RSA NETWITNESS® PLATFORM

ESA Configuration Guide

for RSA NetWitness® Platform 11.3

Contact Information

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

Trademarks

For a list of RSA trademarks, go to https://www.rsa.com/en-us/company/rsa-trademarks.

License Agreement

Third-Party Licenses

This product may include software developed by parties other than RSA. By using this product, a user of this product agrees to be fully bound by terms of the license agreements applicable to third-party software in this product.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

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

April 2020

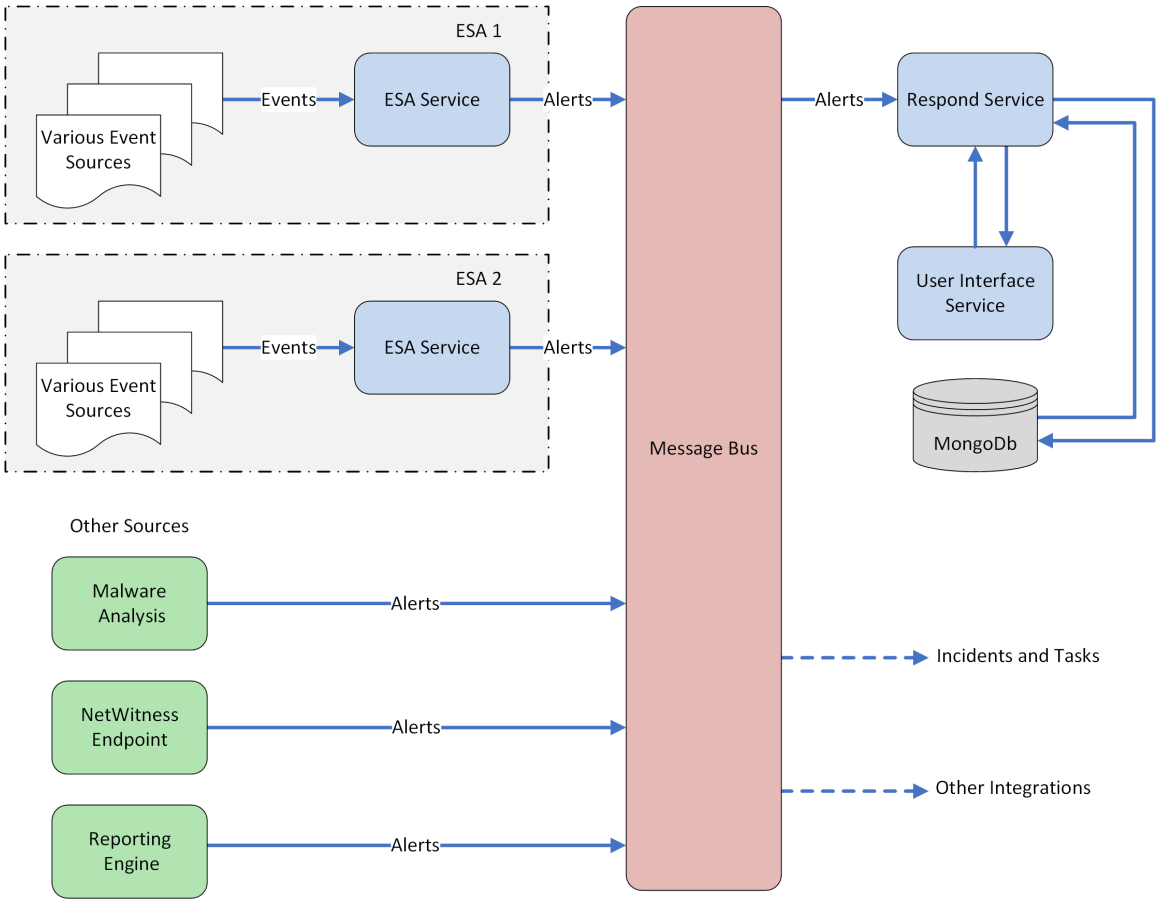
Contents

Event Stream Analysis Overview

RSA NetWitness® Platform 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:



There are two ESA services that can run on an ESA host:

- ESA Correlation (ESA Correlation rules)
- Event Stream Analytics Server (ESA Analytics)

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.

For NetWitness Platform 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 ESA Analytics service, which is used for Automated Threat Detection. Because the ESA Analytics service uses preconfigured ESA Analytics modules for Automated Threat Detection, you do not have to create or download rules to use Automated Threat Detection.

ESA Analytics services use query-based aggregation (QBA) to collect filtered events for the ESA Analytics modules from Concentrators. Only the data required by a module is transferred between the Concentrator and the ESA Analytics system. For example, using a Suspicious Domains ESA Analytics module, such as C2 for Packets (http-packet), an ESA Analytics service can examine your HTTP traffic to determine the probability that malicious activity is occurring in your environment.

Note: The Contexthub Server service, which provides enrichment lookup capability in the Respond and Investigate views, runs only on an ESA Primary host. For information, see the *Context Hub Configuration Guide*.

Configure ESA Correlation Rules

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

Data Source Configuration Changes

In NetWitness Platform 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 "Deploy Rules to Run on ESA" in the *Alerting with ESA Correlation Rules User Guide*.

An Endpoint Risk Scoring Rules Bundle is Available

An Endpoint Risk Scoring Rules Bundle, which contains approximately 400 rules, comes with NetWitness Platform 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*.

Upgrade Considerations for ESA Rule Deployments

Caution: After upgrading to NetWitness Platform version 11.3 or later, due to the ESA Correlation service data source changes, there are necessary data changes to migrated ESA rule deployments.

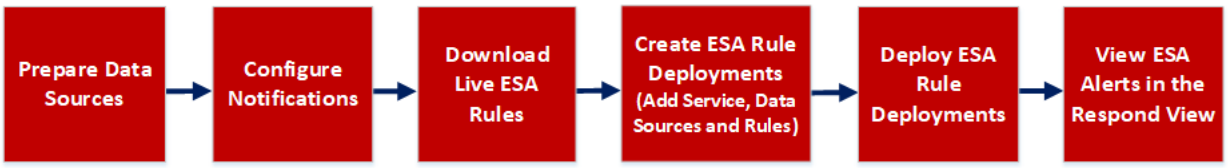
After the upgrade to version 11.3 or later, migrated ESA rule deployments change as follows:

1. If an ESA rule deployment contains two services before 11.3, the deployment splits into two deployments. You can only have one ESA Correlation service in an ESA rule deployment in version 11.3 or later.
2. If an ESA service has multiple ESA rule deployments before 11.3, they combine into one deployment in version 11.3 or later. You can still access your old deployments. For a detailed example, see ESA Rule Deployments Upgrade Example.

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.

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 Platform 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 Platform Live Content Management System (known as *Live*) is a valuable source of the latest internet security resources for NetWitness Platform 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 Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

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" in the *Alerting with ESA Correlation Rules User Guide*.
3. Download Event Stream Analysis rules using Live. Configure the Live ESA Rule parameters for your environment.	Refer to "Download Configurable RSA Live Rules" in the *Alerting with ESA Correlation Rules User Guide*.
4. Create ESA rule deployments*: Choose ESA Rules and the appropriate ESA service to use in the ESA rule deployment. For NetWitness Platform 11.3 and later, you must also choose the data sources to use for these rules.	Refer to "Deployment Steps" in the *Alerting with ESA Correlation Rules User Guide*.
5. Deploy ESA rule deployments.*	Refer to "Deployment Steps" in the *Alerting with ESA Correlation Rules User 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 Platform 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 Rule Deployments Upgrade Example

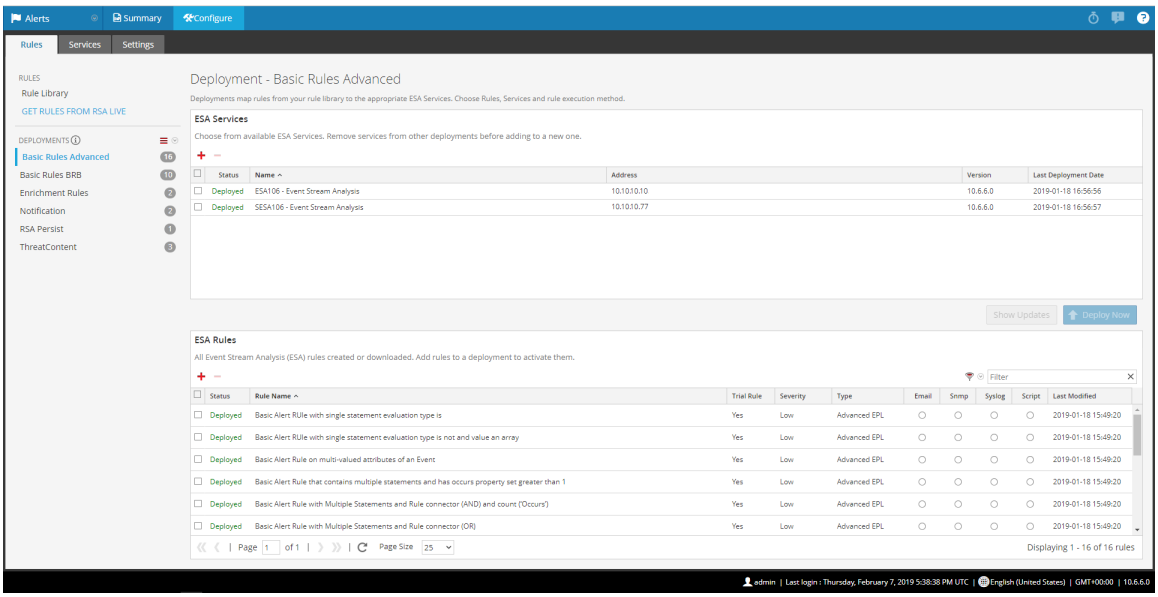
After you upgrade or update to 11.3, verify your ESA rule deployments. For every ESA host, a new deployment is created in the format `<ESA Host name> - ESA Correlation`.

- Verify that a new deployment was created.
- The new deployment should contain an ESA Correlation service, data sources, and rules for all previous deployments on that ESA host.
- The ESA Correlation service should have a status of "Deployed".

The following example shows the changes to NetWitness Platform 10.6.6 ESA rule deployments before and after the upgrade to version 11.3. In this example, before the upgrade there are six 10.6.6 ESA rule deployments. Four deployments have both ESA primary and ESA secondary Event Stream Analysis services. One deployment has only the ESA primary service and another one has only the ESA secondary service. Each 10.6.6 ESA rule deployment before the upgrade has a set of rules as shown in the following table:

10.6.6 ESA Rule Deployment (Before Upgrade)	# of Rules	ESA Primary	ESA Secondary
Basic Rules Advanced	16	x	x
Basic Rules BRB	10	x	x
Enrichment Rules	2	x	x
Notification	2		x
RSA Persist	1	x	
Threat Content	3	x	x
Total # of Rules		**32**	**33**

The following figure shows the 10.6.6 ESA rule deployments before the upgrade.



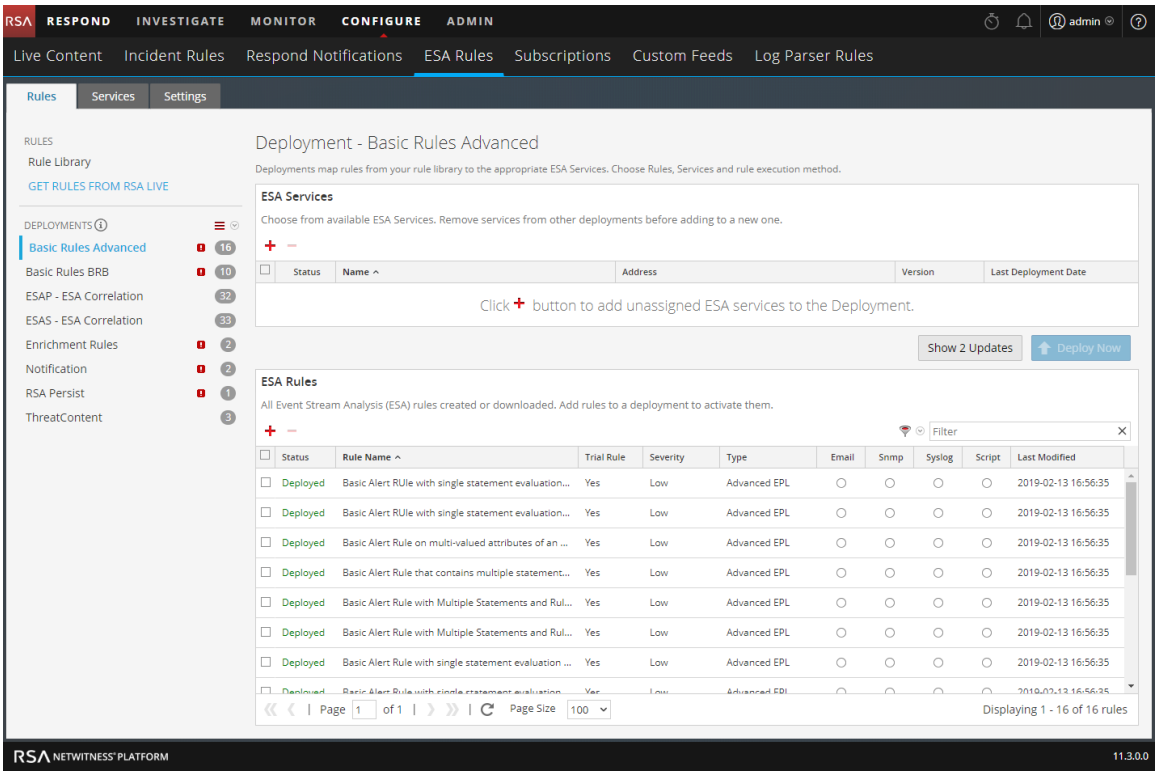
In this example, after the upgrade to 11.3, there are only two functional ESA rule deployments; one has the ESA primary (ESAP) ESA Correlation service and the other has the ESA secondary (ESAS) ESA Correlation service. The ESAP - ESA Correlation service deployment contains 32 rules, which is the total of all of the rules in the 10.6.6 deployments that contained the ESA primary service (16 + 10 + 2 + 1 + 3). The ESA secondary ESA Correlation service contains 33 rules, which is the total of all the rules in the 10.6.6 deployments that contained the ESAS Service (16 + 10 + 2 + 2 + 3). Since the RSA Persist deployment only contained one ESA primary service in 10.6.6, that rule was added to the ESAP 11.3 deployment. Since the Notification 10.6.6 deployment contained one ESA secondary service, the rule was added to the 11.3 ESAS deployment.

The following table shows the 11.3 ESA rule deployments after upgrade, the number of rules in each deployment, and which deployments have the ESA primary and ESA secondary ESA Correlation services.

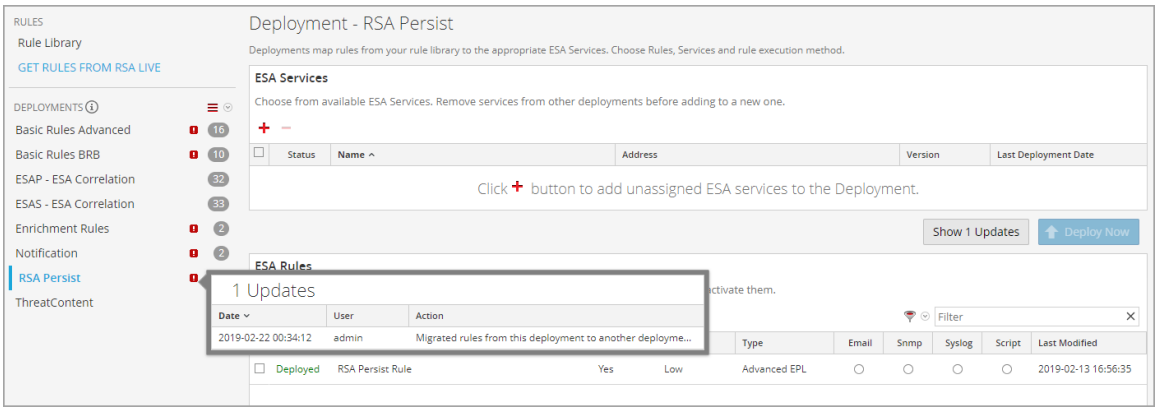
11.3 ESA Rule Deployment (After Upgrade)	# of Rules	ESA Primary	ESA Secondary
Basic Rules Advanced	16		
Basic Rules BRB	10		
ESAP - ESA Correlation	**32**	**x**	
ESAS - ESA Correlation	**33**		**x**
Enrichment Rules	2		
Notification	2		
RSA Persist	1		
Threat Content	3	_	_
Total # of Rules		**32**	**33**

In this example, all of the 10.6.6 ESA rule deployments were moved to 11.3, but they have no services after the upgrade. The only functional 11.3 ESA rule deployments are ESAP and ESAS. The 10.6.6 ESA rule deployments are preserved in case you want to use them.

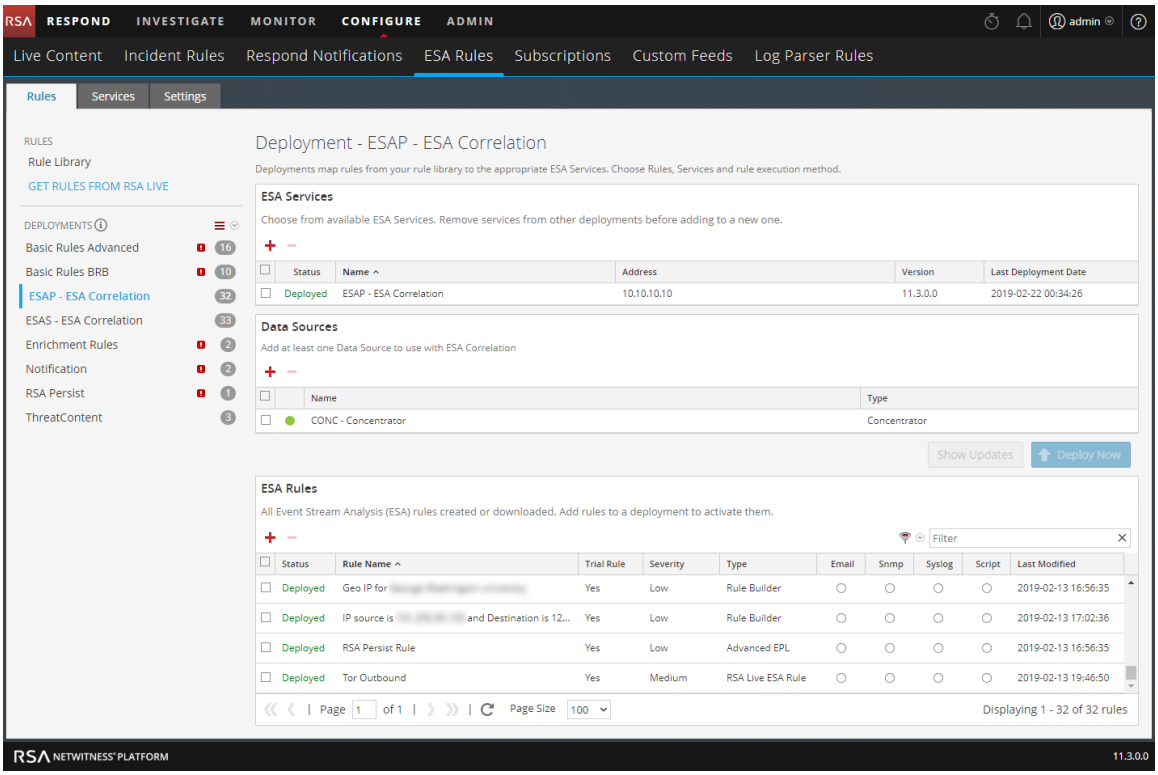
The following figure shows the 11.3 ESA rule deployments after the upgrade. Notice that the Basic Rules Advanced deployment from 10.6.6 does not have any ESA services, but it still contains the original 16 rules.



The 10.6.6 ESA rule deployments show update messages detailing the changes as shown in the following figure.



The following figure shows the ESA primary rule deployment after the upgrade (ESAP - ESA Correlation). Notice that the ESAP - ESA Correlation deployment has only the ESA primary ESA Correlation service.



In NetWitness Platform 11.3 and later, you can only have one ESA Correlation service per deployment, but an ESA Correlation service can be in more than one ESA rule deployment.

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
  - Configure Meta Keys as Arrays in ESA Correlation Rule Values
  - Configure Character Case for Advanced ESA Rules
- Deploy Endpoint Risk Scoring Rules on ESA
- Change Memory Threshold for Trial 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, 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, 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 from versions prior to 11.3, this parameter value is empty.
  - For a new installation of NetWitness Platform 11.3.0.2, 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, 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, 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. Apply the changes on the ESA Correlation service:
6. Go to **CONFIGURE > ESA Rules** and click the **Settings** tab.
   - In the Meta Key References, click the Meta Re-Sync (Refresh) icon ( ).
   - If you have multiple ESA Correlation services, make the same meta key changes on each ESA Correlation service.
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 Platform 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 Advanced Settings for an ESA Correlation Service

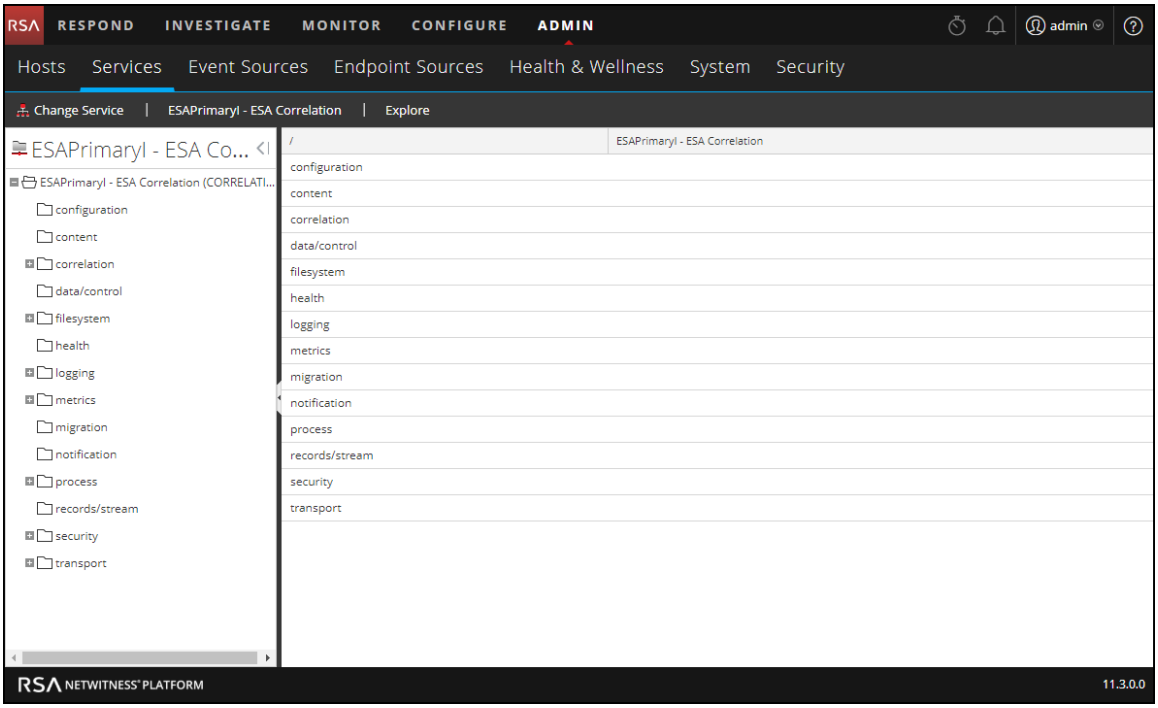
These procedures are optional and they apply only to ESA Correlation Rules.

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
- Configure Meta Keys as Arrays in ESA Correlation Rule Values

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

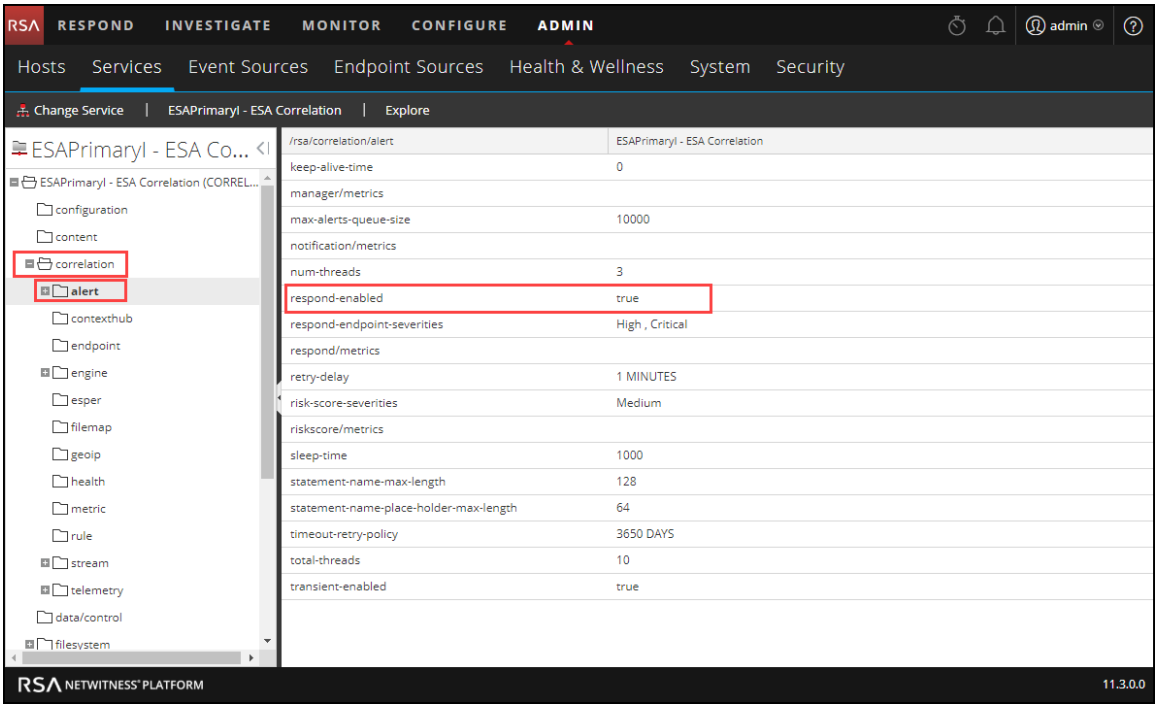
ESA gathers data, runs ESA Correlation rules against the data, captures events that meet rule criteria, and creates alerts for those captured events. You can view those alerts in the Respond view.

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.

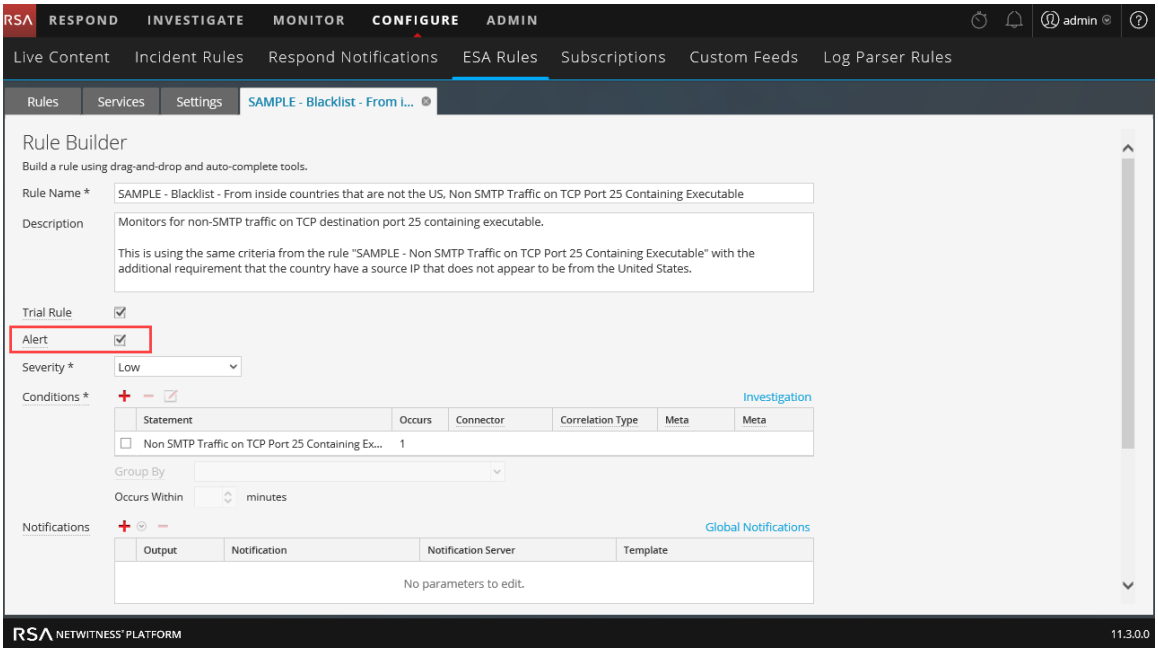
Note: The `respond-enabled` parameter is equivalent to the **Forward Alerts On Message Bus** option in the Event Stream Analysis service in NetWitness Platform version 11.2 and earlier.

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**.

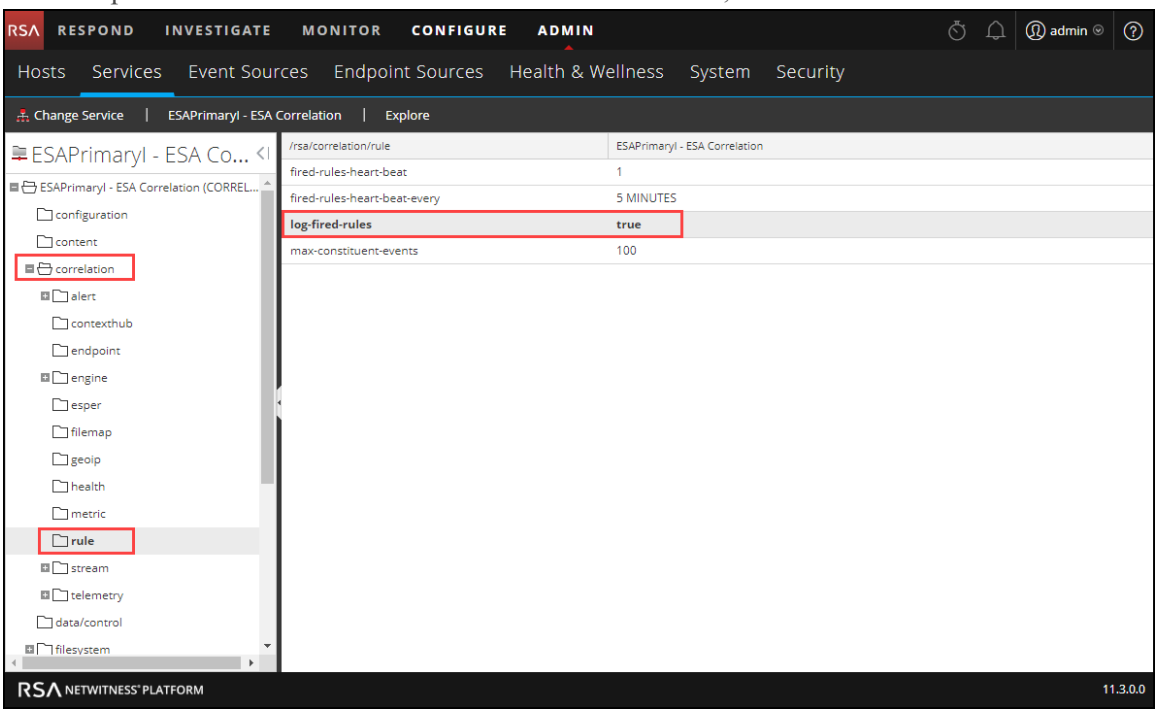
   For more information, see the *Alerting with ESA Correlation Rules User Guide*.

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**.

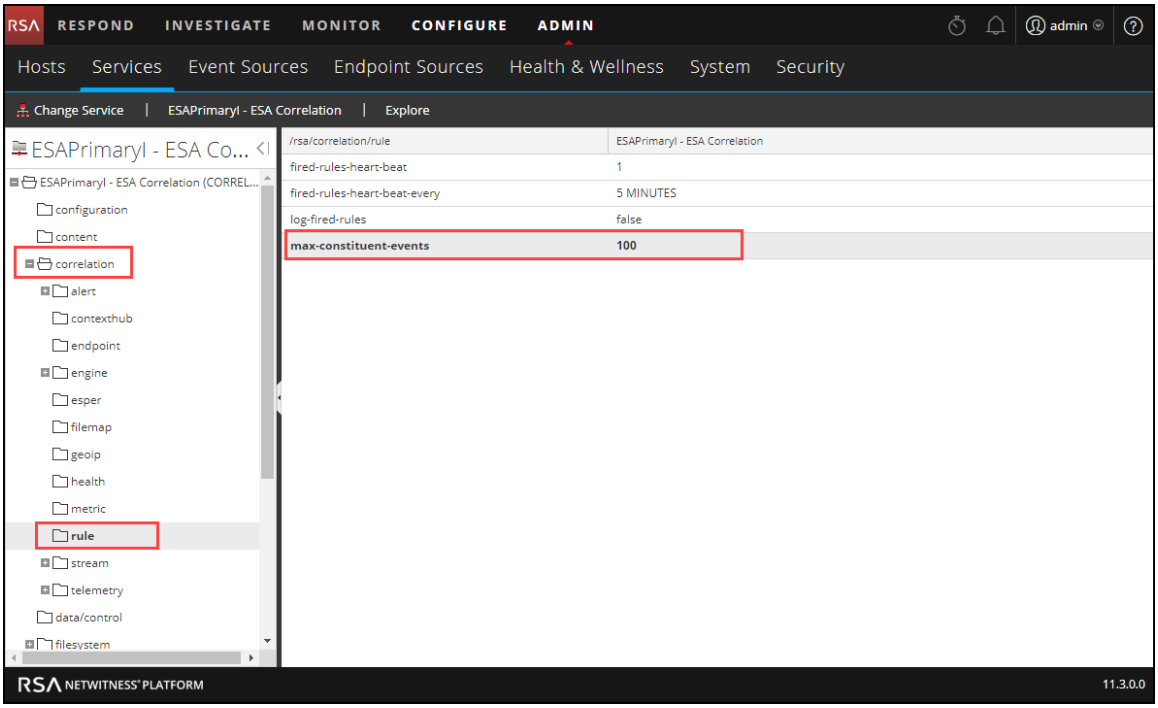


2. Set `log-fired-rules` to **true** to print alerts to the /var/log/netwitness/correlation-server/correlation-server.log for troubleshooting. This is the same as the Debug option in the rule builders for individual ESA rules except that this option enables debugging for all rules.
3. When you are ready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

Configure Meta Keys as Arrays in ESA Correlation Rule Values

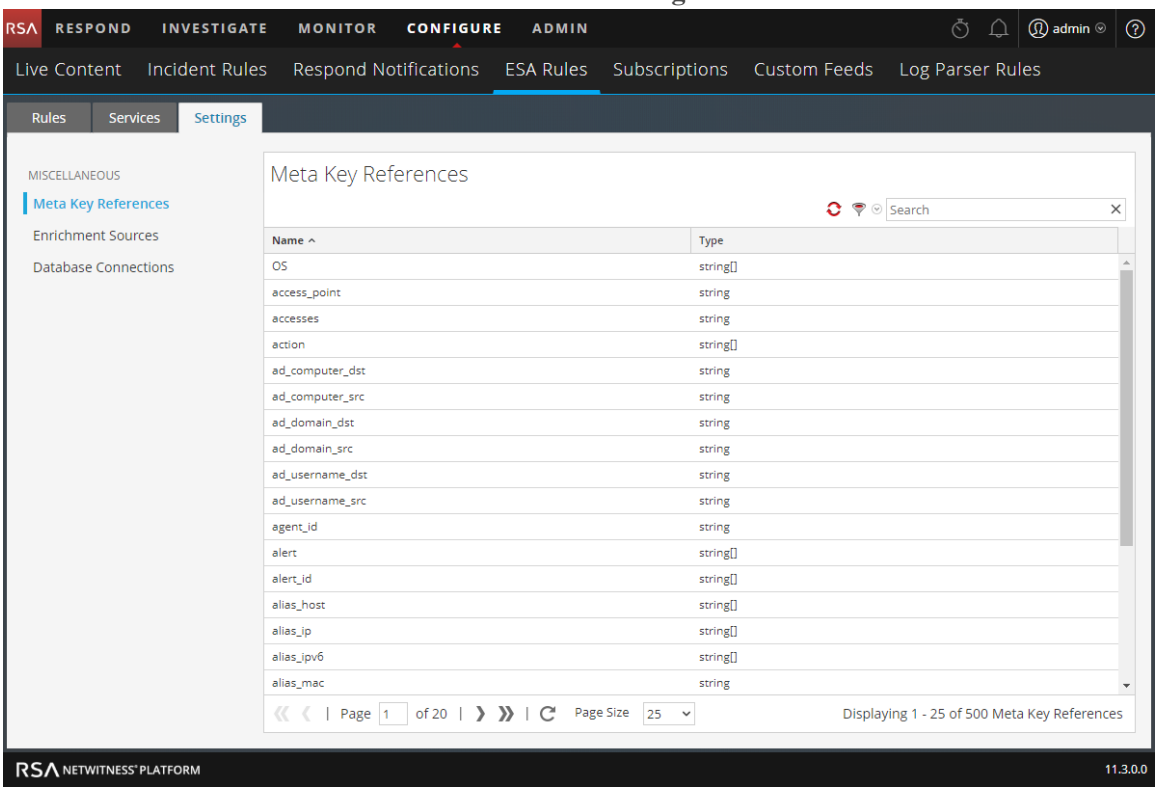
A common reason for an ESA rule to generate an error during deployment is because a meta key in the rule is a string array type, but it shows as a string type on ESA. To prevent or fix this issue, do the following:

- 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 you want to check, 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. If your meta key is a string array (multi-value) type meta key, this is fine.

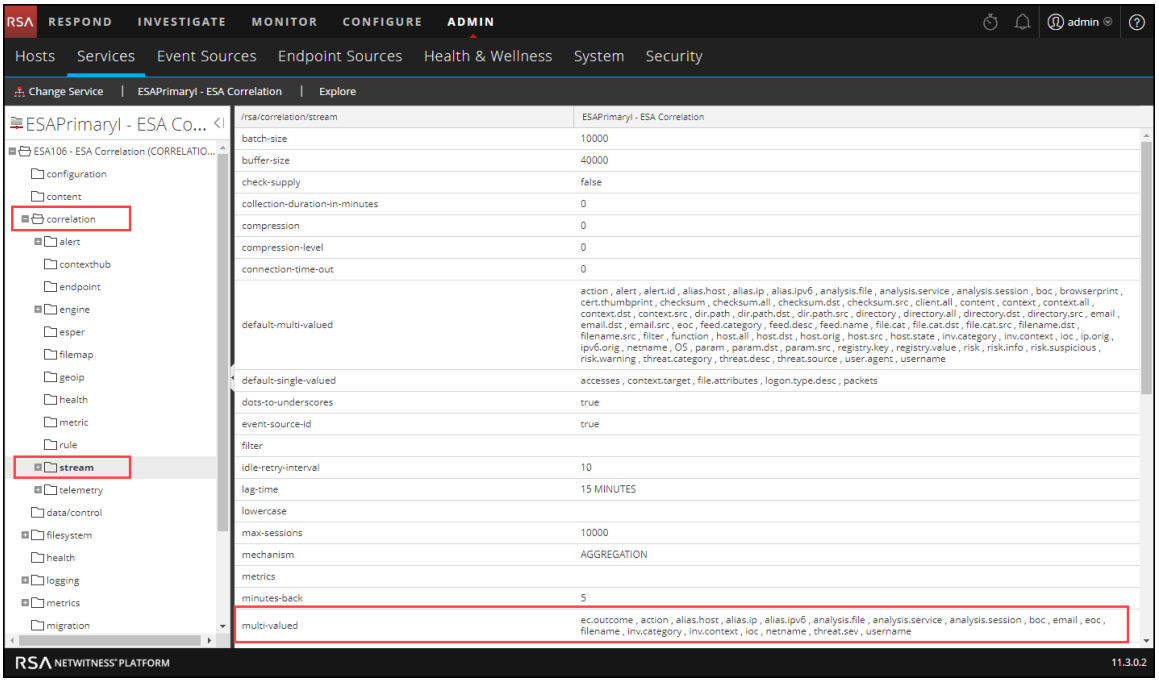
- If it shows `string` without the brackets, it is configured as a string type. Only string (single-value) meta keys should show as `string`. If your meta key is a string array type meta key, you need to fix it on ESA. Go to Add the String Array Type Meta Key to ESA.

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 Platform 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.

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.

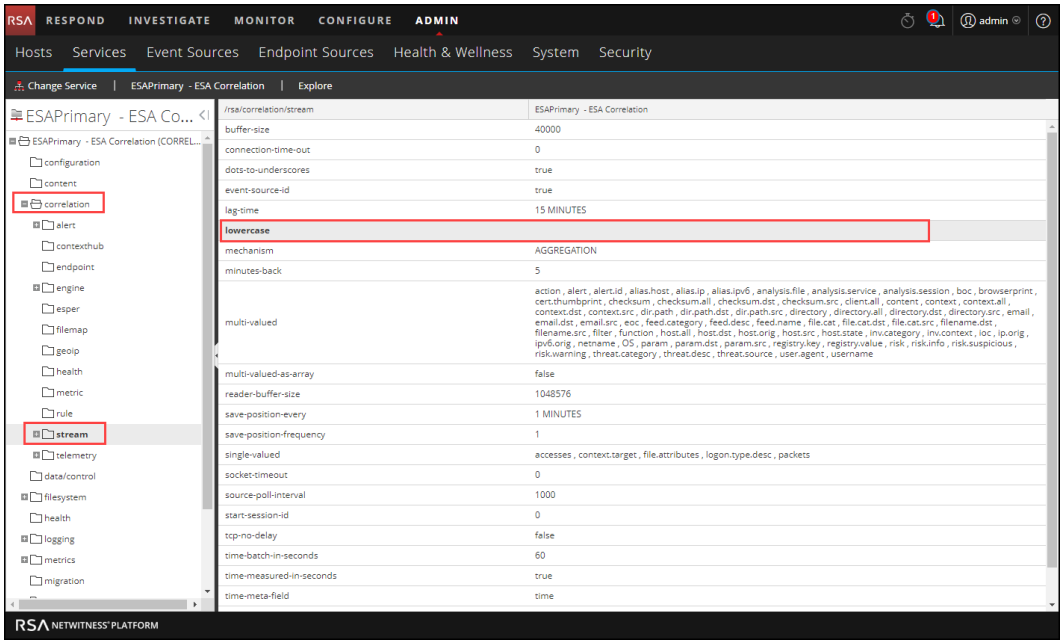
Advanced Event Processing Language (EPL) rules require correct character case, but in the Investigate Navigate view all characters are converted to lowercase. However, the meta keys may not be lowercase despite appearances in the Investigate Navigate view. To ensure you are using the correct case, you 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

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

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 Platform 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 Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

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.

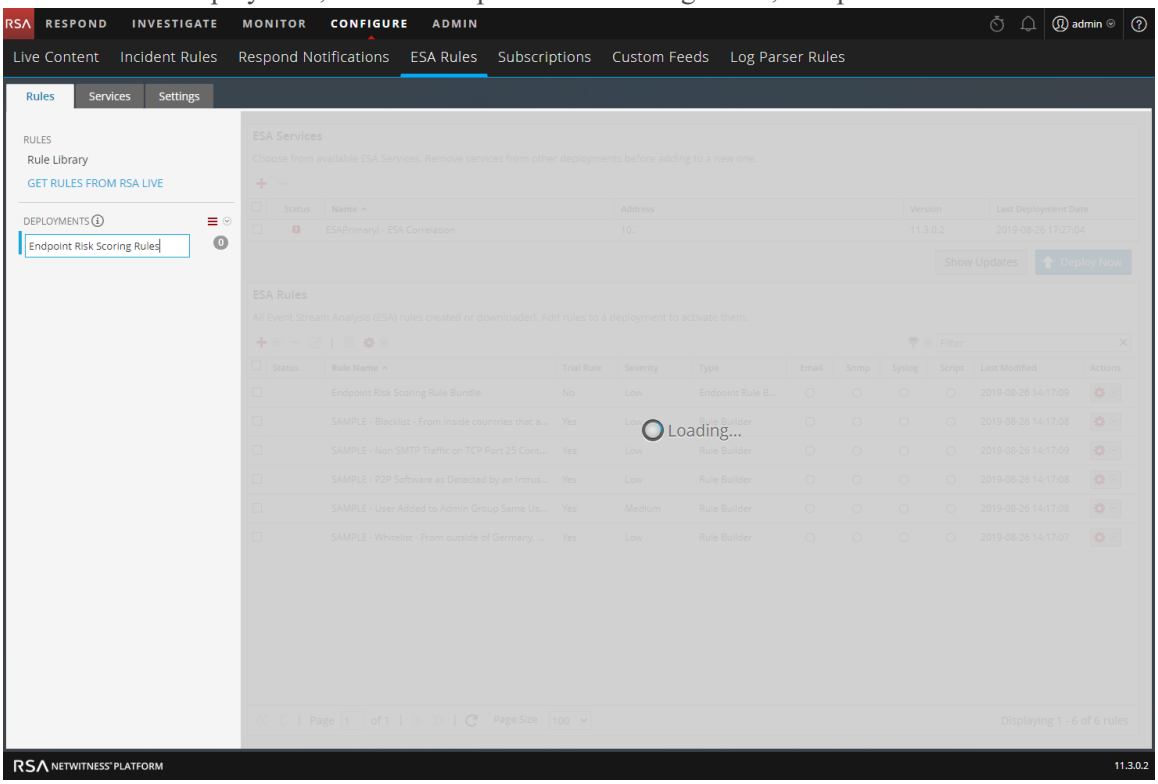
When you deploy the Endpoint Risk Scoring Rules Bundle in an ESA rule deployment, the ESA Correlation service gathers endpoint data in your network and runs endpoint risk scoring rules against the data. The goal is to capture events that match rule criteria, then generate alerts for the captured events.

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.

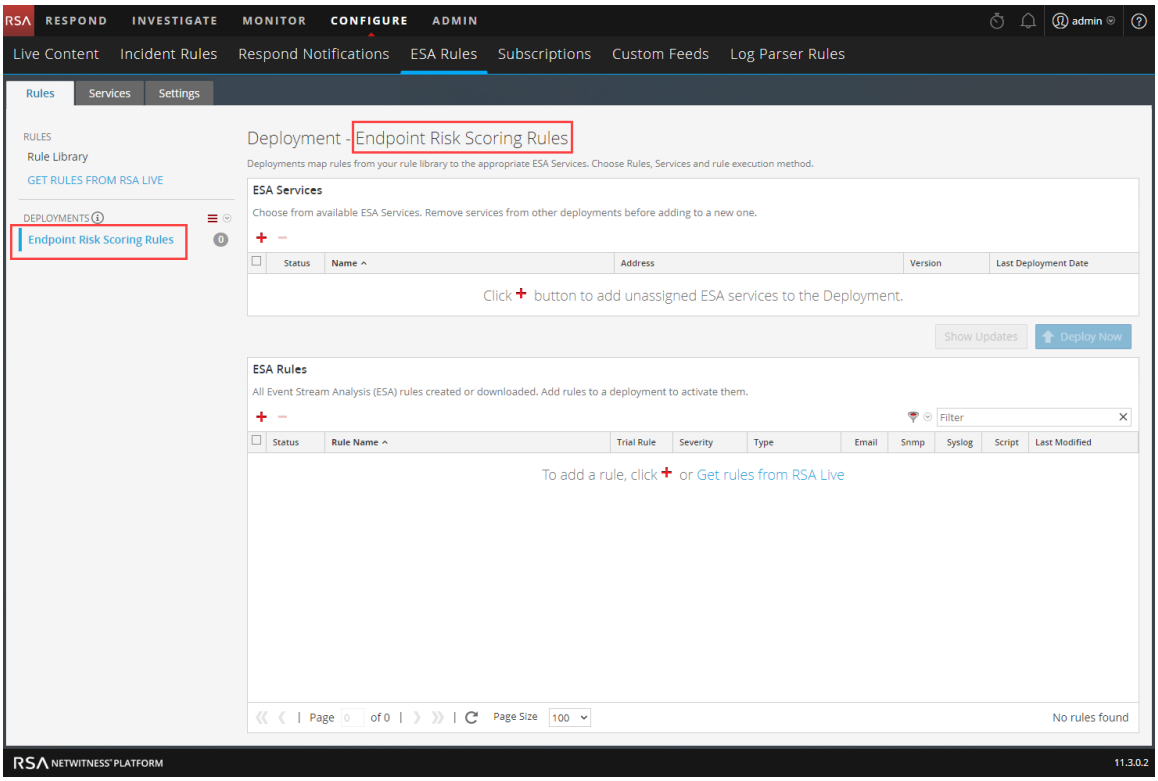
To create and deploy an ESA rule deployment with the Endpoint Risk Scoring Bundle:

1. Go to **CONFIGURE > ESA Rules > Rules tab**.

2. In the options panel on the left, next to Deployments, select  > **Add** to add a deployment, type a name for the deployment, such as Endpoint Risk Scoring Rules, and press **Enter**.



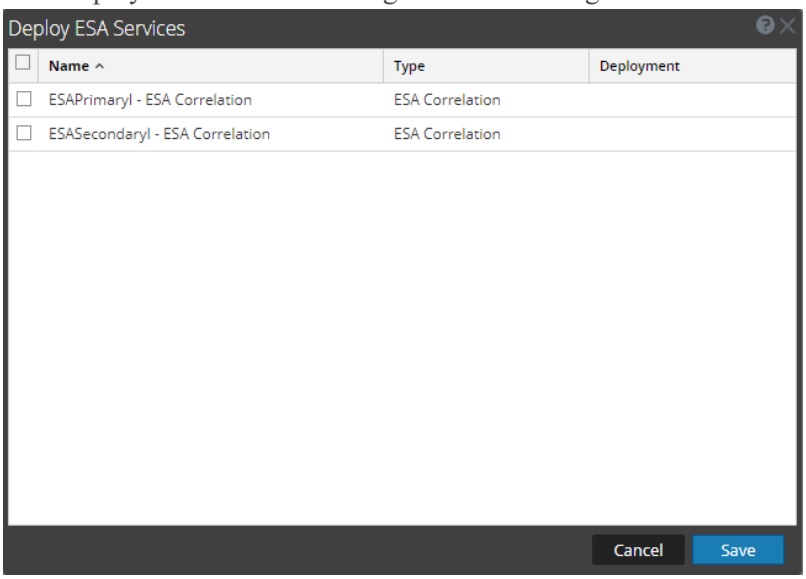
The deployment is added and the Deployment view is displayed on the right.



The deployment name that you choose also appears on a deployment tab in the **CONFIGURE > ESA Rules > Services** tab, where you can view deployment details and statistics.

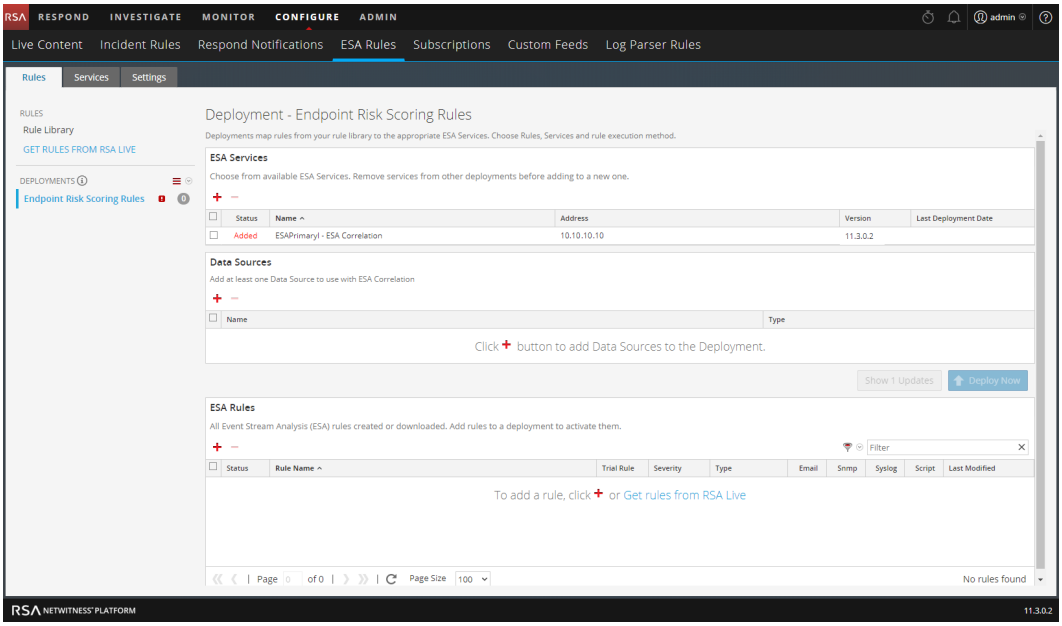
3. Add an ESA Correlation service:

   a. In the **Deployment** view **ESA Services** section, click + .
   The Deploy ESA Services dialog lists each configured ESA Correlation service.



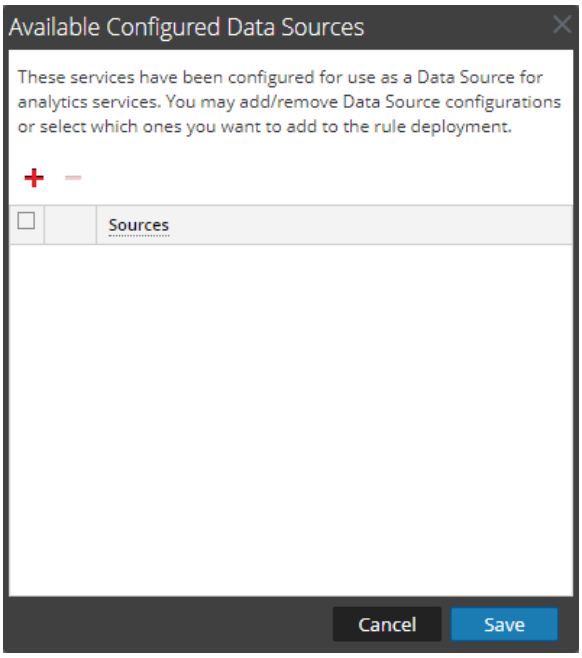
   b. Select an ESA Correlation service and click **Save**.
   The Deployment view is displayed. The ESA Correlation service is listed in the **ESA Services**

section with an **Added** status.

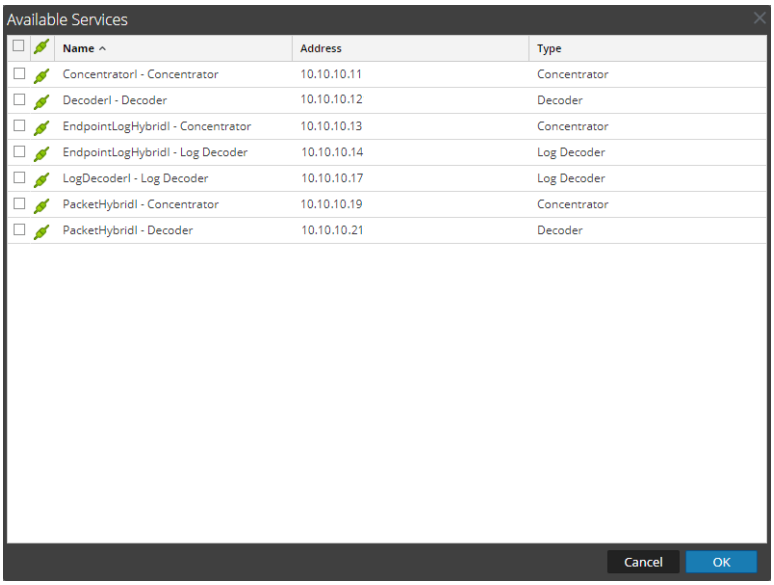


4. Add one or more data sources with endpoint data:

   a. In the **Deployment** view **Data Sources** section, click + .
   The **Available Configured Data Sources** dialog lists the services that have been configured for use as a data source.



   b. To add a data source configuration, click + .
   The **Available Services** dialog lists the available data sources from the ADMIN > Services view.

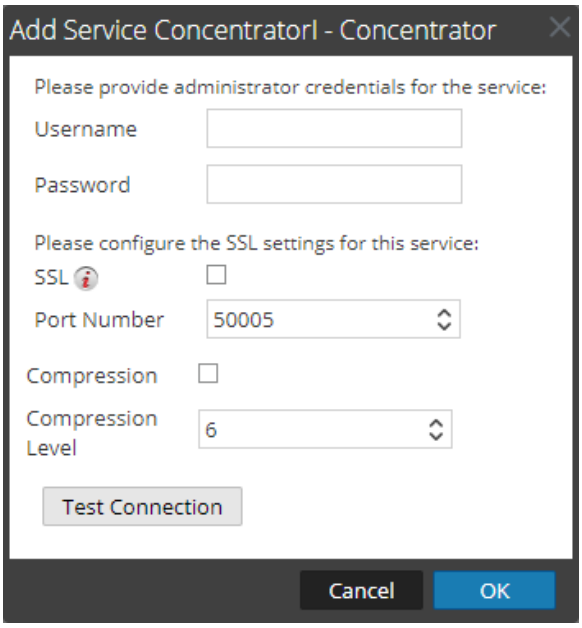


If an endpoint data source (service) that you are looking for is not in the list, see the *Hosts and Services Getting Started Guide* for instructions on how to install a service on a host.

Note: You can add a Log Decoder as a data source for ESA, but it is better to add a Concentrator to take advantage of undivided aggregation as the Decoder may have other processes aggregating from it.

c. In the **Available Services** dialog, select an endpoint data source, such as a Concentrator, and click **OK**.

d. In the **Add Service** dialog, type the Administrator username and password for the endpoint data source.



e. To enable the SSL or Compression options, select the corresponding checkboxes.

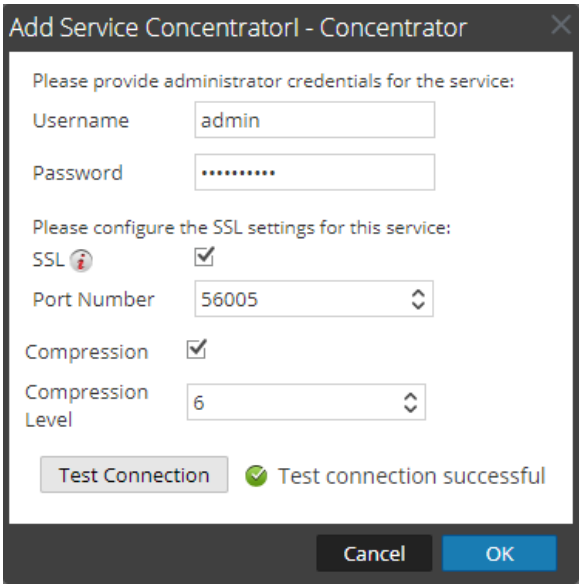
f. (Optional) You have the option to adjust the Compression Level for Concentrators on ESA in NetWitness Platform 11.3 and later. To enable compression, select the **Compression** checkbox. You can set the **Compression Level** for a Concentrator from 0-9:

- Compression Level = **0** (If compression is enabled, it allows Core Services to control the amount of compression.)
- Compression Level = **1** (It uses the lowest amount of compression and has the highest performance.)
- Compression Level = **9** (It uses the highest amount of compression and has the worst performance.)

Somewhere in the middle between 1 and 9 is usually the best setting, which is what you get when you select a compression level of 0. For more detailed information, see the *Core Database Tuning Guide*.

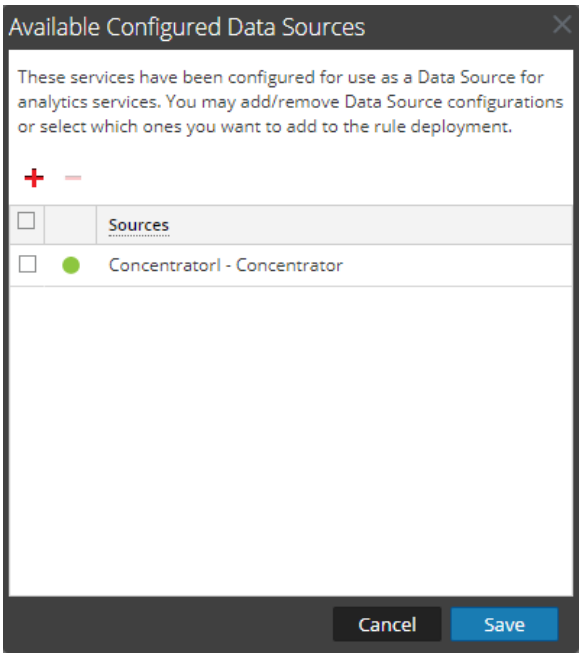
Note: When you set the compression level for a Concentrator on ESA, it sets the same compression level for that Concentrator for ESA Analytics and ESA Correlation Rules.

g. Click **Test Connection** to make sure that it can communicate with the ESA Correlation service.



h. Click **OK**.
After you configure your endpoint data sources and they appear in the **Available Configured Data Sources** dialog, you can use them for your deployment.

i. In the **Available Configured Data Sources** dialog, select at least one endpoint data source to use for the deployment.

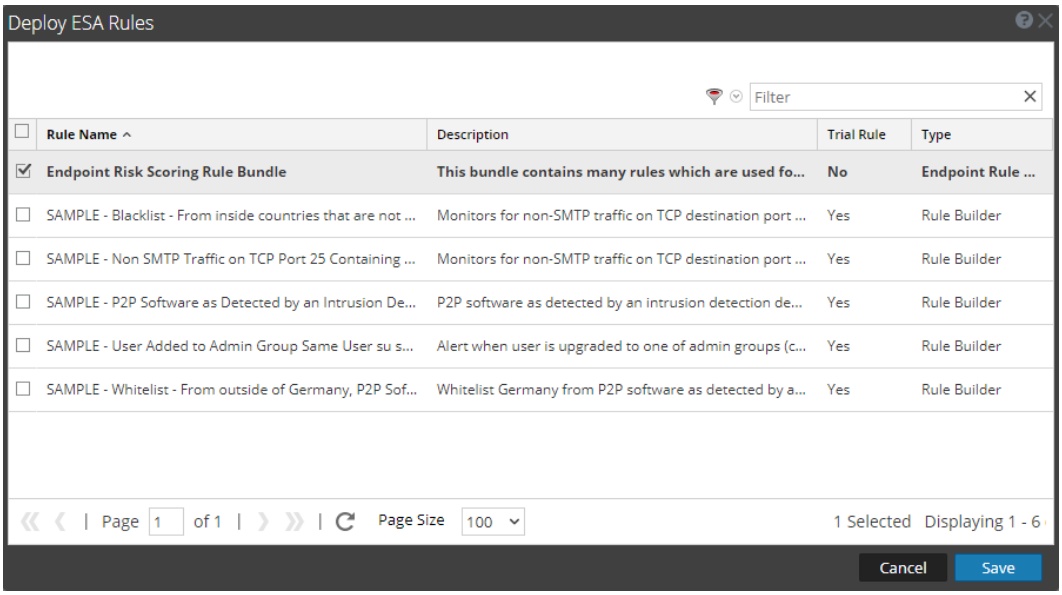


A solid colored green circle indicates a running service and a white circle indicates a stopped service.

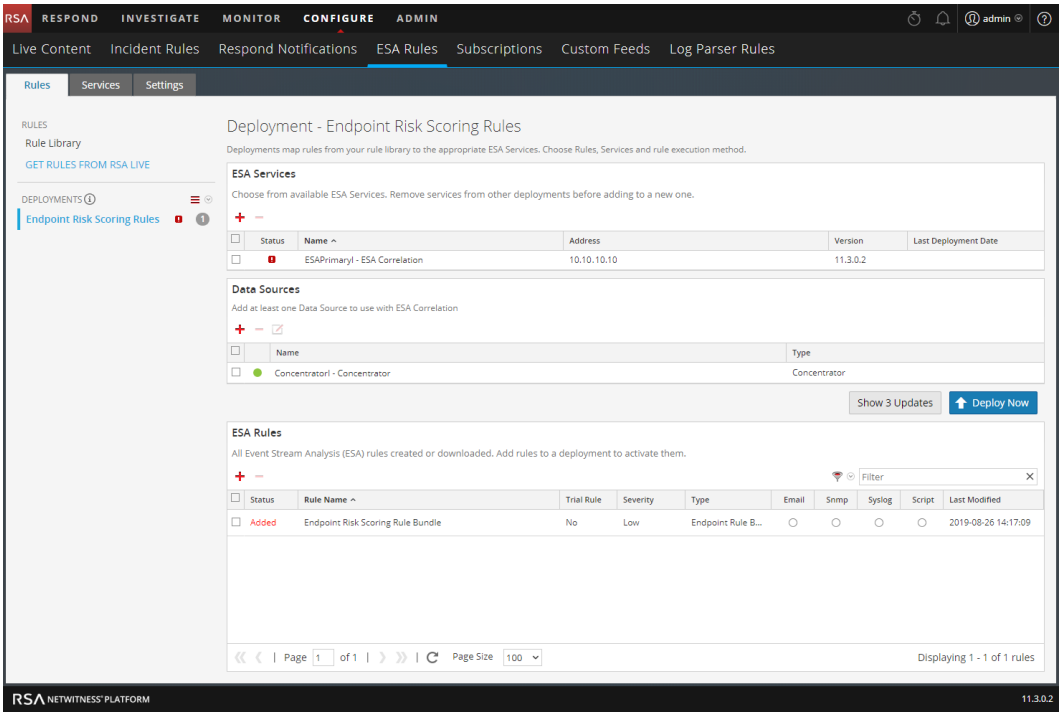
j. Click **Save**.
In the Deployment view **Data Sources** section, the selected data sources are added to the deployment. The **Deploy Now** button activates after a service, data source, and rules are added to an ESA rule deployment.

5. Add the Endpoint Risk Scoring Rules Bundle:

a. In the **Deployment** view ESA Rules section, click  .
The Deploy ESA Rules dialog is displayed and shows each rule in your Rule Library.

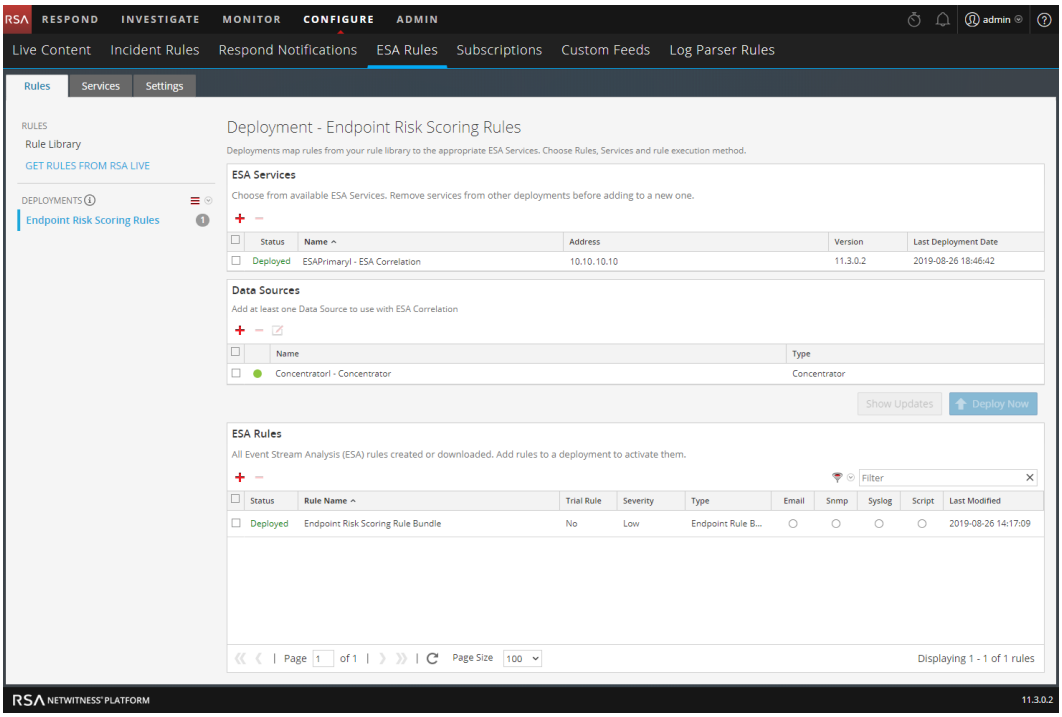


b. Select the Endpoint Risk Scoring Rule Bundle and click **Save**.
The Deployment view is displayed and the **Deploy Now** button is enabled.



The Endpoint Risk Scoring Rules Bundle is listed in the **ESA Services** section with an **Added** status.

6. Click **Deploy Now**.
The ESA Correlation service runs the rules in the Endpoint Risk Scoring Rules Bundle. The status of the bundle changes to **Deployed**.



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.

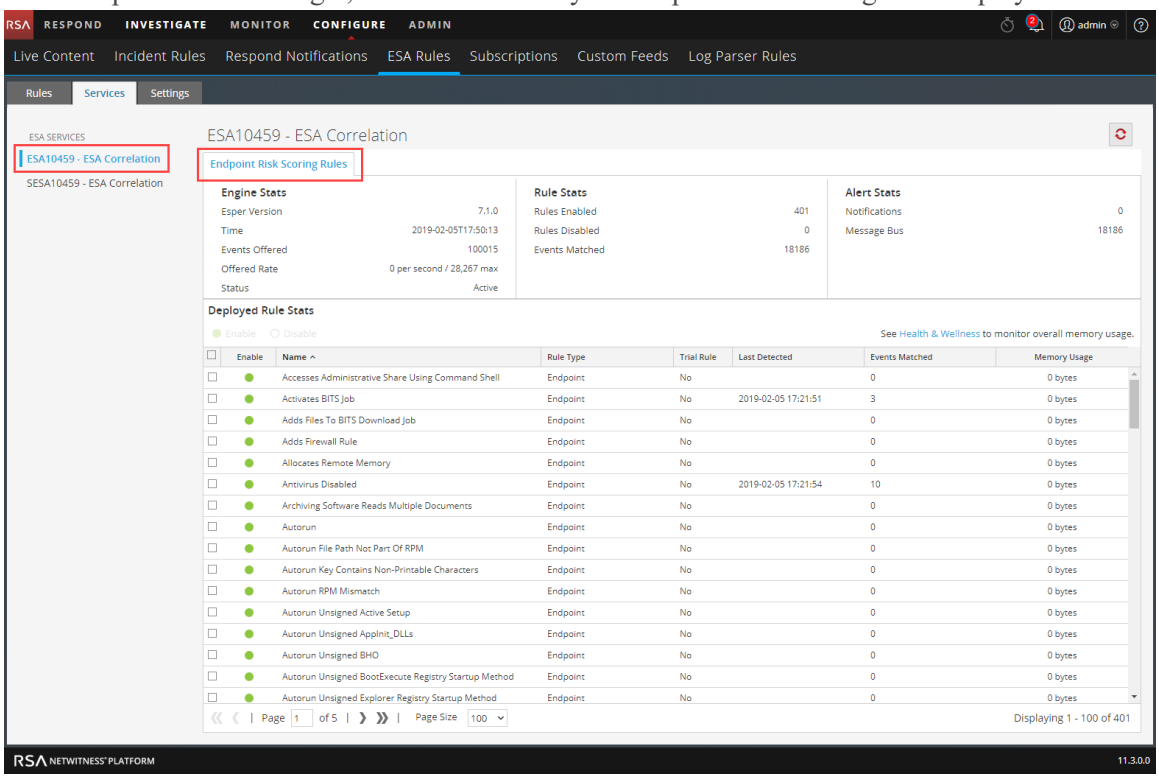
When you make changes to the ESA Rule Deployment containing the Endpoint Risk Scoring Rules Bundle, such as changing the endpoint data sources or changing compression levels, you must redeploy it for the changes to take effect. To redeploy, click the **Deploy Now** button for that deployment.

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.



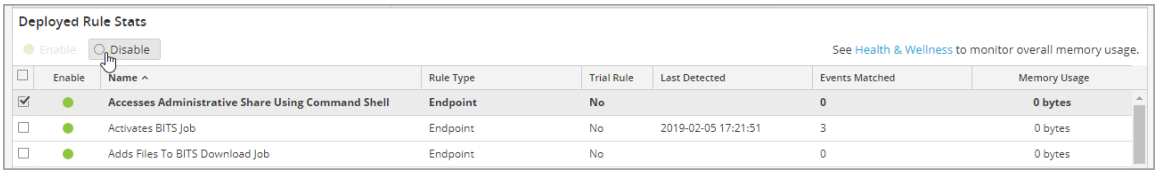
3. In the **Engine Stats**, **Rules Stats** and **Alert Status** sections, look at the statistics related to the deployment, such as Rules Enabled, Rules Disabled, and Events Matched, which show the total numbers for the deployment.
4. In the **Deployed Rules Stats** section, look at the following details 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 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*.

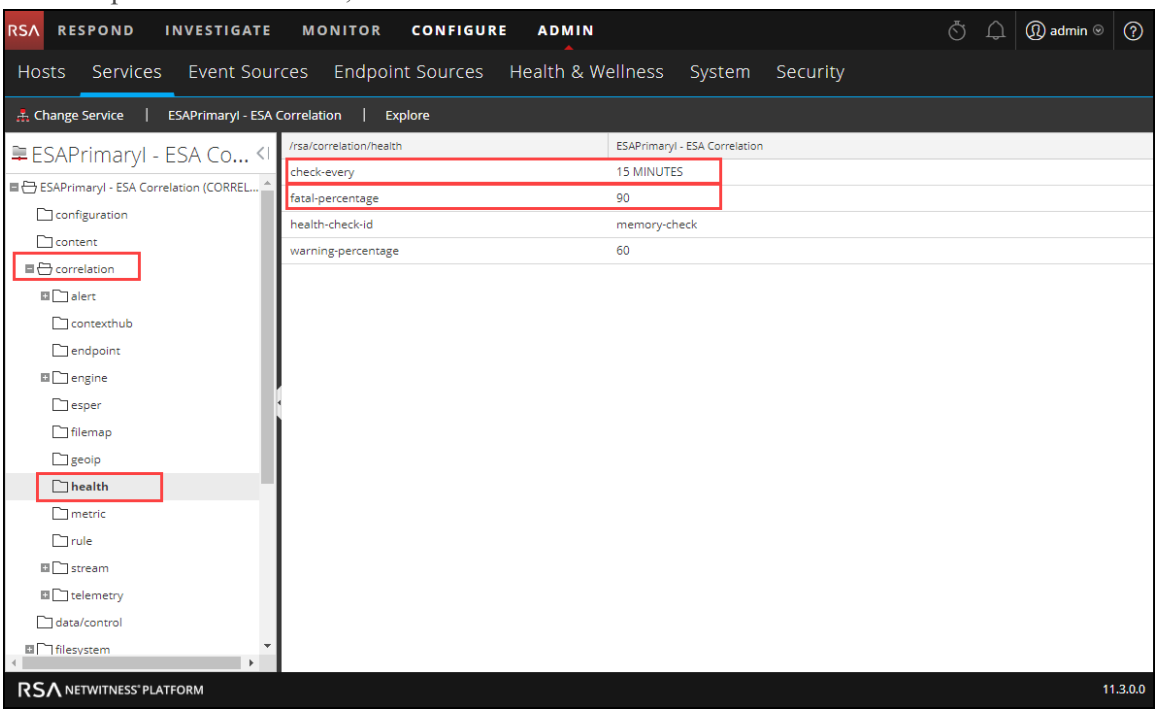
Prerequisites

A role with administrative privileges must be assigned to you.

To change memory threshold for trial rules:

1. Log on to NetWitness Platform 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.

Start, Stop, or Restart ESA Service

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

Start the ESA Service

1. Log on to NetWitness Platform 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 Platform 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 Platform 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 Platform. There are local audit logs in each of the services in NetWitness Platform. When Global Audit Logging is configured, NetWitness Platform 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`

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.

Configure ESA Analytics

This section provides high-level tasks to configure ESA Analytics services for RSA NetWitness® Platform Automated Threat Detection. The Automated Threat Detection functionality enables you to analyze the data that resides on one or more Concentrators by using preconfigured ESA Analytics modules, such as Suspicious Domains. For example, using a Suspicious Domains module, an ESA Analytics service can examine your HTTP traffic to determine the probability that malicious activity is occurring in your environment.

There are two ESA services that can run on an ESA host:

- ESA Correlation (ESA Correlation Rules)
- Event Stream Analytics Server (ESA Analytics)

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. The second service is the ESA Analytics service, which is used for Automated Threat Detection and is configured in this section. Because the ESA Analytics service uses preconfigured ESA Analytics modules for Automated Threat Detection, you do not have to create or download rules to use it.

There are currently two ESA Analytics modules available and they are both for Suspicious Domains:

- C2 for Packets (http-packet)
- C2 for Logs (http-log)

Note: The Contexthub Server service, which provides enrichment lookup capability in the Respond and Investigate views, runs only on an ESA Primary host. For information, see the *Context Hub Configuration Guide*.

Configure the Whois Lookup Service

The RSA NetWitness Platform Automated Threat Detection functionality enables you to automatically analyze data sources by using preconfigured ESA Analytics modules. An ESA Analytics module is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. ESA Analytics services process these modules to identify advanced threats.

The Whois Lookup service configuration is required for the Suspicious Domains modules.

Note: (**Important**) RSA strongly recommends that you configure the Whois Lookup service for accuracy in Automated Threat Detection scoring.

Prerequisites

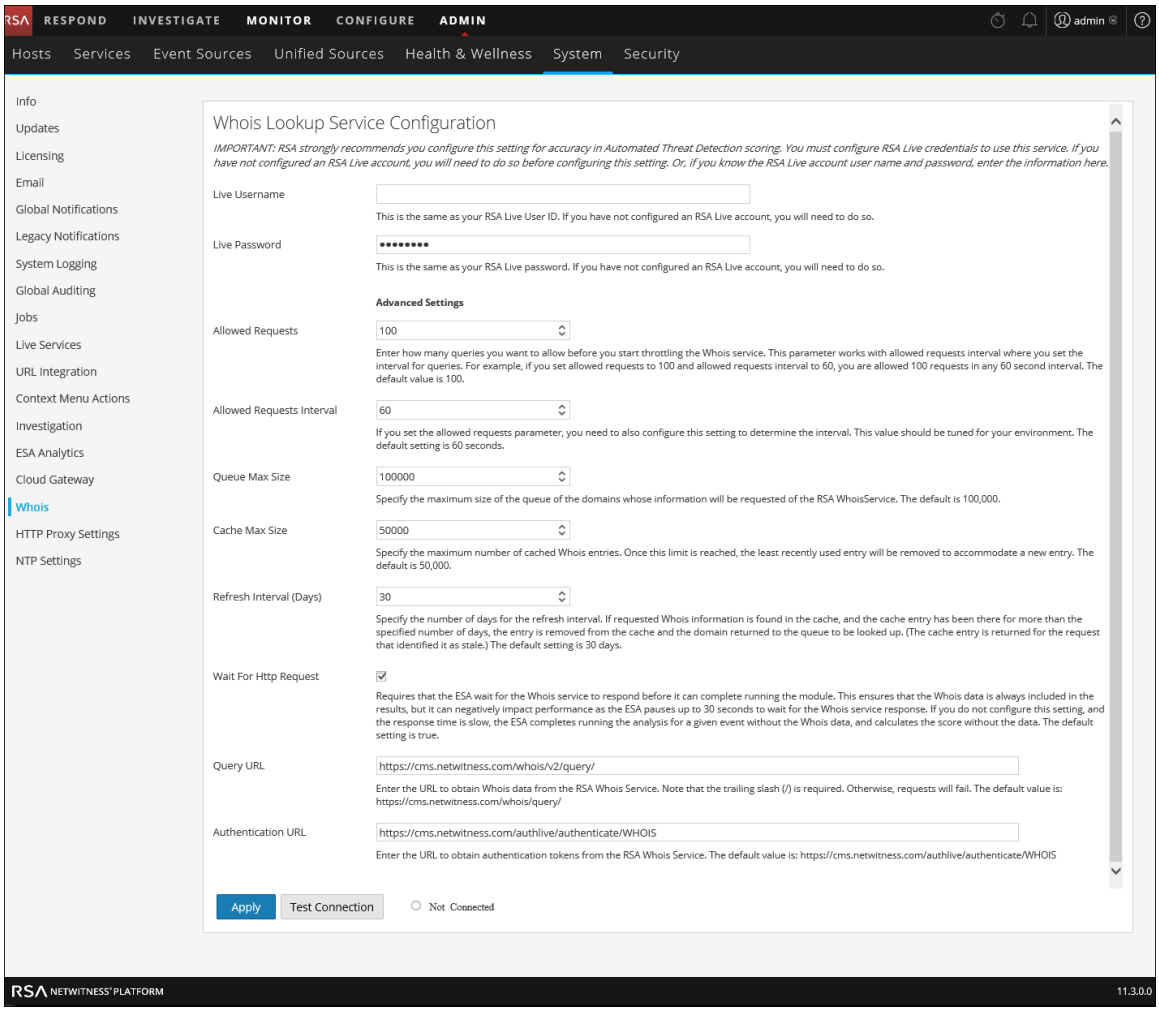
- You must have an RSA Live account to use the Whois Lookup service.
- The ESA Analytics Server service must be available (shows a green circle) in the ADMIN > Services view.

If you configured a Live account in the Live Services panel (ADMIN > System > Live Services), the Whois Lookup Service is automatically configured for you. You only need to check the connection of the Whois Lookup service.

Note: If you do not have an RSA Live account, you can create one at the RSA Live Registration Portal:
https://cms.netwitness.com/registration/
The *Live Services Management Guide* provides additional information.

To configure the Whois Lookup service:

1. Go to **ADMIN > System**.
2. In the options panel, select **Whois**.
3. In the **Whois Lookup Service Configuration** panel, check to see if the Whois Lookup service is connected. At the bottom of the panel, a connected service shows a green circle next to **Connected**:



If it is connected, you are finished with the configuration and you can skip the remaining steps. To adjust the advanced settings, go to step 5.
If the service is not connected, continue to step 4.

4. In the **Live Username** and **Live Password** fields, enter your RSA Live account credentials to access the RSA Whois server.
5. If necessary, you can adjust the advanced settings. However, RSA recommends that you use the default values. Whois Lookup Service Configuration provides additional details.
6. To test your connection, click **Test Connection**.

   A successful connection shows a green circle next to **Connected**: 

7. Click **Apply** to save your changes.

Mapping ESA Data Sources to Analytics Modules

This topic tells Administrators how to map specific ESA Analytics modules to multiple data sources and ESA Analytics services, which can make processing more efficient.

You can analyze the data that resides on one or more Concentrators with the RSA NetWitness Platform Automated Threat Detection functionality by selecting a preconfigured ESA Analytics module. The data analyzed by these modules is used to identify advanced threats. To better utilize your network resources and reduce unnecessary data flow, you can map multiple data sources, such as Concentrators, to multiple ESA Analytics services in order to process data more efficiently and take advantage of additional capacity.

An *ESA Analytics module* is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. ESA Analytics modules reside within ESA Analytics services.

When you deploy your mapping, the selected ESA Analytics services use query-based aggregation to collect the appropriate filtered events for the selected module from the Concentrators. Query-based aggregation is a predefined query that only transfers data for the selected ESA Analytics module. Only the data required by the module is transferred between the Concentrator and the ESA Analytics system.

There are currently two ESA Analytics modules available for Suspicious Domains: C2 for Packets (http-packet) and C2 for Logs (http-log).

Module Deployment Example - Two ESAs

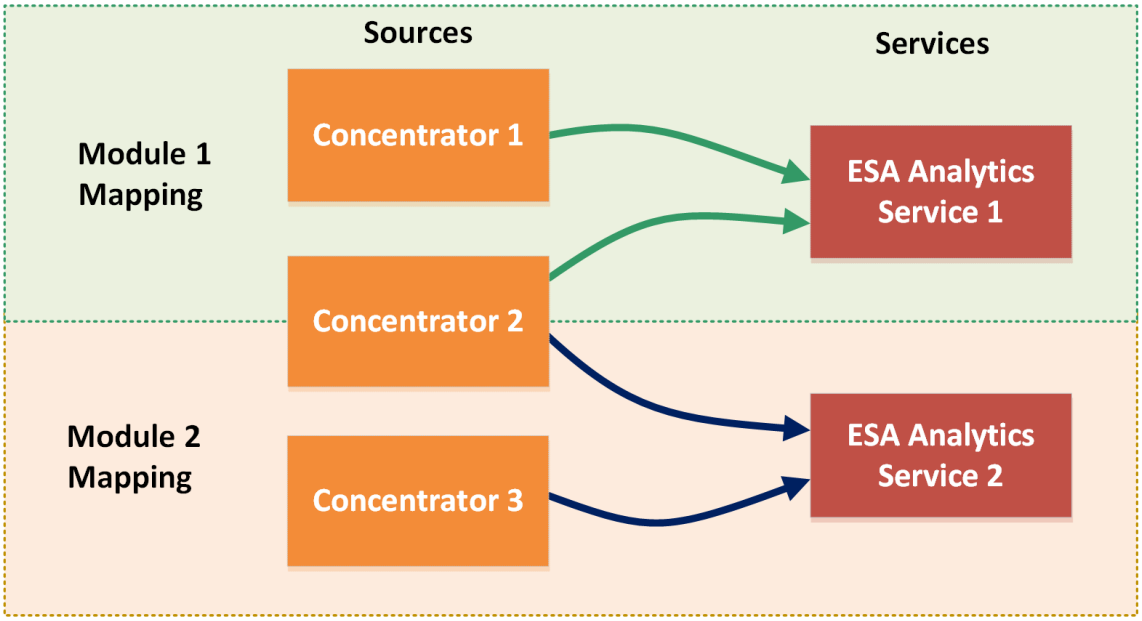
To take advantage of your additional Concentrator capacity, you can map an ESA Analytics module to an ESA Analytics service and deploy it to analyze data from multiple data sources at the same time.

For example, if you have three Concentrators and two ESA Analytics services, you can create and deploy the following mappings:

- Map Module 1 to the Concentrator 1 and 2 sources and the ESA Analytics 1 service. ESA Analytics Service 1 analyzes Module 1 filtered events from Concentrators 1 and 2.
- Map Module 2 to the Concentrator 2 and 3 sources and the ESA Analytics 2 service. ESA Analytics Service 2 processes Module 2 filtered events from Concentrators 2 and 3.

In this example, Module 1 represents an ESA Analytics module, such as C2 for Packets (http-packet) and Module 2 represents another ESA Analytics module, such as C2 for Logs (http-logs) in another location.

Module Deployment Example – Two ESAs



This example shows how both services can process data from the same Concentrator. Notice that ESA Analytics Services 1 and 2 can both process data from Concentrator 2. ESA Analytics Service 1 queries data for Module 1 events and ESA Analytics Service 2 queries different data for Module 2 events.

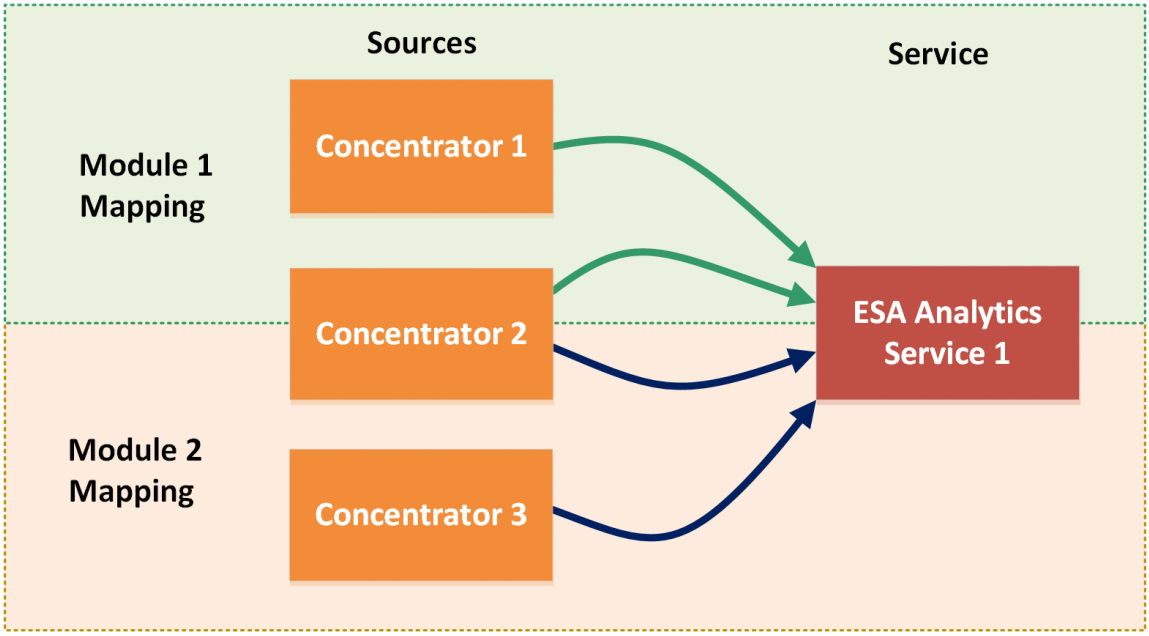
Module Deployment Example - One ESA

In addition to creating module mappings that are processed by different ESA Analytics services, you can map more than one module to the same ESA Analytics service.

For example, if you have three Concentrators and one ESA Analytics service, you can create and deploy the following mappings:

- Map Module 1 to the Concentrator 1 and 2 sources and the ESA Analytics 1 service. ESA Analytics Service 1 analyzes Module 1 filtered events from Concentrators 1 and 2.
- Map Module 2 to the Concentrator 2 and 3 sources and the ESA Analytics 1 service. ESA Analytics Service 1 also processes Module 2 filtered events from Concentrators 2 and 3.

Module Deployment Example – One ESA



This example shows how one service can process data from more than one module. Notice that ESA Analytics Service 1 can process data from Concentrators 1 and 2 for Module 1. It also processes data from Concentrators 2 and 3 for Module 2. ESA Analytics Service 1 queries data for Module 1 events and queries different data for Module 2 events.

Caution: Ensure that all NetWitness Platform host services are in sync with a consistent time source.

Prerequisites

- All NetWitness Platform host services must be in sync with a consistent time source.
- The Concentrator hosts and services must be discovered and available in the NetWitness Platform user interface.
- All module-specific requirements must be followed.
  - For Suspicious Domains:
    - Configure log settings (Suspicious Domains for Logs only)
    - Create a whitelist using the Context Hub service.
    - Configure the Whois Lookup Service.
    - Verify that the C2 incident rule is enabled and monitor it for activity.
    - Verify that the incidents are grouped by Suspected C&C.

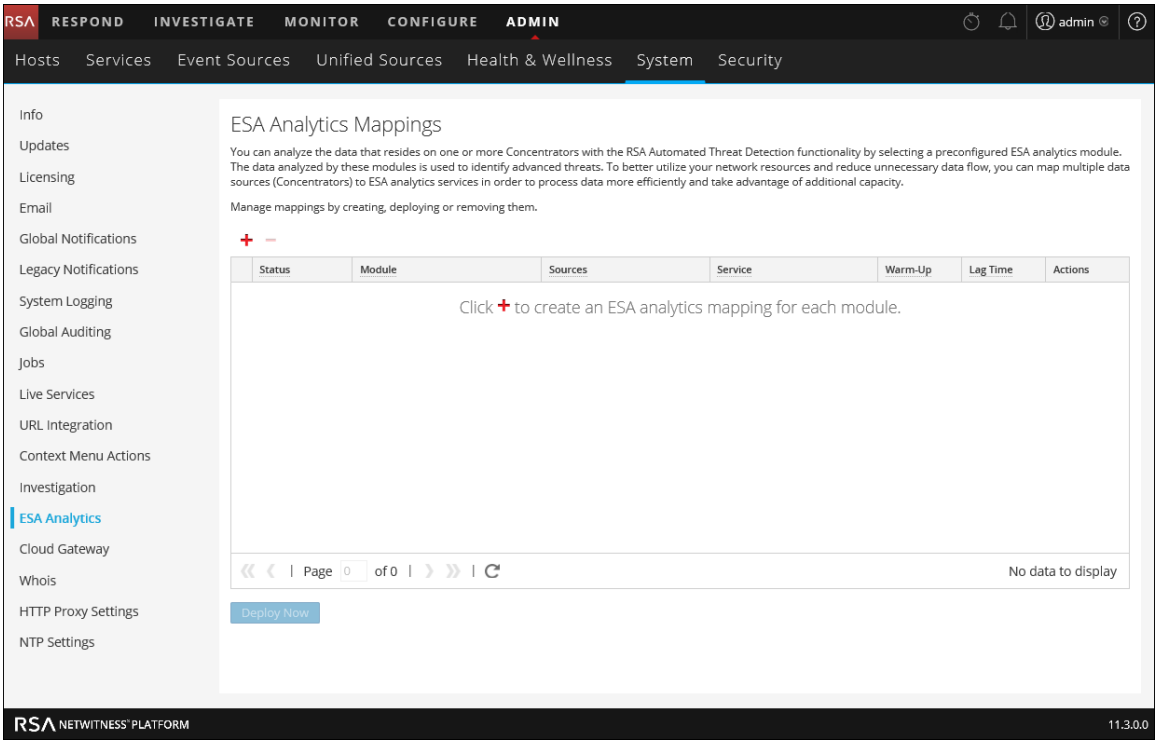
  For step-by-step procedures, see the *NetWitness Platform Automated Threat Detection Configuration Guide*.

  Go to the Master Table of Contents to find all NetWitness Platform Logs & Network 11.x documents.

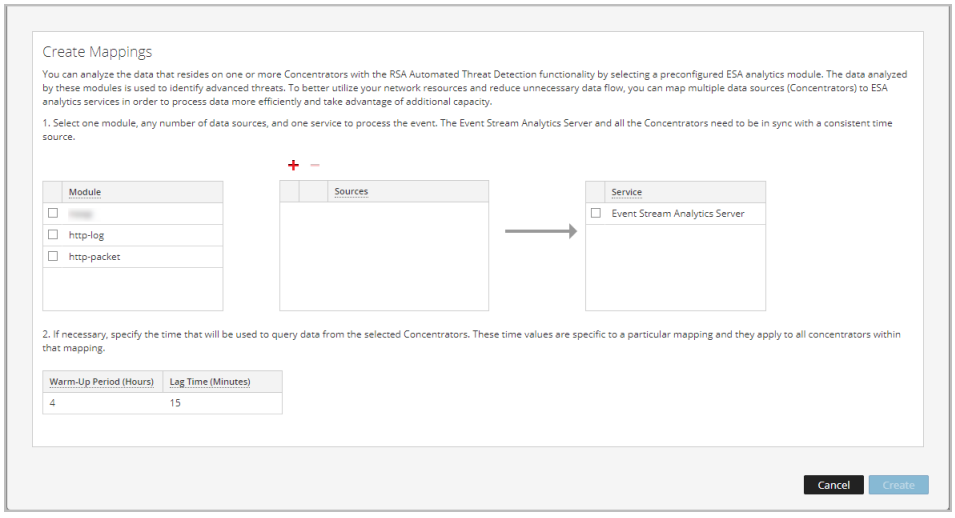
Create ESA Analytics Mappings

The following procedure tells you how to map ESA Analytics modules to sources and services. After creating and reviewing the mappings, you deploy them so that they can start aggregating data.

1. Go to **ADMIN** > **System**, and in the options panel, select **ESA Analytics**.
   The **ESA Analytics Mappings** panel is displayed.



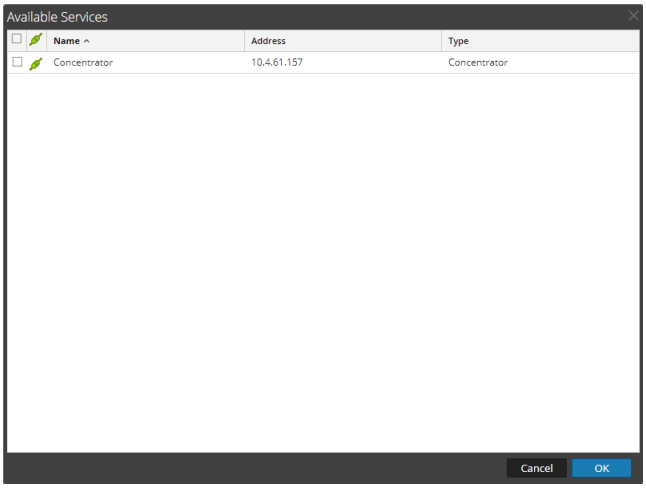
2. Click  to create an ESA Analytics mapping. Create a separate mapping for each module.
   The **Create Mappings** dialog is displayed.



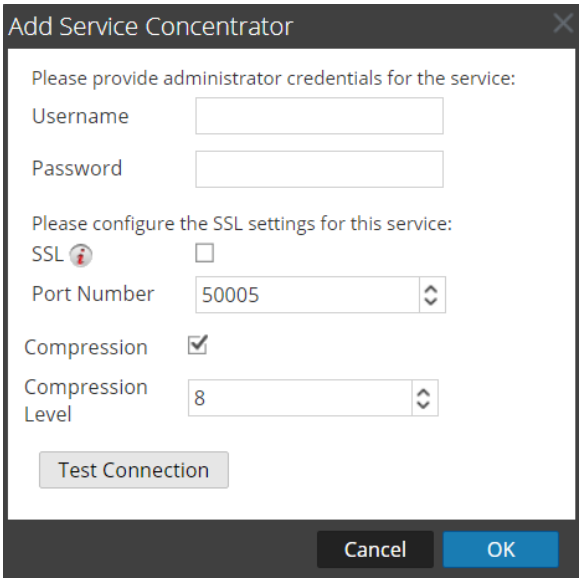
3. In the **Module** list, select a module.

4. Configure one or more data sources (Concentrators) for your mappings. Do the following for each Concentrator:

   a. Click  to view the data sources that are available from the ADMIN > Services view.



   b. In the **Available Services** dialog, select a Concentrator and click **OK**.
   The Add Service dialog is displayed.



   c. In the **Add Service** dialog, type the Administrator username and password for the Concentrator.

   d. (Optional) You have the option to adjust the Compression Level for Concentrators on ESA in NetWitness Platform 11.3 and later. To enable compression, select the **Compression** checkbox. You can set the **Compression Level** for a Concentrator from 0-9:

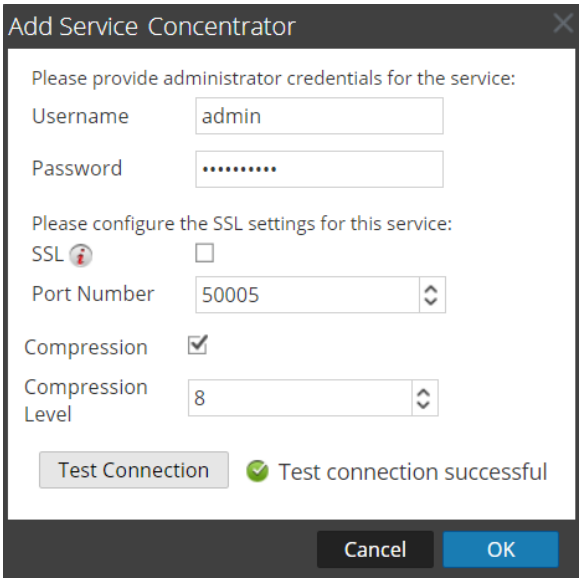
      - Compression Level = **0** (If compression is enabled, it allows Core Services to control the amount of compression.)
      - Compression Level = **1** (It uses the lowest amount of compression and has the highest performance.)

- Compression Level = **9** (It uses the highest amount of compression and has the worst performance.)

Somewhere in the middle between 1 and 9 is usually the best setting, which is what you get when you select a compression level of 0. For more detailed information, see the *Core Database Tuning Guide*.

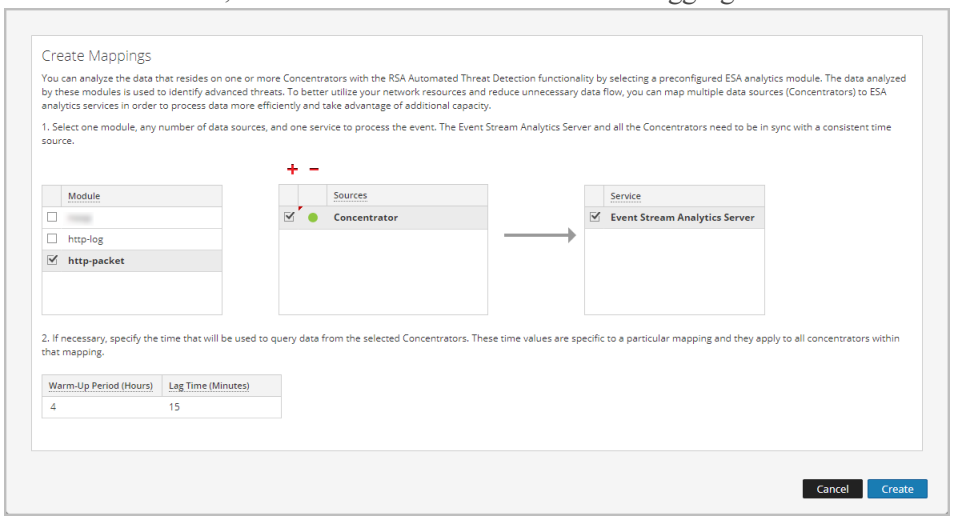
Note: When you set the compression level for a Concentrator on ESA, it sets the same compression level for that Concentrator for ESA Correlation Rules and ESA Analytics.

e. Click **Test Connection** to make sure that it can communicate with the ESA Analytics service.



f. Click **OK**.
After you configure your data sources and they appear in the Sources list, you can reuse them for additional mappings.

5. In the **Sources** list, select one or more data sources to aggregate the data for the module.

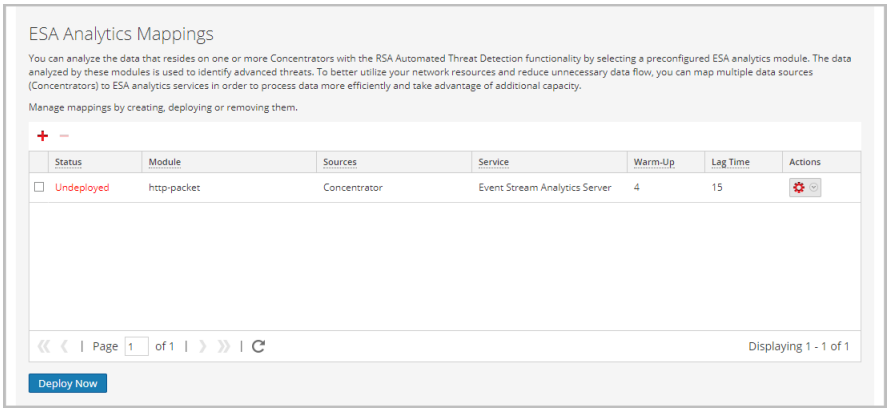


A solid colored green circle indicates a running service and a white circle indicates a stopped service.

6. In the **Service** list, select an ESA Analytics service to process the data for the module.
7. If necessary, specify the time that will be used to query data from the selected Concentrators:

Field	Description
Warm-up Period (Hours)	Specifies a warm-up duration (in hours). A warm-up period is required to allow Automated Threat Detection to "learn" your traffic. The warm-up period should run when typical traffic is running. During this time, alerting for your module mapping is suppressed. The Warm-up Period primes the module with historical data and guarantees that the specified number of hours of data collection completes before sending alerts. RSA provides preconfigured ESA Analytics modules. Each module type has a default warm-up period defined, which you can adjust to your environment, if necessary. After this warm-up period, alerts can be viewed. For more information about Warm-up Period and Lag time, see Module Settings.
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag parameter gives the Concentrator a chance to finish aggregating all of the data. After the warm-up period completes, data aggregation continues at **Current (System) Time - Lag Time**. This is useful when a Concentrator is slow in aggregating data. The Lag time guarantees that the module does not process data that arrives to the Concentrator within the Lag time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by the module. For example, if Lag time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag time defines the buffer between the current time and the time when the module ingests the data. **Caution:** RSA recommends that Administrators adjust the Lag parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. For more information about Warm-up Period and Lag time, see Module Settings.

8. Click **Create**.
   The mappings that you create appear in the list of existing mappings with a status of **Undeployed**.



Important: To start a module so that it starts aggregating data, you need to deploy it.

Deploy ESA Analytics Mappings

After you create your mappings, you need to deploy them in order to start aggregating data for the modules.

1. In the list of mappings, verify that the status of the mappings that you want to deploy show as **Undeployed**.
2. Select one or more mappings with a status of Undeployed and select **Deploy Now**.
   All selected mappings in the Undeployed state start to aggregate data as configured in the mapping.
   The mapping status changes to **Deployed**.
   You cannot deploy a mapping that has already been deployed.

Update a Mapping

You can only have one mapping per module. If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that module.

You can make the following updates to a deployed mapping without deleting it:

- Undeploy the mapping
- Change the warm-up period and lag time

You can also change the warm-up period and lag time for an undeployed module mapping.

Undeploy a Mapping

If you want to stop aggregating data for a module mapping, but you do not want to delete the mapping, you can undeploy it. This gives you the option of deploying it at a later time. When you undeploy a mapping, the specified ESA Analytics service stops pulling data from the data source for that module.

Caution: Undeploying a mapping with a status of Deployed will affect data aggregation for that module.

To undeploy a mapping:

1. In the ESA Analytics Mappings panel, select the deployed mapping that you want to undeploy.
2. In the **Actions** column, select  > **Undeploy**.
   The status changes from Deployed to Undeployed and data aggregation stops.

Delete a Mapping

You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not running, it does not affect data aggregation.

You should undeploy a mapping with a status of Deployed before deleting it. Undeploying and deleting a mapping clears the configuration on the ESA server, reverts the deployment for that mapping, and stops pulling data from the data source for that module.

Caution: Undeploying and deleting a mapping will affect data aggregation for that module.

To delete a mapping:

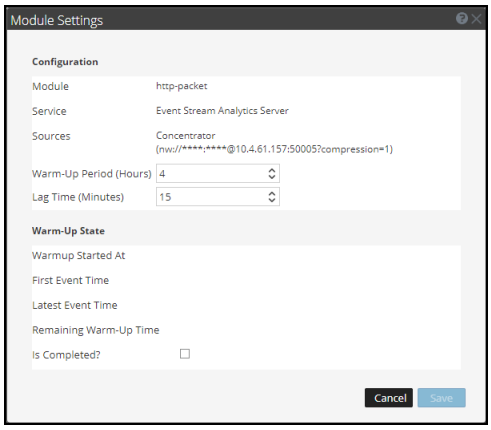
1. In the ESA Analytics Mappings panel, select the mapping that you want to delete. You can only delete one mapping at a time.
2. Click .

Change the Warm-up Period and Lag Time

You may want to adjust the warm-up period for a specific module mapping. For example, after the warm up period is complete, you can increase the warm-up period setting to allow additional warm-up time. You can even increase the warm-up period when your module mapping is actively warming up.

If necessary, you can change the lag time for the module. The lag time defines the buffer between the current (system) time and the time when the module ingests the data.

1. In the ESA Analytics Mappings panel, select the mapping that you want to change and in the **Actions** column, select  > **Edit Module**.
   The Module Settings dialog shows the selected module, ESA Analytics service, and data sources for the mapping. The data sources show the URLs used to communicate with ESA.



2. Review the **Warm-Up State** section to determine the current warm-up state:
   - **Warm Up Started At** - The time when the first event was processed by the ESA Analytics module from the data source.
   - **First Event Time** - The time that the first event occurred. The warm-up time is based on this time.
   - **Latest Event Time** - The time that the latest event occurred.
   - **Remaining Warm Up Time** - The number of hours remaining in the warm-up period.
   - **Is Completed?** - Indicates whether the warm-up period is complete. If it is true, the warm-up period is complete. If it is false, the module is still warming up and you can view the number of hours remaining in the Remaining Warm Up Time field.
3. In the **Configuration** section, you can update the **Warm-Up Period (Hours)** depending on whether or not the warm-up period is complete.
   - **During the warm up period** - You can add hours to the warm-up period or subtract any remaining warm-up time.
   - **The warm-up period is complete** - You can add hours to the warm-up period by adding the difference between the current time and the First Event Time to the hours that you want to add. For example, a warm-up period of 10 hours is complete and the First Event Time shows 12:00:00. The current time is 16:00:00 (4 hours later) and you want to add 5 more hours to the warm-up time. To do this, you need to add 9 hours (4+5=9) to the warm-up period of 10, so you would set the new warm-up period to 19 hours.
     You cannot decrease the warm-up period if it is complete, unless you delete the mapping and create a new one.
4. If necessary, you can adjust the **Lag Time (Minutes)** to give the Concentrators in the mapping additional time to finish aggregating all of the data.
5. Click **Save**.
   Changes DO NOT take effect immediately. For the settings to take effect, you need to undeploy and re-deploy the mapping.

6. To undeploy the mapping, in the ESA Analytics Mappings panel, select the mapping that you want to undeploy and then select  > **Undeploy**.
   Data aggregation stops for the selected mapping.
7. To re-deploy the mapping, select the mapping that you want to deploy and then select  > **Deploy**.
   The selected mapping deploys and starts to aggregate data as configured in the mapping.

References

This section is a collection of references, which describe the user interface for ESA Configuration in NetWitness Platform.

See the following topics for details:

- Services Config View Advanced Tab
- Services Config View Data Sources Tab
- ESA Analytics Mappings
- Module Settings
- Whois Lookup Service Configuration

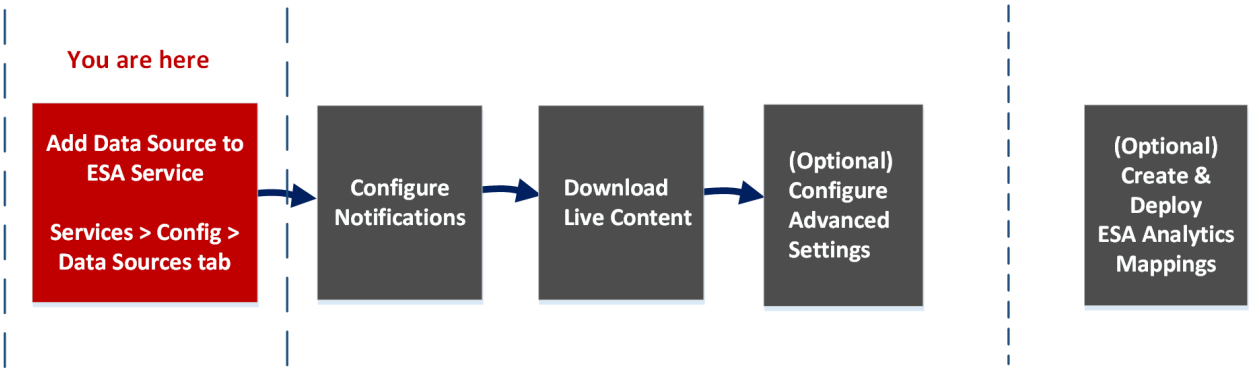
Services Config View Data Sources Tab

Note: The information in this topic applies ONLY to RSA NetWitness® Platform version 11.2 and earlier. For version 11.3 and later, see Data Source Configuration Changes.

The **Services Config view > Data Sources** tab of an ESA service enables you to configure the sources that ESA uses to analyze data. An ESA service ingests data from Concentrators to detect incidents and alert analysts to potential threats.

Workflow

This workflow shows the overall process for configuring ESA. It also shows where configuring data sources is located in the process.



In NetWitness Platform 11.2 and earlier, ESA has two services, the Event Stream Analysis service (ESA Correlation Rules) and the Event Stream Analytics Server service (ESA Analytics). The first four procedures shown pertain to configuring the Event Stream Analysis service:

- Add Data Source to ESA Service*
- Configure Notifications
- Download Live Content
- (Optional) Configure Advanced Settings

The last procedure is separate from the others and pertains to creating mappings for the ESA Analytics services to start automatically detecting advanced threats:

- (Optional) Create and Deploy ESA Analytics Mappings

What do you want to do?

Role	I want to ...	Show me how
Administrator	Add a Concentrator as a data source to the Event Stream Analysis Service *	See "Configure ESA Correlation Rules" and "Step 1. Add a Data Source to an ESA Service" in the *ESA Configuration Guide for version 11.2.*

Role	I want to ...	Show me how
Administrator	Configure Notifications	See "Notification Methods" in the *Alerting with ESA Correlation Rules User Guide for version 11.2.*
Administrator	Download Live Content	See "Download Configurable RSA Live Rules" in the *Alerting with ESA Correlation Rules User Guide for version 11.2.*
Administrator	Configure Advanced Settings	See "Step 2. Configure Advanced Settings for an ESA Service" in the *ESA Configuration Guide for version 11.2.*

*You can complete these tasks here (that is in the Services Config view Data Sources tab).

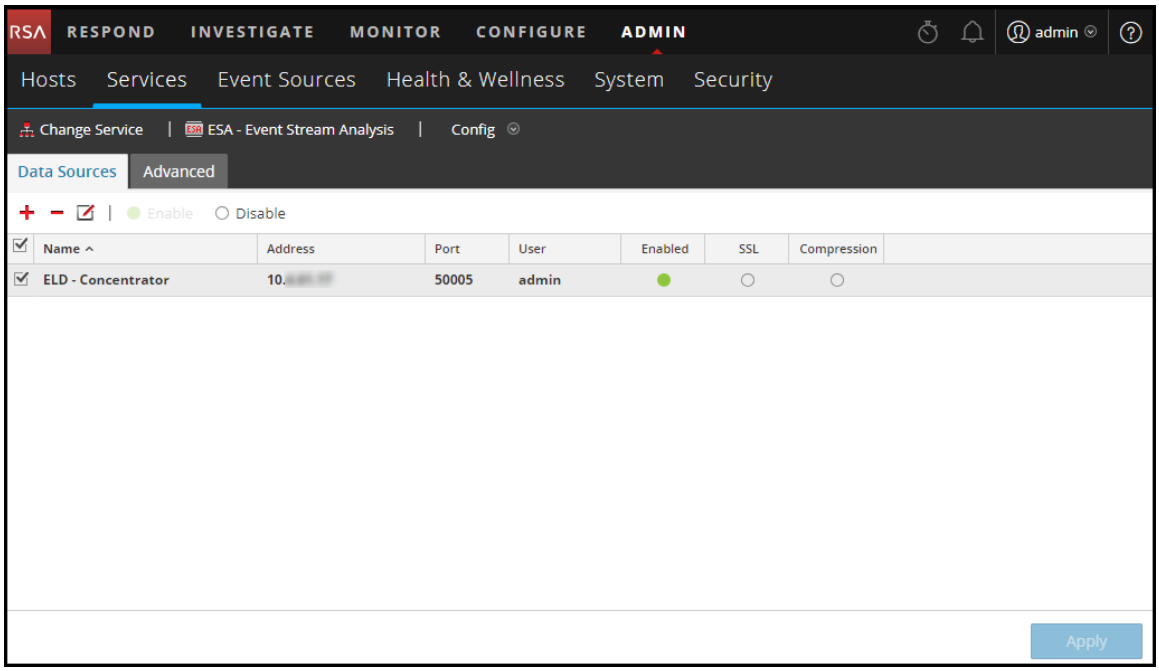
Related Topics

- See "Add or Update a Host" in the *Host and Services Getting Started Guide*.

Quick Look

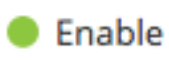
To access the Data Sources tab, go to **ADMIN > Services >** (Select an ESA service) >  **> View > Config**.

The following figure shows the Services Config view Data Sources tab for an ESA service.



Toolbar

The following table describes the options in the toolbar.

Option	Description
	Adds a new data source to the ESA service.
	Deletes a data source from the ESA service.
	Edits a data source. You must have the username and password credentials for the service in order to make changes.
	Enables the selected data source.
	Disables the selected data source.

Data Sources

The Data Sources list shows all of the data sources added to the ESA service. The following table describes the columns the Data Sources list.

Column	Description
Name	The name of the data source service.
Address	The address of the data source service.
Port	The port used by the data source.
User	The user connected with the data source.
Enabled	Indicates if the data source is enabled.
SSL	Indicates if SSL communication is enabled.
Compression	Indicates if compression is enabled.

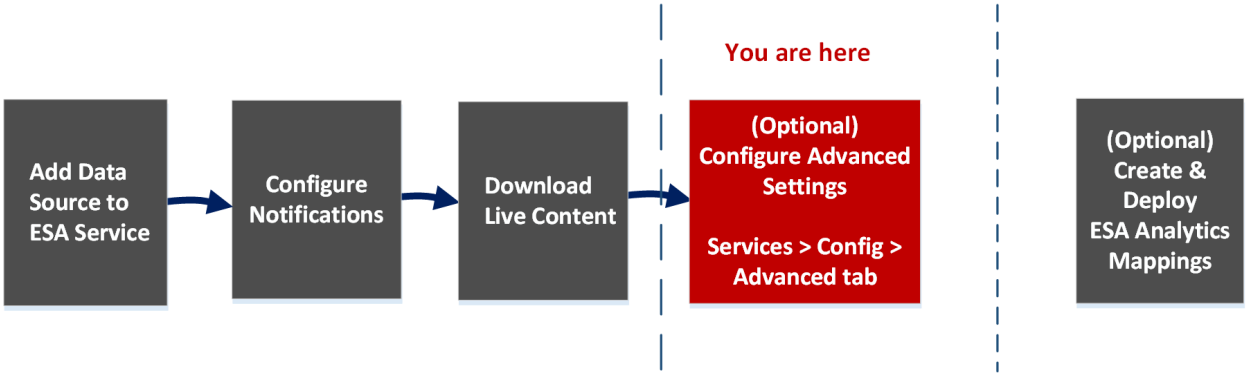
Services Config View Advanced Tab

Note: The information in this topic applies ONLY to RSA NetWitness® Platform version 11.2 and earlier. For version 11.3 and later, see Configure Advanced Settings for an ESA Correlation Service.

The **Services Config view > Advanced** tab of an ESA service enables you to configure advanced settings. In the Advanced view, you can configure advanced settings to improve performance, to preserve events for rules with multiple events, to buffer events in memory, and to set the number of events to be stored on the ESA.

Workflow

This workflow shows the overall process for configuring ESA. It also shows where configuring advanced settings is located in the process.



In NetWitness Platform 11.2 and earlier, ESA has two services, the Event Stream Analysis service (ESA Correlation Rules) and the Event Stream Analytics Server service (ESA Analytics). The first four procedures shown pertain to configuring the Event Stream Analysis service:

- Add Data Source to ESA Service
- Configure Notifications
- Download Live Content
- (Optional) Configure Advanced Settings*

The last procedure is separate from the others and pertains to creating mappings for the ESA Analytics services to start automatically detecting advanced threats:

- (Optional) Create and Deploy ESA Analytics Mappings

What do you want to do?

Role	I want to ...	Show me how
Administrator	Add a Concentrator as a data source to the Event Stream Analysis Service	See "Configure ESA Correlation Rules" and "Step 1. Add a Data Source to an ESA Service" in the *ESA Configuration Guide for version 11.2*.
Administrator	Configure Notifications	See "Notification Methods" in the *Alerting with ESA Correlation Rules User Guide for version 11.2*.
Administrator	Download Live Content	See "Download Configurable RSA Live Rules" in the *Alerting with ESA Correlation Rules User Guide for version 11.2*.
Administrator	Configure Advanced Settings *	See "Step 2. Configure Advanced Settings for an ESA Service" in the *ESA Configuration Guide for version 11.2*.

*You can complete these tasks here (that is in the Services Config view Advanced tab).

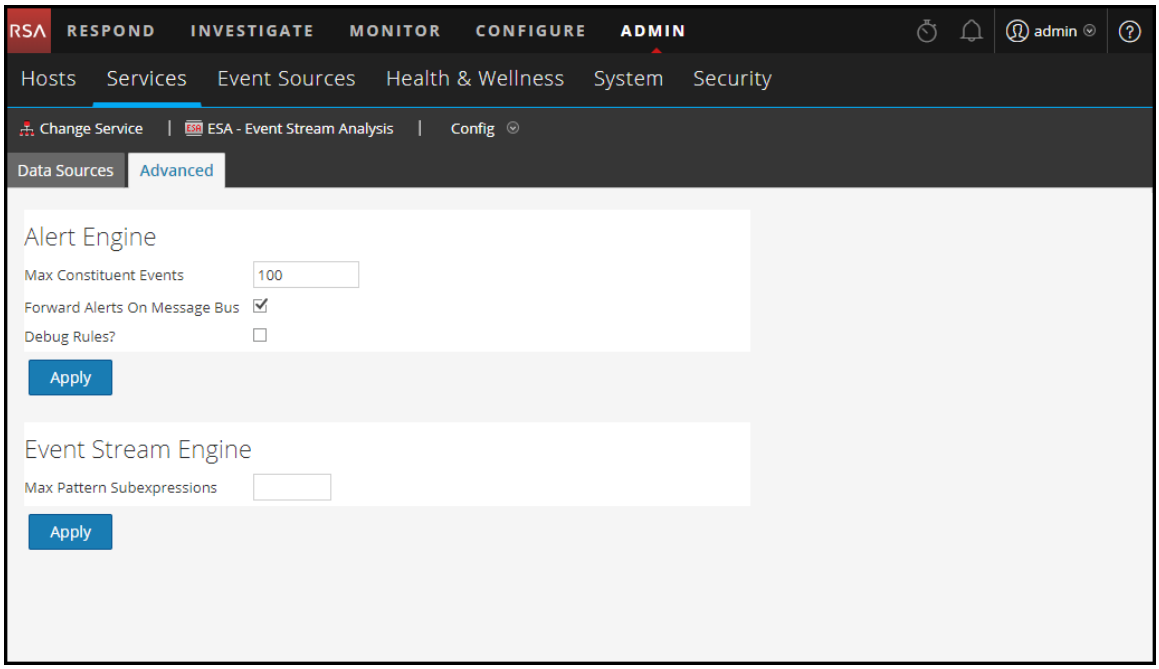
Related Topics

- See "Add or Update a Host" in the *Host and Services Getting Started Guide*

Quick Look

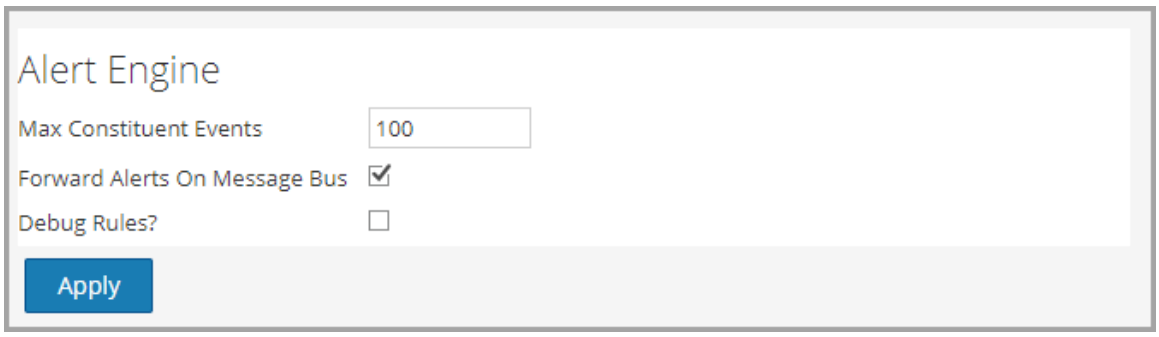
To access the Advanced tab, go to **ADMIN** > **Services** > (Select an ESA service) >  > **View** > **Config**.

The following figure shows the Services Config view Advanced tab for an ESA service.



Alert Engine Settings

In the Alert Engine section, you specify values to preserve events for rules that choose multiple events. The following figure shows the Alert Engine section.



The following table lists the parameters in the Alert Engine section and their descriptions.

Parameter	Description
Max Constituent Events	For rules that contain multiple events, this configuration value determines how many of the associated events are preserved. 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.
Forward Alerts On Message Bus	To forward ESA alerts for NetWitness Respond, you must select this option. The ESA alerts generated will be sent to the Message Bus and subsequently to Respond. This option is selected by default. You may want to ensure that the Respond Server service is running.
Debug Rules?	Selecting enables debugging rules.

Event Stream Engine Settings

In the Event Stream Engine section, you specify details to improve performance. The following figure shows the Event Stream Engine section.

The following table lists the parameter in the Event Stream Engine section and its description.

Parameter	Description
Max Pattern Subexpressions	Certain rules require ESPER to maintain subexpressions in memory before deciding to fire them or not. These subexpressions consume memory and if left unchecked may cause the service to go down with memory exhaustion. This parameter is a safety measure that keeps such memory hogging rules under check. If a rule exceeds the specified number of subexpressions, its processing is delayed. The default value is 0, which means this setting is disabled. You must set a value if there are service stability issues.

Whois Lookup Service Configuration

In the Whois Lookup Configuration panel (ADMIN > System > Whois), you configure a connection to the Whois Lookup service for your preconfigured ESA Analytics modules used in RSA Automated Threat Detection. The Whois Service enables you to get accurate data about domains that you connect to. In order to ensure effective scoring, it is important that you configure the Whois service settings.

You must have an RSA Live account to use this service.

If you configured a Live account in the Live Services panel (ADMIN > System > Live Services), the Whois Lookup Service is automatically configured for you. You just need to check the connection of the Whois Lookup service.

Note: If you do not have an RSA Live account, you can create one at the RSA Live Registration Portal: https://cms.netwitness.com/registration/ The *Live Services Management Guide* provides additional information.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure the Whois Lookup service.	Configure the Whois Lookup Service
Administrator	Check the connection of the Whois Lookup service.	Configure the Whois Lookup Service

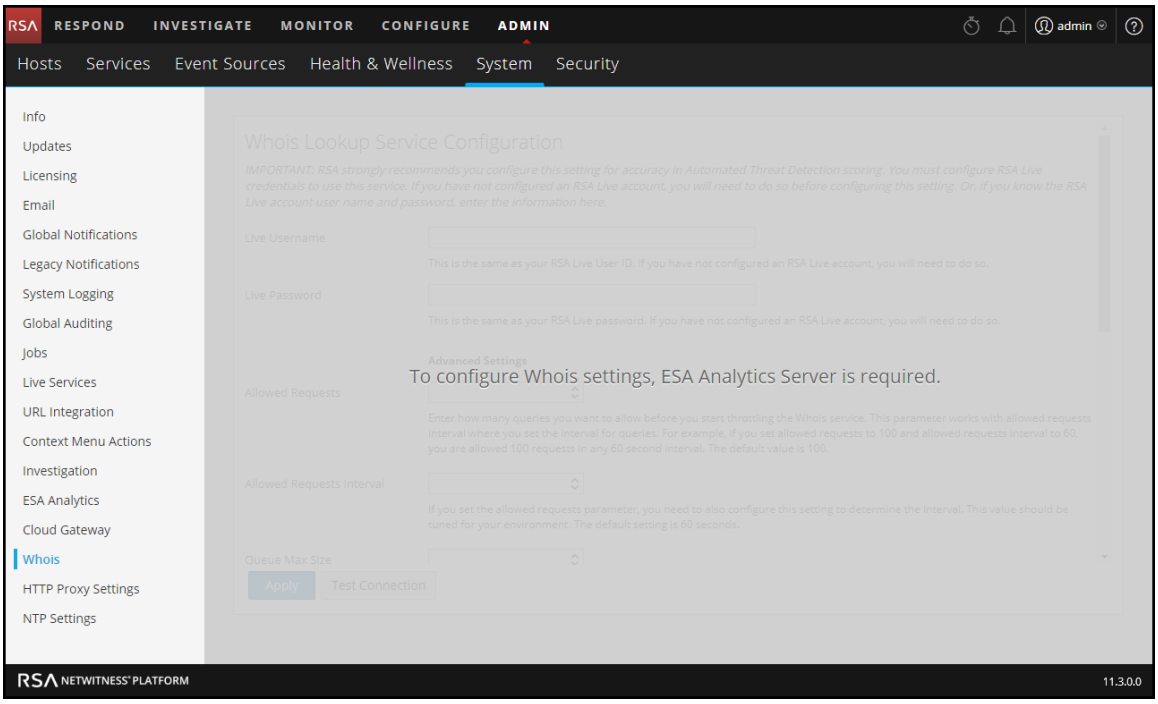
Related Topics

- ESA Analytics Mappings

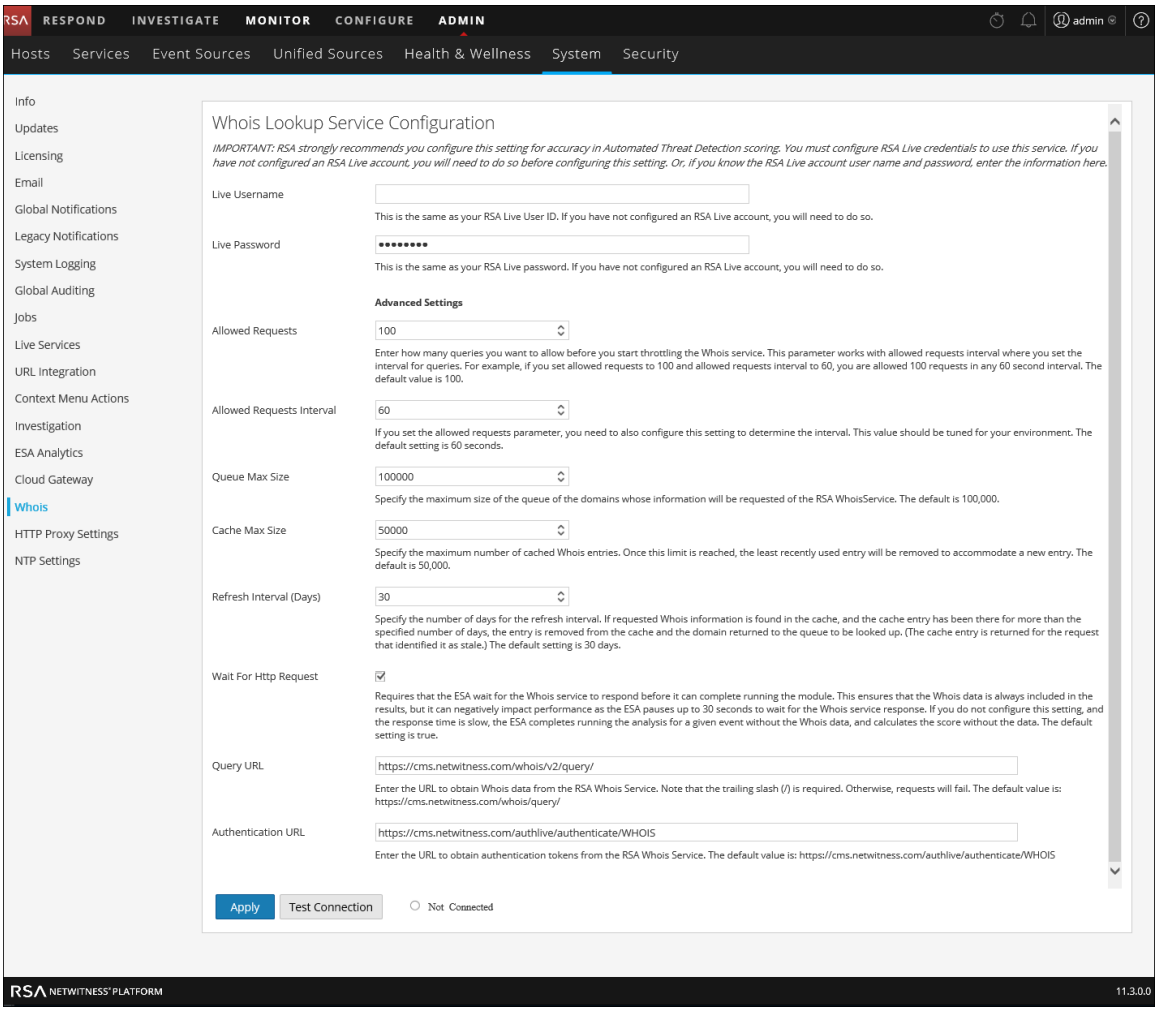
Quick Look

To access the Whois Lookup Service Configuration, go to ADMIN > System and in the options panel, select Whois.

The ESA Analytics Server service must be available (shows a green circle) in the ADMIN > Services view. If you do not have an ESA Analytics Server service available, you will see the following panel.



If you have an ESA Analytics Server service available, you will see the following panel.



The following table describes the listed Whois Lookup Service configuration settings.

Parameter	Description
Live Username	**Required only if you did not already configure the Whois Lookup service.** Enter the authentication credential for the RSA Whois Server. This is the same as your RSA Live User ID. If you have not configured an RSA Live account, you will need to do so. The default value is "whois."
Live Password	**Required only if you did already configure the Whois Lookup service.** Enter the authentication credential for the RSA Whois Server. This is the same as your RSA Live password. If you have not configured an RSA Live account, you will need to do so. The default value is null.

Parameter	Description
Allowed Requests	(Optional) Enter how many queries you want to allow before you start throttling the Whois service. This parameter works with **Allowed Requests Interval** (in seconds), where you set the interval for queries. For example, if you set **Allowed Requests** to 100 and **Allowed Requests Interval** to 60, you are allowed 100 requests in any 60 second interval. The default value is 100.
Allowed Requests Interval	(Optional) If you set the **Allowed Requests** parameter, you need to also configure this setting to determine the interval. This value should be tuned for your environment. The default setting is 60 seconds.
Queue Max Size	(Optional) Specify the maximum size of the queue of the domains whose information will be requested of the RSA WhoisService. The default is 100,000.
Cache Max Size	(Optional) Specify the maximum number of cached Whois entries. Once this limit is reached, the least recently used entry will be removed to accommodate a new entry. The default is 50,000.
Refresh Interval (Days)	(Optional) Specify the number of days for the refresh interval. If requested Whois information is found in the cache, and the cache entry has been there for more than the specified number of days, the entry is removed from the cache and the domain returned to the queue to be looked up. (The cache entry is returned for the request that identified it as stale.) The default setting is 30 days.
Wait For HTTP Request	(Optional) Requires that the ESA wait for the Whois service to respond before it can complete running the module. This ensures that the Whois data is always included in the results, but it can negatively impact performance as the ESA pauses up to 30 seconds to wait for the Whois service response. If you do not configure this setting, and the response time is slow, the ESA completes running the analysis for a given event without the Whois data, and calculates the score without the data. The default setting is true.
Query URL	(Optional) Enter the URL to obtain Whois data from the RSA Whois service. The trailing slash ('/') is required. Otherwise, requests will fail. The default value is: `https://cms.netwitness.com/whois/v2/query/`
Authentication URL	(Optional) Enter the URL to obtain authentication tokens from the RSA Whois service. The default value is: `https://cms.netwitness.com/authlive/authenticate/WHOIS`

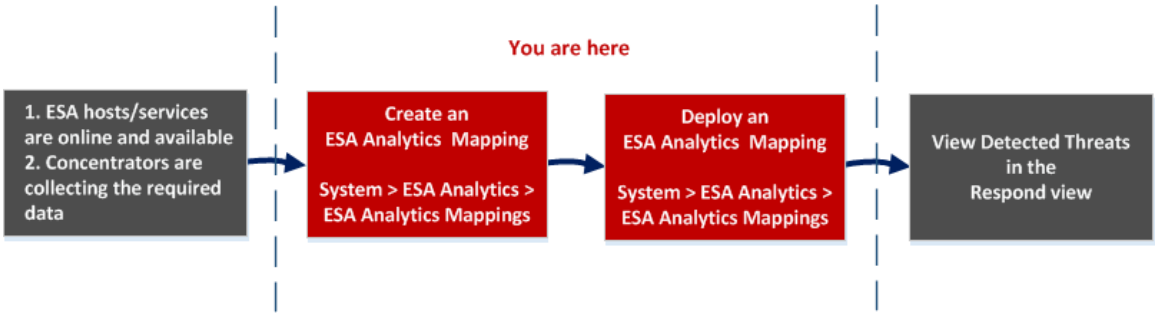
ESA Analytics Mappings

In the ESA Analytics Mappings panel (ADMIN > System > ESA Analytics), you define how the RSA Automated Threat Detection functionality should automatically detect advanced threats. You can analyze the data that resides on one or more Concentrators by selecting a preconfigured ESA Analytics module.

To better utilize your network resources and reduce unnecessary data flow, you can map multiple data sources, such as Concentrators, to available ESA Analytics services in order to process data more efficiently and take advantage of additional capacity.

Workflow

This workflow shows the process for creating and enabling an ESA Analytics mapping to start automatically detecting advanced threats.



Before you create an ESA Analytics mapping, ensure that the ESA hosts and services that you want to use for your mappings are online and available. All of the services need to be in sync with a consistent time source. Also ensure that the Concentrators are collecting the required data. When you create an ESA Analytics mapping, you select an ESA Analytics module to map, such as Suspicious Domains. Then you select the data sources, such as Concentrators, to use for that module along with an ESA Analytics service to process the data. When you are ready to start aggregating data, you deploy the mapping. Analysts can view detected threats for that module in the Respond view.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Verify that the ESA hosts and services are online and available.	ADMIN > HOSTS and ADMIN > SERVICES See *Hosts and Services Getting Started Guide*.
Administrator	Ensure that the Concentrators are collecting the required data.	See *Broker and Concentrator Configuration Guide*
Administrator	Create ESA Analytics mappings.*	Mapping ESA Data Sources to Analytics Modules
Administrator	Deploy ESA Analytics mappings.*	Mapping ESA Data Sources to Analytics Modules

Role	I want to ...	Show me how
Administrator, Analyst	View detected threats.	See *NetWitness Respond User Guide*.

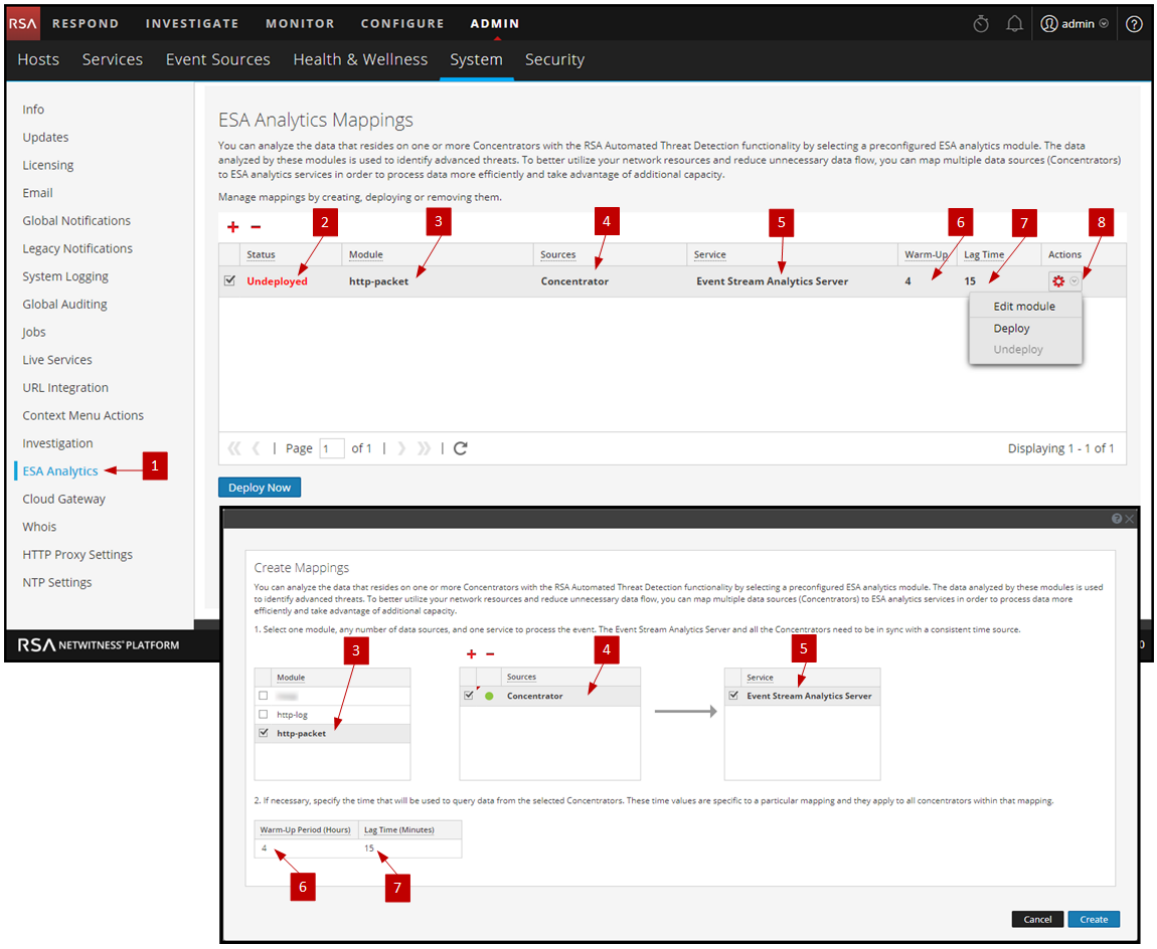
*You can complete these tasks here (that is in the ESA Analytics Mappings panel).

Related Topics

- Configure ESA Analytics
- Update a Mapping
- Undeploy a Mapping
- Delete a Mapping
- Change the Warm-up Period and Lag Time
- Module Settings

Quick Look

The following example illustrates an ESA Analytics mapping. The configuration defines the data sources for the selected module and the ESA Analytics service that will process the events from those data sources.



1	Displays the ESA Analytics Mappings panel.
2	Shows the status of the ESA Analytics mapping.
3	The name of the module that is mapped.
4	Data sources, such as Concentrators, assigned to the mapping.
5	ESA Analytics service that processes the data for the mapping.
6	Warm-up period configuration (in hours) on the data sources for the mapping.
7	Lag configuration (in minutes) on the data sources for the mapping.
8	Actions for changing module settings, deploying module mappings, and undeploying module mappings.

Toolbar

The following table describes the toolbar actions.

Icon / Button	Description
	Opens the Create Mappings dialog where you can create an ESA Analytics mapping. Create a separate mapping for each module. After creating and reviewing the mappings, you deploy them.
	Deletes an ESA Analytics Mapping. • You can delete a mapping with a status of Undeployed at any time. Since a mapping in the Undeployed state is not deployed and is not running, it does not affect data aggregation. • Deleting a deployed mapping clears the configuration on the ESA server, reverts the deployment for that mapping, and stops pulling data from the data source for that module. You should undeploy a mapping with a status of Deployed before deleting it.
Deploy Now	After you create your mappings, you need to deploy them in order to start aggregating data for the modules. You can select one or more mappings with a status of Undeployed to deploy.

Note: If you want to make changes to a deployed mapping, such as adding or removing Concentrators or changing the service, you must undeploy and delete the existing mapping and then create and deploy a new mapping for that module.

ESA Analytics Mappings

The following table describes the listed ESA Analytics mappings.

Title	Description
	To select an individual mapping, select the checkbox next to the mapping.
Status	Shows the status of the mapping. There are two statuses: **Undeployed** - An undeployed mapping maps an ESA Analytics module to sources and an ESA Analytics service. It does not start aggregating data for the module until you deploy the mapping. **Deployed** - A deployed mapping is deployed and running. In a deployed mapping, the selected ESA Analytics service uses query-based aggregation to collect the appropriate filtered events for the selected module from the Concentrators.
Module	Indicates the selected ESA Analytics module. An ESA Analytics module is a pipeline composed of activity objects that enrich an event with additional information through mathematical computations. The module resides within the ESA Analytics service.

Title	Description
Sources	Sources are the data sources, such as Concentrators, from which ESA will aggregate the data for the specified module.
Service	Indicates the ESA Analytics service that will process the data for the specified module. The selected service needs to be in sync with a consistent time source.
Warm-Up Period (Hours)	Specifies a warm-up duration (in hours). A warm-up period is required to allow Automated Threat Detection to "learn" your traffic. The warm-up period should run when typical traffic is running. During this time, alerting for your module mapping is suppressed. The Warm-up Period primes the module with historical data and guarantees that the specified number of hours of data collection completes before sending alerts. RSA provides preconfigured ESA Analytics modules. Each module type has a default warm-up period defined, which you can adjust to your environment, if necessary. After this warm-up period, alerts can be viewed. For more information about Warm-up Period and Lag time, see Module Settings.
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag parameter gives the Concentrator a chance to finish aggregating all of the data. After the warm-up period completes, data aggregation continues at **Current (System) Time - Lag Time**. This is useful when a Concentrator is slow in aggregating data. The Lag time guarantees that the module does not process data that arrives to the Concentrator within the Lag time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by the module. For example, if Lag time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag time defines the buffer between the current time and the time when the module ingests the data. **Caution:** RSA recommends that Administrators adjust the Lag parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. For more information about Warm-up Period and Lag time, see Module Settings.

Title	Description
	Enables you to select additional actions for the selected module mapping: • **Edit Module** - Enables you to configure the warm-up period and lag time for the selected module mapping. • **Deploy** - Deploys the selected module mapping. The specified ESA Analytics service starts pulling data from the data sources for that module. • **Undeploy** - Undeploys the selected module mapping. The specified ESA Analytics service stops pulling data from the data sources for that module. **Caution:** Undeploying a mapping with a status of Deployed will affect data aggregation for that module.

Module Settings

After you create or deploy a module mapping in the ESA Analytics Mappings panel (ADMIN > System > ESA Analytics), you have the option to change some module configurations for that mapping.

What do you want to do?

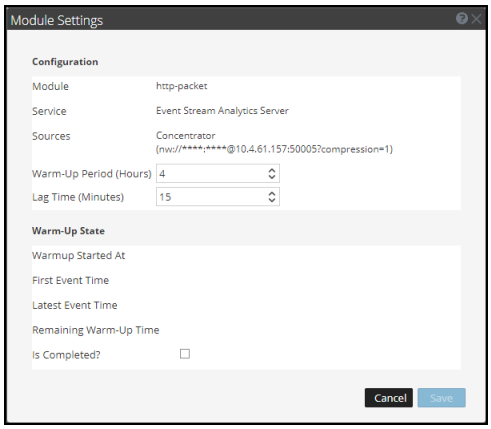
Role	I want to ...	Show me how
Administrator	Change the warm-up period for an undeployed module mapping.	Change the Warm-up Period and Lag Time
Administrator	Change the warm-up period for a module mapping during the warm-up period.	Change the Warm-up Period and Lag Time
Administrator	Change the warm-up period for a module mapping after the warm-up period is complete.	Change the Warm-up Period and Lag Time

Related Topics

- Mapping ESA Data Sources to Analytics Modules
- ESA Analytics Mappings

Quick Look

To access the module settings, in the ESA Analytics Mappings panel, select the mapping that you want to change and in the **Actions** column, select  **> Edit Module**. The Module Settings dialog has a Configurations section and a Warm-Up State section.



Configurations

The Configurations section enables you to change the Warm-Up Period and Lag Time configurations.

The following table describes the settings available for an ESA Analytics module mapping.

Field	Description
Module	Shows the name of the mapped module.
Service	Shows the ESA Analytics service that processes the data for the mapping.
Sources	Shows the mapped data sources and the URLs used to communicate with ESA.
Warm-Up Period (Hours)	Specifies a warm-up duration in hours. A warm-up period is required to allow Automated Threat Detection to "learn" your traffic. The warm-up period should run when typical traffic is running. During this time, alerting for your module mapping is suppressed. The Warm-up Period primes the module with historical data and guarantees that the specified number of hours of data collection completes before sending alerts. RSA provides preconfigured ESA Analytics modules. Each module type has a default warm-up period defined, which you can adjust to your environment, if necessary. After this warm-up period, alerts can be viewed. You can update the Warm-Up Period of a deployed module mapping depending on whether or not the warm-up period is complete: • **During the warm up period** - You can add hours to the warm-up period or subtract any remaining warm-up time. • **The warm-up period is complete** - You can add hours to the warm-up period by adding the difference between the current time and the First Event Time to the hours that you want to add. For example, a warm-up period of 10 hours is complete and the First Event Time shows 12:00:00. The current (system) time is 16:00:00 (4 hours later) and you want to add 5 more hours to the warm-up time. To do this, you need to add 9 hours (4+5=9) to the warm-up period of 10, so you would set the new warm-up period to 19 hours. You cannot decrease the warm-up period if it is complete, unless you delete the mapping and create a new one. The Warm-up Period value is specific to a particular mapping and it applies to all Concentrators within that mapping after you deploy it. If a Concentrator is shared between two modules with different warm-up times, the Concentrator uses separate Warm-up Period values for each module mapping.

Field	Description
Lag Time (Minutes)	Specifies a constant time delay in minutes, which is added to avoid losing events being processed by the data sources during periods of heavy activity. For example, Concentrator performance varies depending on factors such as incoming load, ongoing queries, and indexing. Due to these factors, a Concentrator may not aggregate events in real-time, which leads to the delay. The Lag parameter gives the Concentrator a chance to finish aggregating all of the data. When you specify a Lag time, the first time the module deploys, data aggregation starts at **Current (System) Time - Lag Time - Warm-Up Time**. For example, if the current time is 2:00 PM, Lag time is 30 minutes, and Warm-up time is 4 hours, when the module deploys for the first time, data collection starts at 9:30 AM (2:00 PM - .5 hour - 4 hours). After the warm-up period completes, data aggregation continues at **Current (System) Time - Lag Time**. This is useful when a Concentrator is slow in aggregating data. The Lag time guarantees that the module does not process data that arrives to the Concentrator within the Lag time window so there is adequate delay to ensure all events that get generated in the enterprise can be processed by the module. For example, if Lag time is 30 minutes, and the current time is 2:00 PM, the Concentrator starts pulling records at 1:30 PM. The Lag time window, 30 minutes in this example, remains constant as time advances. When the current time advances to 2:01 PM, the Concentrator pulls the next minute of data at 1:31 PM, and so on. **Important**: The Lag time defines the buffer between the current time and the time when the module ingests the data. The Lag time value is specific to a particular mapping and it applies to all Concentrators within that mapping after you deploy it. If a Concentrator is shared between two modules with different Lag times, the Concentrator uses separate Lag values for each module mapping. **Caution:** RSA recommends that Administrators adjust the Lag parameter dynamically based on the performance of each of the individual Concentrators to avoid missing any events during aggregation. To determine the correct Lag Time, add together the following to get an environmental lag time: 1. **Log or Packet Latency** - This is the time it takes for the Log Decoder to receive the logs or the (Packet) Decoder to receive packets. For example, the Log Decoder may get logs every 20 minutes. In this case, you would want to set Lag time to at least 20 minutes, preferably 25 minutes, so that you do not miss events. 2. **Aggregation Latency** - This is the time it takes to get the data from the Log Decoder to the Concentrator. 3. **Other Buffer** - Add in any additional time delay specific to your environment.

Warm-Up State

The Warm-Up State section provides information about the warm-up state, which you can use to determine the appropriate adjustments to the warm-up period.

Field	Description
Warmup Started At	The time when the first event was processed by the ESA Analytics module from the data source.
First Event Time	The time that the first event occurred. The warm-up time is based on this time.
Latest Event Time	The time that the latest event occurred.
Remaining Warm-Up Time	The number of hours remaining in the warm-up period.
Is Completed?	Indicates whether the warm-up period is complete. If it is true, the warm-up period is complete. If it is false, the module is still warming up and you can view the number of hours remaining in the Remaining Warm Up Time field.