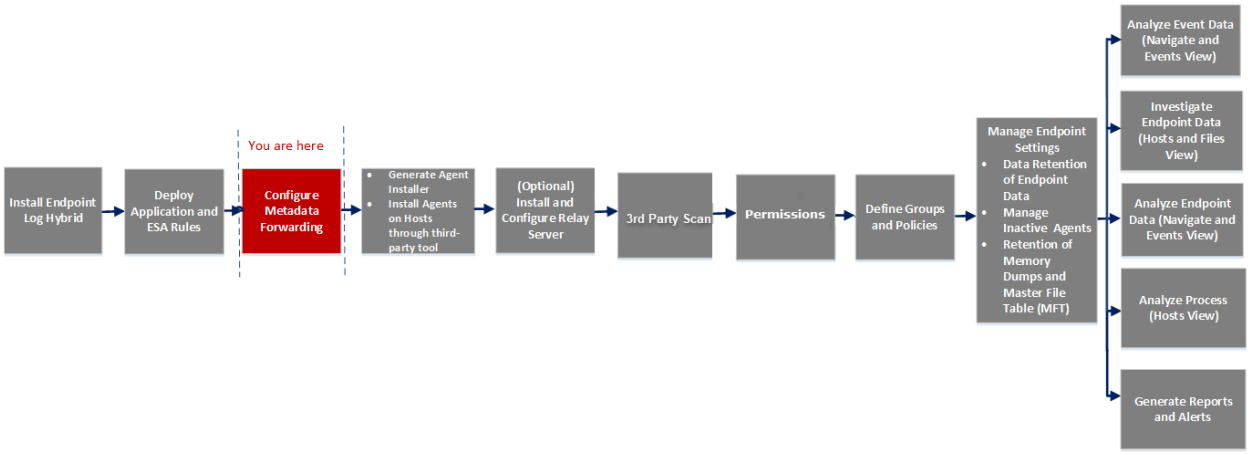
You can view the complete service nodes in tree form in the Services Explore view. For more information, see the "Services Explore View" topic in the *Hosts and Services Getting Started Guide*.

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



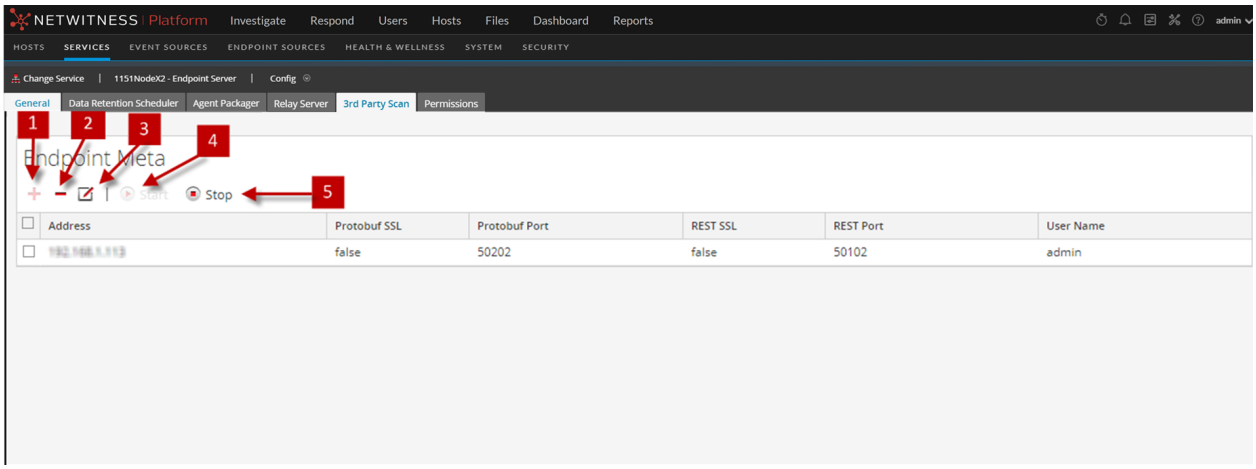
What do you want to do?

User Role	I want to ...	Show me how
Administrator	Configure Endpoint Metadata Forwarding for the NetWitness Endpoint Agents*	Configuring Metadata Forwarding

*You can perform this task in the current view

Quick Look

The following figure is an example of the General tab.



1 Click + to view the Available Services dialog.

2 Click − to delete the added service.

3 Click to edit the information for the added service.

4 Click Start to start the Endpoint metadata forwarding.

5 Click Stop to stop the Endpoint metadata forwarding.

The following table describes the fields in the General tab.

Field	Description
Address	Displays the IP address of the Log Decoder.
Protobuf SSL	Indicates if SSL is enabled on Protobuf. By default, this option is disabled.
Protobuf Port	Displays the port used for Protobuf. By default, the port is 50202.
REST SSL	Indicates if SSL is enabled on the REST port in the Log Decoder. By default, this option is disabled.
REST Port	Displays the port used for REST communication. The default value is 50102 (for non-SSL) and value 56102 (for SSL).
User Name	Displays the user name.
Raw Data	Sends a brief summary of the session along with the metadata if enabled. By default, this option is disabled.

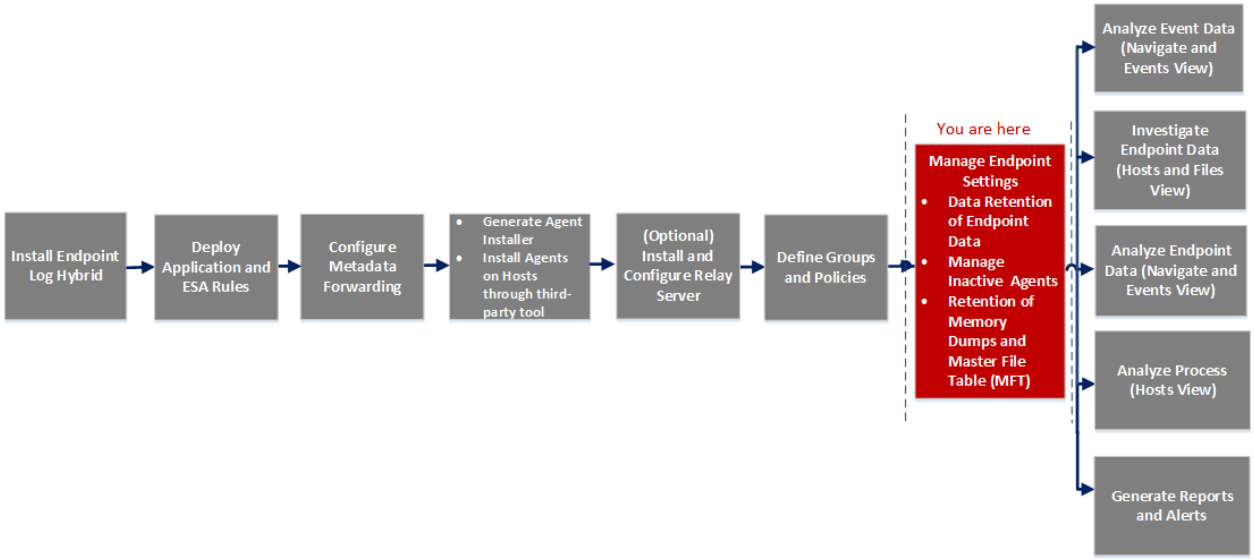
Data Retention Scheduler Tab

In the **Data Retention Scheduler** tab, you can configure data retention, inactive agents, and downloaded data retention 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



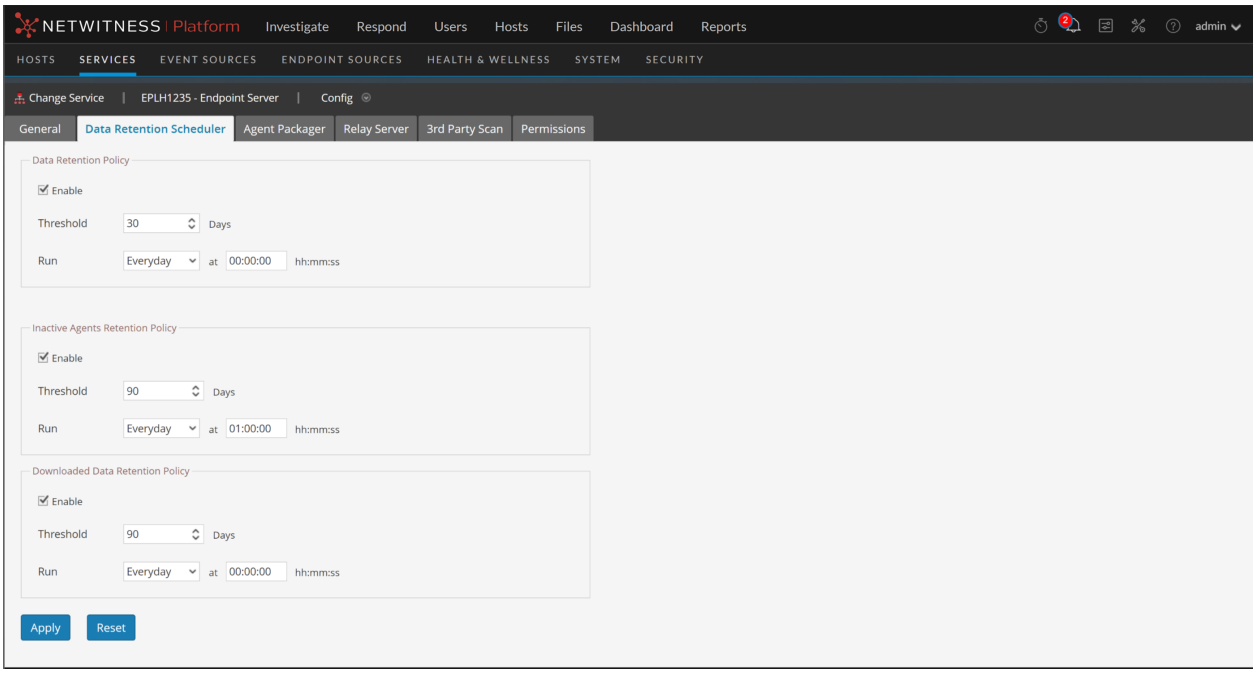
What do you want to do?

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

*You can perform this task in the current view

Quick Look

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



Features

The following table lists the fields for **Data Retention Policy**.

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

The following table lists the fields for **Inactive Agents Retention Policy**.

Fields	Description
Enable	Enables the configuration for the Inactive Agents Retention Policy. By default, this option is enabled.

Fields	Description
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.

The following table lists the fields for **Downloaded Data Retention Policy**.

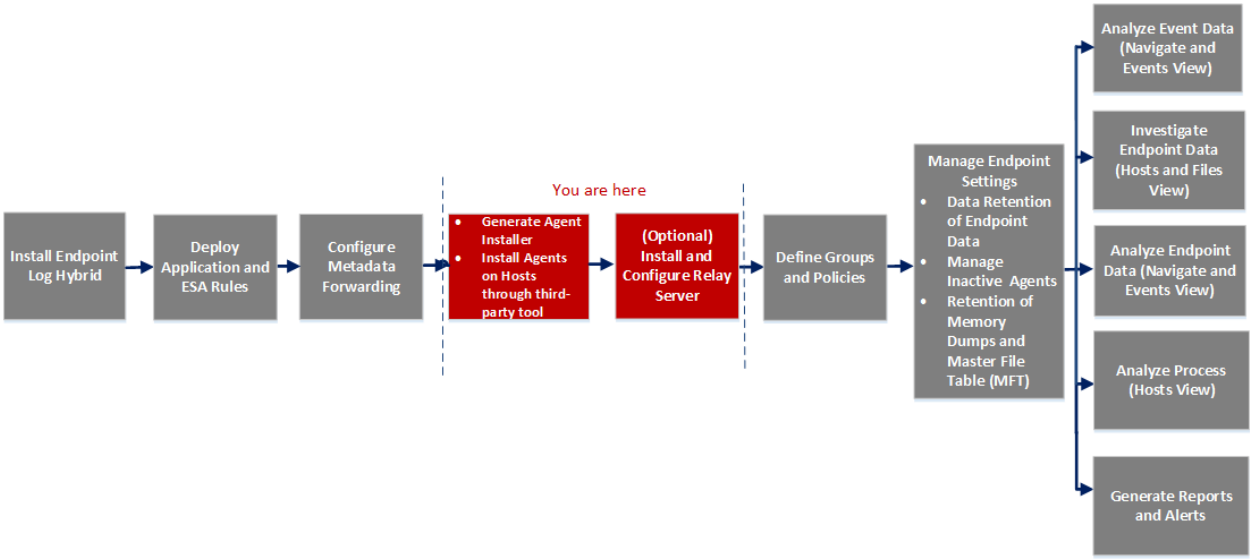
Fields	Description
Enable	Enables the configuration for the Downloaded Data Retention Policy. By default, this option is enabled. **Note:** The downloaded data can be Files, Process Dump, System Dump, and MFT.
Threshold	Displays the number of days the downloaded data is retained in the Endpoint Server. By default, the Threshold is set to 90 days. The data older than 90 days is deleted from the Endpoint Server.
Run	Displays the schedule for running the 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 retention policy and applies the new schedule immediately.
Reset	Resets the schedule to the default settings.

Agent Packager Tab

In the **Agent 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



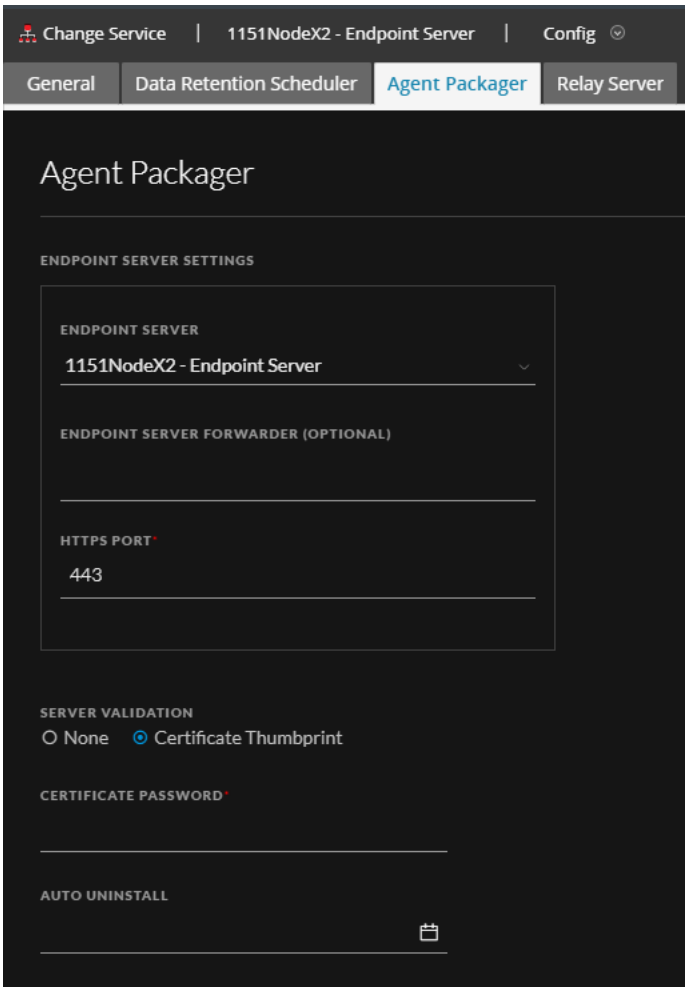
What do you want to do?

User Role	I want to ...	Show me how
Administrator	Generate an Agent Packager for Endpoint Data Collection*	*NetWitness Endpoint Agent Installation Guide*
Administrator	Generate an Agent Installer*	
Administrator	Install and Configure Relay Server*	*NetWitness Endpoint Configuration Guide*

*You can perform this task in the current view

Quick Look

The following figure is an example of the Agent Packager tab.


Change Service | 1151NodeX2 - Endpoint Server | Config
General
Data Retention Scheduler
Agent Packager
Relay Server
Agent Packager
ENDPOINT SERVER SETTINGS
ENDPOINT SERVER
1151NodeX2 - Endpoint Server
ENDPOINT SERVER FORWARDER (OPTIONAL)
HTTPS PORT*
443
SERVER VALIDATION
None
Certificate Thumbprint
CERTIFICATE PASSWORD*
AUTO UNINSTALL

Relay Server Tab

In the **Relay Server** tab, you can download and configure Relay Server . 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 **Relay Server** tab.

Workflow

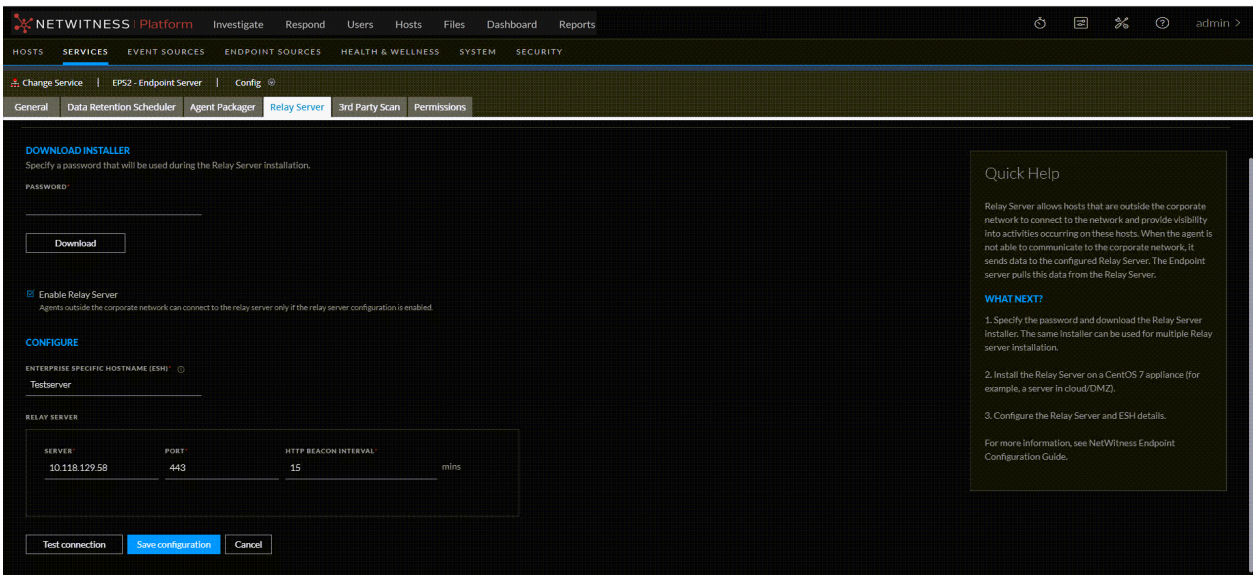
What do you want to do?

User Role	I want to ...	Show me how
Administrator	Install Relay Server*	(Optional) Installing and Configuring Relay Server
Administrator	Configure Relay Server*	(Optional) Installing and Configuring Relay Server

* You can perform this task in the current view.

Quick Look

The following figure is an example of the Relay Server tab.



Features

The following table lists the fields for Relay Server tab.

Field	Description
Download Installer	
Password	Enter the relay server installation password. For example, netwitness. Password must be minimum of 3 characters and can contain alphanumeric and special characters. **Note:** You must provide the same password when prompted during Relay Server installation.
Download	Click to download the Relay Server installer.
Enterprise Specific Hostname (ESH)	Enter the hostname which can be resolved only within the corporate network.
Enable Relay Server	Check Enable Relay Server for Agents outside the corporate network to connect to the configured relay server. By default, this option is disabled.
Configure	
Server	Hostname or IP of the Relay Server.
Port	Port number. For example, 443.
HTTP Beacon Interval	Enter the Interval value ranges from 60 – 1440 minutes.
Test Connection	Click test connection to check if the relay server is reachable by the agents.

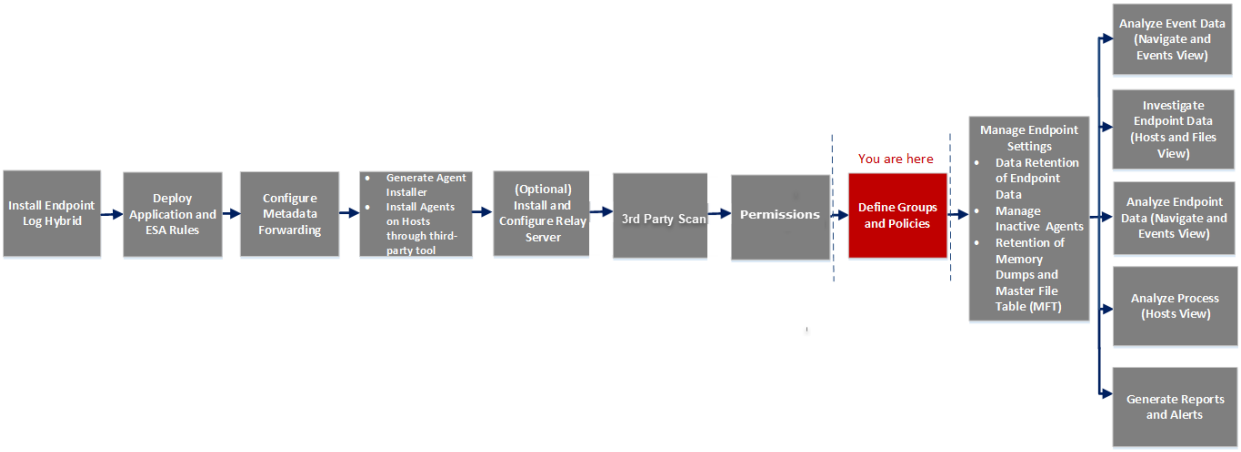
Field	Description
Save Configuration	Saves the relay server configuration.
Cancel	Cancel the unsaved changes.

Endpoint Sources - Groups

Note: The information in this topic applies to NetWitness 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*	Managing 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

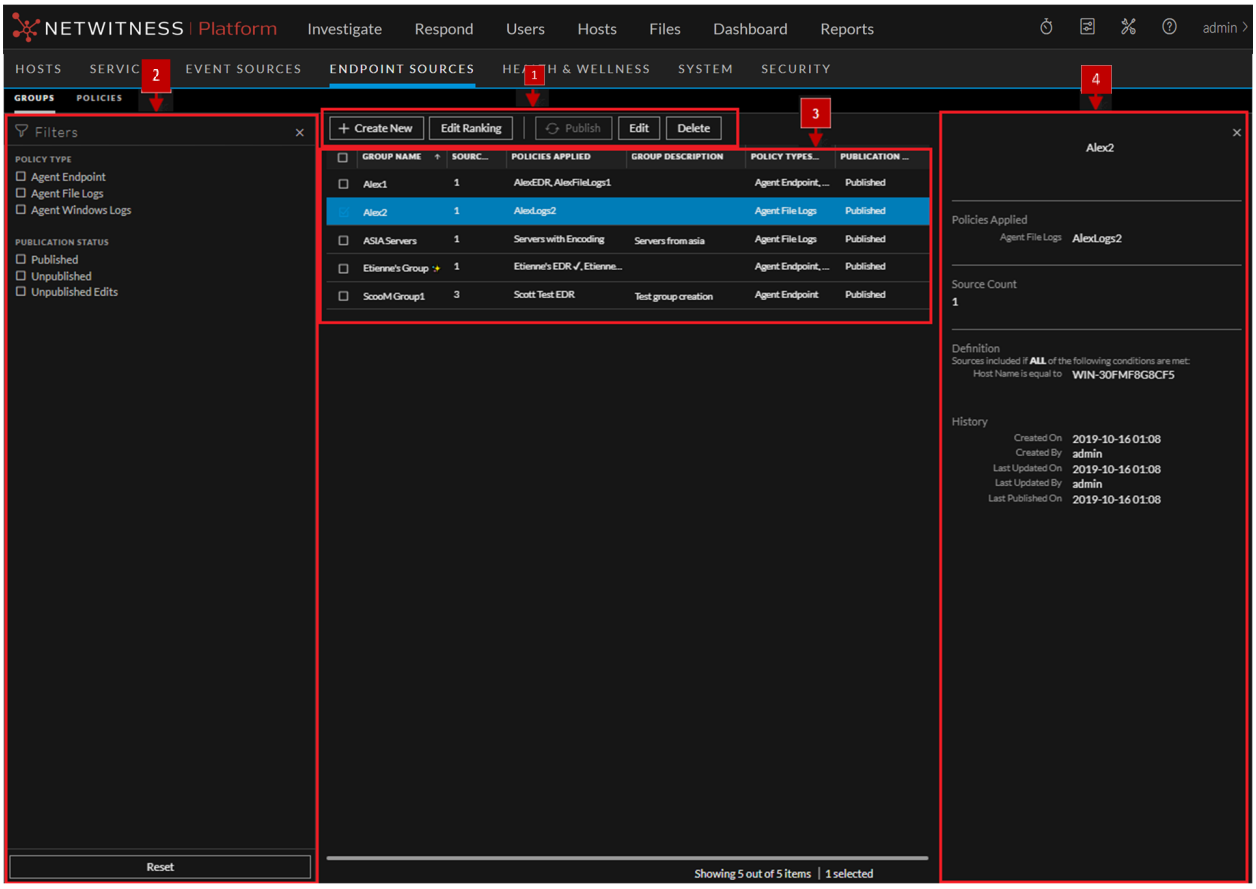
*You can perform this task in the current view.

Related Topics

- Endpoint Sources
- Managing Policies

Quick Look

Below is an example of the Groups tab:



1 **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 Managing 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 **Filter Pane**

- **Filters**: You can filter groups based on Policy 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 **Groups List Pane**

- **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.
- **Policy Types Applied:** Type of policies applied to the group: Agent Endpoint, Agent File Logs, Agent Windows Logs, or any combination of these.
- **Publication Status**: Status of the group - Published or Unpublished.

You can also sort on any column. If you mouse over a column header, a sort icon is displayed:  . Click the icon to sort by the selected column.

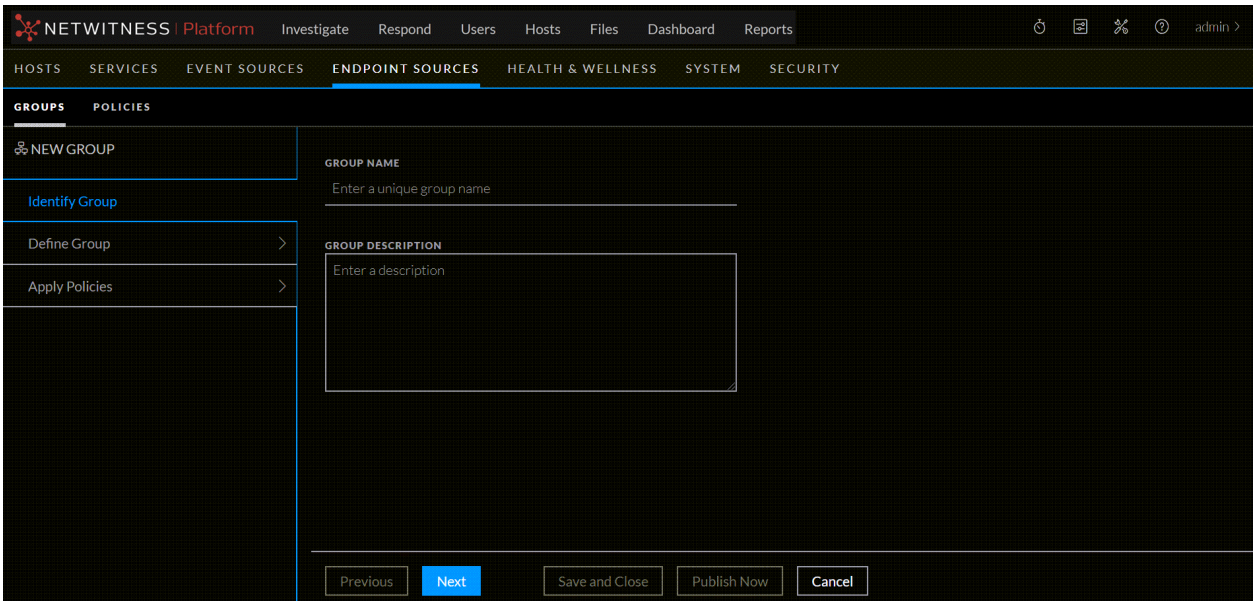
4 **Group Details Pane**

Displays the properties of the selected group.

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

Create Group

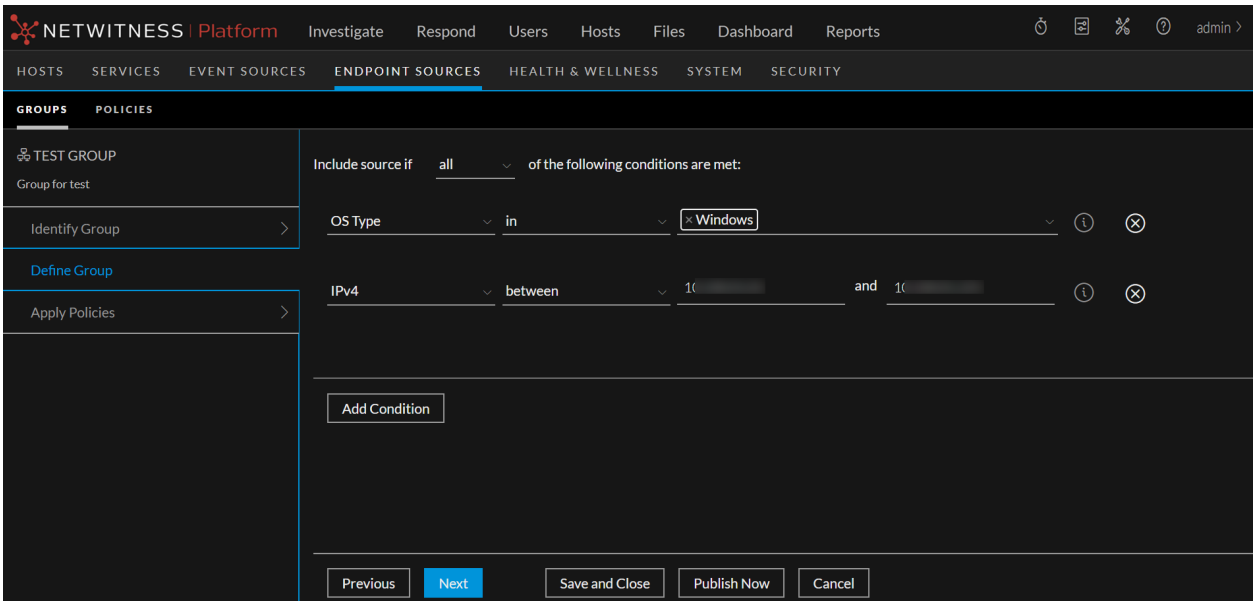
Below is an example of the Create Group dialog. The table describes the information and options in the Create Group dialog.



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.

Define Group

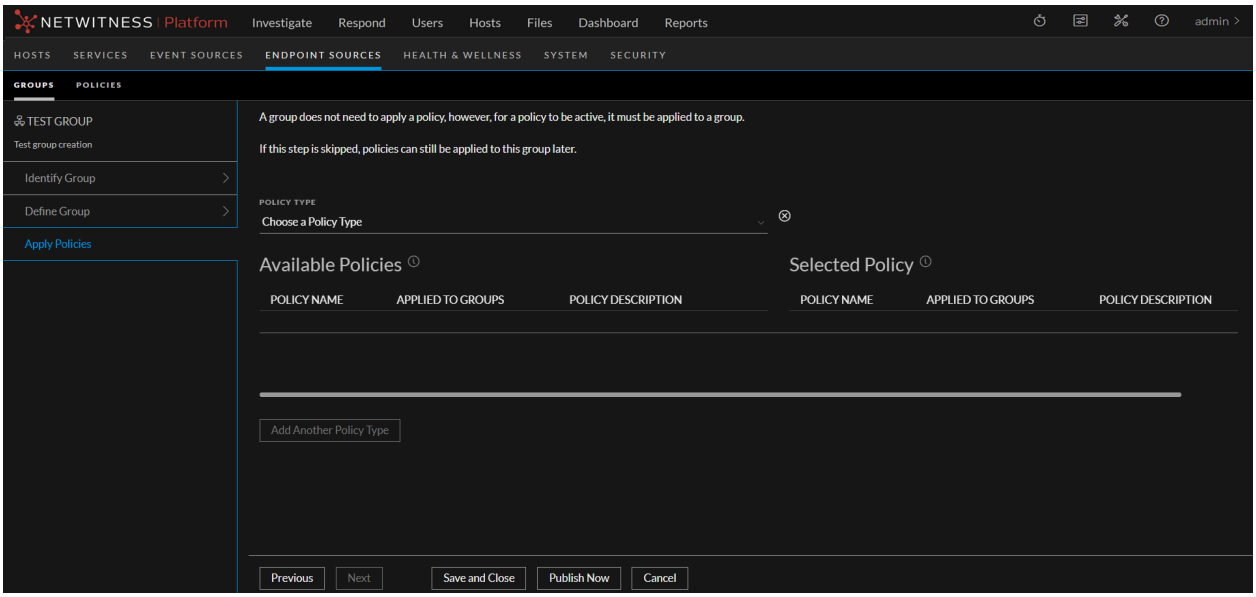
Below is an example of Define Group panel. The table describes the information and options in the Define Group panel:



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	The parameter can be OS Type, OS Description, Host Name, IPv4, IPv6, Machine OU, Tag, and Subnet. • 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. • Machine OU - Name of the Machine OU. Available operators are: **is equal to**, **contains**. For example, OU=Win10, OU=Contractors, DC=corp, DC=com • Tag - Name of the tag that already exists. Available operators are: **is equal to**, **contains**, and **in**. • Subnet - The value of the Subnet Mask. Available operator is: **in**. **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.
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. **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.
Add condition	Lets you add another condition.

Apply Policies

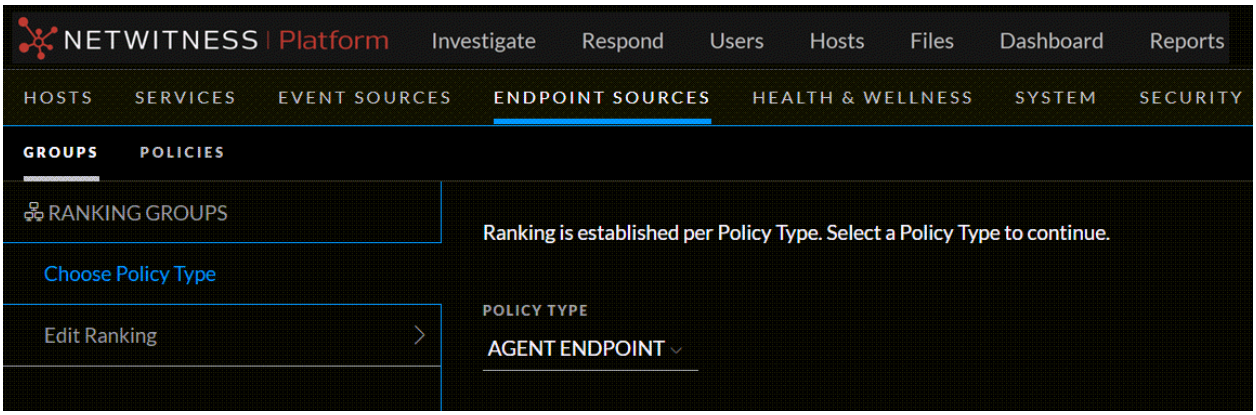
Below is an example of Apply Policies panel. The table describes the information and options in the Apply Policies panel:



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.
Publish Now	Publishes the created group.

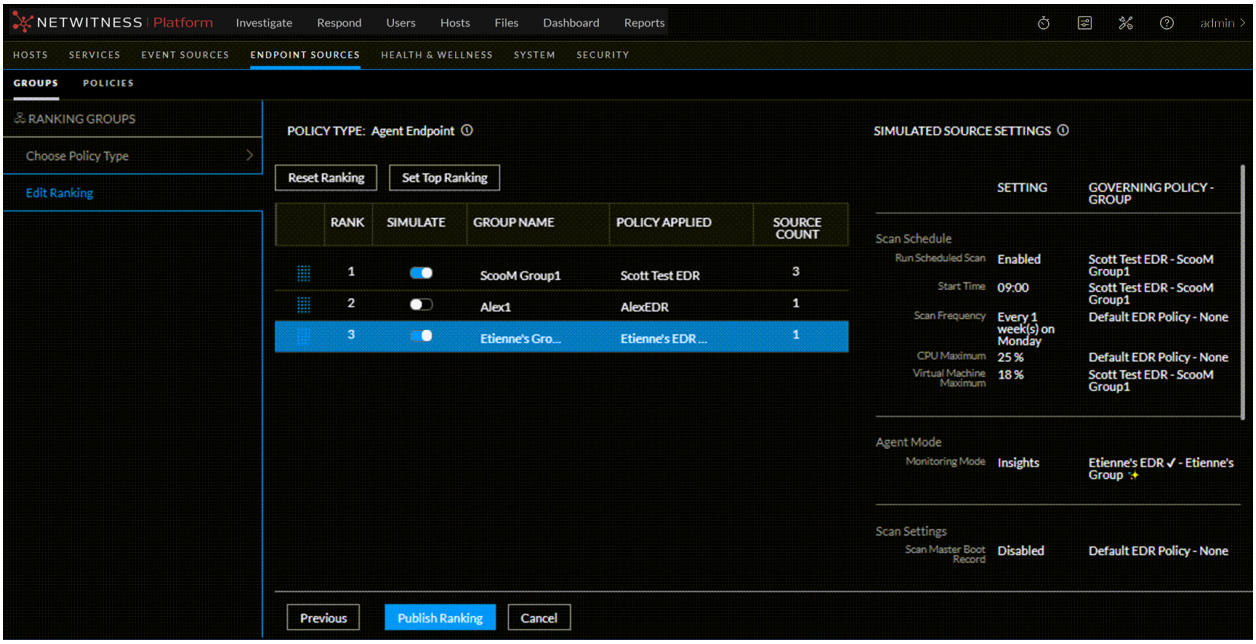
Ranking Groups

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.



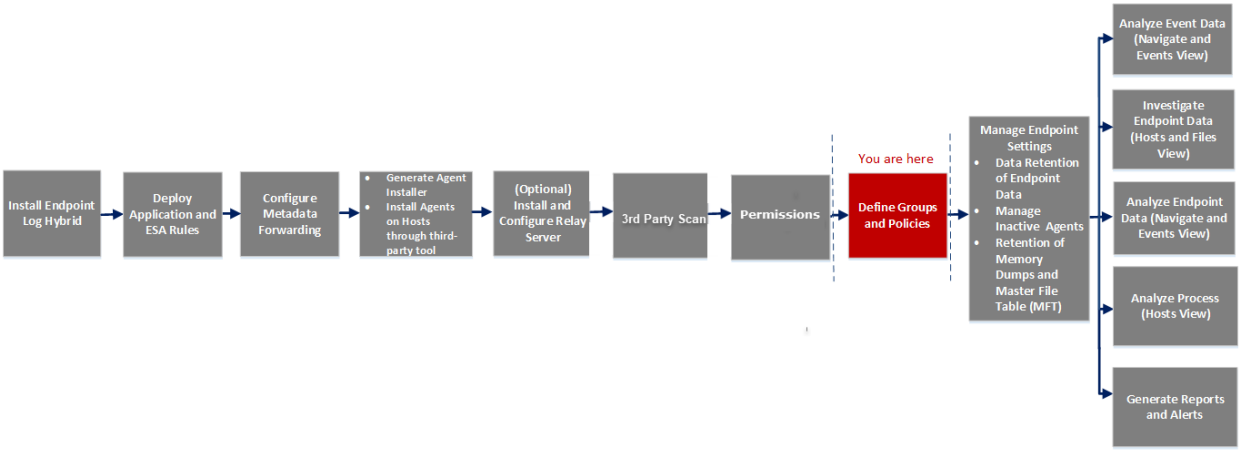
From this panel, you can do the following:

- Drag the group up or down to change the priority. Priority decreases from top to bottom.
- Turn the Simulate slider on or off, to simulate your policy settings and how they affect the endpoints within their groups. For more details, see Simulation Examples.
- Use the available buttons to perform actions:
  - **Reset Ranking**: Resets the ranking to the original order.
  - **Set Top Ranking**: Moves the selected group to the top.
  - **Previous**: Navigates to the Choose Source Type panel.
  - **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

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	Managing 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	create a File Log policy*	Create a File Log Policy
Administrator	edit policies*	Edit a Policy
Administrator	delete policies*	Delete a Policy

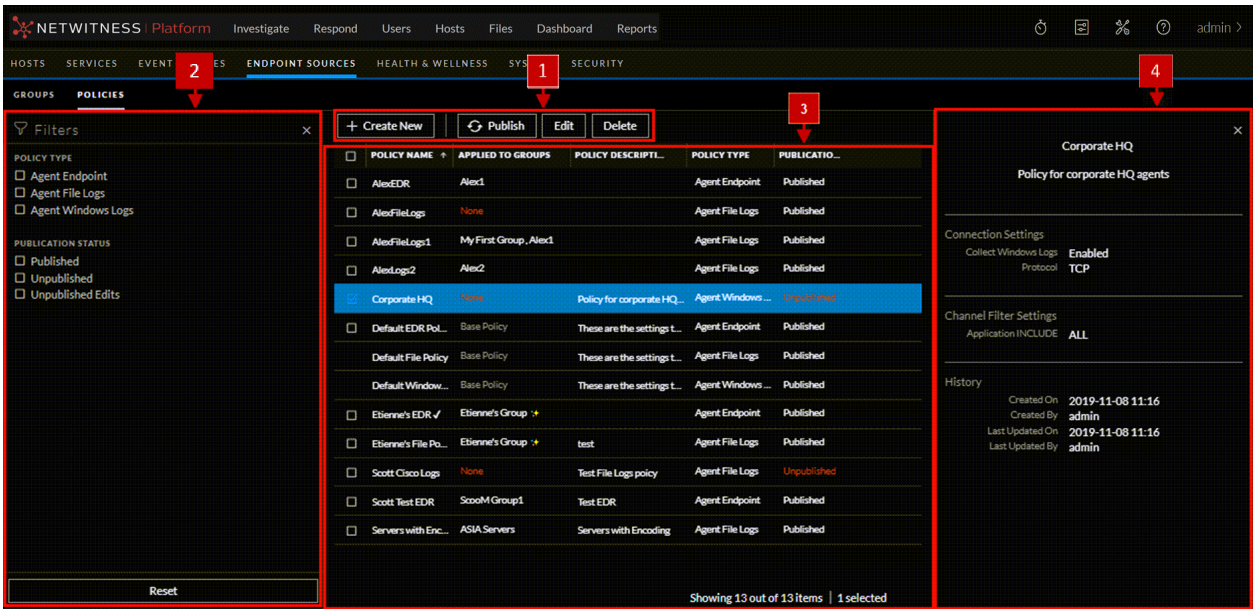
*You can perform this task in the current view

Related Topics

- Endpoint Sources
- Managing Groups

Quick Look

Below is an example of the Policies tab:



1 **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.

2 **Filter Panel**

- **Filters**: You can filter policies based on Policy 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.

3 **Policies List Panel**

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**: Displays the first portion of the description.
- **Policy type**: Displays the policy type: Agent Endpoint, Agent File Logs, or Agent Windows Logs.
- **Publication Status**: Status of the policy: Published or Unpublished.

You can also sort on any column. If you mouse over a column header, a sort icon is displayed:  . Click the icon to sort by the selected column.

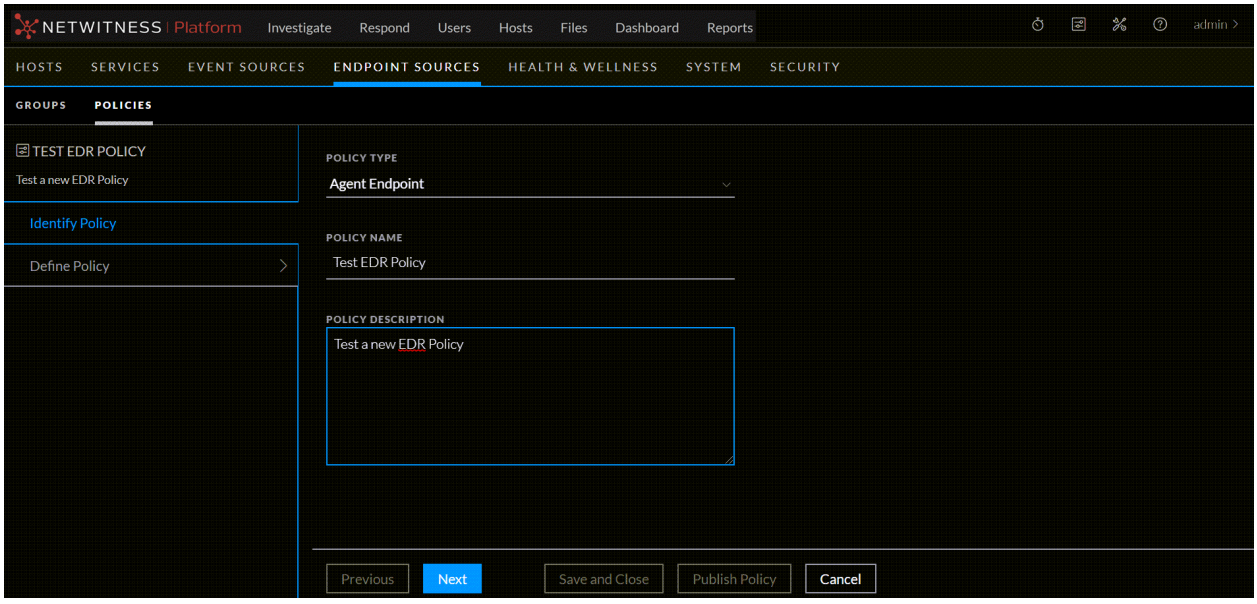
4 **Policy Details Panel**

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
Policy Type	Displays the type for the policy. Available options are Agent Endpoint, Agent File Logs, and Agent Windows Logs.

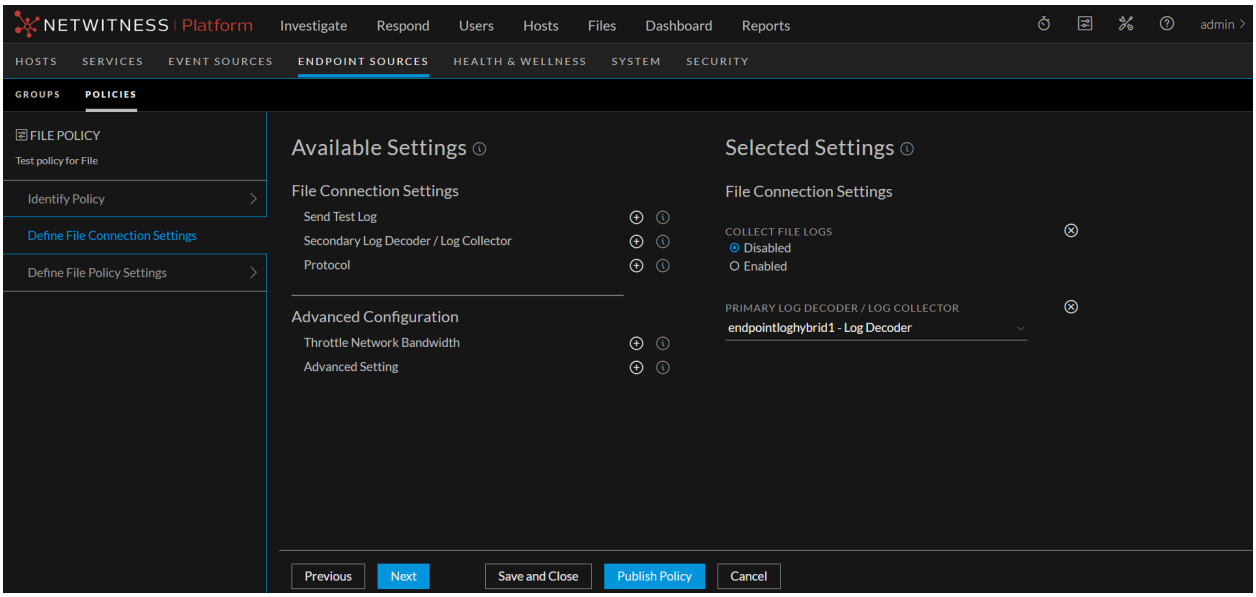
Field	Description
Policy Name	Name of the policy. The name should be unique.
Policy Description	Description of the policy. Description should not exceed 8000 characters.

Panels for Log File Policy

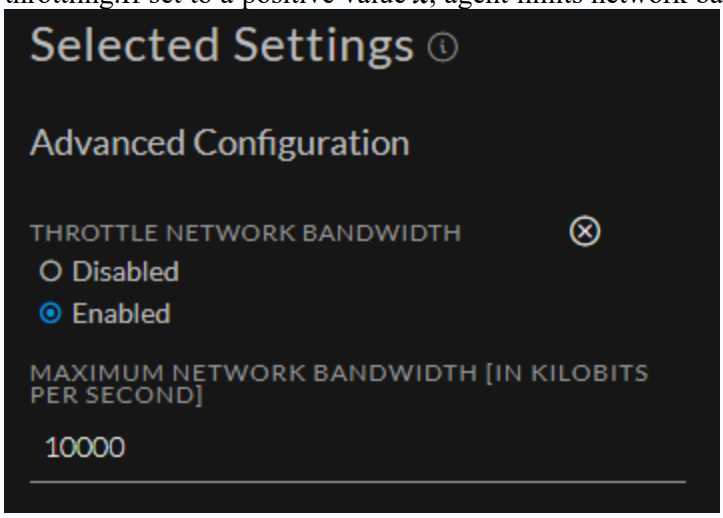
There are two panels for defining the parameters for an Agent Log File Policy: **Define Connection Settings** and **Define File Policy Settings**.

Define Connection Settings

Below is an example of Define Connection Settings panel. The table describes the information and available options.

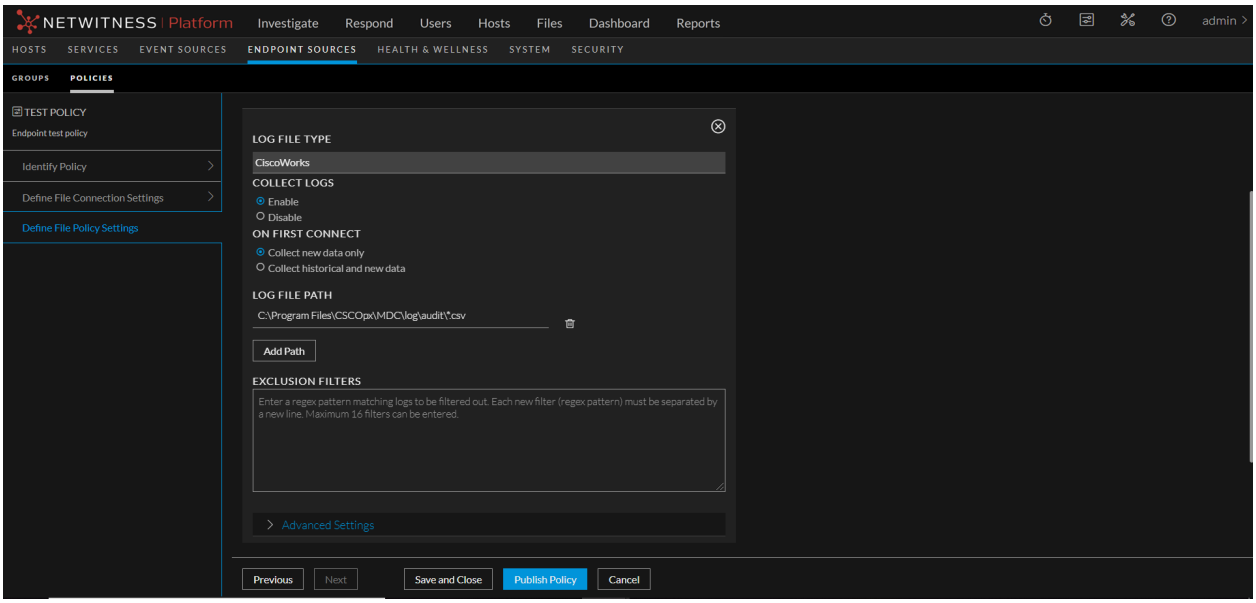


Field	Description
Collect File Logs	If enabled, the log file collection capability of the agent is activated. Logs are collected and forwarded to the NetWitness as they are generated. If disabled, no defined event source logs are collected. **Note:** This option must be enabled for any file event sources to be collected.
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.

Field	Description
Primary Log Decoder / Log Collector	The primary Log Decoder or Log Collector to which the collected file logs will be forwarded.
Secondary Log Decoder / Log Collector	If the primary Log Decoder or Log Collector is not reachable, collected file logs are forwarded to the secondary Log Decoder or Log Collector. **Note:** The NetWitness cannot detect failures when UDP protocol is used.
Protocol	Select the transport protocol that is used to forward the collected file logs to the NetWitness servers. The following options are available: • SSL: Recommended, but also the most resource-intensive option. • TCP: Sends the logs in clear text over a reliable TCP connection. May be acceptable within a corporate network. • UDP: Sends the log in clear text over a non-guaranteed UDP connection. This is the least resource intensive option. **Note:** Resource intensity is dependent upon the Log Decoder, since there is only a single connection per agent.
Advanced Configuration	
Throttle Network Bandwidth	Use this setting to limit network bandwidth that the Agent uses to connect to NetWitness. This setting is disabled by default: click **Enabled** to turn it on, and then enter a value in kilobits per second.If not set, Agent does not do any network throttling.If set to a positive value ***x***, agent limits network bandwidth to ***x*** kbps. 

Field	Description
Advanced Setting	**Caution:** It is strongly recommended not to use this setting unless advised to do so by NetWitness.

Define File Policy Settings



Field	Description
Log File Type	From the drop-down menu, select the type of event source to be monitored. The list of available event source is based on all the event source types defined on your NetWitness. You can add event source types using the Live Services module. For details, see "Find and Deploy Live Resources" in the *Live Services Management Guide*.
Collect Logs	If enabled, log files for this file type instance are collected and forwarded to the NetWitness. File collection must be enabled on each source applying this policy for these specific logs to be collected.
On First Connect	Determines whether the NetWitness Agent collects all logs or only newly created logs located in the specified paths upon initial collection. In both cases, new logs are collected. **Note:** Historical logs cannot be collected after an agent has begun collecting logs.

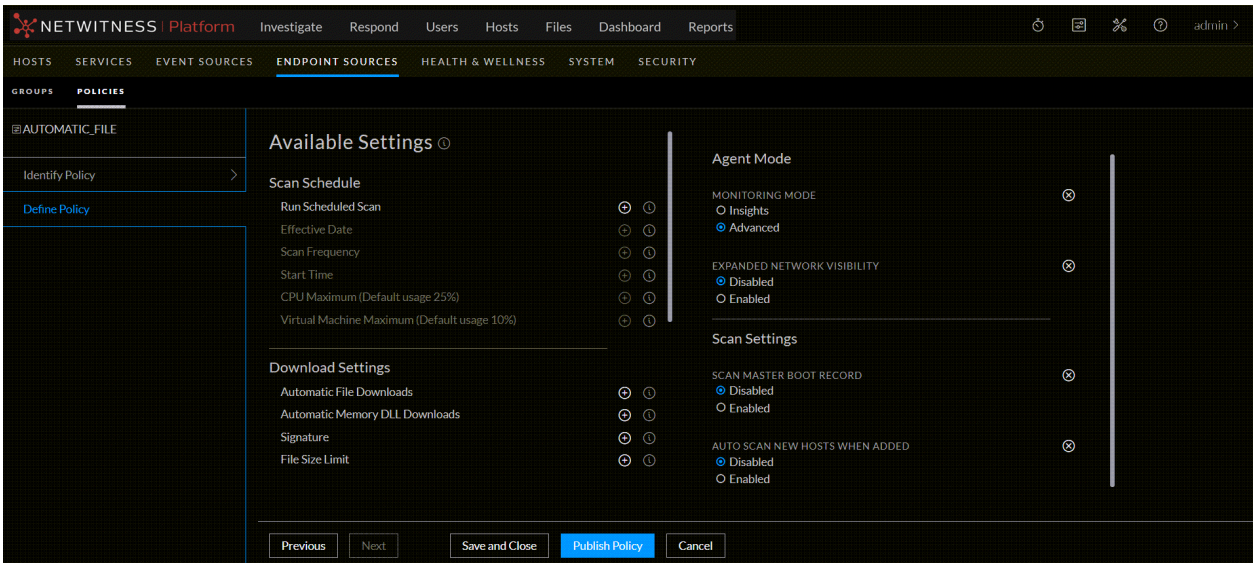
Field	Description
Log File Path	One or more paths to be used by the agent to locate the log files. Represents the location of the log files to be read. **Note:** The Path value cannot end at a directory—the final portion of the path must represent a file name or set of files (using wildcard characters). You can use wildcards for both files and directories. Each source is limited to entry of 16 paths. This setting must include a path and a file spec. For example: `C:\Program Files\apache-tomcat-*\logs\*.log`. In this case, the file spec is all files with a ".log" extension in the specified path. If you cannot use wildcards to specify multiple files, you can add additional paths to accommodate the differences in path locations on a specific endpoint agent. This might be due to installation locations or version information. Only the paths with valid locations and files on the specific endpoint agent are used, and the others are ignored. For many event source types, there is a default path. If so, you only need to enter a path if the log files are not stored in the standard directory for that event source type. **Note:** This can be a standard Windows pathname (such as `C:\Program Files\Apache\error_logs\logfile.log`) or a UNC (Universal Naming Convention) pathname (`\\host-name\share-name\file-path`). For more details about UNC paths, see Endpoint Sources - Policies below.
Exclusion Filters	An optional list of regex patterns which can be used to filter out any logs that match the patterns. Each separate filter should be entered on a new line. Each source is limited to 16 exclusion filters. **Note:** Each filter needs to be entered as a valid regex string, or the system does not allow you to save it.
Advanced Settings	

Field	Description
Source Alias	Optionally, enter a hostname, IPv4 or IPv6 address to identify individual sources. This is recommended when there are two or more sources of the same type on the same server: For example, a server that runs two instances of Apache web server. **Note:** This value only rarely needs to be entered. One example is if you have more than one Web Server, and they are running different Apache servers. Note the following: • If you enter a value for this parameter, the event source is applicable to a single Endpoint server. • This optional address or hostname is included in the meta for any logs originating from this source. This can be used by analysts to assist in identifying the source. • Set a value for this parameter if two sources of the same event source type are configured in the same policy. • This setting is not commonly needed: it is only useful if the policy is only applied to a single endpoint.
File Encoding	Specifies the type of character encoding of the log files. If **Local Encoding** is selected, the NetWitness Agent uses the default encoding of the Windows machine upon which it is running. This setting must match the encoding of the log files, or they will not be processed correctly. **Note:** UTF-8/ASCII is recommended (and the default). UTF-8 is a super-set of ASCII Note that all logs are re-encoded to UTF-8 before being sent to the NetWitness.

For a list of the currently supported types, see Currently Supported File Log Event Source Types.

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:



Settings	Description
	Scan Schedule
Run Scheduled Scan	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 **Hosts** view. **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.
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.
Scan Frequency	Determines how often the scheduled scan runs on a host. By default, this is set to every 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. Select Days or Weeks: • 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	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.

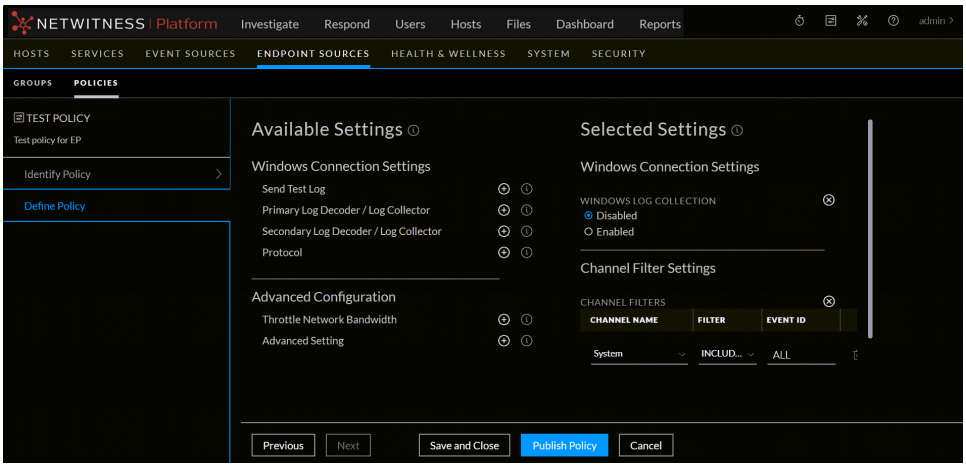
Settings	Description
CPU Maximum	Amount of CPU the agent can use to run scheduled scans on physical hosts. By default, the value is set at 25%. Increasing the CPU maximum increases the speed of scan snapshot retrieval. Drag the slider to specify the maximum CPU usage by the created policy. Minimum value 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.
Virtual Machine Maximum	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. 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.
Agent Mode	
Monitoring mode	Allows you to specify whether an agent should operate in Insights (free) or Advanced mode (license). By default, it is set to Advanced.
Expanded Network Visibility	Enables network tracking and monitoring on Windows hosts in Insights mode. **Note:** For network tracking in Insights mode, verify that the Windows Management Instrumentation (WMI) service should be enabled. It also optimizes the frequency of agents sending network events for network packet correlation for both Insights and Advanced modes. By default, this option is disabled.
Scan Settings	
Scan Master Boot Record	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.
Auto Scan New Systems When Added	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 **Hosts** view until a manual or scheduled scan is run on these hosts. Existing hosts will not be affected. **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.
Download Settings	
Automatic File Download	Automatically download the files to the NetWitness Endpoint Server based on the file size and signature. If a file is present on multiple hosts or multiple Endpoint Servers, only one instance of the file is downloaded. By default this option is enabled.

Settings	Description
Automatic Memory DLL Downloads	In latest version, all memory DLLs that are detected during a scan, will be automatically downloaded regardless of the file size. This option is enabled by default.
Signature	Limits the download of files based on the signature. The options are : • Exclude All Signed - Downloads all the unsigned files to the NetWitness Endpoint Server and exclude all the signed files. • Exclude only Microsoft and Apple signed - Downloads all the unsigned files and exclude the files signed by Microsoft and Apple. • Include All- Downloads all the signed and unsigned files. **Note:** . In case of Linux, **Exclude all signed** and Exclude **Microsoft and Apple** signed options will download the files that are not part of any installed RPMs or files which are part of RPM but the hashes does not match with RPM.
File Size Limit	Limits the download of files based on the file size. The File size should be between 1 KB and 10 MB. By default, file size lesser than or equal to 1 MB are downloaded automatically.
Response Action Settings	
Blocking	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. **Note:** Blocking is only supported on Windows agent (in Advanced mode) with NetWitness latest version.
Network Isolation	Allows an analyst to block hosts that are compromised from connecting to the network. This controls the spread of an attack and help analyze the malware behavior after the network isolation. All attempted network connections are monitored and reported to the Endpoint Server. By default, this option is disabled. **Note:** Network isolation is only supported on Windows agent (in Advanced mode) with NetWitness latest version.
Endpoint Server Setting	
Endpoint Server	Displays all available Endpoint servers in the deployed. **Note:** If you do not select an Endpoint Server, the agent uses the default Endpoint Server that is configured during packager generation.
Server Alias (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.

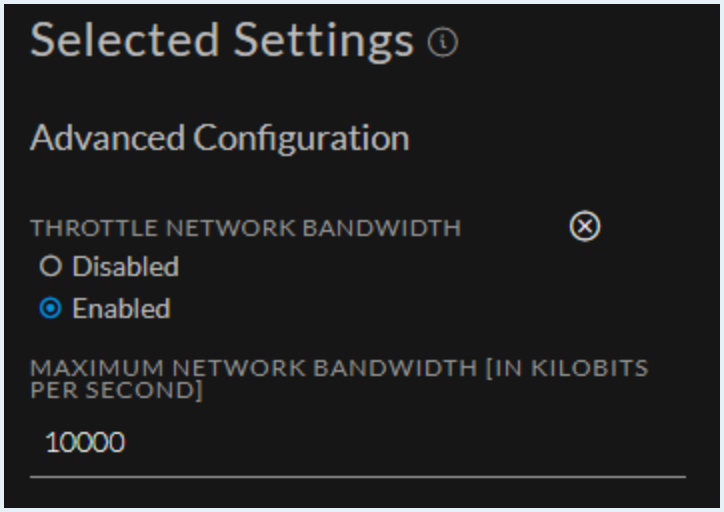
Settings	Description
HTTPS Port	Port number used for HTTPS communication. By default, the port is set to 443. If you want to change this port, make sure that it matches the server configuration. If you enter the wrong port, the agents can no longer communicate with the Endpoint server and the system will be non-functional.
HTTPS Beacon Interval	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.
UDP Port	Port number used for UDP communication. By default, the port is set to 444. 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.
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.

Settings	Description
Primary Log Decoder / Log collector	Primary NetWitness 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. **Note:** NetWitness cannot detect failures when UDP protocol is used.
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	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. 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.
Advanced Configuration	
Throttle Network Bandwidth	Use this setting to limit network bandwidth that the Agent uses to connect to NetWitness. This setting is disabled by default: click **Enabled** to turn it on, and then enter a value in kilobits per second. • If not set, Agent does not do any network throttling. • If set to a positive value ***x***, agent limits network bandwidth to ***x*** kbps. 

Settings	Description
Advanced Setting	**Caution:** It is strongly recommended not to use this setting unless advised to do so by NetWitness.

Troubleshooting

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

Agent Communication Issues

Issue	Agent **Last Seen Time** column is not updated in the UI.
Explanation	The issue could be due to any one of the following: • Agent is inactive • Agent data is not processed if the **Endpoint.Health.Overall-Health** statistic shows **Unhealthy** due to which all the agent data including agent last seen time is not updated.
Resolution	See the resolution for these statistics in the Health and Wellness Issues section.

Issue	Agent is unable to communicate with the Endpoint Server.
Explanation	This could be due to one of the following reasons: • Agent is inactive. • Endpoint Server settings is incorrect in the agent packager or policy configuration, or not available for communication. • Endpoint Server or Nginx Server is not running . • Firewall or IP table rules are blocking the connection between the host and Endpoint Server.
Resolution	• Check if the Endpoint Server and Nginx Server are reachable. • If the Endpoint Server settings are incorrect, uninstall the agent, download the agent packager, 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 `<service.exe>` (name provided in the packager, by default, the service name is `NWEAgent.exe`) file in the antivirus suite.

Issue	You want to change the responsiveness of the Agent.

Explanation	Depending on your installation, you can adjust Beaconing 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.

Issue	Agent is unable to generate network tracking events in Insights mode.
Explanation	Verify that Windows Management Instrumentation (WMI) service is running.
Resolution	• Run `Services.msc` and look for Windows Management Instrumentation (WMI) service. • Go to properties and change the **Startup type** to Automatic.

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.

Health and Wellness Issues

Endpoint Issues

Behavior	The health check of the **Endpoint.Health.Overall-Health** statistic shows **Unhealthy**.
Issue	Endpoint Server service or required resources are not available or not in a usable state. This could be due to one of the following reasons: • Unable to forward Endpoint meta data to the Log Decoder. • Endpoint Log Hybrid disk usage reaches the specified limit. • Mongo DB is down or excessive read and write errors during processing.
Resolution	• For Log Decoder issue, see Log Decoder Issues section. • For disk usage and Mongo DB issues, see Disk Usage and Mongo Issues section.

Disk Usage and Mongo Issues

Behavior	The health check of the **Data.Application.Connection-Health Application**, **Data Store Disk Usage** or **Data Persistence** for Endpoint Server shows Unhealthy.
Issue	• **Data.Application.Connection-Health Application** or **Data Persistence** shows Unhealthy, if Mongo service is down or fails due to authentication. • **Data Store Disk Usage** shows **Unhealthy**, if Endpoint Server Mongo storage size has exceeded the threshold. By default, the server automatically delete the old data when it reaches 80% of the disk space.
Resolution	• For **Data.Application.Connection-Health Application** or **Data Persistence** issue, you must check the Endpoint server logs (`/var/log/netwitness/endpoint-server/endpoint-server.log`) and Mongo logs (`/var/log/mongodb/mongod.log`), and: ◦ If the issue is due to authentication, you must reissue the certificate. For more information, see "Service Certificate Reissue" section in the *System Maintenance Guide*. ◦ If the issue is due to Mongo service is down, you must restart the Mongo. • For **Data Store Disk Usage** issue, you must increase the storage or configure data retention settings to clear the old data. For more information, see Configuring Data Retention Policy.

Log Decoder Issues

Behavior	Endpoint metadata is not available in the **Investigate > Navigate** or **Events** view.
Issue	The health check of the **Log Decoder Buffer** and **Meta Forward** shows **Unhealthy** in the Health and Wellness.
Explanation	The issue could be due to any of the following reasons: • Log Decoder capture is not started. • Concentrator aggregation is not started. • Log Decoder connection issue. • Log Decoder buffer usage is beyond the specified limit.
Resolution	Make sure that: • Capture is enabled on the Log Decoder. • Aggregation is enabled on the Concentrator. • Meta forwarding is configured properly.

	Note: Make sure **Capture Autostart** is enabled in the Service Config view for Log Decoder and **Aggregate Autostart** is enabled in the Service Config view for Concentrator.

File Log Policy Issues

Invalid Policy or Bad Connection Issues

Issue	Policies can be invalid for a variety of reasons. Some examples: • No sources found if the policy is enabled. • Invalid or missing typespec file • No destination is reachable for a file log policy event source type Additionally, if capture is stopped on the destination Log Decoder, Endpoint Agents will send an error to the Endpoint Server saying that they failed to connect. Also, if there is a lot of data to be processed for Agents collecting File data (when File Policy is enabled) , there is a possibility that Log Decoder buffer becomes full. If this happens, the Log Decoder cannot process any requests from the Agents communicating via EPS.
Explanation	The system is dynamic in nature, which means its state can change: event sources can lose their connection, typespec files can be altered or deleted, and other changes can occur that can invalidate a previously valid policy.
Resolution	To help identify the specific issue, check the log file on the Endpoint Server that reports the error: `/var/log/netwitness/endpoint-server/endpoint-server.audit.log` Relevant errors will be listed as **FileLogError** in the log file. If you experience this issue, you can do the following: 1. Try to identify and target higher-value data, thus limiting the total amount of data being processed. 2. Enable throttling in the File policy to smooth out the peaks in usage. 3. If you really do need to process more data on a regular basis, consider server-side hardware upgrades.

Reset File Collection Bookmarks

Issue	If the system is not configured correctly, NetWitness might collect logs and not be able to parse them. Or, files might get sent, but for some reason, not make it to the Log Decoder (for example if communication is via UDP and there is a network connectivity issue).

	In these and other cases, you can reprocess these "missing" log files.
Explanation	For whatever reason, you may need to reprocess logs from the beginning of the file.
Resolution	Reset bookmarks for an event source type using the procedure described here: Reset File Collection Bookmarks.

Missing Log Collectors and Event Sources in the User Interface

Issue	Some log collectors or event sources seem to be missing from the list of available items.
Explanation	The Filter drop-down menus (types, log collectors, and log decoders) only show values that are in the event sources database, rather than all possible values. For example, if you have a log collector that has not yet collected any logs, then it is missing from the list.
Resolution	Collect logs from a specific log collector and event source, and then they should appear as items in the appropriate menu.

Relay Server Issues

Test Connection Issues

Issue	Relay Server test connection failed.

Resolution	1. Check if the hostname or IP and port of the Relay Server are correct.
	2. Make sure that the hostname or IP of the Relay Server is resolvable from the Endpoint Server. Perform the following:
	a. In the Endpoint Log Hybrid console, verify if the Relay Server is reachable using the following command:
	`nc -zvw3 <relayhost> <relayport>`
	If the Relay Server is not reachable contact your Administrator.
	b. If the Relay Server is reachable, verify if the correct Relay Server installer is used by getting the Endpoint Server revision ID from the Relay Server host (`/var/log/relay-install.log`) and check the Endpoint Server RPM on Endpoint Log Hybrid using the following command:
	`rpm -qa | grep <Endpoint Server Revision ID>`
	c. Make sure if the Relay Server is installed and running.
	• Verify the Relay Server installation logs using the following command:
	`/var/log/relay-install.log`
	• Verify the status of Relay Server using the following command:
	`systemctl status rsa-nw-relay-server`

Issue	Test fails when installing relay server in cloud, using CentOS 7 configuration

Resolution	1. Check if you have entered the suggested port numbers.
	2. If you have entered any other port number than the suggested one
	3. Make sure that the hostname or IP of the Relay Server is resolvable from the Endpoint Server. Perform the following:
	a. In the Endpoint Log Hybrid console, verify if the Relay Server is reachable using the following command:
	`nc -zvw3 <relayhost> <relayport>`
	If the Relay Server is not reachable contact your Administrator.
	b. If the Relay Server is reachable, verify if the correct Relay Server installer is used by getting the Endpoint Server revision ID from the Relay Server host (`/var/log/relay-install.log`) and check the Endpoint Server RPM on Endpoint Log Hybrid using the following command:
	`rpm -qa | grep <Endpoint Server Revision ID>`
	c. Make sure if the Relay Server is installed and running.
	• Verify the Relay Server installation logs using the following command: `/var/log/relay-install.log`
	• Verify the status of Relay Server using the following command: `systemctl status rsa-nw-relay-server`

Issue	Relay Server installer generation fails with an error message ‘Unable to download the installer. Retry after sometime’.
Explanation	Dependencies of the Relay Server are not resolved or downloaded completely.
Resolution	You must retry the download after 5-10 minutes. If the download still fails even after all dependencies are downloaded in the Endpoint Server, contact the NetWitness Customer Support. **Note:** You can check ‘Finished downloading all Relay Server dependencies’ message in the Endpoint Server logs at `/var/log/netwitness/endpoint-server/endpoint-server.log`, to see if the dependencies are downloaded. If the download fails due to yum related issues, then you must clean yum repo using the command `yum clean all` and restart the Endpoint Server.

Issue	After the removal of DNSMasq in 12.1 and later versions, test connection fails between the Endpoint server and relay server.
Resolution	For the test connection to succeed, perform the following.

	1. SSH to Endpoint server. 2. Edit the `/etc/nginx/conf.d/relay.conf` file and go to `resolver nw-node-zero ipv6=off;` line. 3. Replace `nw-node-zero` with the nameserver IP or hostname. 4. Run the following command to restart nginx service. `systemctl restart nginx` 5. Try **Test Connection** again.

Installation Issues

Issue	Relay Server installation fails due to missing or corrupted dependencies.
Resolution	Re-download the installer dependencies, perform the following: 1. Go to **(Admin) > Endpoint Server** service > select > **View** > **Explore**. 2. In the Endpoint server configuration, make sure **endpoint.relay.installer.download-on-restart** boolean is set to true (by default it is true). 3. Restart the Endpoint server using the following command: `systemctl restart rsa-nw-endpoint-server` Fresh dependencies will be downloaded to the local directory in the Endpoint Server. This may take few minutes. 4. Download the Relay Installer. 5. Run the Relay Server Installation Script. For more information, see (Optional) Installing and Configuring Relay Server.

YARA Issues

Issue	Failure in saving YARA configuration.
Explanation	The rule-folder path is under some Linux user home-directory such as /root or /home/user1.
Resolution	Choose other paths such as /var or /tmp etc. or change the owner of the directory to 'netwitness' user.

OPSWAT Issues

Files can not be scheduled for scan

Issue	Some files cannot be scheduled for the scan. See Endpoint Configuration Guide > Troubleshooting
Explanation	The issue could be due to any one of the following: 1. One of the endpoint servers is either down or not responsive. 2. OPSWAT is not configured in one or more of the endpoint servers.
Resolution	1. Ensure all the endpoint servers are up and running. 2. Ensure OPSWAT is configured in all the endpoint servers.

OPSWAT not configured on all endpoint servers

Issue	OPSWAT is not configured on appropriate Endpoint servers.
Explanation	The issue could be due to any one of the following: 1. OPSWAT is not configured in any of the endpoint servers. 2. One or more endpoint servers are down.
Resolution	1. Ensure OPSWAT is configured in all the endpoint servers. 2. Ensure all the endpoint servers are functioning.

OPSWAT scan results not getting updated

Issue	OPSWAT scan is scheduled successfully, but no results are getting updated.
Explanation	The issue could be due to any one of the following: 1. Either you have selected unsupported file extensions, or some files are larger than the configured file size limit. 2. OPSWAT server is either down or not responsive.
Resolution	1. Ensure only the files with supported extensions are selected, and file size has not exceeded the configured maximum file size. 2. Contact OPSWAT support for additional information.

Appendices

Reset File Collection Bookmarks

In cases where issues have caused logs to be lost, or not correctly sent to the Log Decoder, you can resend messages in log files by resetting the bookmarks for those log files.

Note: For security reasons, NetWitness does not allow resetting bookmarks from the agents. Rather, you must do so from an Endpoint Server.

The following procedure describes how to reset bookmarks for file collection logs.

Note: Currently, you can reset bookmarks for all sources or just one specific source, by providing a list in a JSON file.

Construct a JSON File to Identify Agents and Event Source Types for Reset

First, you need to construct a JSON file using the following structure:

```
{

     "agentIds": [],
     "sourceType" : ""

}
```

where:

- `agentIds`: a list of the IDs for one or more Endpoint Agents: these are the individual agents on which the source log files reside.
- `sourceType`: this is a list of the file event source type or types for which you want the log file bookmarks to be reset.

For details on finding agent IDs and source types, see How to Find Agent IDs and Source Types below.

For example, the following source code snippet could be used to delete bookmarks for **all** sources on 3 agents:

```
{

     "agentIds": ["43F27B6E-A02D-955A-9607-2DFC5D17B6E7",
        88AD4B2C-192B-B50E-A125-C05B801301AA"
        "3899038D-8F42-BC93-5BA7-ECBFC309D6A3"],
     "sourceType": "ALL"

}
```

Similarly, the following source code snippet could be used to delete bookmarks for **apache** sources on 3 agents:

```
{
```

```
    "agentIds": ["43F27B6E-A02D-955A-9607-2DFC5D17B6E7",
       88AD4B2C-192B-B50E-A125-C05B801301AA"
       "3899038D-8F42-BC93-5BA7-ECBFC309D6A3"],
    "sourceType": "apache"

}
```

Reset Bookmarks

Perform the following steps to reset the bookmarks that you specified in a JSON-formatted file:

1. SSH to the NetWitness Admin Server.
2. Run `nw-shell` command. for details about using the NetWitness shell, see the *Shell User Guide*, available in NetWitness Link.
3. After nw-shell starts, connect to an Endpoint Server service, using the following command:

   `connect --service endpoint-server.`*`serviceID`*

   where *serviceID* is identifier for the Endpoint Server that hosts the agents you are changing. See How to Find Endpoint Service IDs for details on how to retrieve the service ID.
4. Change to the directory where the reset command resides:

   `cd endpoint/command/reset-bookmark`
5. Login with an administrator account.
   a. Type the login command:

      `login`

   b. Enter the user name for your admin account.

   c. Enter the password for your admin account.
6. Run the reset command: you need to provide the JSON path and filename that you created earlier.

   `invoke --file <path and filename for JSON>`

   For example:

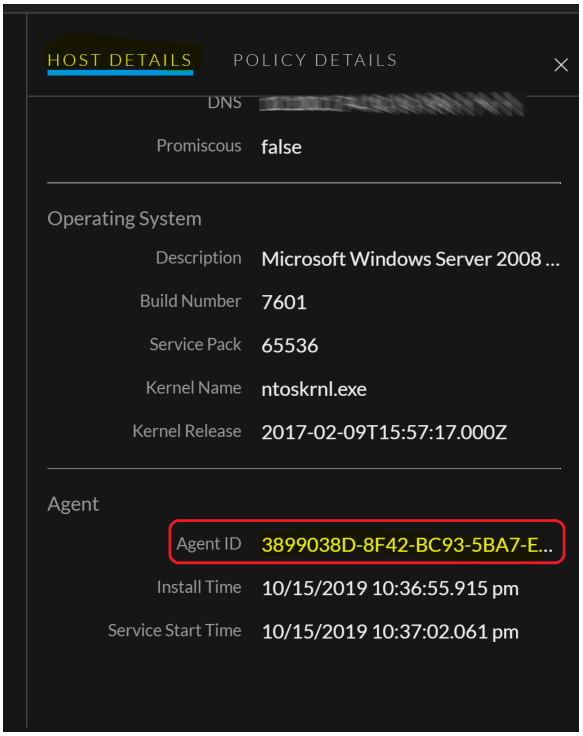
   `invoke --file /tmp/test.json`

The bookmarks for each log file identified in your JSON file are reset. The following image shows an example NetWitness Shell session:

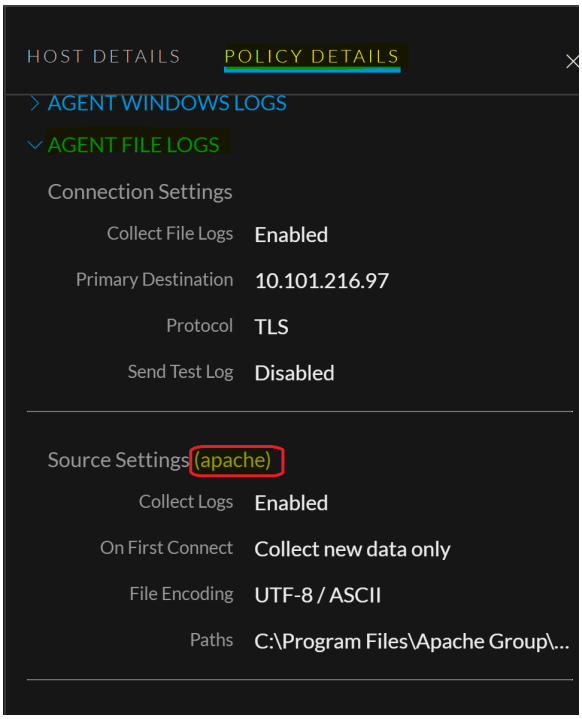
```
[root@SA ~]# nw-shell
RSA Netwitness Shell. Version: 5.15.0-SNAPSHOT

offline » connect --service endpoint-server.38909c2f-7a9b-415a-b567-f49a19cf250e
INFO: Connected to endpoint-server (38909c2f-7a9b-415a-b567-f49a19cf250e)
endpoint-server:Folder:/rsa » cd endpoint/command/reset-bookmark
endpoint-server:Method:/rsa/endpoint/command/reset-bookmark » login
user: admin
password: **********
admin@endpoint-server:Method:/rsa/endpoint/command/reset-bookmark » invoke --file /tmp/test.json
```

How to Find Agent IDs and Source Types

To find the Agent IDs for agents, go to **Hosts** > ***<select an Agent>***, then click the **Host Details** panel, and scroll down to the **Agent** section, where the Agent ID is shown:



To find the source types, go to **Hosts** > ***<select an Agent>***, then click the **Policy Details** panel, expand Agent File Logs, view the Source Settings for the source type name to use:



How to Find Endpoint Service IDs

You can retrieve the service ID for an Endpoint Server by using SSH to connect to it.

To retrieve the service ID for an Endpoint Server:

1. SSH to the NetWitness Endpoint Server for which you need to retrieve the ID. The IP address is available under  **(Admin) > Hosts**. The IP address for each host is listed in the **Host** column of the table.
2. View the file that contains the ID by running the following command:

   ```
   cat /etc/netwitness/endpoint-server/service-id
   ```

   It returns the Endpoint Server ID, for example:

   ```
   38909c2f-7a9b-415a-b567-f49a19cf250e
   ```

Currently Supported File Log Event Source Types

The following event source types are currently supported:

Apache Tomcat	Apache Web Server	CA Siteminder
CiscoWorks	CiscoWorks	Citrix XenMobile Device Manager
Courion Password Courier	EMC NetWorker	EMC Symmetrix
GlobalSCAPE EFT Server	IBM TAM WebSEAL	IBM WebSphere
IBM WebSphere MQ	JBoss Application Server	Kaspersky Anti-Virus
McAfee Endpoint	Microsoft DHCP	Microsoft Exchange
Microsoft Exchange 2007	Microsoft Exchange 2010	Microsoft Exchange 2013
Microsoft Exchange 2016	Microsoft Exchange SMTP	Microsoft Forefront Threat Management Gateway
Microsoft IAS (TVM)	Microsoft ISA	Microsoft ISA 2006
Microsoft ISA PF	Microsoft SQL Server	MSIAS
Oracle Access Management	Oracle iPlanet Web Server	Oracle WebLogic
Oracle WebLogic Audit Recorder	Perforce	Perforce AL
Perforce P4D	Rapid7 NeXpose	RIM Blackberry Enterprise Server
RSA Access Manager	RSA ACE Server	RSA ACE Server
RSA ACE Server AM	RSA ACE Server AMX	RSA Adaptive Auth (Hosted)
RSA Certificate Manager	RSA Federated Identity Manager	SAP ERP Central Component
Steel-Belted Radius Accounting	Steel-Belted Radius Authentication	SunOne LDAP Directory Server
Trend Micro IMSS	Trend Micro IWSS	Trend Micro IWSS Audit
VMware View	Windows DNS Debug Logs	MicrosoftIIS (W3C Format)

Specify UNC (Universal Naming Convention) Paths

During configuration of a Log File Policy, you can specify the log file path. You can set one or more paths to be used by the agent to locate the log files. The path can be a standard Windows pathname (such as `C:\Program Files\Apache\error_logs\logfile.log`) or a UNC (Universal Naming Convention) pathname (`\\host-name\share-name\file-path`). This topic describes how to specify a UNC path.

Secure the UNC Path Location

When you use a UNC path to collect log data on a remote system, make sure that you secure the UNC path location. One solution that works with minimal risk in a Windows domain environment is to do the following:

1. Create a share on the directory on the computer where the log data exists in isolation.
2. Name the share to something like **LOGDATA$** for example. (Shares can be hidden from curious browsers by adding a "$" to the end of the share name).
3. Remove all the default share permissions except local admin so it can be changed.
4. Add a share permission for the agent computer system. This allows any user on the agent system to access the shared location. On the agent system collecting the remote log data, nothing else should be required to properly collect the log data from the UNC path.

Note: You may not be able to view the UNC directory contents from file explorer. Seek advice from your IT or security group for additional guidence to setting up and securing a UNC directory share.

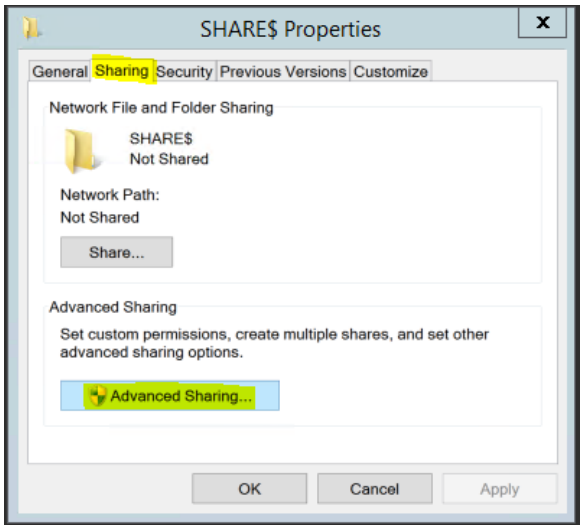
The following procedures describe how to:

- Share a folder between machines in a domain, and
- Share a folder between machines in a Workgroup

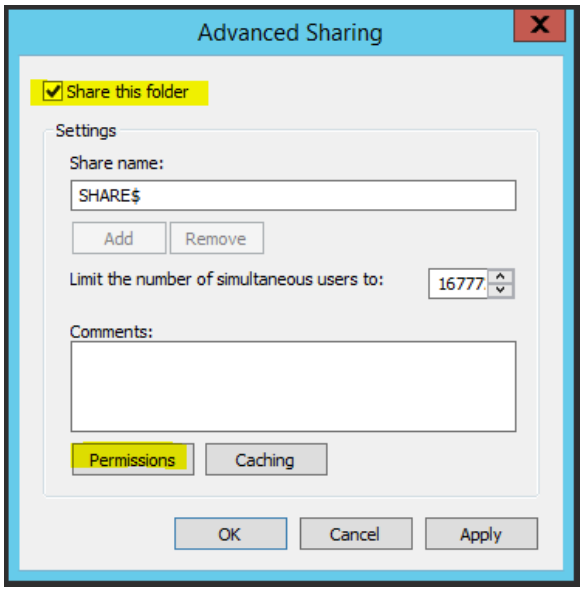
Share a folder between machines in a domain

This procedure describes how to share a folder between Windows machines that are both in the same domain.

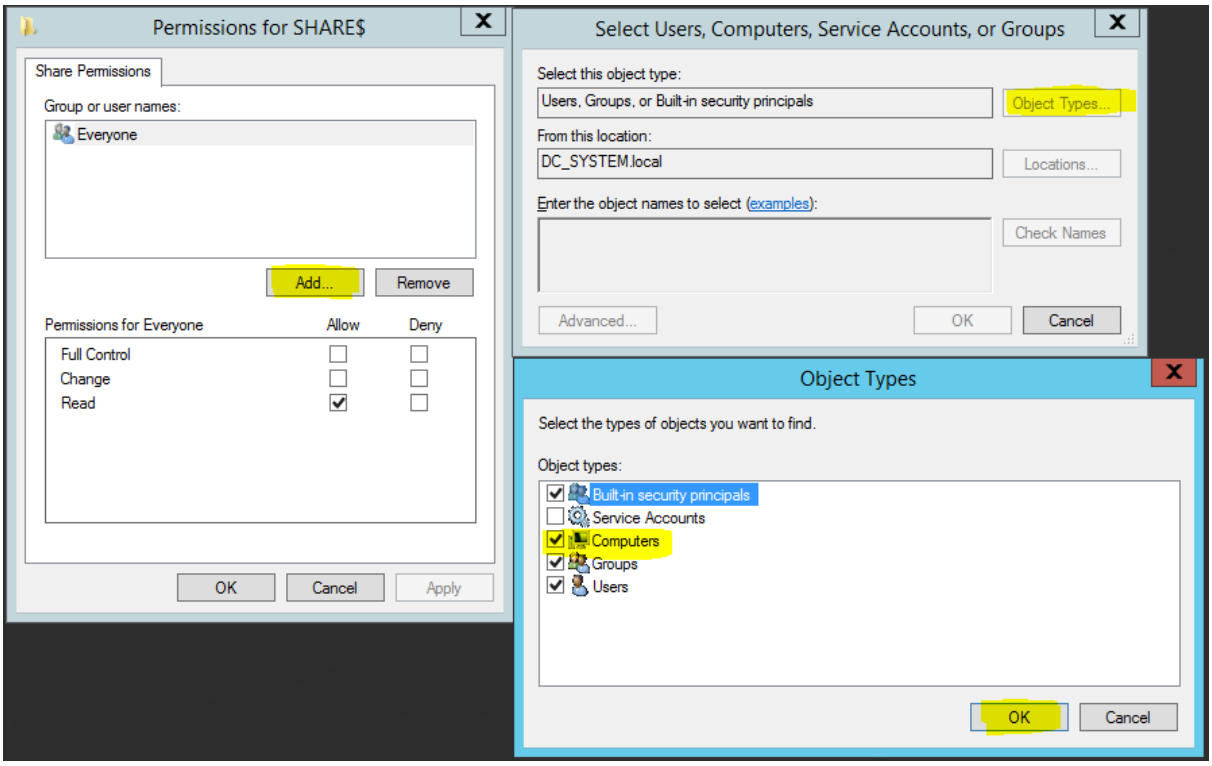
1. Log on to a Domain member machine that contains the logs folder you want to collect using an agent.
2. Right click on the folder you want to share with the agent to collect logs from, and click **Properties**: **SHARE$** in this example.



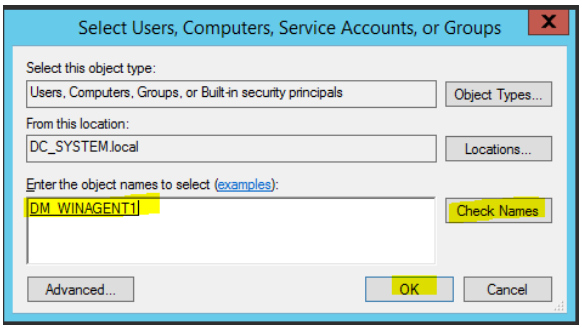
3. Click Advanced Sharing, select Share this folder, and then click Permissions.



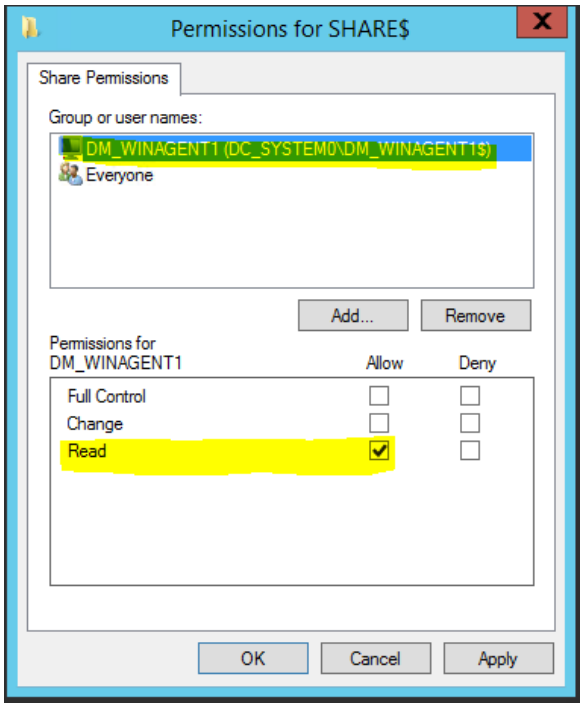
4. Click **Add**, and then on the next window click **Object Types**, check **Computers**, hit **OK**.



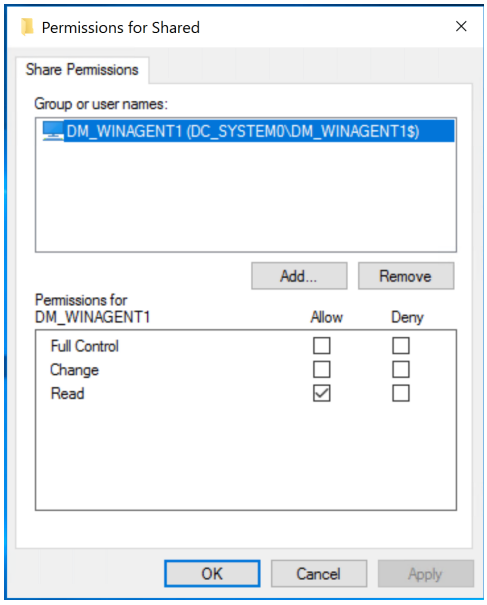
5. Search for the Agent computer name as shown below and click **OK**.



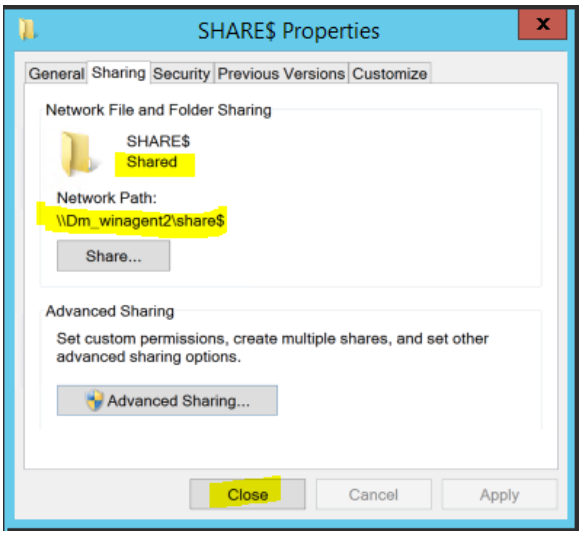
6. In the Permissions screen, provide **Read** permission to the agent, click **Apply**, and then click **OK**.



7. Remove **Everyone** from the Share Permissions list.



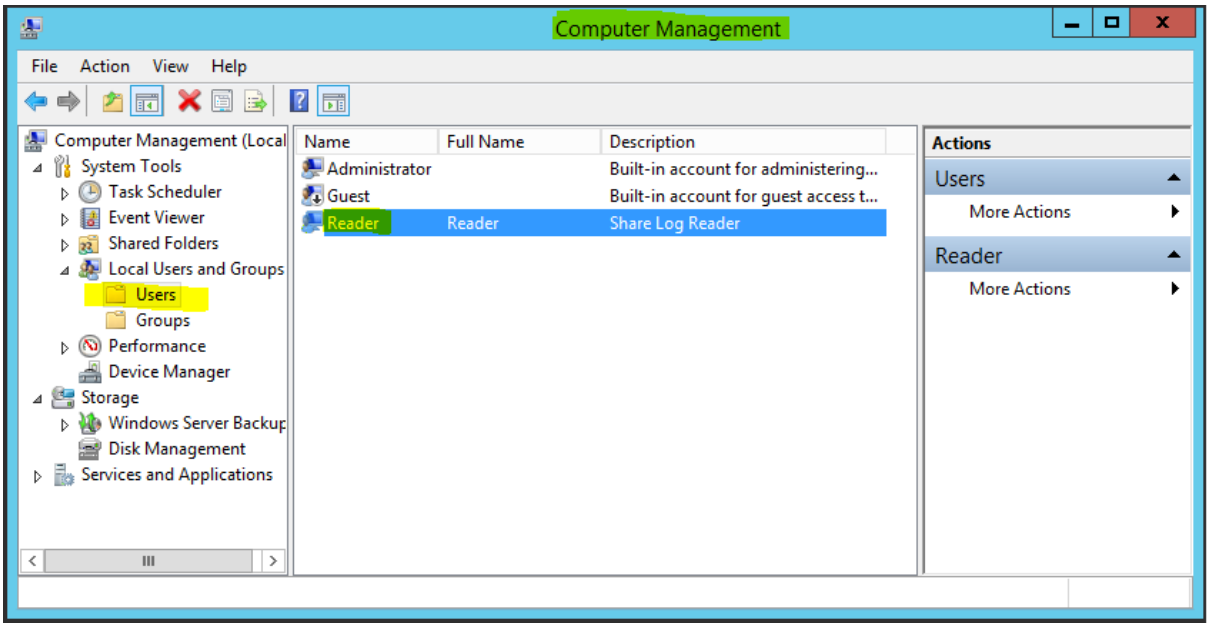
8. Verify that now the **SHARE$** folder status is correct, and note the network path so that you can enter it later, when you configure the policy that will use this shared folder.



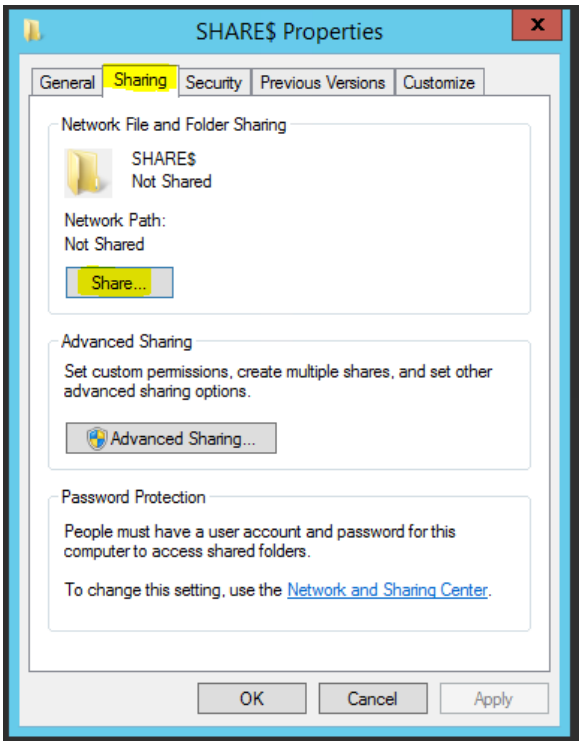
Share a folder between machines in a Workgroup

This procedure describes how to share a folder between Windows machines that are both in the same Workgroup.

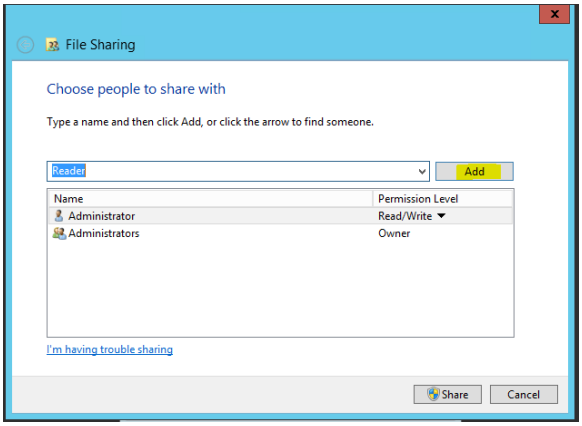
1. Log on to a workgroup machine that contains the logs folder you want to collect using an agent.
2. Create a non-admin user for log collection: **Reader** in this example.



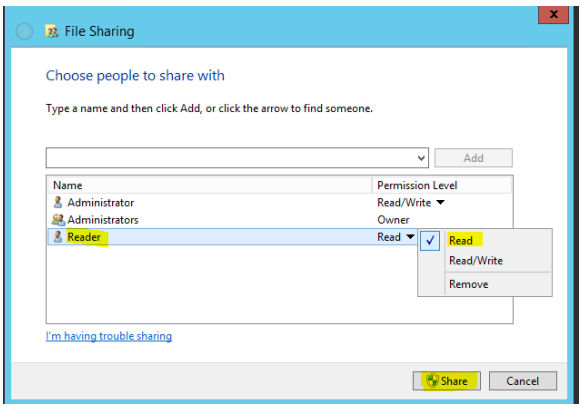
3. Right click on the folder you want to share with the agent to collect logs from, and click **Properties**: **SHARE$** in this example.
4. Click the **Sharing** tab, then click **Share**.



5. Choose the newly-created user and click **Add**.



6. Select the **Read** permission and click **Share**.



7. Log onto the Agent to add credentials, so that the system can read logs from the shared folder.
   a. Download the `psexec` tool from the Microsoft web site.
   b. Run the following command:

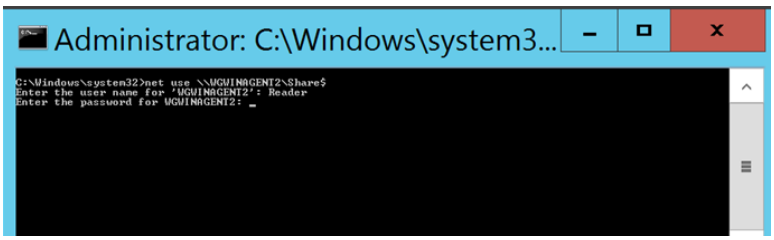
      ```
      psexec -i -s cmd.exe
      ```

      A new command window opens, running as **system**.
   c. In the command window, run the following command to cache credentials for the newly-created user to access logs on shared folder from a workgroup machine:

      ```
      net use \\hostname of machine with logs\Share$
      ```

      For example:

      ```
      net use \\WGWINAGENT2\Share$
      ```
   d. Provide the username and password for the non-admin user created earlier (in step 2).



This command adds credentials to read logs from the shared folder on the workgroup machine.