NetWitness® Platform XDR

Version 12.3.0.0

ESA Configuration Guide

NETWITNESS

Platform XDR

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.

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/.

September, 2023

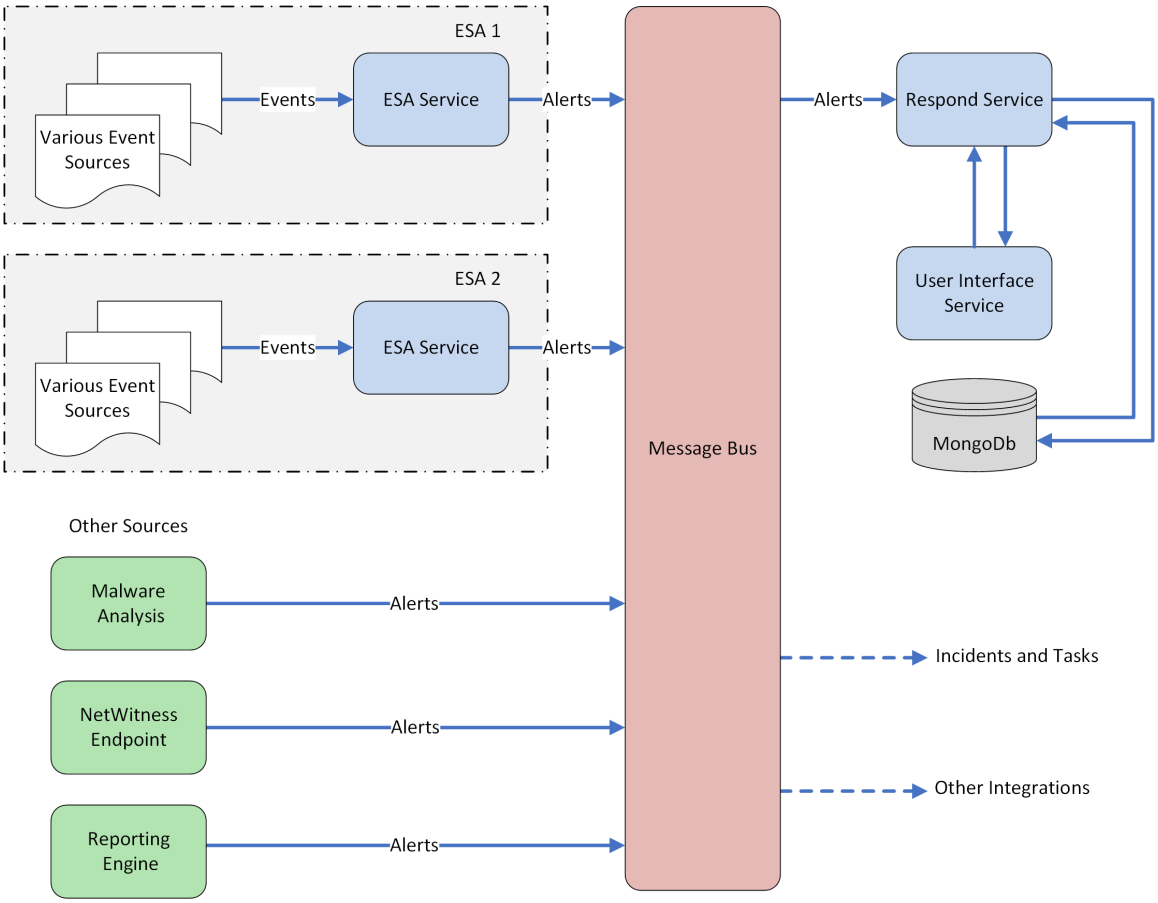
Contents

Event Stream Analysis Overview

NetWitness Event Stream Analysis (ESA) provides advanced stream analytics such as correlation and complex event processing at high throughputs and low latency. It is capable of processing large volumes of disparate event data from Concentrators.

ESA's advanced Event Processing Language allows you to express filtering, aggregation, joins, pattern recognition, and correlation across multiple disparate event streams. Event Stream Analysis helps perform powerful incident detection and alerting.

The following diagram shows the high-level data workflow:



In NetWitness version 11.5 and later, There are only two services that can run on an ESA host:

- **ESA Correlation (ESA Correlation rules):** Creates alerts from ESA rules.
- **Contexthub Server (Context Hub):** Runs only on an ESA primary host. Contexthub Server provides enrichment lookup capability in the Respond and Investigate views. For information, see the *Context Hub Configuration Guide*.

Note: The Event Stream Analytics Server (ESA Analytics) service is not supported in NetWitness Platform version 11.5 and later.

The first service is the ESA Correlation service that creates alerts from ESA rules, also known as ESA Correlation Rules, which you create manually or download from Live.

In NetWitness 11.3 and later, the ESA Correlation service replaces the Event Stream Analysis service and is also known as ESA Correlation Server. The ESA Correlation service provides the same services as the Event Stream Analysis service with the added benefit of enabling you to specify different data sources for your ESA correlation rules. Like the Event Stream Analysis service, the ESA Correlation service installs on the ESA Primary and ESA Secondary host types.

The second service is the Contexthub Server service, which provides enrichment lookup capabilities in the Respond and Investigate views. It runs only on an ESA Primary host. For information, see the *Context Hub Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

IMPORTANT: Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.5 and later. The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

Upgrade Considerations for ESA Analytics

The Event Stream Analytics Server (ESA Analytics) service is not supported or available in NetWitness version 11.5 and later. The Whois Lookup Configuration and ESA Analytics Mapping panels are no longer in the user interface [(Admin) > **System**].

Note: Event Stream Analysis (ESA) is not end of life. ESA Correlation rules and the ESA Correlation service are supported. ESA Analytics, which is used for Automated Threat Detection, is different from ESA Correlation Rules and is EOL. In its place, you can use ESA Correlation as is offers more functional capabilities and better performance.

Configure ESA Correlation Rules

This topic provides high-level tasks to configure NetWitness Event Stream Analysis (ESA) Correlation Rules using the ESA Correlation service.

IMPORTANT: Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.5 and later. The NetWitness server, ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

Data Source Configuration Changes

In NetWitness version 11.3 and later, the ESA Correlation service enables you to specify different data sources for different sets of rules. Instead of adding data sources, such as Concentrators, to the entire ESA Correlation service, you can specify different data sources for each ESA rule deployment. An ESA rule deployment includes an ESA Correlation service with its associated data sources and a set of ESA rules. For example, you may want to use Concentrators with HTTP packet data in one deployment and Concentrators with HTTP log data in another deployment. For more detailed information, see "Manage ESA Datasources" in Live Services Management Guide.

In NetWitness Platform 11.5 and later, you can add an optional data source filter to the data sources in your ESA rule deployments to improve performance. This allows your data sources to be filtered further so that only the data relevant to the deployment is forwarded to ESA. The filter is comprised of application rules, which are applied to the Decoders mapped to your selected data sources.

Caution: The data source filter is intended for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

Using a data source filter can be performance intensive for data aggregation. A filter slows the event aggregation rate, but when you are filtering a large amount of traffic, it can have performance benefits on ESA Correlation server. However, if you use a complex filter and do not filter a large amount of traffic, the event aggregation rate may be lower than expected.

IMPORTANT: If an application rule linked to a data source filter is modified on a Decoder, the filter must be removed, added again, and redeployed. The changes take effect on ESA after the deployment is redeployed.

For more information, see “Create a Deployment” topic in Live Services Management Guide.

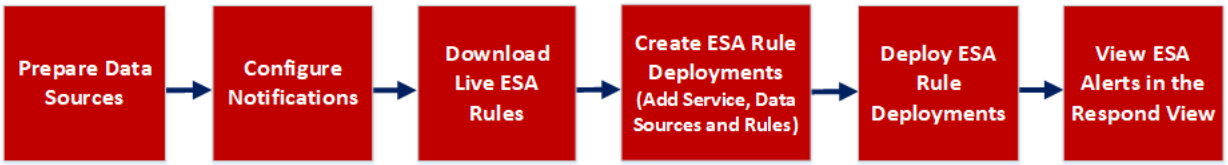
Endpoint Risk Scoring Rules Bundle

An Endpoint Risk Scoring Rules Bundle, which contains approximately 400 rules, comes with NetWitness 11.3 and later. Endpoint risk scoring rules only apply to NetWitness Endpoint. You can add the Endpoint Risk Scoring Rules Bundle to an ESA rule deployment in the same way that you would add any ESA rule. However, you must specify endpoint data sources (Concentrators) in the ESA Rule Deployment.

The ESA Correlation service can process endpoint risk scoring rules, which generate alerts that are used in risk scoring calculations to identify suspicious files and hosts. To turn on risk scoring for NetWitness Endpoint, you must deploy endpoint risk scoring rules on ESA. For instructions, see Deploy Endpoint Risk Scoring Rules on ESA. To configure NetWitness Endpoint, see the *NetWitness Endpoint Configuration Guide*. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

ESA Correlation Rules Configuration Workflow

The following diagram shows the high-level workflow for configuring ESA Correlation Rules with the ESA Correlation service.



ESA Rule Deployments are groups of ESA Rules processed by an ESA service to create alerts. In NetWitness 11.3 and later, the ESA Correlation service processes the ESA rules and creates alerts.

Before you can configure ESA Correlation Rules, install and configure the data sources (Concentrators) to use for the ESA rules. For example, you may have a Concentrator with HTTP packet data and another with Windows Log data. Next, configure the global notification methods that content experts can use for the ESA rules. For example, they may want to send an email notification when a rule creates an alert.

The NetWitness Live Content Management System (known as *Live*) is a valuable source of the latest internet security resources for NetWitness customers. RSA Live contains an extensive library of ESA rules to detect threats that you can use to save time. Download the rules for the events that you want to detect in your network to the ESA Rule Library and adjust them as needed for your network environment.

After you prepare your data sources and download Live ESA rules, you can create one or more ESA rule deployments. An ESA rule deployment contains an ESA service, one or more data sources, and a set of ESA rules. For example, you can create an ESA rule deployment that contains an ESA Correlation service, a Concentrator with HTTP packet data, and a set of ESA rules for HTTP packet data. When you are ready to have the ESA service run the rule set, you deploy the ESA rule deployment, which places the rules on ESA.

After you deploy an ESA rule deployment, verify that you can view the ESA alerts in the Respond view (**Respond** > **Alerts**).

Prerequisites

Make sure that you:

- Install the ESA Correlation service in your network environment.
- Install and configure one or more Concentrators in your network environment.
- Download or ensure that you have access to the Alerting with Correlation Rules User Guide for version 11.3 or later. Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Procedure

The following table shows the high level tasks required to configure ESA Correlation Rules.

Tasks	Reference
1. Prepare data sources, such as Concentrators, to use for your ESA Correlation Rules.	Refer to Broker and Concentrator Configuration Guide.
2. Configure notifications for the ESA Correlation service.	Refer to Notification Methods.
3. Working with Event Stream Analysis rules using Live. Configure the Live ESA Rule parameters for your environment.	Refer to Working with RSA ESA Live Rules.
4. Create ESA rule deployments*: Choose ESA Rules and the appropriate ESA service to use in the ESA rule deployment.	Refer to **Create a Deployment** topic in Live Services Management Guide.
5. Deploy ESA rule deployments.*	Refer to **Create a Deployment** topic in Live Services Management Guide.
6. View ESA alerts in the Respond view.	Refer to the NetWitness Respond User Guide.

*ESA rule deployments are groups of ESA Rules that are processed by an ESA service, such as the ESA Correlation service in NetWitness version 11.3 and later.

For additional optional advanced ESA Correlation Rules configuration procedures, see Additional ESA Correlation Rules Procedures.

For more information on alerting with ESA Correlation rules best practices, creating rules, working with trial rules, adding data enrichment sources, viewing statistics for an ESA service, and troubleshooting, see the Alerting with ESA Correlation Rules User Guide.

ESA Correlation Health and Wellness Monitoring

In NetWitness version 11.5 and later, New Health and Wellness provides improved and intuitive dashboards, monitors, and visualizations. The ESA Correlation Overview dashboard provides health statistics and trends on ESA rule deployments.

For more information, see "Monitor New Health and Wellness" and "Appendix A: New Health and Wellness Dashboards / ESA Correlation Overview Dashboard" in the System Maintenance Guide.

Upgrade Considerations for ESA Hosts

Mixed mode is not supported for ESA hosts in NetWitness Platform version 11.5 and later.

IMPORTANT: The NetWitness server (Admin server), ESA primary host, and ESA secondary host must all be on the same NetWitness Platform version.

Trial Rule Status Changes

In NetWitness Platform 11.4 and later, ESA trial rules no longer change status after an upgrade or deployment. For example, if you change the status of a trial rule to disabled [(Configure) > **ESA Rules** > **Services** tab] and redeploy the ESA rule deployment [(Configure) > **ESA Rules** > **Rules** tab], the trial rule remains disabled. Previously, ESA trial rules could change status after an upgrade or when they were redeployed.

Upgrade Considerations for ESA Rule Deployments for version 12.1 and later

Before upgrading to the 12.1 version, NetWitness recommends that all the ESA deployments maintain an error-free state and remove any unused ESA deployments, as ESA deployments will be migrated to policies and groups after upgrading to the 12.1 version.

Note: Make sure that you plan the upgrade process so that correlation servers are upgraded immediately after the Admin Server is done. The deployments will not be accessible until the corresponding correlation servers are upgraded. This action will not affect the events and alerts processing by correlation servers.

IMPORTANT: If there is any need to import ESA Rules and Enrichments. NetWitness recommends importing those missing rules and enrichments before the upgrade.

The pre-upgrade and post-upgrade states of deployments are represented in the following table.

SINo	Pre-upgrade Deployment State	Post-upgrade Deployment State		
		Creates Policy	Creates Group	The policy will be Published
1	Healthy deployment	Yes	Yes	Yes
2	Deployment with errors	Yes	Yes	Yes
3	Deployment with only rules	Yes	No	No
4	Deployment with no rules	No	No	No

After upgrading to the 12.1 version, all the ESA deployments will be migrated to (**CONFIGURE**) > **Policies** page. Each deployment will be converted into a policy and group and will be available to manage only after the upgrade of the correlation server to the 12.1 version. Verify if all the ESA deployments are in a healthy state. For more information, see **View a Deployment** topic in the *Live Services Management Guide*.

Note: Analysts must have appropriate permissions to view the ESA rules under (**CONFIGURE**) > **ESA Rules** and (**CONFIGURE**) > **Policies** pages. For more information, see the **Source-server** section in the "Role Permissions" topic in the *System Security and User Management Guide*.

(Optional) Using the **Merge Policy** button, you can merge a policy having ESA content with a policy with no ESA content.. For more information, see "Merge Policy with ESA Content" topic in the *Live Services Management Guide*.

To support Endpoint and UEBA content as well as changes to ESA rules from Live, a data change from single-value (string) to multi-value (string array) is required for several meta keys within the ESA Correlation service. Some single-value meta keys are also required. See Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys.

Additional ESA Correlation Rules Procedures

This topic is a collection of individual procedures, which an Administrator may perform at any time and they are not required to complete the initial setup of ESA Correlation Rules.

Use this section when you are looking for instructions to perform a specific task after the initial setup of ESA.

- Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys
- Configure Advanced Settings for an ESA Correlation Service
  - Enable or Disable Sending ESA Rule Alerts to the Respond View
  - Enable ESA Correlation Service Debugging for All Rules
  - Configure Maximum Events per Alert for All Rules
  - Adjust Maximum Sessions for the ESA Data Source Filter
  - Configure Meta Keys as Arrays in ESA Correlation Rule Values
  - Remove Sensitive Meta Keys Globally from All Alerts for Data Privacy
- Configure Character Case for Advanced ESA Rules
- Deploy Endpoint Risk Scoring Rules on ESA
- Change Memory Threshold for ESA Rules
- Start, Stop, or Restart ESA Service
- View Audit Logs and Verify ESA Component Versions

Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys

Note: This procedure applies only to ESA Correlation Rules in NetWitness Platform 11.3.0.2 and later versions.

To support Endpoint, UEBA, and RSA Live content, a data change from single-value (string) to multi-value (string array) is required for several meta keys within the ESA Correlation service for 11.3 and later. Additional string meta keys are required within the ESA Correlation service for 11.3.0.2 and later.

If the meta keys used for your ESA rules are different from the required default multi-value meta keys, your ESA rules continue to work, but you should update your ESA rules to use the required meta keys as soon as possible to ensure that your rules continue to deploy properly.

Note: On a new installation of ESA on 11.3.0.2 and later, no ESA rule adjustments are necessary.

The ESA Correlation service has the following multi-valued (string array) and single-valued (string) parameters:

- **`multi-valued`** - Shows the string array meta keys currently used for your ESA rules.
  - For an upgrade to NetWitness Platform 11.3.0.2 and later, it shows the existing string array meta keys before the upgrade. (This parameter is equivalent to the Event Stream Analysis service ArrayFieldNames parameter in NetWitness Platform versions 11.2 and earlier.)
  - For a new installation of NetWitness Platform 11.3.0.2 and later, it contains all the required string array meta keys for the latest version.
- **`single-valued`** - Shows the string meta keys currently used for your ESA rules.
  - For an upgrade to NetWitness Platform 11.3.0.2 and later from versions prior to 11.3, this parameter value is empty.
  - For a new installation of NetWitness Platform 11.3.0.2 and later, it contains all the required string meta keys for the latest version.
- **`default-multi-valued`** - Shows the required string array meta keys for the latest version.
  - For a new installation of NetWitness Platform 11.3.0.2 and later, this parameter value is empty.
- **`default-single-valued`** - Shows the required string meta keys for the latest version.
  - For a new installation of NetWitness Platform 11.3.0.2 and later, this parameter value is empty.

Note: If you have the same value in the `single-valued` and `multi-valued` parameter fields, the `single-valued` meta key value takes precedence over the `multi-valued` meta key value.

To use the latest Endpoint, UEBA, and Live content rules, you must update the **`multi-valued`** parameter on the ESA Correlation service to include all of the meta keys in the **`default-multi-valued`** field. You must also update the **`single-valued`** parameter field to include all of the meta keys in the **`default-single-valued`** field. To do this, follow the Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules procedure.

Caution: Any changes that you make to the `multi-valued` parameter may cause an error when you deploy your existing rules. You can update the `multi-valued` parameter, resync your meta keys, and update the ESA rules at your convenience. You may want to add a couple meta keys at a time to reduce the number of reported errors.

Note: If you are using multiple ESA Correlation services, the `multi-valued` and `single-valued` parameters should be the same on each ESA Correlation service.

In NetWitness Platform 11.3.0.2 and later, ESA automatically adjusts the operator in the rule statement when there is a change from string to string array, but you still may need to make manual adjustments to adjust for the string array changes.

To change the string type meta keys to string array type meta keys manually, see Configure Meta Keys as Arrays in ESA Correlation Rule Values.

To use the latest Endpoint, UEBA, and Live content rules, the following default **multi-valued** meta keys are required on the ESA Correlation service in NetWitness Platform version 11.3 and later:

```
action , alert , alert.id , alias.host , alias.ip , alias.ipv6 , analysis.file
, analysis.service , analysis.session , boc , browserprint , cert.thumbprint ,
checksum , checksum.all , checksum.dst , checksum.src , client.all , content ,
context , context.all , context.dst , context.src , dir.path , dir.path.dst ,
dir.path.src , directory , directory.all , directory.dst , directory.src ,
email , email.dst , email.src , eoc , feed.category , feed.desc , feed.name ,
file.cat , file.cat.dst , file.cat.src , filename.dst , filename.src , filter
, function , host.all , host.dst , host.orig , host.src , host.state ,
inv.category , inv.context , ioc , ip.orig , ipv6.orig , netname , OS , param
, param.dst , param.src , registry.key , registry.value , risk , risk.info ,
risk.suspicious , risk.warning , threat.category , threat.desc , threat.source
, user.agent , username
```

The following default **single-valued** meta keys are also required on the ESA Correlation service in NetWitness Platform 11.3.0.2 and later:

```
accesses , context.target , file.attributes , logon.type.desc , packets
```

If you used any meta keys in the ESA rule notification templates from the Required String Array or String Meta Keys list, update the templates with the meta key changes. See "Configure Global Notification Templates" in the *System Configuration Guide*.

Note: Advanced EPL rules may get disabled and are not automatically updated so they must be fixed manually.

For additional troubleshooting information, see “Troubleshoot ESA” in the *Alerting with ESA Correlation Rules User Guide*.

Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules

To use the latest Endpoint, UEBA, and Live content rules, you must update the **multi-valued** parameter field on the ESA Correlation service to include all of the meta keys in the **default-multi-valued** field. You must also update the **single-valued** parameter field to include all of the meta keys in the **default-single-valued** field.

Caution: Any changes that you make to the `multi-valued` parameter may cause an error when you deploy your existing rules. You can update the `multi-valued` parameter, resync your meta keys, and update the ESA rules at your convenience. You may want to add a couple meta keys at a time to reduce the number of reported errors.

Note: If you see a warning message in the ESA Correlation server error logs for missing multi-valued meta keys, there is a difference between the `default-multi-valued` parameter and `multi-valued parameter` meta key values, and the new Endpoint, UEBA, and Live content rules will not work. The same is true for missing single-valued meta keys. Completing this procedure should fix the issue. For example warning messages, see Example ESA Correlation Server Warning Message for Missing Meta Keys.

1. After an upgrade to 11.3.0.2 or later, go to  **(Admin) > Services**, and in the Services view, select an ESA Correlation service and then select  **> View > Explore**.
2. In the Explore view node list for the ESA Correlation service, select **correlation > stream**.

3. Compare the **multi-valued** parameter meta keys with the required **default-multi-valued** meta keys. Copy and paste the missing string array meta keys from the **default-multi-valued** parameter to the **multi-valued** parameter. (You may want to copy only a couple meta keys at one time to reduce the number of reported errors).
4. Copy and paste the string meta keys from the **default-single-valued** parameter to the **single-valued** parameter.
5. If you have multiple ESA Correlation services, make the same meta key changes on each ESA Correlation service.
6. Apply the changes on the ESA Correlation services:
   a. Go to  **(Configure) > ESA Rules** and click the **Settings** tab.
   b. In the Meta Key References, click the Meta Re-Sync (Refresh) icon ().
7. If you are using any of the **default-multi-valued** or **default-single-valued** meta keys in your ESA Advanced rules, update the rule syntax. See also Adjust Custom ESA Rule Builder and ESA Advanced Rules.
8. If you used any meta keys in the ESA rule notification templates from the **default-multi-valued** parameter list, update the templates with the meta key changes. See "Configure Global Notification Templates" in the *System Configuration Guide*.
9. Deploy your ESA rule deployments.
10. Check your rules for error messages in the ESA Rules section of the ESA rule Deployment or check the ESA Correlation error logs for errors.
    - (This option is available in NetWitness verson 11.3.0.2 and later.) To access the error messages in the ESA rule deployment, go to  **(Configure) > ESA Rules > Rules** tab, select a deployment in the options panel on the left, and go to the **ESA Rules** section. If the ESA rule status shows "Disabled" or shows the  icon in the Status column, you need to determine the issue to fix the rule. If a disabled rule has an error message, it shows  in the Status field. You can hover over the rule to view the error message tooltip without going to the error log.
    - To access the ESA Correlation service logs, you can use SSH to get in the system and go to: `/var/log/netwitness/correlation-server/correlation-server.log`.

Adjust Custom ESA Rule Builder and ESA Advanced Rules

Update your ESA Rule Builder and ESA Advanced rules to work with the string and string array meta keys listed in the `default-multi-valued` and `default-single valued` parameter fields for the ESA Correlation service. You can add additional meta keys to the `multi-valued` and `single-valued` parameters.

For example, if you use ec.outcome as a single-valued meta key in your ESA rule as shown below:

```
@RSAAlert
SELECT * FROM Event((ec_outcome IN ( 'Success' )))
.win:time_length_batch(2 Minutes, 2)
```

```
HAVING COUNT(*) >= 2;
```

If you add ec.outcome to the **multi-valued** parameter field, you need to update your rule as shown below:

```
@RSAAlert
SELECT * FROM Event(( 'Success' = ANY( ec_outcome ) ))
.win:time_length_batch(2 Minutes, 2)
HAVING COUNT(*) >= 2;
```

For more information, see Configure Meta Keys as Arrays in ESA Correlation Rule Values.

Example ESA Correlation Server Warning Message for Missing Meta Keys

If you see a warning message in the ESA Correlation server error logs for missing multi-valued meta keys, there is a difference between the `default-multi-valued` parameter and `multi-valued parameter` meta key values, and the new Endpoint, UEBA, and Live content rules will not work. The same is true for missing single-valued meta keys. Completing the Update the Multi-Valued and Single-Valued Parameter Meta Keys for the latest Endpoint, UEBA, and RSA Live Content Rules procedure should fix the issue.

Multi-Valued Warning Message Example

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id,
browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst,
checksum_src, client_all, content, context, context_all, context_dst,
context_src, dir_path, dir_path_dst, dir_path_src, directory,
directory_all, directory_dst, directory_src, email_dst, email_src,
feed_category, feed_desc, feed_name, file_cat, file_cat_dst, file_cat_
src, filename_dst, filename_src, filter, function, host_all, host_dst,
host_orig, host_src, host_state, ip_orig, ipv6_orig, OS, param, param_
dst, param_src, registry_key, registry_value, risk, risk_info, risk_
suspicious, risk_warning, threat_category, threat_desc, threat_source,
user_agent] are still MISSING from multi-valued
```

Single Value Warning Message Example

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_
target, file_attributes, logon_type_desc, packets] are still MISSING
from single-valued
```

Configure Meta Keys on New ESA Hosts to Match Upgraded ESA Hosts in the Same NetWitness Platform Network

Note: If you are upgrading from version below 11.4.x.x, make sure that meta keys on new ESA hosts are updated to match upgraded ESA Hosts in the Same NetWitness Platform Network.

If you have one or more ESA hosts in a NetWitness Platform network, which were upgraded from a version before 11.3.0.2 to 11.6, and you add a new ESA host, you must configure the meta keys on the new ESA host to match the other ESA hosts. All ESA Correlation services on the same NetWitness Platform network must have the same Meta Key configurations.

1. For each ESA Correlation service on an upgraded ESA host and for the ESA Correlation service on the newly installed ESA host:
   a. Open a new tab, go to  **(Admin) > Services**, and in the Services view, select the ESA Correlation service and then select  **> View > Explore**.
   b. In the Explore view node list for the ESA Correlation service, select **correlation > stream**.
2. Ensure that the **`multi-valued`** and **`single-valued`** meta key values are the same on each of the upgraded ESA Correlation services.
3. Ensure that the **`multi-valued`** and **`single-valued`** meta key values on the newly installed ESA host are the same as those on the upgraded services.
4. To apply any changes on the ESA Correlation services, go to  **(Configure) > ESA Rules** and click the **Settings** tab. In the Meta Key References, click the **Meta Re-Sync (Refresh)** icon ().
5. If you updated the ESA Correlation services, redeploy the ESA rule deployments.

For more information, see Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys.

Configure Advanced Settings for an ESA Correlation Service

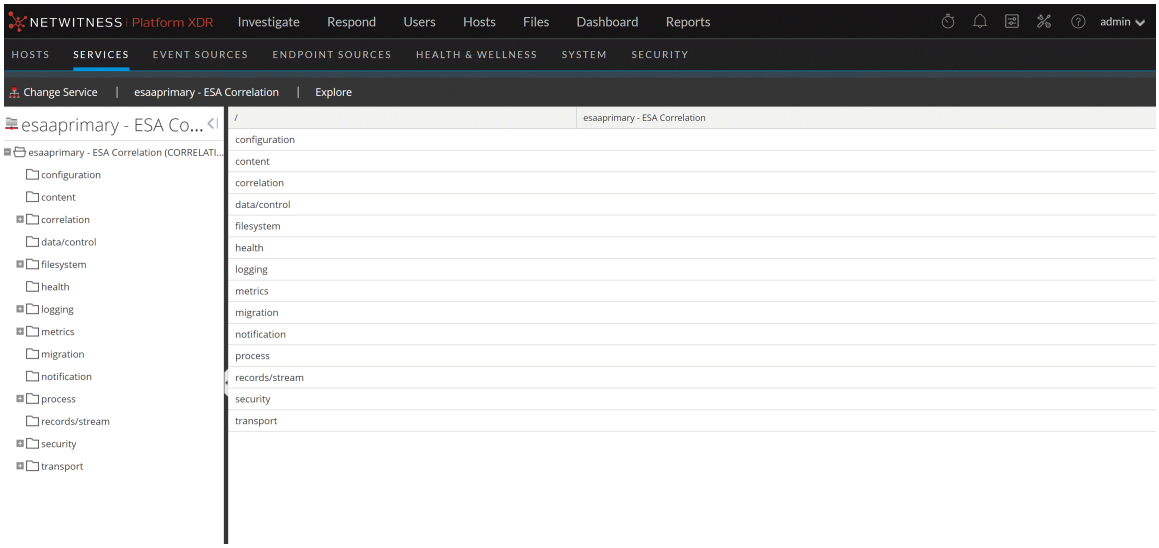
These procedures are optional and they apply only to ESA Correlation Rules.

In the Explore view for an ESA Correlation service, you can manage sending ESA rule alerts to the Respond view, turn on debugging for all rules, configure the events to preserve for rules with multiple events, and configure meta keys as string array values on ESA.

- Enable or Disable Sending ESA Rule Alerts to the Respond View
- Enable ESA Correlation Service Debugging for All Rules
- Configure Maximum Events per Alert for All Rules
- Adjust Maximum Sessions for the ESA Data Source Filter
- Configure Meta Keys as Arrays in ESA Correlation Rule Values
- Remove Sensitive Meta Keys Globally from All Alerts for Data Privacy

Access Advanced Settings for an ESA Correlation Service

1. Go to  **(Admin) > Services**.
   The Services view is displayed.
2. In Services view, select an ESA Correlation service and then select  **> View > Explore**.
   The Explore view is displayed.



Enable or Disable Sending ESA Rule Alerts to the Respond View

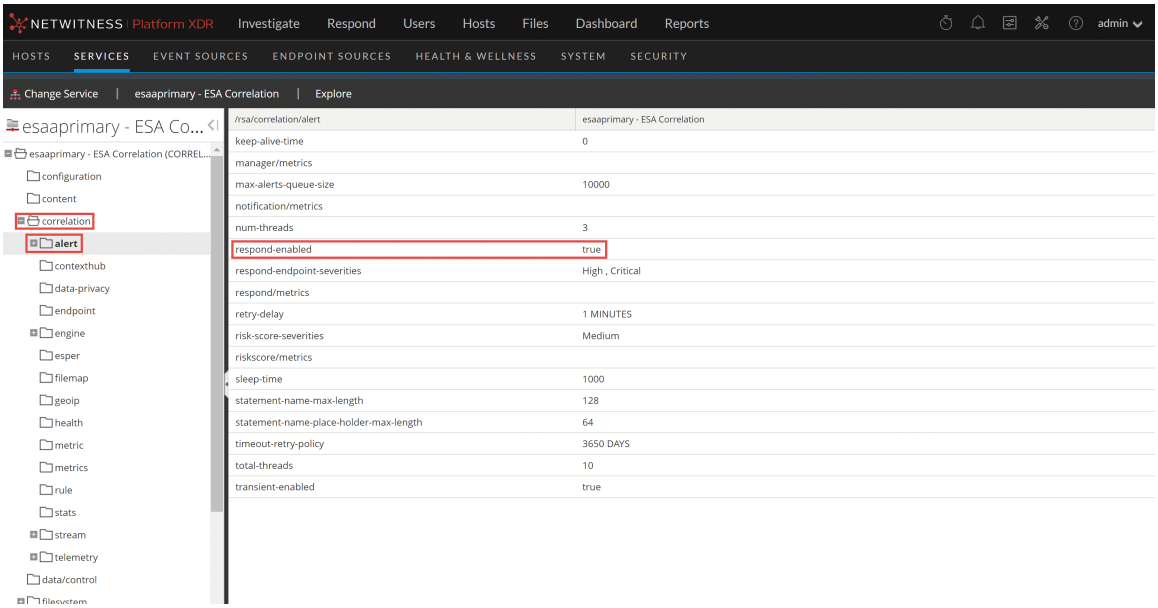
ESA gathers data, runs ESA Correlation rules against the data, captures events that meet rule criteria, and creates alerts for those captured events. You can view those alerts in the Respond view.

Before an ESA Correlation rule alert can go to the Respond view, both of the following settings must be enabled:

1. For all rules, the ESA Correlation service must have the `respond-enabled` parameter set to **true**. (The default is true.)
2. For an individual rule, the ESA Correlation rule must have the **Alert** option selected in the rule builder for that rule.

To enable or disable alert forwarding to the Respond view for ALL ESA Correlation rules:

1. In the Explore view node list for an ESA Correlation service, select **correlation > alert**.



2. To allow all ESA Correlation Rule alerts to go to the Respond view, set `respond-enabled` to **true**. Alerts for ESA rules that have the **Alert** option selected are visible in the Respond view.
3. To stop all ESA Correlation Rule alerts from going to the Respond view, set `respond-enabled` to **false**.
   ESA Correlation Rules do not go to the Respond view, even if you select the **Alert** option in the rule.

   The changes take effect immediately.

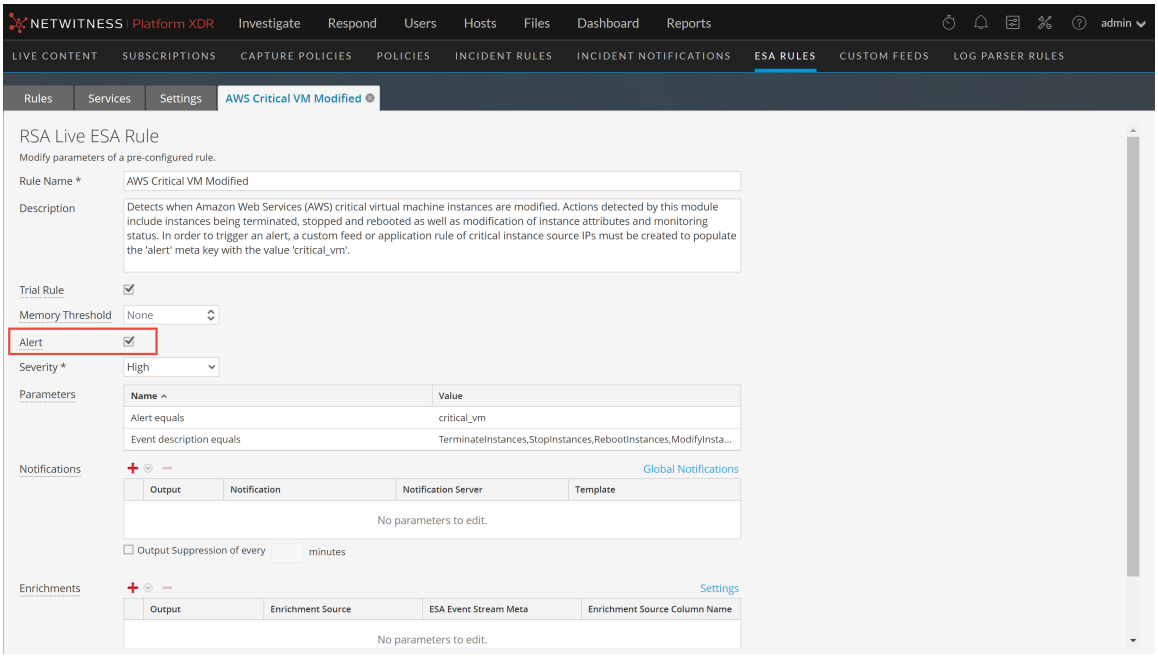
Note: The `respond-enabled` parameter is equivalent to the **Forward Alerts On Message Bus** option in the Event Stream Analysis service in NetWitness Platform version 11.2 and earlier.

To send or not send alerts to the Respond view for a single ESA Correlation rule:

Content experts managing the ESA Correlation rules can decide whether to send alerts to the Respond view for each rule.

1. Go to  **(Configure) > ESA Rules > Rules** tab.
   The Rules tab is displayed.

2. In the **Rule Library**, select the rule you want to edit and click  .
   Depending on the rule type, the respective rule tab is displayed.



   - To turn on Respond alerts for a rule, select the **Alert** checkbox.
   - To turn off Respond alerts for a rule, clear the **Alert** checkbox.

3. Click **Save**.

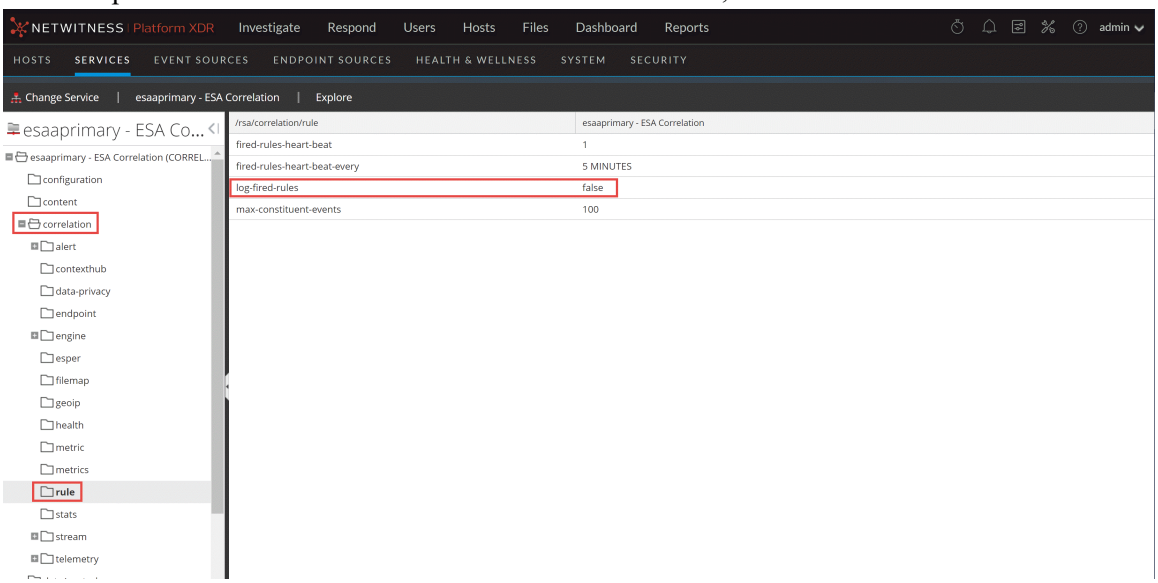
   For more information, see the *Alerting with ESA Correlation Rules User Guide*.

Enable ESA Correlation Service Debugging for All Rules

You can turn on debugging for all ESA rules to see if rules are creating (firing) alerts and data is being processed properly by the ESA Correlation service. This can also be helpful when writing or fixing global notification templates, such as syslog or email. You can see the actual content of an alert before sending the notification.

When you disable ESA Correlation service debugging for all rules, you can still turn on debugging for an individual rule at any time.

1. In the Explore view node list for an ESA Correlation service, select **correlation > rule**.

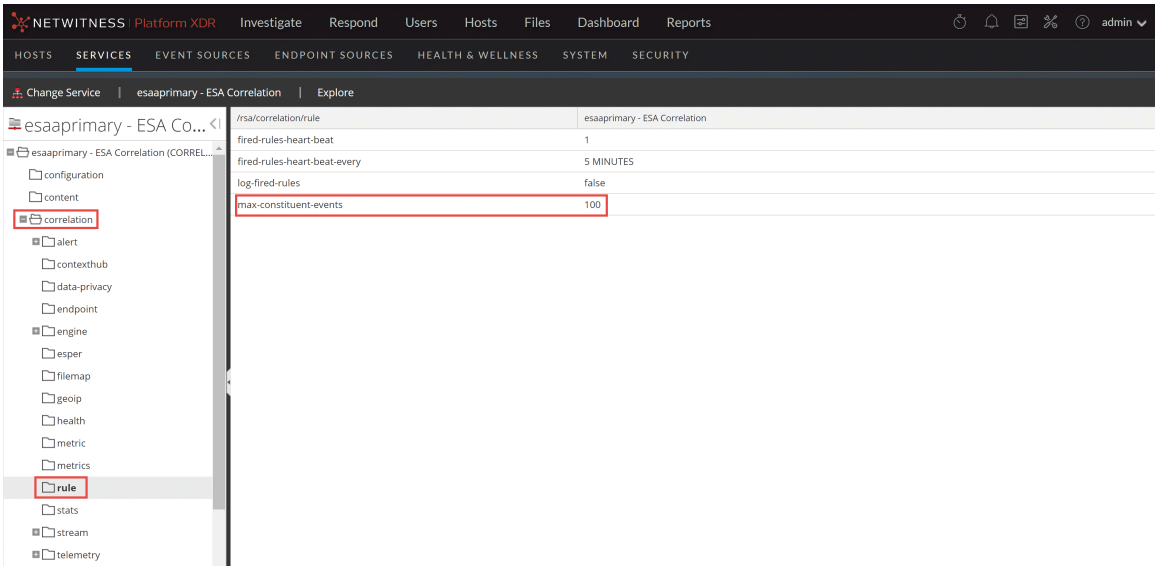


2. Set `log-fired-rules` to **true** to print alerts to the /var/log/netwitness/correlation-server/correlation-server.log for troubleshooting. This is the same as the Debug option in the rule builders for individual ESA rules except that this option enables debugging for all rules.
3. When you are ready to turn off debugging for all ESA rules, set `log-fired-rules` to **false**. The changes take effect immediately.

Note: The `log-fired-rules` parameter is equivalent to the **Debug Rules?** option in the Event Stream Analysis service in NetWitness Platform version 11.2 and earlier.

Configure Maximum Events per Alert for All Rules

1. In the Explore view node list for an ESA Correlation service, select **correlation > rule**.



2. For rules that contain multiple events, in `max-constituent-events`, enter how many of the associated events to preserve. For example, if a rule fires an alert with 200 associated events and this parameter is set to 100, only the first 100 are preserved by ESA, the rest are dropped. The default value is **100**.
   The changes take effect immediately.

Note: The `max-constituent-events` parameter is equivalent to the **Max Constituent Events** option in the Event Stream Analysis service in NetWitness Platform version 11.2 and earlier.

Adjust Maximum Sessions for the ESA Data Source Filter

Note: This procedure applies only to NetWitness Platform version 11.5 and later.

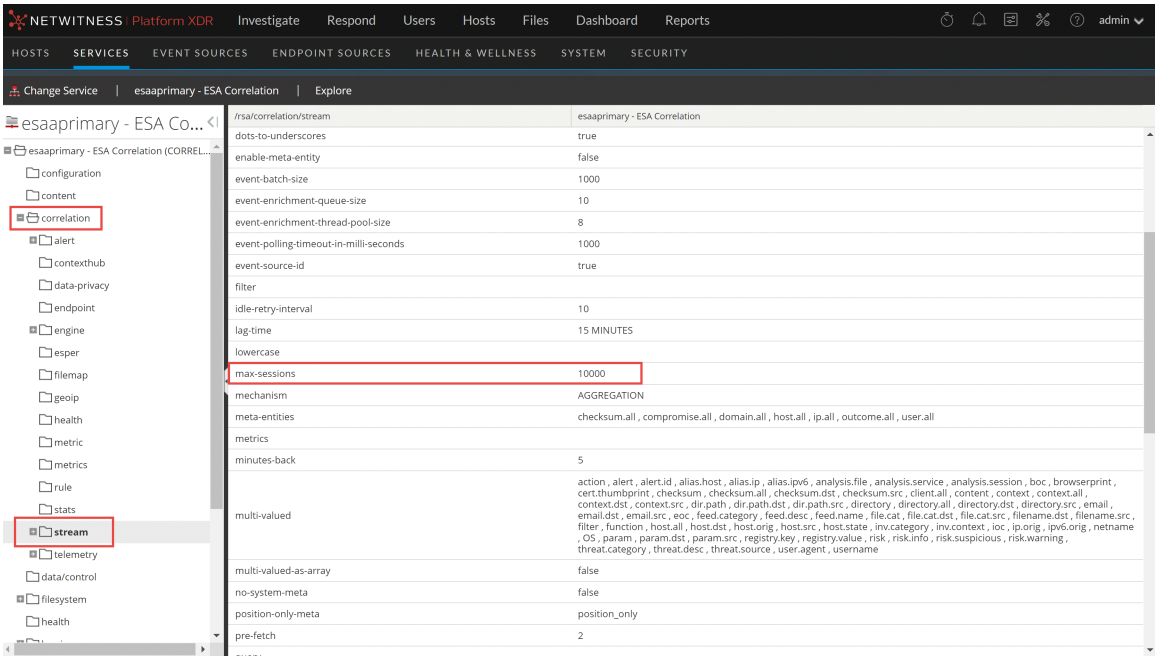
In NetWitness Platform 11.5 and later, you can add an optional data source filter to the data sources in your ESA rule deployments to improve performance. This allows your data sources to be filtered further so that only the data relevant to the deployment is forwarded to ESA. The filter is comprised of application rules, which are applied to the Decoders mapped to your selected data sources.

Caution: The data source filter is intended for advanced users familiar with Decoder application rules. Improper filtering can cause the required data to not be forwarded to and analyzed by ESA.

Using a data source filter can be performance intensive for data aggregation. A filter slows the event aggregation rate, but when you are filtering a large amount of traffic, it can have performance benefits on ESA Correlation server. However, if you use a complex filter and do not filter a large amount of traffic, the event aggregation rate may be lower than expected.

When filtering out a large portion of the traffic, you may see an "Invalid header size" error while communicating with Core services in the ESA Correlation log file. (You can use SSH to get in the system and go to: `/var/log/netwitness/correlation-server/correlation-server.log`). Lower the `max-sessions` parameter until you no longer see the error in the log. The more you filter out the traffic, the lower you should set the `max-sessions` parameter.

1. In the Explore view node list for an ESA Correlation service, select **correlation > stream**.



2. In `max-sessions`, lower the value until you no longer see the error in the ESA Correlation log file. The default value is **10000**.

3. Restart the ESA Correlation service. Go to **(Admin) > Services**, select the ESA Correlation service, and then select **> Restart**.

IMPORTANT: If an application rule linked to a data source filter is modified on a Decoder, the filter must be removed, added again, and redeployed. The changes take effect on ESA after the deployment is redeployed.

For more information, see “(Optional) Add a Data Source Filter” in the *Alerting with ESA Correlation Rules User Guide*.

Configure Meta Keys as Arrays in ESA Correlation Rule Values

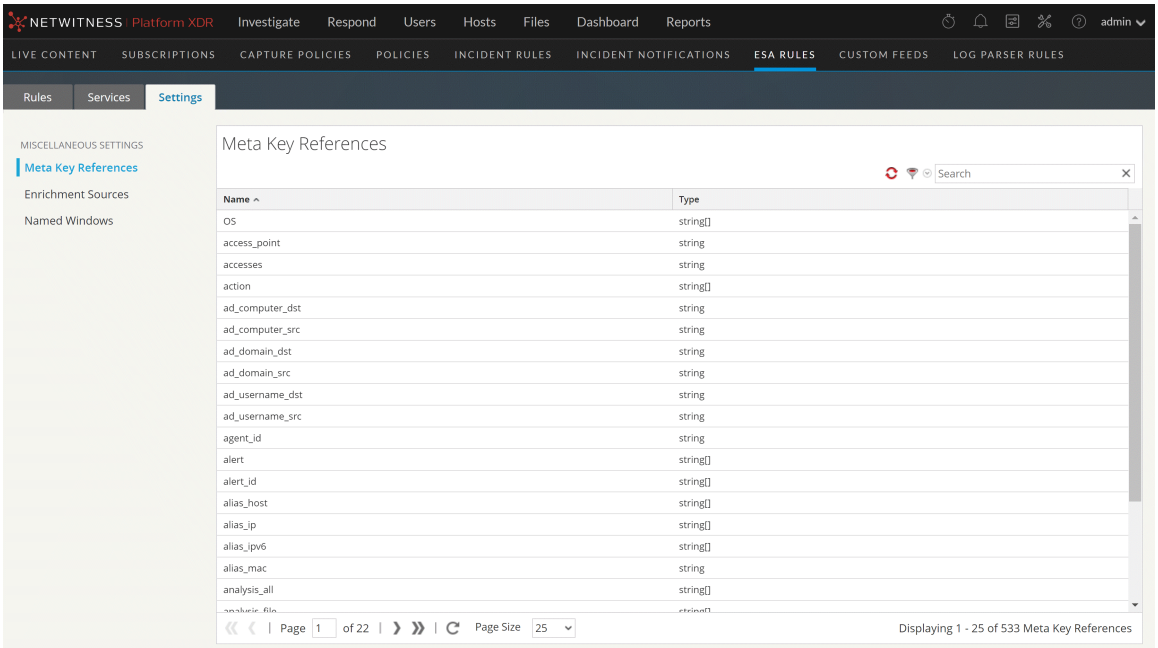
A common reason for an ESA rule to generate an error during deployment is because a meta key in the rule is a string array type, but it shows as a string type on ESA. To prevent or fix this issue, do the following:

- Determine if a Meta Key is a String Array Type on ESA
- Add the String Array Type Meta Key to ESA
- Verify that the String Array Type Meta Key is Configured Correctly on ESA

Caution: Changing string to string array type is not necessary for all fields. To support Endpoint, UEBA, and RSA Live content, specific string array (multi-value) and string (single-value) meta keys are required. See Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys.

Determine if a Meta Key is a String Array Type on ESA

1. Go to **(Configure) > ESA Rules** and click the **Settings** tab.



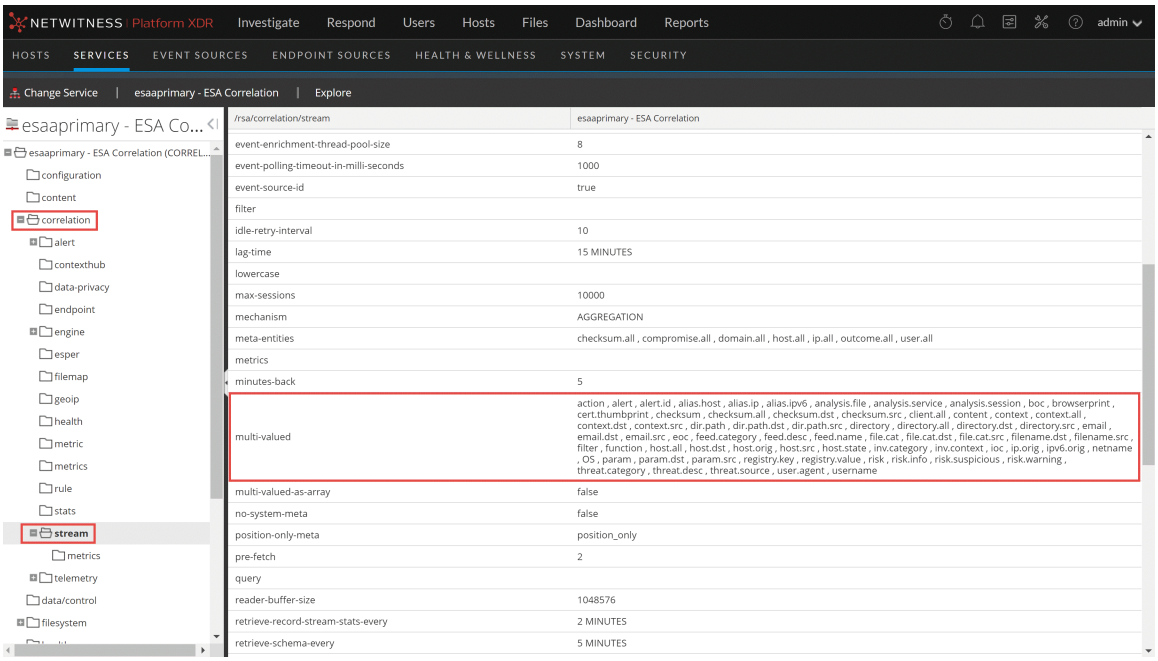
2. In the Meta Key References, for each meta key that is a string array type, locate the meta key in the Name field and then check the value.
   - If it shows `string[]`, it is configured as a string array type on ESA. This is fine.
   - If it shows `string` without the brackets, it is configured as a string type and you need to fix it on ESA. Go to Add the String Array Type Meta Key to ESA.

Caution: Changing string to string array type is not necessary for all fields. To support Endpoint, UEBA, and RSA Live content, specific string array (multi-value) and string (single-value) meta keys are required. See Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys.

Add the String Array Type Meta Key to ESA

Caution: Any changes that you make to the `multi-valued` parameter may cause an error when you deploy your existing rules. If you add a meta key to the `multi-valued` parameter field that you use in other ESA rules, ensure that those rules are using the string array syntax.

1. In the Explore view node list for an ESA Correlation service, select **correlation > stream**.
2. Add string array meta keys to the **`multi-valued`** list to allow them to be used as an array in ESA rules.



3. Verify the configuration on ESA. Go to Verify that the String Array Type Meta Key is Configured Correctly on ESA.

Note: The `multi-valued` parameter is equivalent to the `arrayFieldNames` parameter in the Event Stream Analysis service in NetWitness version 11.2 and earlier.

Verify that the String Array Type Meta Key is Configured Correctly on ESA

1. Go back to **(Configure) > ESA Rules** and click the **Settings** tab.
2. In the Meta Key References, click the Meta Re-Sync (Refresh) icon ( ).
3. Verify that the meta keys with a string array type show a value of `string[]`.

Required String Array Meta Keys on the ESA Correlation Service

To use the latest Endpoint, UEBA, and Live content rules, the following default **multi-valued** meta keys are required on the ESA Correlation service in NetWitness Platform version 11.3 and later:

```
action , alert , alert.id , alias.host , alias.ip , alias.ipv6 , analysis.file
, analysis.service , analysis.session , boc , browserprint , cert.thumbprint ,
checksum , checksum.all , checksum.dst , checksum.src , client.all , content ,
context , context.all , context.dst , context.src , dir.path , dir.path.dst ,
dir.path.src , directory , directory.all , directory.dst , directory.src ,
email , email.dst , email.src , eoc , feed.category , feed.desc , feed.name ,
file.cat , file.cat.dst , file.cat.src , filename.dst , filename.src , filter
, function , host.all , host.dst , host.orig , host.src , host.state ,
inv.category , inv.context , ioc , ip.orig , ipv6.orig , netname , OS , param
, param.dst , param.src , registry.key , registry.value , risk , risk.info ,
risk.suspicious , risk.warning , threat.category , threat.desc , threat.source
, user.agent , username
```

The following default **single-valued** meta keys are also required on the ESA Correlation service in NetWitness Platform 11.3.0.2 and later:

```
accesses , context.target , file.attributes , logon.type.desc , packets
```

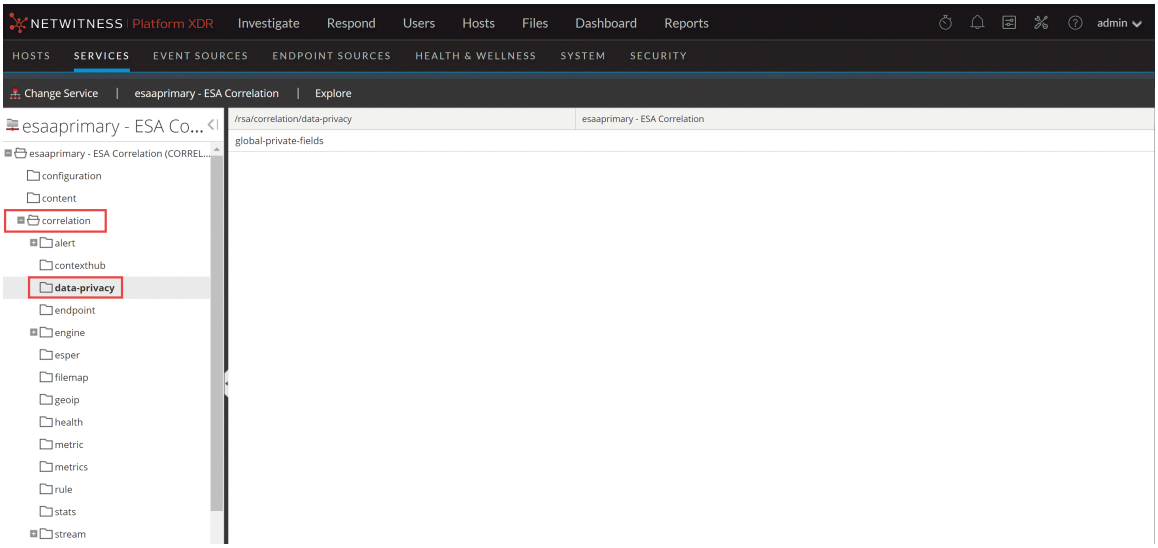
Note: Check the `default-multi-valued` and `default-single-valued` parameters on your ESA Correlation service for the latest required fields. For more information, see Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys.

Remove Sensitive Meta Keys Globally from All Alerts for Data Privacy

Note: This procedure applies only to ESA Correlation Rules in NetWitness Platform 11.4 and later versions.

For data privacy reasons, it may be necessary to remove some sensitive meta keys from the alert output globally, regardless of the data source. In the ESA Correlation service, you can set the **`global-private-fields`** parameter to remove the meta keys from all alert output.

1. Go to  **(Admin) > Services**, and in the Services view, select an ESA Correlation service and then select  **> View > Explore**.
2. In the Explore view node list for the ESA Correlation service, select **correlation > data-privacy**.
3. In the **`global-private-fields`** parameter, add the sensitive meta keys that you want removed from all alerts.



The changes are effective immediately.

For more information, see "How ESA Handles Sensitive Data" in the *Alerting with ESA Correlation Rules Configuration Guide*. For more information on the strategy and benefits of obfuscating data, see the *Data Privacy Management Guide*.

Configure Character Case for Advanced ESA Rules

Note: This procedure applies only to ESA Correlation Rules in NetWitness Platform 11.3.0.2 and later versions, however, it is not supported in version 11.3.1.0.

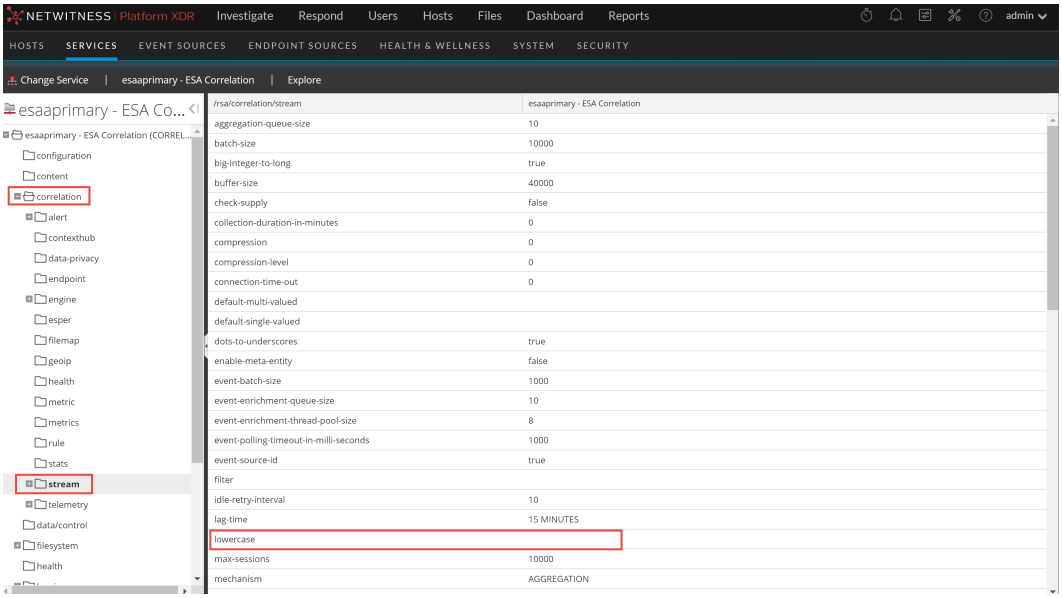
Advanced Event Processing Language (EPL) rules require correct character case, but in the Investigate Navigate view all characters are converted to lowercase. However, the meta keys may not be lowercase despite appearances in the Investigate Navigate view. To ensure you are using the correct case, you can use the `toLowerCase`() function. However, care should be taken to only add the case-insensitive `toLowerCase()` function on string and string array meta keys as needed. The `toLowerCase()` function can cause significant performance decreases. Consider checking the Investigate Events view or the Event Analysis view to see the real character case for meta fields and avoid unnecessary usage of the function. For more information, see "Event Process Language (EPL)" in the *Alerting with ESA Correlation Rules User Guide*.

You can optimize your rule performance by identifying the meta keys used most often in your environment. Instead of using the `toLowerCase()` function with the original meta key, replace the meta key throughout the rule with `<meta.key>_lower`. You can also use the special case-insensitive meta keys in your Rule Builder rules.
For example, you can configure ESA Correlation to use `filename_lower` (which is case insensitive) instead of using the original `filename` meta key. In your rule, replace `filename` with `filename_lower`.

To configure special case-insensitive meta keys to use in your ESA rules:

1. Go to  **(Configure) > ESA Rules > Rules** tab. In your ESA rule deployments, identify any ESA rules using the `toLowerCase()` function more than ten times for a particular string or string array meta key. Keep track of these ESA rules and meta keys.
2. Go to  **(Admin) > Services**, select an ESA Correlation service, and then select  **> View > Explore**.

3. In the Explore view node list, select **correlation > stream**.
   Notice that there is a **`lowercase`** parameter with empty values.



4. Update the **`lowercase`** parameter with the string or string array meta keys identified in step 1 using a comma separated list, for example: `protocol,alias.host,action,alert`

> **Note:** String and string array are the only data types supported for the ESA Correlation service **`lowercase`** parameter.
>
> Use NWDB format (decimal), NOT Esper format (underscore). Do not press **Enter** to commit or it will put in a return. Instead, click another parameter.

5. After you add all of the meta keys, validate the meta keys on ESA.

   a. Go to **(Configure) > ESA Rules > Settings tab > Meta Key References** and click the Meta Re-Sync (Refresh) icon ( ).

   b. Search for **`_lower`** or **`<meta key>_lower`**, for example: `protocol_lower`.

   - The meta keys with a string array type should show a value of `string[]`.
   - The meta keys with a string type should show a value of `string` (without the brackets).

6. Update all of your ESA rules that use `.toLowerCase` meta keys and replace them with `<meta key>_lower` (Example: filename_lower IN ('svchost.exe'))
7. Deploy the ESA rule deployment again.

> **Note:** If you remove a meta key from the `lowercase` parameter list and re-sync the meta key references, you also need to update the rules that use the corresponding lowercase meta key (`<meta.key>_lower`).

Deploy Endpoint Risk Scoring Rules on ESA

Endpoint Risk Scoring Rules only apply to NetWitness Endpoint.

The ESA Correlation service processes and deploys endpoint risk scoring rules. These rules generate alerts that are used in risk scoring calculations to identify suspicious files and hosts. To turn on Risk Scoring for NetWitness Endpoint, you must deploy endpoint risk scoring rules on ESA. An *Endpoint Risk Scoring Rules Bundle* comes with NetWitness along with the sample ESA rules. The Endpoint Risk Scoring Bundle contains approximately 400 rules. You add this rule bundle to an ESA Rule Deployment in the same way that you would add any ESA rule. However, you must specify endpoint data sources (Concentrators) during ESA Rule Deployment.

For complete information on configuring NetWitness Endpoint, see the *NetWitness Endpoint Configuration Guide*. For more information about ESA rule deployments, see "Deploy Rules to Run on ESA" in the *Alerting with ESA Correlation Rules User Guide*.

Go to the NetWitness All Versions Documents page and find NetWitness Platform guides to troubleshoot issues.

Important Considerations when Deploying the Endpoint Risk Scoring Rules Bundle

- If you add the Endpoint Risk Scoring Bundle to an ESA rule deployment, the deployment should have data sources with endpoint data.
- An ESA rule deployment can have only one ESA Correlation service. You can, however, use the same ESA Correlation service in multiple deployments.
- If you have two ESA Correlation services with the same endpoint data sources, deploy the Endpoint Risk Scoring Rules Bundle on only one of them.

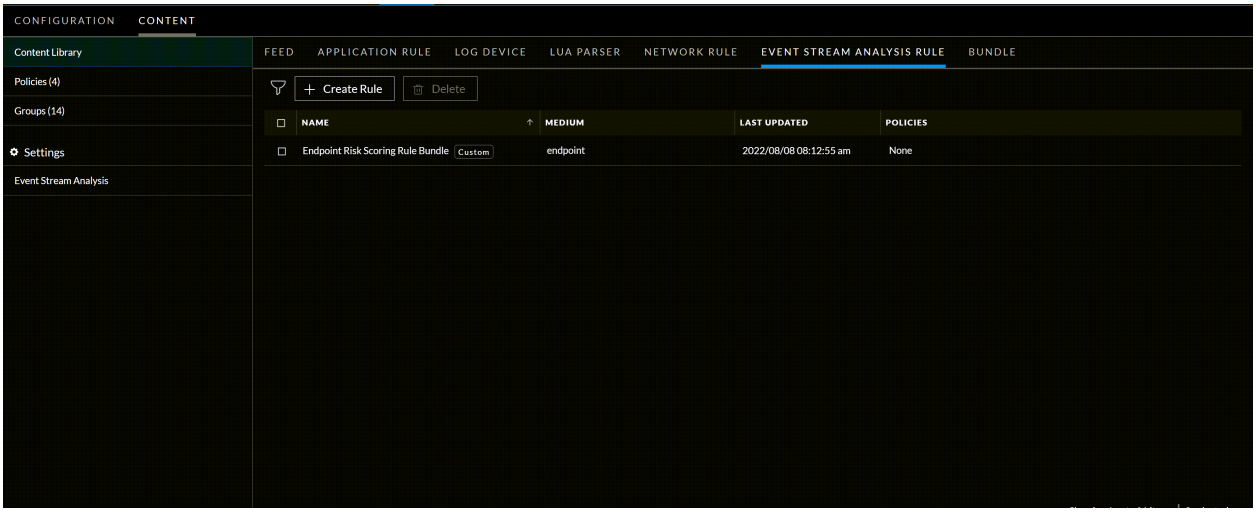
Deploy the Endpoint Risk Scoring Rules Bundle on ESA

Caution: Before you deploy the Endpoint risk scoring rules, update your meta keys. See Update Your ESA Rules for the Required Multi-Value and Single-Value Meta Keys.

When you deploy the Endpoint Risk Scoring Rules Bundle in an ESA rule deployment, the ESA Correlation service gathers endpoint data in your network and runs endpoint risk scoring rules against the data. The goal is to capture events that match rule criteria, then generate alerts for the captured events.

The following procedure shows how to create an ESA rule deployment with the Endpoint Risk Scoring Rules Bundle and deploy it. If you already have an ESA rule deployment with endpoint data sources, you can add the Endpoint Risk Scoring Rules Bundle to the existing deployment.

The following figure shows the Endpoint Risk Scoring Bundle available in (Configure) > **Policies** > **Content Library** > **Event Stream Analysis Rule** page.



To create and deploy an ESA rule deployment with the Endpoint Risk Scoring Bundle

1. Go to **(Configure)** > **Policies**.
2. Add the endpoint data sources, for more information, see Add an ESA Datasource.
3. Create a deployment with Endpoint Risk Scoring Bundle. For more information, see Create a Deployment.

   You can now view information and statistics on the **(Configure) > ESA Rules > Services** tab. See View the Status of the Endpoint Risk Scoring Rules Deployment.

Change the Endpoint Risk Scoring Rule Bundle in a Deployment

You cannot edit or duplicate the Endpoint Risk Scoring Rules Bundle. After the bundle is deployed, you can enable and disable individual rules within the bundle. See Disable or Enable Individual Endpoint Risk Scoring Rules.

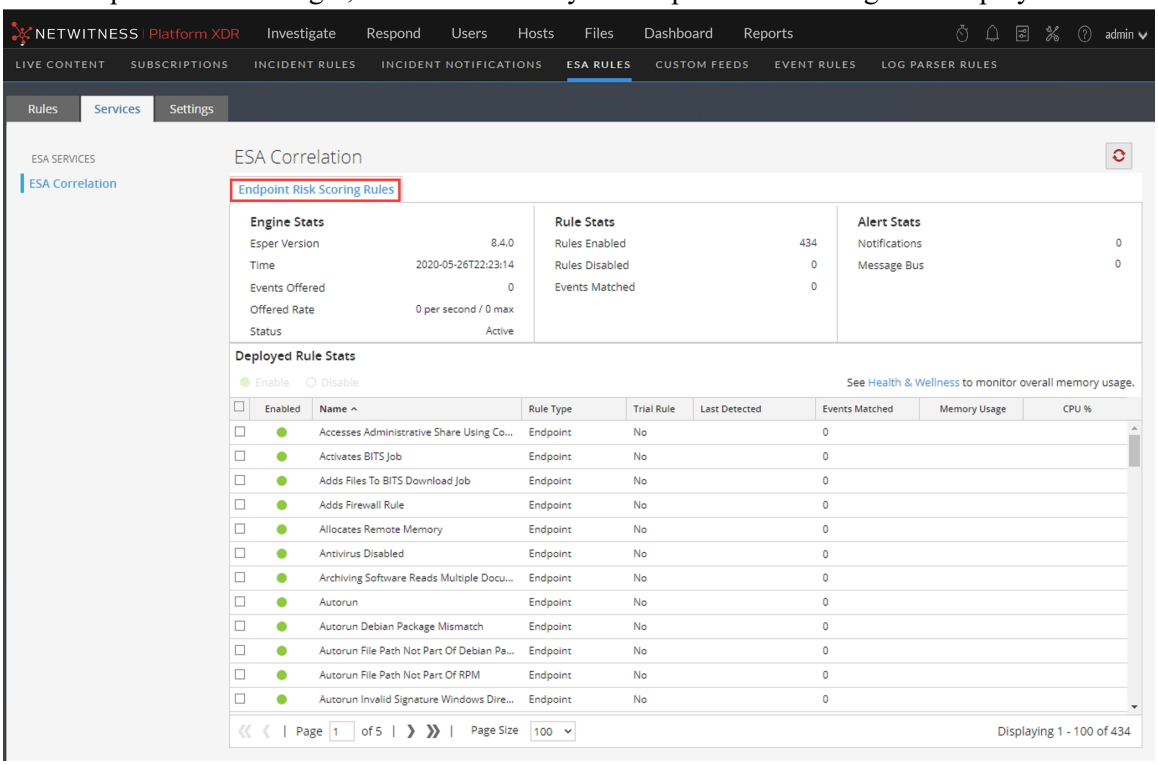
When you make changes to the ESA Rule Deployment containing the Endpoint Risk Scoring Rules Bundle, such as changing the endpoint data sources or changing compression levels, you must redeploy it for the changes to take effect. To redeploy, click the **Deploy Now** button for that deployment.

Caution: Deleting an ESA Rule Deployment with an Endpoint Risk Scoring Rule Bundle stops the Risk Scoring alerts that are used in risk scoring calculations to identify suspicious files and hosts.

For more information about changing ESA rule deployments, see "Additional ESA Rule Deployment Procedures" in the *Alerting with ESA Correlation Rules User Guide*.

View the Status of the Endpoint Risk Scoring Rules Deployment

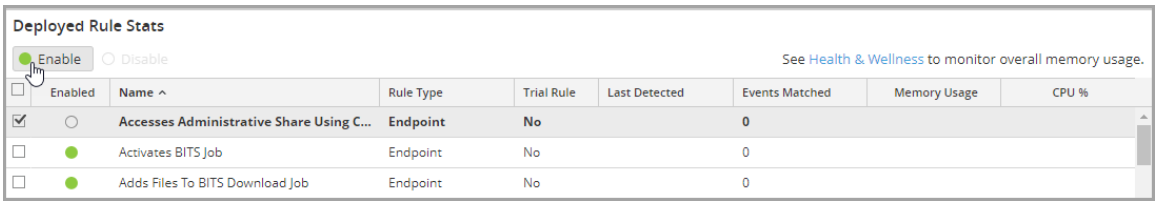
1. Go to the ESA Rules Services tab (**(Configure) > ESA Rules > Services**).
2. In the options panel on the left, select your ESA Correlation service.
   Your deployment name shows on a tab to the right, for example, Endpoint Risk Scoring Rules. If you see multiple tabs on the right, select the tab for your endpoint risk scoring rules deployment.



3. In the **Engine Stats**, **Rules Stats** and **Alert Status** sections, look at the statistics related to the deployment, such as Rules Enabled, Rules Disabled, and Events Matched, which show the total numbers for the deployment.
4. In the **Deployed Rules Stats** section, look at the following details for each Endpoint Risk Scoring Rule:
   - **Enable**: Indicates the enabled status. A green circle icon ● indicates that the rule is enabled. A white circle icon ○ indicates that the rule is disabled.
   - **Name**: Shows the name of the rule.
   - **Rule Type**: Endpoint indicates a rule from the Endpoint Risk Scoring Bundle and Esper indicates Esper-specific rules, such as Rule Builder and Advanced EPL rules.
   - **Last Detected**: Shows the last time an alert was triggered for the rule.
   - **Events Matched**: Shows the total number of events that matched the rule.

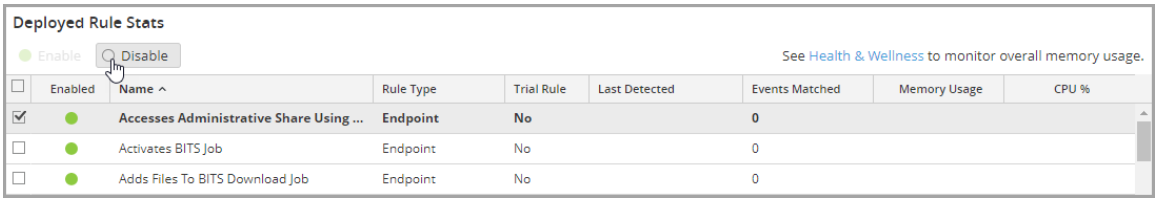
Disable or Enable Individual Endpoint Risk Scoring Rules

1. Go to the ESA Rules Services tab (**(Configure) > ESA Rules > Services**).
2. In the options panel on the left, select your ESA Correlation service.
   Your deployment name shows on a tab to the right, for example, Endpoint Risk Scoring Rules. If you see multiple tabs on the right, select the tab for your endpoint risk scoring rules deployment.
3. In the **Deployed Rules Stats** section, do one of the following:
   - To enable rules, select the rules that you want to enable in the rules list and click the **Enable** button above the list.



   The selected rules are enabled and a message shows that the rules enabled successfully.

   - To disable rules, select the rules that you want to disable in the rules list and click the **Disable** button above the list.



   The selected rules are disabled and a message shows that the rules disabled successfully.

Change Memory Threshold for ESA Rules

The following procedures pertain to setting memory thresholds for ESA rules to prevent them from using excessive memory.

Change Memory Threshold for All Trial Rules

This procedure is optional and applies only to ESA Correlation Rules.

Administrators can increase or decrease the memory threshold for trial rules. Threshold refers to the ESA memory usage, which includes ESA base memory, trial rules, and non-trial rules. When the threshold is exceeded, all deployed trial rules on an ESA service are disabled.

You use trial rules to see if a rule runs efficiently and does not use excessive memory, which can impact performance or force the service to shut down.

By default, the memory threshold is 90, which is the percentage of Java Virtual Memory (JVM).

- The memory threshold is per ESA, not per rule.
- When the memory threshold is exceeded, all trial rules running on the ESA are automatically disabled.
- The ESA configuration has the following parameters for trial rules:
  - `fatal-percentage`: If memory rises above this percentage, ESA disables trial rules. For example, if fatal-percentage is set to 90, when memory rises above 90 percent, ESA disables trial rules.
  - `check-every`: This parameter determines how often ESA checks the fatal-percentage to disable trial rules.

For more information, see "Work with Trial Rules" in the *Alerting with ESA Correlation Rules User Guide*.

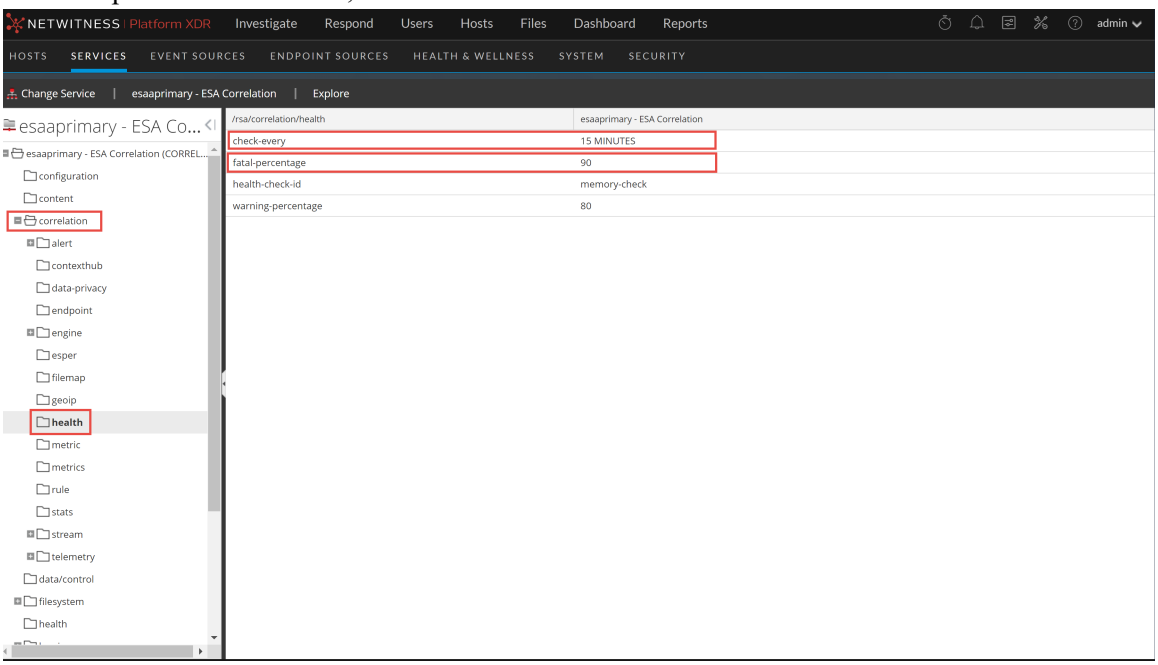
Prerequisites

A role with administrative privileges must be assigned to you.

To change memory threshold for trial rules:

1. Log on to NetWitness as admin.
2. Go to  **(Admin) > Services**.
3. Select the ESA Correlation service and then select  **> View > Explore**.

4. In the Explore view node list, select **correlation > health**.



5. In the right panel, in `fatal-percentage`, type a percentage of JVM that trial rules on the ESA cannot exceed.
   The new memory threshold takes effect immediately.
6. If necessary, you can also adjust the `check-every` parameter, which determines how often ESA checks the fatal-percentage to disable trial rules. By default, ESA checks the fatal-percentage every 15 minutes.

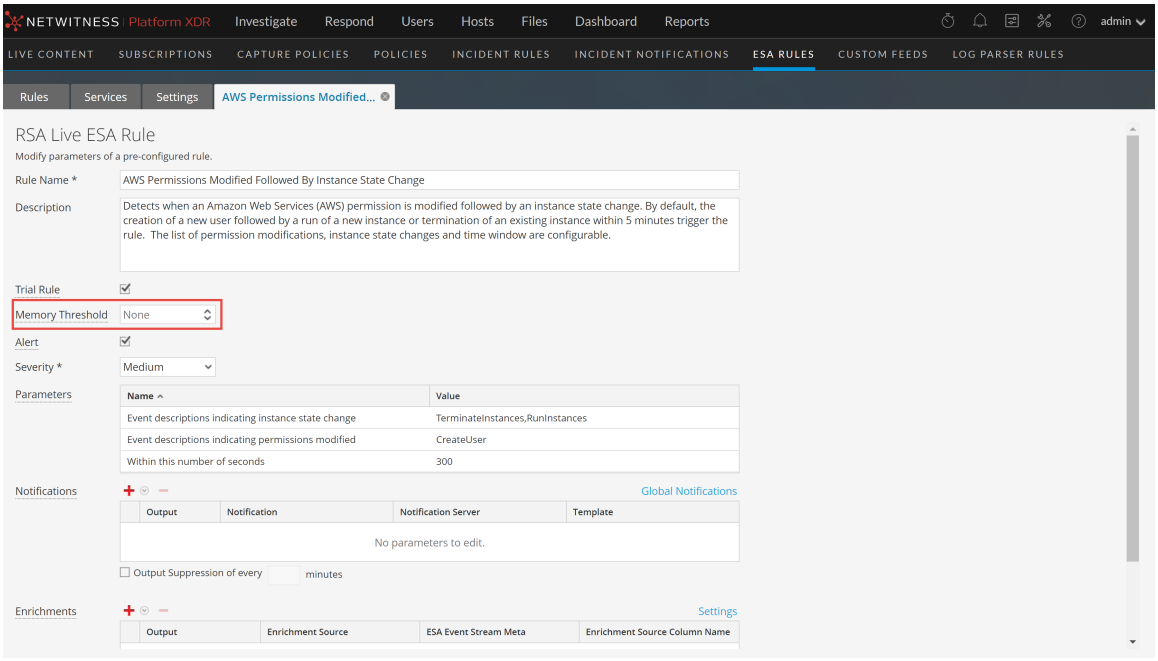
Change Memory Threshold for Individual Trial Rules and Non-Trial Rules

Note: This option is available in NetWitness Platform version 11.5 and later.

In addition to setting a memory threshold for all trial rules, you can set a memory threshold individually for both trial rules and non-trial rules. New rules default to a 100 MB memory threshold. Rules that existed before version 11.5 do not have a default value and a memory threshold is not set. You should configure a memory threshold for rules that use memory, such as a rule that contains windows or pattern matching. If the configured memory threshold is exceeded, the rule gets disabled individually and an error is displayed for that rule on the (Configure) > ESA Rules > Services tab.

1. Go to **(Configure) > ESA Rules >Rules** tab.
2. In the **Rule Library**, select the rule you want to configure and click .
   The rule details are displayed.

3. In the **Memory Threshold** field, add the maximum memory usage allowed for this rule in MB. **100 MB** is the default for new rules.



4. Click **Save**.
5. When you are finished changing the memory thresholds for individual rules in an ESA rule deployment, redeploy the deployment.
   For more information, see the *Alerting with ESA Correlation Rules User Guide*.

Start, Stop, or Restart ESA Service

This topic provides instructions to start, stop, or restart the ESA Correlation service from the NetWitness user interface and from the command line. These procedures apply to ESA Correlation Rules.

Start the ESA Service

1. Log on to NetWitness as admin.
2. Go to **(Admin) > Services**.
3. Select the ESA Correlation service and then select **> Start**.

Stop the ESA Service

1. Log on to NetWitness as admin.
2. Go to **(Admin) > Services**.
3. Select the ESA Correlation service and then select **> Stop**.

Restart the ESA Service

1. Log on to NetWitness as admin.
2. Go to **(Admin) > Services**.
3. Select the ESA Correlation service and then select **> Restart**.

Start the ESA Service from the Command Line

1. Use ssh to connect to the ESA Correlation service and log in as the root user.
2. Type the following command and press **ENTER**:
   ```
   systemctl start rsa-nw-correlation-server
   ```

Stop the ESA Service from the Command Line

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press **ENTER**:
   ```
   systemctl stop rsa-nw-correlation-server
   ```

Restart the ESA Service from the Command Line

1. Use ssh to connect to the ESA service and log in as the root user.
2. Type the following command and press **ENTER**:
   `systemctl restart rsa-nw-correlation-server`

View Audit Logs and Verify ESA Component Versions

This topic provides details about audit logging and instructions to verify the versions of the ESA components installed. These procedures apply to ESA Correlation Rules.

View Audit Logs for Rules

Audit logging allows you to view details about rules that are created and changed in NetWitness. There are local audit logs in each of the services in NetWitness. When Global Audit Logging is configured, NetWitness audit logs collect in a centralized system that converts them into the required format and forwards them to an external syslog system.

For details on how to access your local audit logs, see "Local Audit Log Locations" in the *System Configuration Guide*. To set up Global Audit Logging, see "Configure Global Audit Logging" in the *System Configuration Guide*.

The following Syslog global audit log examples show create, update, remove rule, and delete deployment actions for the ESA Correlation service (correlation-server).

Create Action

```
09-17-2018 08:59:50 System3.Info 10.0.0.0 Sep 17 15:59:54 esaprimary
{deviceVendor=RSA, deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} DataAccess{action=create, success=true,
identity=admin, parameters={EngineSettings=}}09-17-2018 08:59:50 System3.Info
10.0.0.0 Sep 17 15:59:54 esaprimary {deviceVendor=RSA, deviceVersion=11.3.0.0,
deviceService=correlation-server, deviceServiceId=1abc9465-d0d4-48a9-9205-
414066fabc2f, deviceProduct=NetWitness} DataAccess{action=create,
success=true, identity=admin, parameters={EngineSettings=}}09-17-2018 08:59:50
System3.Info 10.0.0.0 Sep 17 15:59:54 esaprimary {deviceVendor=RSA,
deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} API{action=/rsa/correlation/module/settings/set,
success=true, identity=admin, parameters={Arguments=[ModuleSettings(id=null,
name=a-d-v:multiple_failed-login_successful-login-rule-module,
displayName=ADV: Multiple_FailedLogin_SuccessfulLogin, enabled=true,
eplStatements=[module GHmoduleId15;@Name('GHmoduleName15') @Description
('GHmoduleDesc15') @RSAAlert(oneInSeconds=0, identifiers=
{"user_dst"}
) SELECT * FROM Event(ec_outcome in ('Success', 'Failure') AND ec_
activity='Logon').win:time(5 min) match_recognize (measures F as f_array, S as
s pattern (F F F F F+ S+) define F as F.ec_outcome= 'Failure', S as S.ec_
outcome= 'Success');], queries=[], maxConstituentEvents=null,
logFiredRules=null, trial=false, alert=ModuleSettings.Alert
(respondEnabled=true, severity=9, notificationReasons=[], uniqueIdentifiers=
[], rateLimit=RateL...09-17-2018 08:59:50 System3.Info 10.0.0.0 Sep 17
15:59:54 esaprimary {deviceVendor=RSA, deviceVersion=11.3.0.0,
deviceService=correlation-server, deviceServiceId=1abc9465-d0d4-48a9-9205-
414066fabc2f, deviceProduct=NetWitness} DataAccess{action=create,
success=true, identity=admin, parameters={ModuleSettings=}}
```

Update Action

```
09-17-2018 08:54:21 System3.Info 10.0.0.0 Sep 17 15:54:25 esaprimary
{deviceVendor=RSA, deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} DataAccess{action=update, success=true,
identity=admin, parameters={EngineSettings=5b9fce315068213b17760553}}09-17-
2018 08:54:21 System3.Info 10.0.0.0 Sep 17 15:54:25 esaprimary
{deviceVendor=RSA, deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} DataAccess{action=update, success=true,
identity=admin, parameters={EngineSettings=5b9fce315068213b17760553}}09-17-
2018 08:54:21 System3.Info 10.0.0.0 Sep 17 15:54:25 esaprimary
{deviceVendor=RSA, deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} API{action=/rsa/correlation/engine/settings/set,
success=true, identity=admin, parameters={Arguments=[EngineSettings(id=null,
name=endpoint-sa-managed, displayName=endpoint, description=endpoint,
enabled=true, eventType=Event, instanceId=1abc9465-d0d4-48a9-9205-
414066fabc2f, streamId=5b9fce314a5b1f5951babc29, moduleIds=
[5b9fce314a5b1f5951babc2a, 5b9fce314a5b1f5951babc2b],
enableStatementMetric=null)]}}
```

Remove Rule Action

```
09-17-2018 09:01:11 System3.Info 10.0.0.0 Sep 17 16:01:15 esaprimary
{deviceVendor=RSA, deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} API{action=/rsa/correlation/stream/settings/remove,
success=true, identity=admin, parameters={Arguments=
[5b9fcf7a4a5b1f5951babc2c]}}09-17-2018 09:01:11 System3.Info 10.0.0.0 Sep 17
16:01:15 esaprimary {deviceVendor=RSA, deviceVersion=11.3.0.0,
deviceService=correlation-server, deviceServiceId=1abc9465-d0d4-48a9-9205-
414066fabc2f, deviceProduct=NetWitness} API
{action=/rsa/correlation/stream/settings/remove, success=true, identity=admin,
parameters={Arguments=[5b9fcf7a4a5b1f5951babc2c]}}09-17-2018 09:01:11
System3.Info 10.0.0.0 Sep 17 16:01:15 esaprimary {deviceVendor=RSA,
deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} DataAccess{action=remove, success=true,
identity=admin, parameters={StreamSettings=5b9fcf7a4a5b1f5951babc2c}}
```

Delete Deployment Action

```
09-17-2018 09:02:45 System3.Info 10.0.0.0 Sep 17 16:02:50 esaprimary
{deviceVendor=RSA, deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} API{action=/rsa/correlation/engine/settings/remove,
success=true, identity=admin, parameters={Arguments=
[5b9fcfcb4a5b1f5951babc2f]}}09-17-2018 09:02:45 System3.Info 10.0.0.0 Sep 17
16:02:50 esaprimary {deviceVendor=RSA, deviceVersion=11.3.0.0,
deviceService=correlation-server, deviceServiceId=1abc9465-d0d4-48a9-9205-
414066fabc2f, deviceProduct=NetWitness} API
{action=/rsa/correlation/engine/settings/remove, success=true, identity=admin,
parameters={Arguments=[5b9fcfcb4a5b1f5951babc2f]}}09-17-2018 09:02:45
```

```
System3.Info 10.0.0.0 Sep 17 16:02:50 esaprimary {deviceVendor=RSA,
deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} DataAccess{action=remove, success=true,
identity=admin, parameters={EngineSettings=5b9fcfcb4a5b1f5951babc2f}}09-17-
2018 09:02:45 System3.Info 10.0.0.0 Sep 17 16:02:50 esaprimary
{deviceVendor=RSA, deviceVersion=11.3.0.0, deviceService=correlation-server,
deviceServiceId=1abc9465-d0d4-48a9-9205-414066fabc2f,
deviceProduct=NetWitness} API{action=/rsa/correlation/engine/stop,
success=true, identity=admin, parameters={Arguments=[madhavi-sa-managed]}}
```

Each log contains the following parameters:

- **Time stamp**: Time the rule was modified. Example: `09-17-2018 08:54:21`
- **System Info**: Information about the system where the action was performed, such as IP address. Example: `10.0.0.0`
- **deviceVersion**: Version of your ESA service. Example: `11.3.0.0`
- **deviceService**: Example: `correlation-server`
- **action**: Examples: `create`, `update`, `remove`
- **Parameters**: Placeholder for the following keys:
  - **Epl Module Identifier (moduleIds)**: unique identifier for the rules. Example: `5b9fce314a5b1f5951babc2a, 5b9fce314a5b1f5951babc2b`
  - **enabled**: Shows if the rule is enabled or not. Example: `enabled=true`
  - **respondEnabled**: Shows if alerts from this rule can go to the Respond view. Example: `respondEnabled=true`
  - **trial**: Displays if the rule is configured as a trial rule or not. Example: `trial=false`
  - **EplStatements**: Displays the rule syntax. Example:

    ```
    eplStatements=[module GHmoduleId15;@Name('GHmoduleName15') @Description
    ('GHmoduleDesc15') @RSAAlert(oneInSeconds=0, identifiers=

    {"user_dst"}

    ) SELECT * FROM Event(ec_outcome in ('Success', 'Failure') AND ec_
    activity='Logon').win:time(5 min) match_recognize (measures F as f_array,
    S as s pattern (F F F F F+ S+) define F as F.ec_outcome= 'Failure', S as
    S.ec_outcome= 'Success');]
    ```

  - **identity**: Example: `admin`

ESA Audit Logs on NW Server (11.5 and Later)

In NetWitness Platform 11.5 and later, in addition to the audit logs available on ESA Correlation-server, new audit logs on the NW Server (SA_SERVER) show when users add, modify, filter, delete, export, and import ESA rules in the Rule Library. The NW Server audit logs also show when users add, modify, and deploy ESA rule deployments. Modifications to an ESA rule deployment include adding, deleting, or updating a rule in a deployment as well as adding a data source or an ESA Correlation service to a deployment.

Verify ESA Correlation Version

1. Use ssh to connect to the ESA Correlation service and log in as the root user.
2. Type the following command and press ENTER:
   ```
   rpm -qa | grep rsa-nw-correlation-server
   ```
   The ESA Correlation server version is displayed.