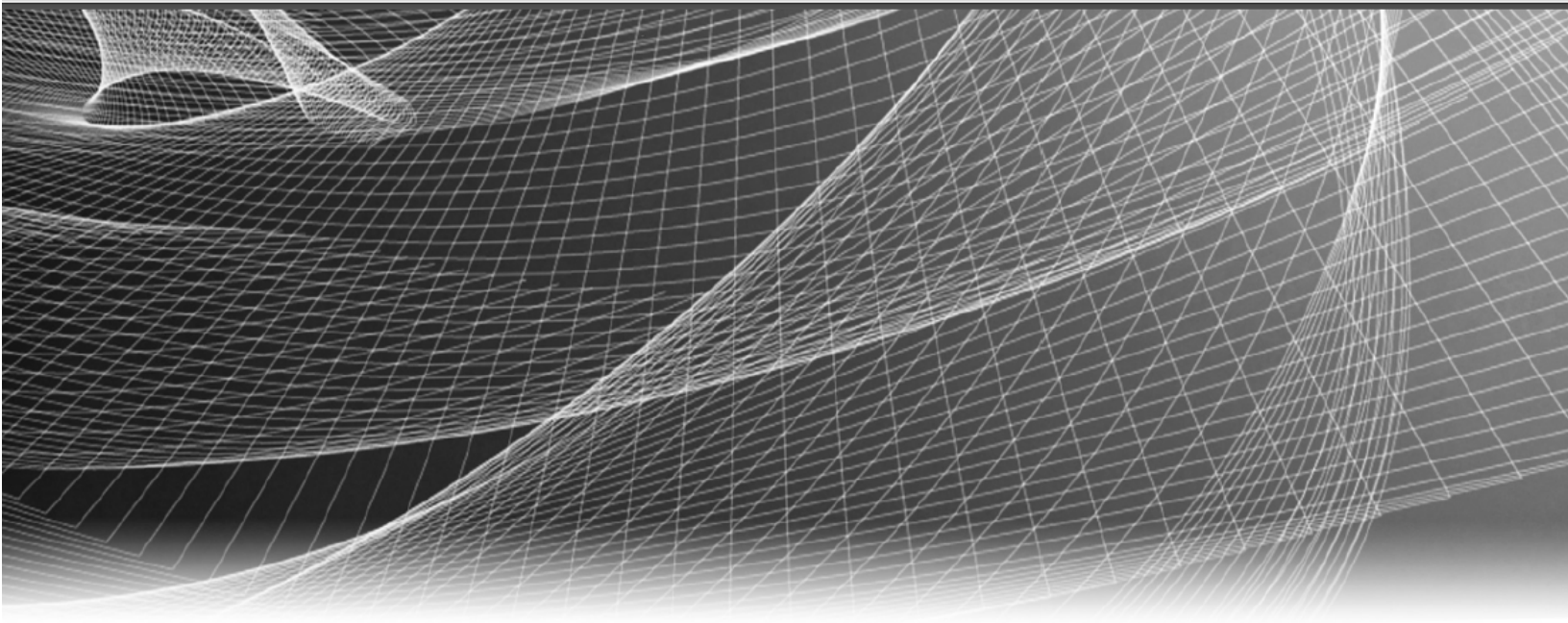


RSA | Security Analytics

RSA ECAT Integration Guide

for Version 10.6.5

RSA

EMC²

Contact Information

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

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

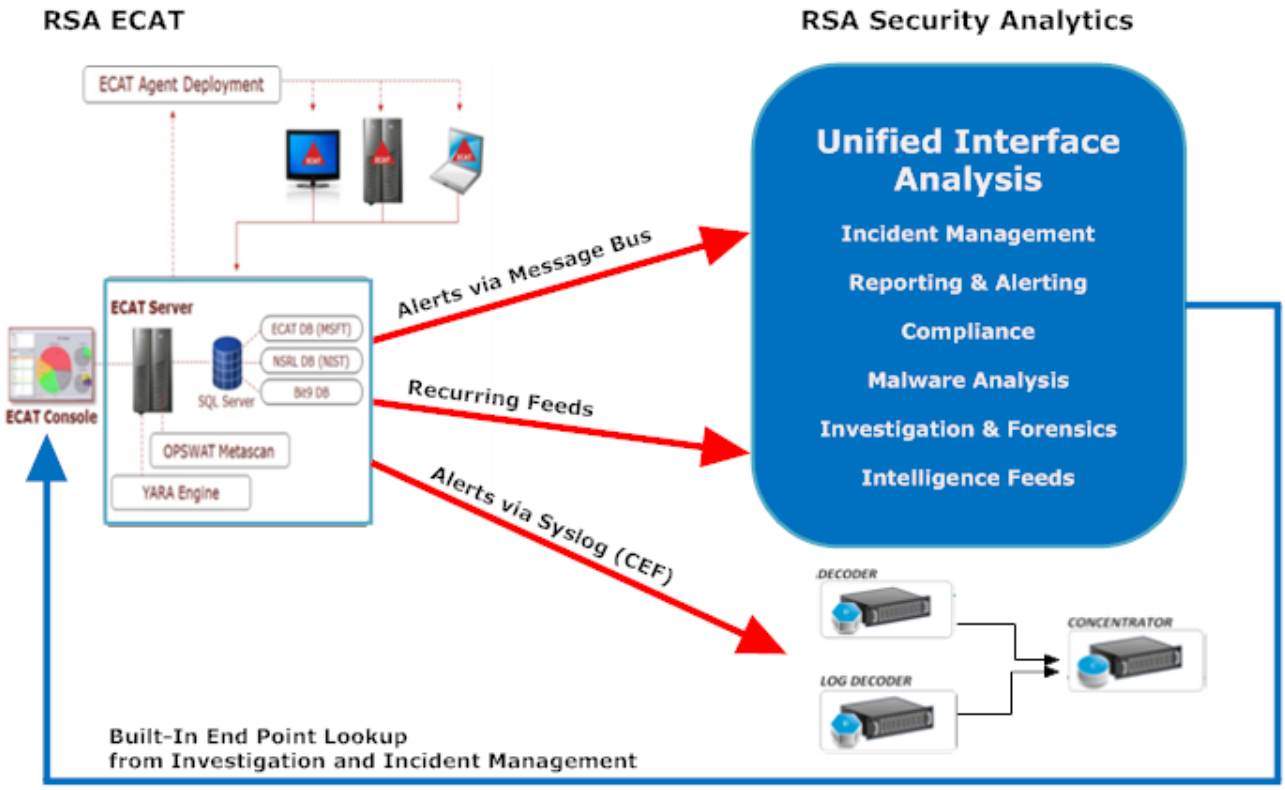
December 2017

Contents

RSA ECAT Integration

RSA customers who are using both RSA ECAT 4.0 and later, and RSA Security Analytics 10.4 and later, can integrate ECAT and Security Analytics in several different ways. This guide is for Security Analytics version 10.6 and later.

Integration Options



Built-in Endpoint Lookup

With the RSA ECAT user interface (UI) installed on the same machine where the analyst is using a browser to access Security Analytics, the built-in Endpoint Lookup from Security Analytics Investigation and Security Analytics Incident Management provides right-click access to the ECAT console server for the following meta keys: IP address (ip-src, ip-dst, ipv6-src, ipv6-dst, orig_ip), host (alias-host, domain.dst), client, and file-hash. These are described in the **Launch an External Lookup of a Meta Key** topic in *Investigation and Malware Analysis* and the **Alerts View** topic in *Incident Management*.

No Security Analytics configuration is required for endpoint lookup when you are using one of the the built-in parsers, RSA ECAT or CEF, and you have not customized the default meta keys used when loading meta data in Investigation see **Manage and Apply Default Meta Keys in an Investigation** in *Investigation and Malware Analysis*.

Note: The exception occurs if you customize Security Analytics by editing the display setting for the default meta keys in Investigation, add meta keys to the table-map-custom.xml file, or customize RSA ECAT feeds. Some configuration is required to add the custom meta keys to the context menu ECAT Lookup in the Administration > System view as described in the **Add Custom Context Menu Actions** topic in the *System Configuration* guide.

Additional Integrations

With an RSA ECAT 4.0 or later console server installed on a Windows host and proper configuration of ECAT and Security Analytics by an administrator, four additional integrations of ECAT analysis data are possible as depicted using red arrows below.

Possible RSA ECAT integrations with Security Analytics include:

- **ECAT alerts via syslog (CEF)into Security Analytics Log Decoders**. This integration provides the capability to apply Live intelligence to ECAT alerts and to correlate ECAT events with other log or packet metadata in the Security Analytics ecosystem (see Configure ECAT Alerts via Syslog into a Log Decoder).
- **ECAT alerts via message businto Security Analytics Incident Management**. This integration provides the capability for centralized Incident Management and workflow in Security Analytics (see the **Configure Alert Sources to Display Alerts in Incident Management** topic in the *Incident Management Configuration Guid*e).
- **Contextual data from ECAT via a Security Analytics Live recurring feed**. This integration can enrich the session displayed in Security Analytics Investigation with contextual information; some examples include the host operating system, MAC address, score, and other data that may not be present in the log or packet data (see Configure Contextual Data from ECAT via Recurring Feed).
- **RSA Live feeds to ECAT 4.0 and later**. This integration can enrich ECAT Instant Indicators of Compromise (IOCs) using several feeds in RSA Live that contain suspicious domains and IP addresses. Instant IOCs defined within ECAT can benefit from these feeds from an intelligence perspective. ECAT 4.0 does not publish any feeds into RSA Live (see Configure ECAT to Receive RSA Live Feeds).

ECAT Alerts and Indicators of Compromise

An ECAT Instant IOC (Indicator of Compromise) is a database query that RSA ECAT runs on collected ECAT scan data to determine the presence of potential malware on scanned hosts. RSA ECAT 4.0 and later ships with IOCs that the user can enable and mark as alertable. RSA ECAT runs IOC queries regularly on new scan data, which is collected and stored in the database. If the IOC query is satisfied, this indicates a potential indicator of compromise, and the event can be reported to a user or sent to an external system as an alert.

Possible types of alerts are:

- Machine alert: This alert indicates that the machine in question is suspicious.
- Module alert: This alert indicates that a module, such as a file, a dll, or an executable, is suspicious. It contains details about the module in question.
- IP alert: This alert indicates that there has been suspicious internet activity (traffic).
- Event alert: This alert represents any other suspicious activity detected by ECAT that does not fall into the above categories.

Each of these alert types can be associated sent to Security Analytics.

Topics

Configure ECAT to Receive RSA Live Feeds

RSA ECAT 4.0 and later can be configured to receive feeds from RSA Live. Several feeds in RSA Live contain suspicious domains and IP addresses, and several Instant Indicators Of Compromise (IOC)s defined within ECAT can benefit from these feeds from an intelligence perspective. None of the feeds are enabled by default in ECAT. When a feed is enabled, ECAT Console server connects to RSA Live https://cms.netwitness.com and periodically downloads feed data into the ECAT system.

Note:
• ECAT does not publish any feeds into RSA Live. It is only a consumer of feeds.
• The procedure to configure ECAT to receive RSA Live feeds is different for ECAT version 4.0 and ECAT version 4.1. We have included instructions for both versions.

Prerequisites

The following are required for this integration:

- Version 4.0 or later ECAT UI and Version 10.6 Security Analytics Server installed.
- An RSA Live account, for which you can get a username and password from RSA Support.
- ECAT Console Server should be able to connect to https://cms.netwitness.com.

Enable or Disable Feeds

For ECAT version 4.0

1. Open the ECAT user interface and log on using the proper credentials.
2. From the menu bar at the top of the page, select **Database > Import Checksums**.
   The Import Checksum dialog is displayed.
3. Select the **RSA Live** tab, and then the **Settings** sub-tab.
4. Fill in the details of the RSA Live server and credentials.
   The host value is usually cms.netwitness.com.
   The port is usually 443.
5. To validate connectivity, click **Test Connection**.
   A Passed message is displayed if all settings are correct.
6. Click **Apply**.

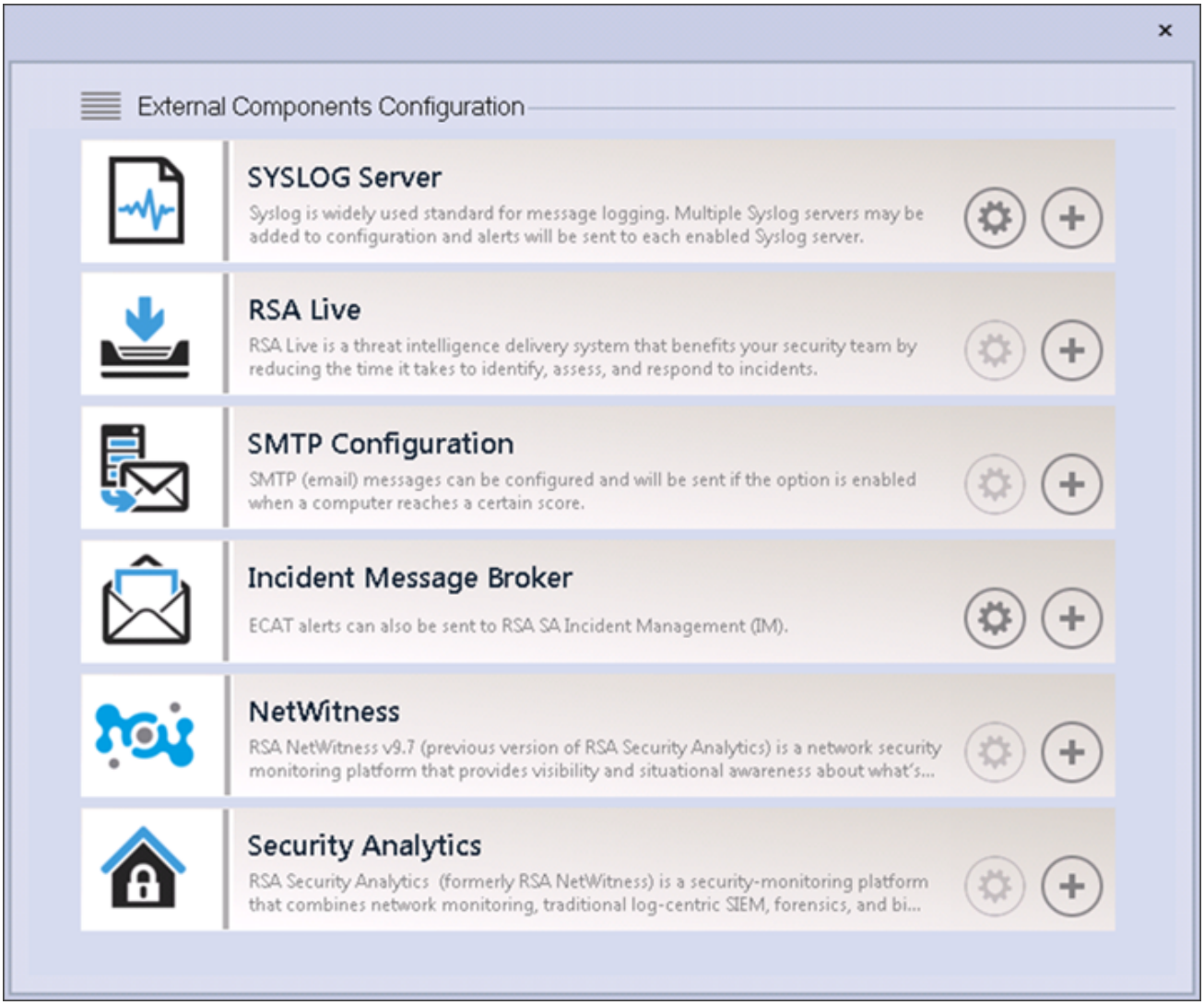
7. Select the **Subscribed Feeds** sub-tab.
   A list of all feeds is displayed.
8. Select the feeds that you want ECAT to import from RSA Live.
9. Enter an appropriate interval. The recommended time is 24 hours, which configures ECAT to connect to RSA Live every 24 hours to update the imported data.
10. (Optional) Click **Refresh Now** to download the feeds right away.
11. Click **Save**.

To view the status of imported known bad domains and IPs from various feeds, select the **Status** tab and select the feed. The number of entries per feed varies from a few hundred to several thousand.

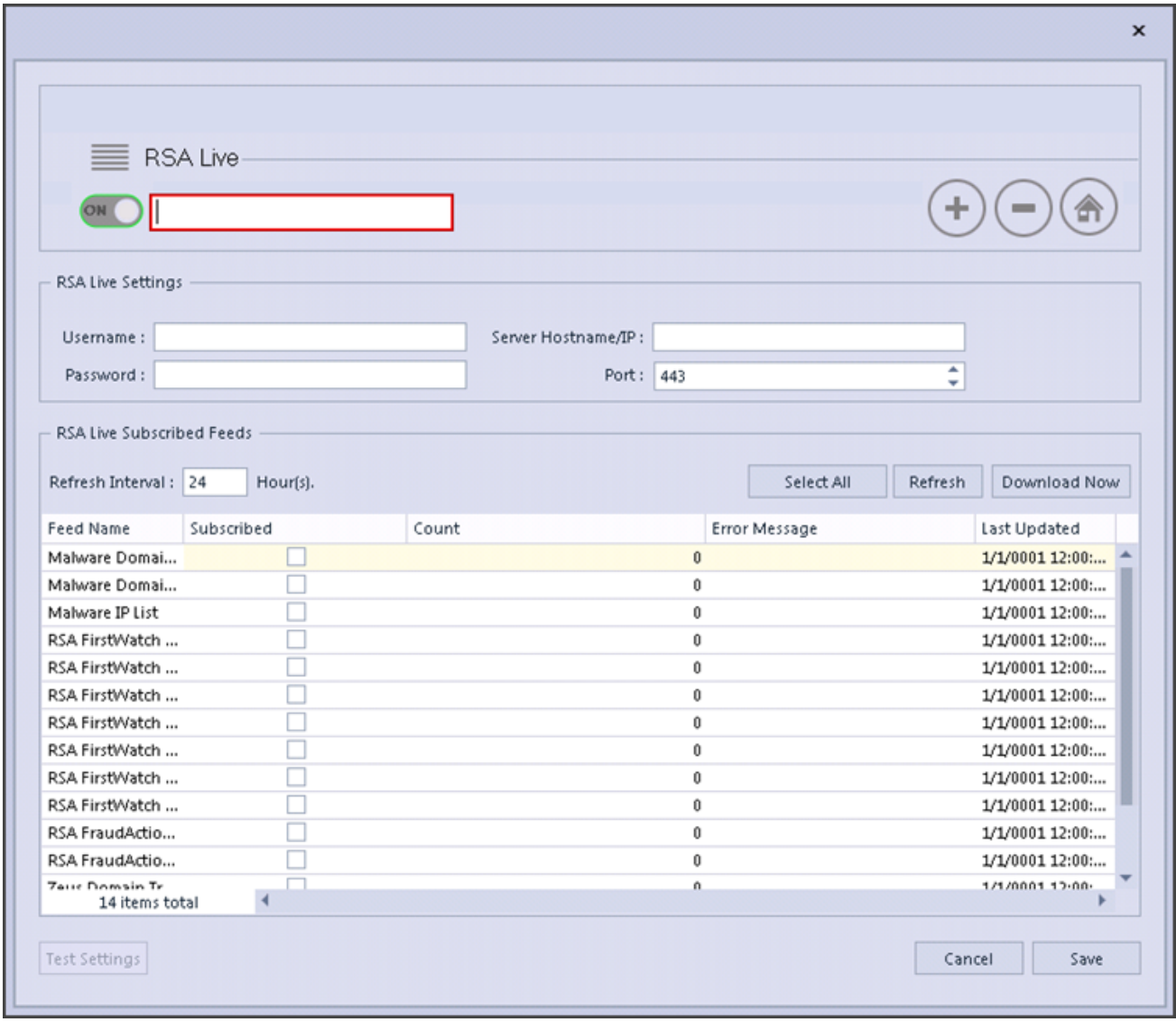
For ECAT version 4.1

1. Create a SQL user with credentials in ECAT:
   a. Open the ECAT user interface and log on using the proper credentials.
   b. Click **Configure** > **Manage Users and Roles**.
   c. In **Security**, right-click in the pane and select **Create a new SQL User**.
   d. Provide the login name and the password.
2. From the menu bar at the top of the page, select **Configure > Monitoring and External Components**.

3. The External Components Configuration window is displayed. Select **RSA Live** and click +.



4. The RSA Live dialog is displayed.



5. Under **RSA Live**, in **On**, type a name to identify this component.
6. In **RSA Live Settings**, do the following.
   a. In **Username** and **Password**, type the credentials to use for accessing this component.
   b. In **Server Hostname/IP**, the default value is `cms.netwitness.com`. Update the field if needed.
   c. In **Port**, the default port number is `443`. Update the field if needed.

7. In **RSA Live Subscribed Feeds**, do the following.
   a. In **Refresh Interval**, enter an appropriate interval. The recommended interval is 24 hours, which means that ECAT connects to RSA Live every 24 hours to update the imported data.
   b. Select the feeds for ECAT to import from RSA Live.
8. Click **Save**.
   The RSA Live component is added to ECAT and the feeds are activated.
9. To validate the connectivity, select the newly added component and then click **Test Settings**.
   If all settings are correct, a Passed message is displayed.

RSA Live Feeds for ECAT 4.0 and later

Feed Name	Description
IDefense Threat Indicators Domains	Verisign iDefense security intelligence services gives information security executives access to accurate and actionable cyber intelligence related to vulnerabilities, malicious code, and global threats 24 hours a day, 7 days a week. Verisignidefense in-depth analysis, insight, and response recommendations help keep businesses and government organizations ahead of new and evolving threats and vulnerabilities.
Malware Domain List	List of domains commonly associated with malware sourced from www.malwaredomainlist.com
Malware Domains	List of domains associates with malware sourced from www.malwaredomains.com
Malware IP List	List of ip addresses commonly associated with malware sourced from www.malwaredomainlist.com

Feed Name	Description
RSA FirstWatch APT Threat Domains	This feed contains domains known to be associated with APTs.
RSA FirstWatch APT Threat IPs	This feed contains IPs known to be associated with APTs.
RSA FirstWatch Command and Control Domains	This feed contains Domains that are known to be associated with malware command and control.
RSA FirstWatch Command and Control IPs	This feed contains IPs that are known to be associated with malware command and control.
RSA FirstWatch Criminal SOCKS node IPs	This feed contains IPs that represent known SOCKS nodes for criminal anonymization services.

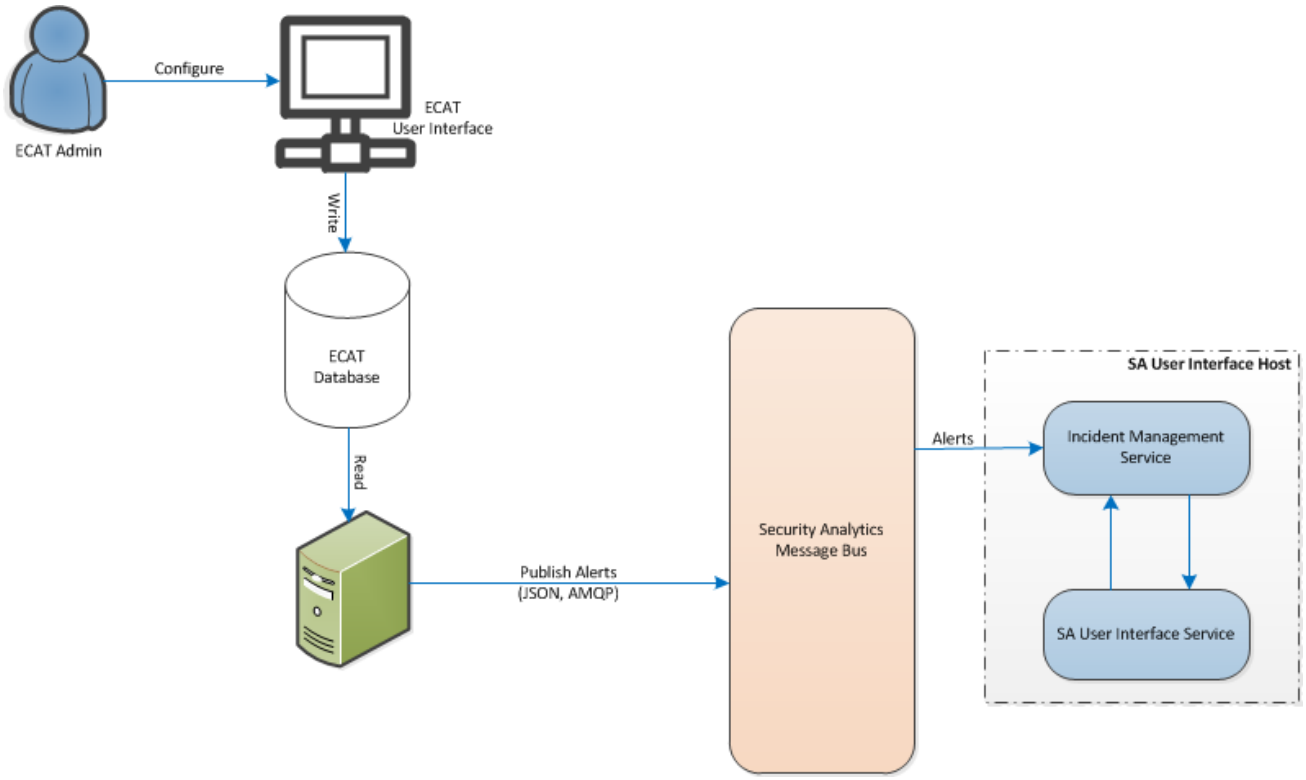
Feed Name	Description
RSA FirstWatch Criminal Socks User IPs	This feed contains IPs that have been observed using criminal anonymization services.
RSA FirstWatch Criminal VPN Entry IPs	This feed contains ips that represent known VPN entry nodes for criminal anonymization services.
RSA FirstWatch Criminal VPN Exit IPs	This feed contains ips that represent known VPN exit nodes for criminal anonymization services.
RSA FirstWatch IP Reputation	This feed contains IP that are known to be compromised.
RSA FraudAction Domains	This feed contains domains from the RSA FraudAction feed.
RSA FraudAction IPs	This feed contains IPs from the RSA FraudAction feed.

Feed Name	Description
Spamhaus DROP List IP Ranges	DROP (Don't Route Or Peer) and EDROP are advisory "drop all traffic" lists, consisting of stolen 'hijacked' netblocks and netblocks controlled entirely by criminals and professional spammers.
SpyEye Domain Tracker	SpyEye domain tracker is a list of spyeye (also known as zbot, prg, wsnpoem, gorhax and kneber) command&control domain names. SpyEye tracker has tracked more than 2,800 malicious spyeye c&c servers. SpyEye is spread mainly through drive-by downloads and phishing schemes.
Tor Exit Nodes	This feed contains IPs that are listed as active exit nodes for the Tor network.
Tor Nodes	This feed contains IPs that are listed as active nodes in the Tor network.

Configure ECAT Alerts via Message Bus

This procedure is required to integrate ECAT with Security Analytics so that the ECAT alerts are picked up by the Incident Management component of Security Analytics and displayed in the **Incident > Alerts** view.

The diagram below represents the flow of ECAT alerts to the Incident management queue of Security Analytics and display of alerts in the **Incident > Alerts** view.



Prerequisites

Ensure that you have the following:

- The Incident Management service is installed and running on Security Analytics 10.4 or later.
- ECAT 4.0 or later is installed and running.

Configure the Incident Management Broker as an External ECAT Component

For ECAT version 4.0

To configure ECAT to send alerts over the message bus to the Security Analytics user interface:

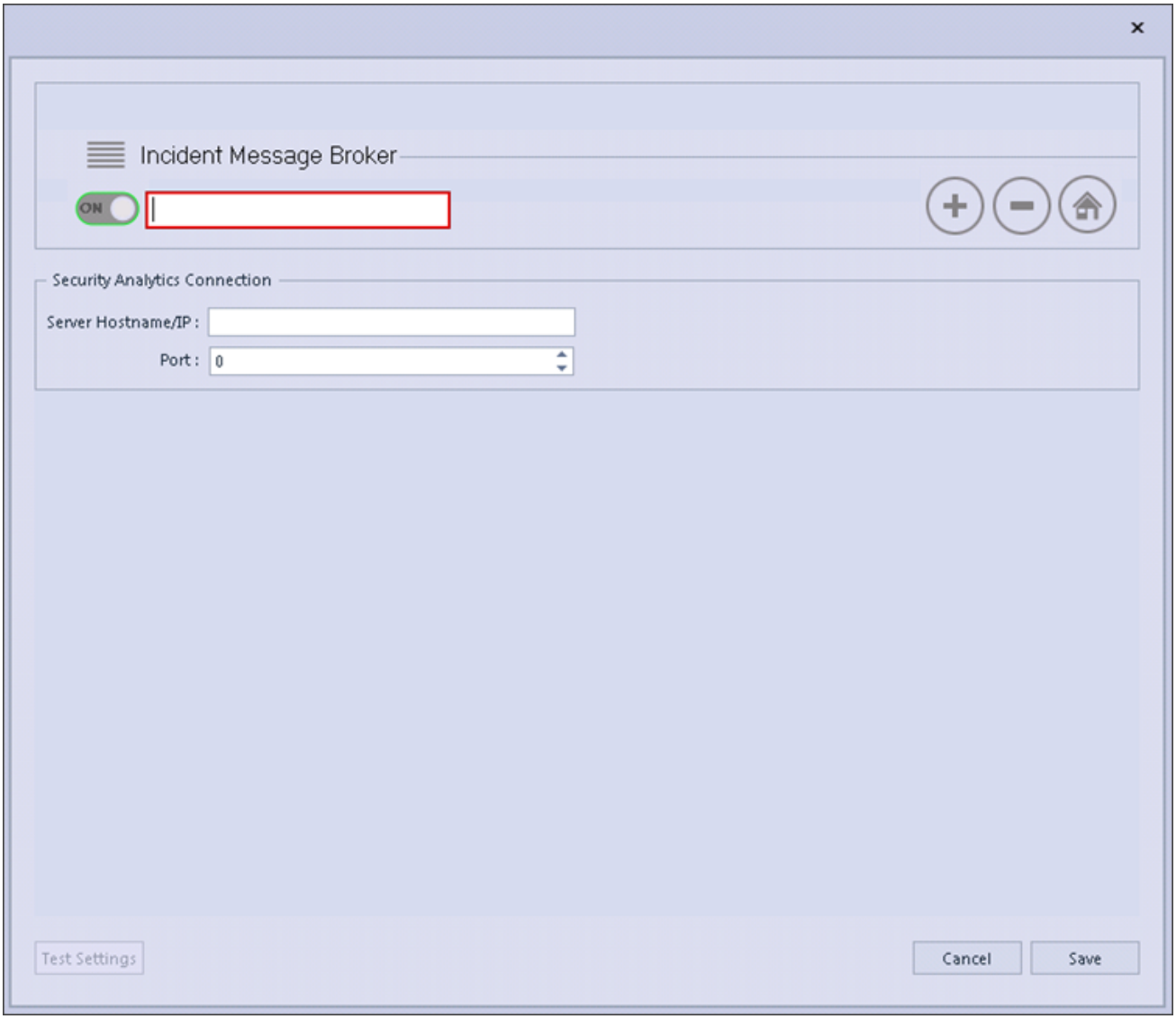
1. Open the ECAT user interface and log in using the proper credentials.
2. From the menu bar, select **Configure > Monitoring and External Components**.
   The Monitoring and External Components dialog is displayed.
3. Right click anywhere on the dialog and select **Add Component**.
   The Add Component dialog box is displayed.
4. Provide the following information:
   - Select IM broker for the Component Type from the drop down options.
   - Type a user name to identify the IM broker.
   - Type the Host DNS or IP address of the IM broker.
   - Type the Port number.
5. Click **Save** and **Close** to close all the dialog boxes.

For ECAT version 4.1

To configure ECAT to send alerts over the message bus to the Security Analytics user interface:

1. Open the ECAT user interface and log in using the proper credentials.
2. From the menu bar, select **Configure > Monitoring and External Components**.
   The External Components Configuration dialog is displayed.

3. In **Incident Message Broker**, click + to add an Incident Message (IM) Broker.
   The Incident Message Broker dialog is displayed.



4. Under **Incident Message Broker**, in **On**, type a name for the message broker.
5. Under **Security Analytics Connection**, do the following.
   a. In **Server Hostname/IP**, type the IP address for the Security Analytics server.
   b. In **Port**, the default port number is 5671. Update the field if needed.
6. Click **Save**.

Configure the ECAT CA Certificate on the Security Analytics Broker

To set up SSL for Incident Management alerts:

1. On the ECAT primary console server, export the ECAT CA certificate to `.cer` format (Base-64 encoded X.509) from the local computer's personal certificate store (without selecting the private key).
2. On the ECAT primary console server (from the computer and location where the ECAT **`makecert`** executable file is located), generate a client certificate for ECAT using the ECAT CA certificate. (You must set the CN name to ecat).
   ```
   makecert -pe -n "CN=ecat" -len 2048 -ss my -sr LocalMachine -a sha1 -sky exchange -eku 1.3.6.1.5.5.7.3.2 -in "EcatCA" -is MY -ir LocalMachine -sp "Microsoft RSA SChannel Cryptographic Provider" -cy end -sy 12 client.cer
   ```
3. On the ECAT primary console server, make a note of the thumbprint of the client certificate generated in step 2. Enter the thumbprint value of the client certificate in the **`IMBrokerClientCertificateThumbprint`** section of the**`ConsoleServer.Exe`** file as shown.
   ```
   <add key="IMBrokerClientCertificateThumbprint" value="?896df0efacf0c976d955d5300ba0073383c83abc"/>
   ```

Note: When you enter the thumbprint value in the value field, be sure to remove the question mark (?), enter the value, and then save the file.

4. On the Security Analytics server, append the content of the ECAT CA certificate file in **`.cer`** format (from step 1) to **`/etc/puppet/modules/rabbitmq/files/truststore.pem`**
5. On the Security Analytics server, do one of the following:
   - Run the puppet agent using the following command: **`puppet agent -t`**
   - Wait 30 minutes for the Security Analytics server to run the agent.
6. On the ECAT primary console server, import the **`/var/lib/puppet/ssl/certs/ca.pem`** file from the Security Analytics server to the Trusted Root Certification authorities store.

This ensures that ECAT, as a client, can trust the Incident Management server certificate.

7. Restart the ECAT server to enable ECAT to send alerts to Security Analytics.

Configure Contextual Data from ECAT via Recurring Feed

This topic provides instructions for configuring use of RSA ECAT data in Security Analytics to provide contextual data from ECAT to Decoder and Log Decoder sessions. This configuration adds contextual meta values in addition to the instant IOC alerts that can be used to build correlations to other meta data in the Security Analytics ecosystem.

Administrators can configure Security Analytics to consume system scan contextual data from ECAT via a Security Analytics Live recurring feed. This integration can enrich the session from a Decoder or Log Decoder with contextual information displayed in Security Analytics Investigation; some examples include the host operating system, MAC address, score, and other data that may not be present in the log or packet data. into sessions from a Decoder or Log Decoder.

Note: Although this feature is targeted for customers with a packet Decoder, a recurring feed can also be implemented in Log Decoders.

Caution: In environments with many ECAT hosts, use of this recurring feed may result in decreased performance on the Security Analytics ingest devices (Decoder and Log Decoder).

Prerequisites

- Version 4.0 or later ECAT Console server and Security Analytics Server Version Version 10.4 and above installed.
- Version 10.4 or later RSA Decoder and Concentrator connected to the Security Analytics Server in the network.

Configuration

To configure this integration:

1. Enable the ECAT Feed for Security Analytics in the ECAT User Interface.
2. Export the ECAT CA Certificate from the eCAT Console server and Import into Security Analytics trust store.
3. Configure the Security Analytics Concentrator service to define which meta keys are indexed.
4. Create a recurring feed in Security Analytics Live.

Enable the ECAT Feed for Security Analytics

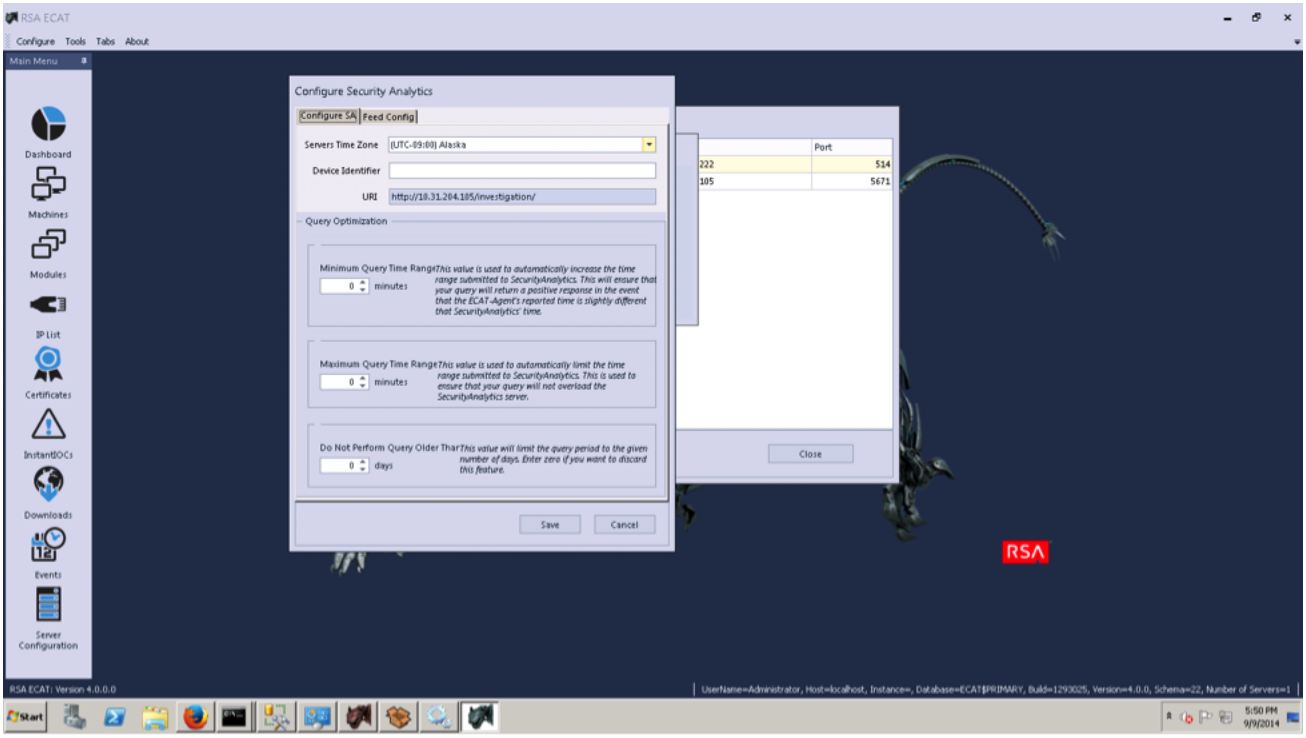
For ECAT version 4.0

1. Open the ECAT user interface and log on using the proper credentials.
2. From the menu bar, select **Configure > Monitoring External Components**.

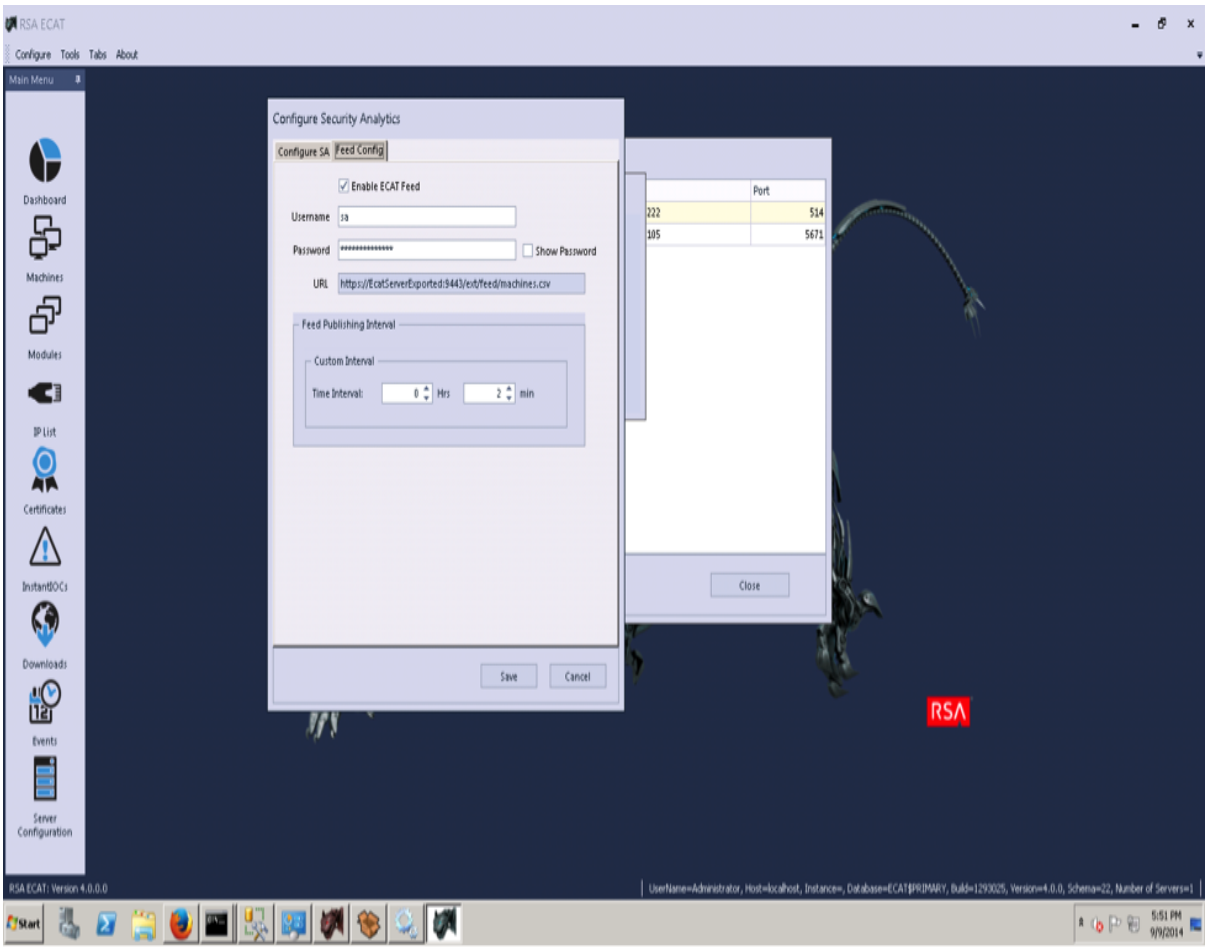
   The Add Components dialog is displayed.

3. Add a Security Analytics component. Enter the **Unique Name**, **Host DNS or IP**, and click **Settings**.

   The Configure Security Analytics dialog is displayed.



4. Enter the **Timezone** and click the **Feed Config** tab.



5. Select **Enable ECAT Feed**, enter the **Username** and **Password**. Configure the **Feed Publishing Interval**. Click **Save**.

   A feed is created.

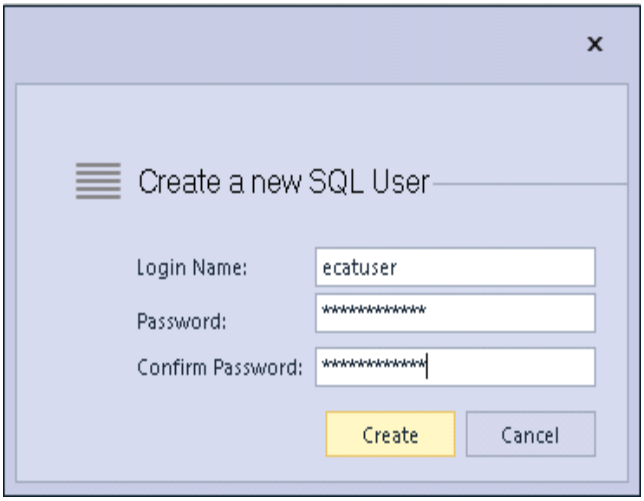
6. Make a note of the URL assigned to the feed, and the username and password. This information is used in Security Analytics.

7. To verify that the feed has been successfully created, open a browser and type in the URL. When prompted, enter the username and password. Check to see if a file named `machines.csv` is downloaded.

For ECAT version 4.1

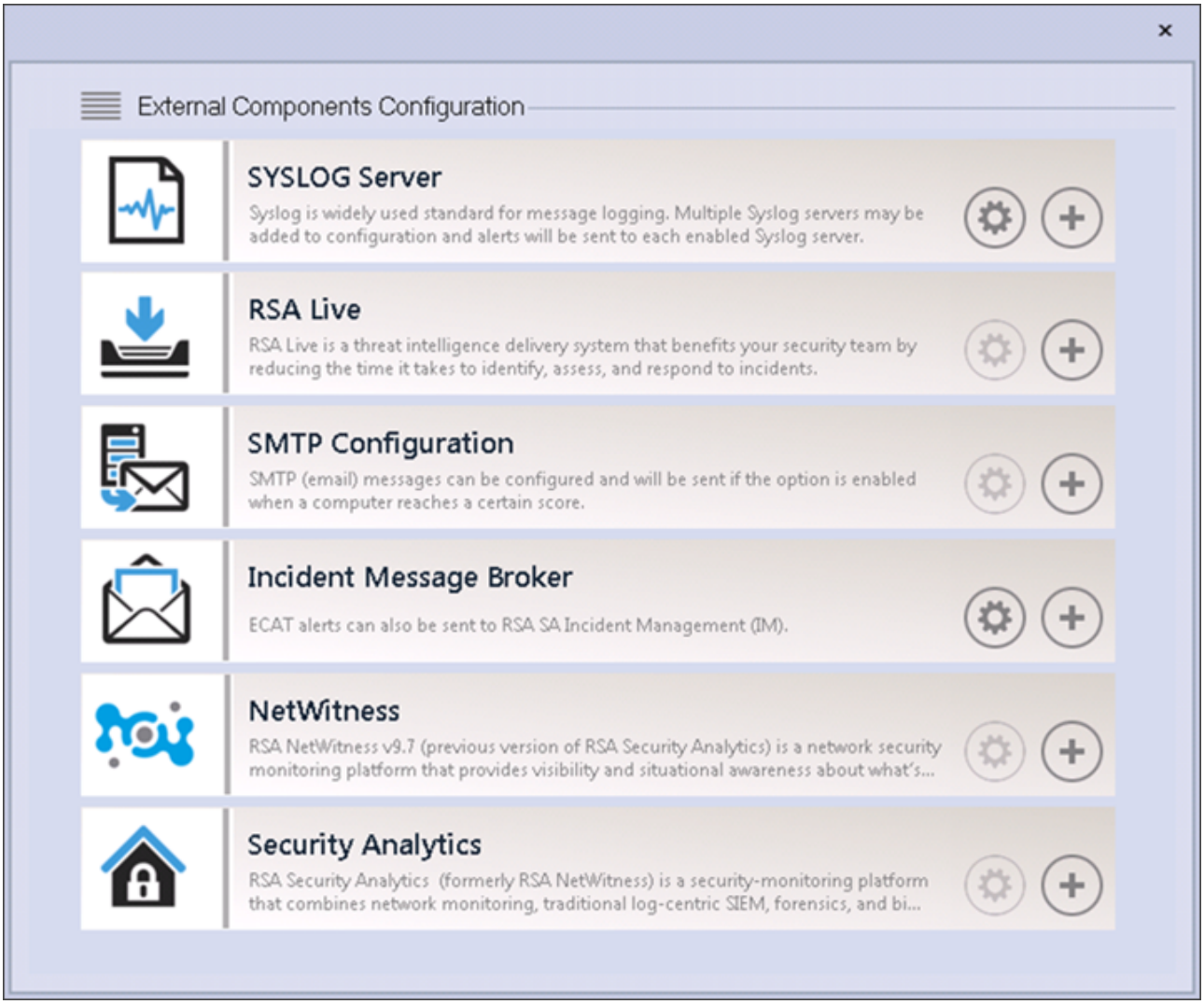
In the ECAT User Interface:

1. Create an SQL user in ECAT:
   a. Open the ECAT user interface and log on using the proper credentials.
   b. Under Security, right-click in the pane and select **create sql user**.
      The Create a new SQL User dialog is displayed.

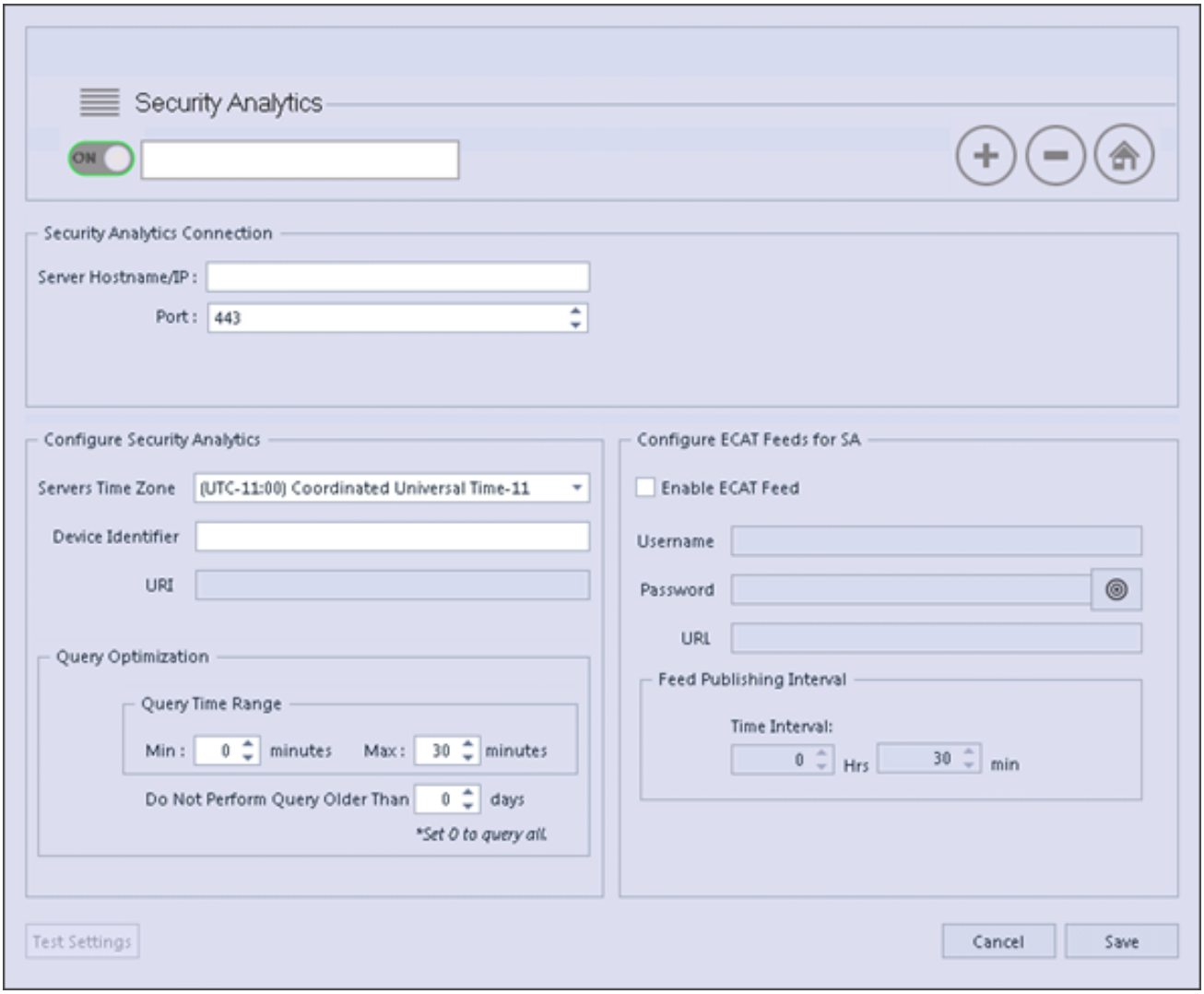


   c. Provide the login name and the password.

2. From the menu bar, select **Configure > Monitoring External Components**.
   The External Components Configuration dialog is displayed.



3. In Security Analytics, click +.
   The Security Analytics dialog is displayed.



4. Under **Security Analytics**, in **On**, type a name to identify the Security Analytics component.
5. Under **Security Analytics Connection**, do the following.
   a. In **Server Hostname/IP**, type the host name or IP address of the Security Analytics server.
   b. In **Port**, the default port number is 443. Update the field if needed.
6. Under **Configure Security Analytics**, do the following:
   a. In **Servers Time Zone**, enter a time zone for the component.
   b. In Device Identifier, type the Security Analytics concentrator device ID.

Note: You can find the Device Identifier in Security Analytics when you look up a Concentrator or Broker in **Investigation > Navigate >*<Concentrator or Broker Name>***. The Device Identifier is the number in the URL after "investigation." For example, in the URL `https://<IP address>investigation/319/navigate/values`, the Device Identifier is **319**.

The **URI** field is populated when you click **Save**.

7. In **Query Optimization**, do the following:
   a. In **Min**, enter the number of minutes for the minimum query time range. This value is used to automatically increase the time range submitted to Security Analytics. This ensures that a query returns a positive response if the ECAT Agent's reported time is slightly different than Security Analytic's time.
   b. In **Max**, enter the number of minutes to limit the time range. This value is used to automatically limit the time range submitted to Security Analytics, so that a query does not overload the Security Analytics server.
   c. In **Do Not Perform Query Older Than**, enter a number of days to limit the query period. Enter **0** if you want to discard this feature.
8. In **Configure ECAT Feeds for SA**, do the following:
   a. Select **Enable ECAT Feed**.
   b. Enter the SQL **Username** and **Password** (configured in step 1) to access the location of the feed.
      The **URL** field is populated when you click **Save**.
   c. Enter the time interval for the frequency at which feeds are published.
9. Click **Save**.
   A feed is created.

Export the ECAT SSL Certificate

Note: This procedure works only for Security Analytics 10.5 and above because Java 8 support was added for 10.5. If you are using an earlier version of Security Analytics, refer to the applicable version of this guide.

To export the ECAT CA certificate from the ECAT Console server and copy it to the Security Analytics host:

1. Log on to the ECAT Console
2. Open **MMC**.

3. Add a certificate snap-in for **Computer account**.
4. Export the certificate named **EcatCA**.
   a. Export without private key.
   b. Export in DER encoded binary X.509 (.CER) format.
   c. Name it **EcatCA.cer**.
5. Copy the ECAT CA certificate to the Security Analytics host:
   scp EcatCA.cer root@<sa-machine>:.
6. To import the ECAT CA certificate into the Security Analytics Trusted store, enter the following commands:
   JDK=/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.65-0.b17.el6_7.x86_64/jre/
   $JDK/bin/keytool -import -v -trustcacerts -alias ecatca -file ~/EcatCA.cer -keystore $JDK/lib/security/cacerts -storepass changeit
   When prompted for certificate update confirmation, enter **Yes**.
7. On the Security Analytics host, edit **/etc/hosts** to map the IP address of the ECAT Console server to the name **ecatserverexported** by adding the following line to the file:
   <ip-address-ecat-cs> ecatserverexported
8. To restart Security Analytics, enter the following commands:
   stop jettysrv
   start jettysrv

Configure the Security Analytics Concentrator Service

1. Log on to Security Analytics and navigate to **Administration > Services**.
2. Select a concentrator from the list, and select **View > Config.**
3. Select the **Files** tab, and from the **Files to Edit** pull-down menu, select **index-concentrator-custom.xml**.
4. Add the following ECAT meta keys to the file and click **Apply**. Make sure that this file contains the XML sections already; if the lines are not included, add them. The following lines are examples; make sure the values match your configuration and the column names you included in the feed definition, where:
   description is the name of the meta key you want to display in Security Analytics Investigation.
   level is "IndexValues"
   name matches the column name of the CSV file that Security Analytics uses while defining

the recurring feed (see the table in *Configure the Recuring Custom Feed Task in Security Analytics* below).

```
<key description="Gateway" format="Text" level="IndexValues" name="gateway" valueMax="250000" defaultAction="Open"/><key description="Risk Number" format="Float64" level="IndexValues" name="risk.num" valueMax="250000" defaultAction="Open"/><key description="Strans Addr" format="Text" level="IndexValues" name="stransaddr" valueMax="250000" defaultAction="Open"/>
```

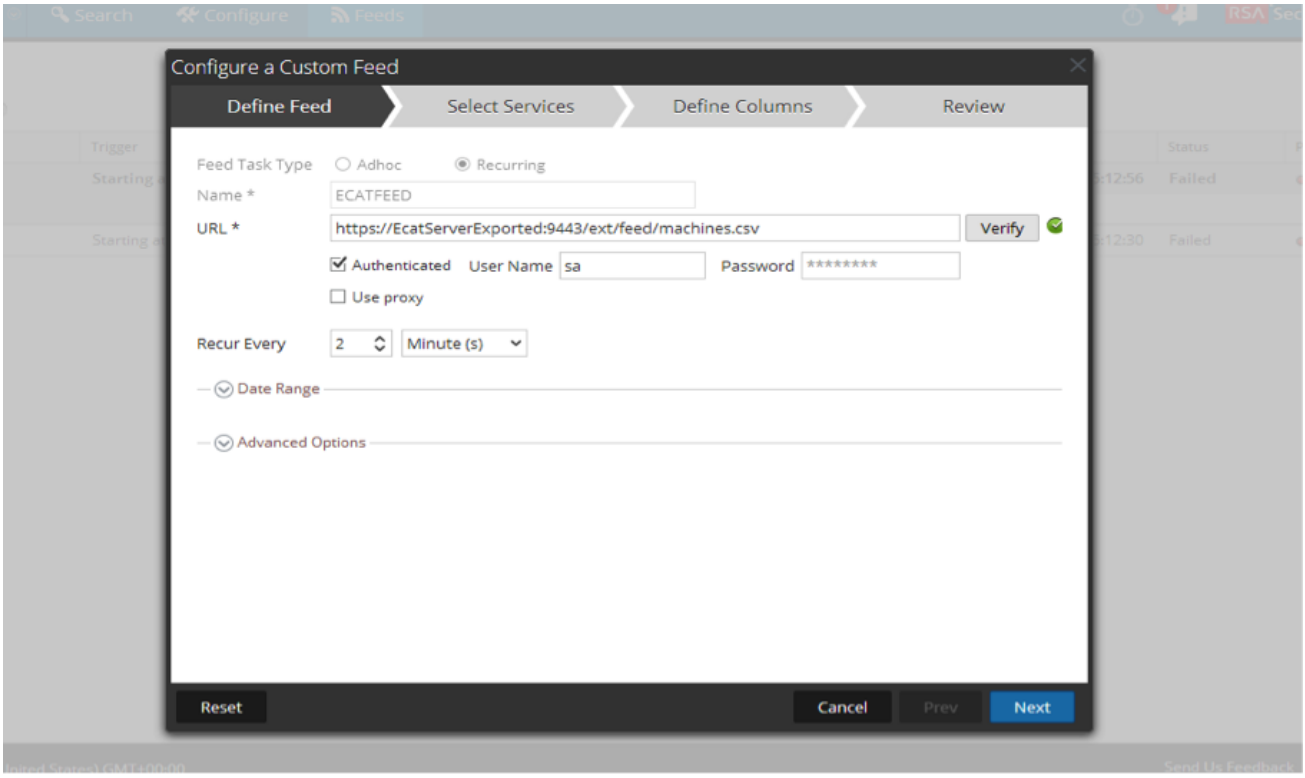
5. Restart the Concentrator to activate the custom key updates.

Configure the Recurring Custom Feed Task in Security Analytics

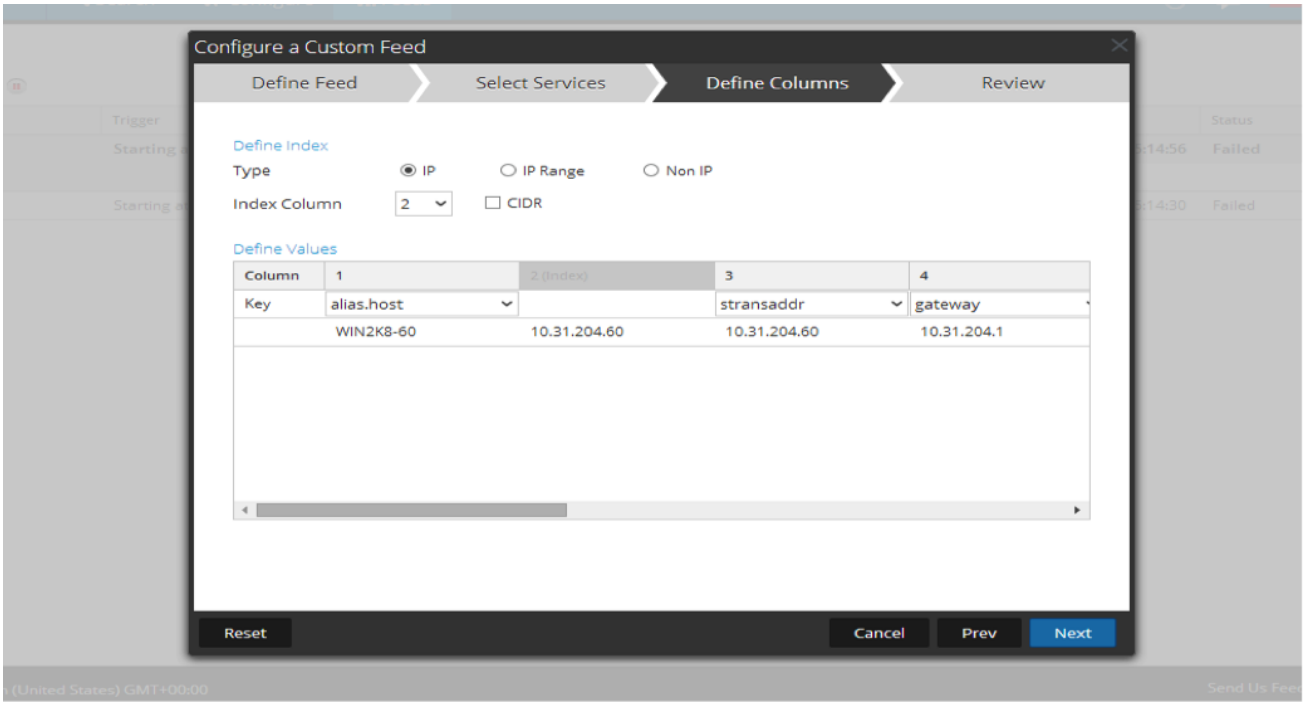
To configure the recurring feed task in Security Analytics:

1. Log on to Security Analytics and navigate to **Live > Feeds**.
2. Select **Custom Feed > Next**.
3. Do the following:
   a. Select **Recurring**.
   b. Enter a **Name**, for example: **EcatFeed**.
   c. Enter the URL with the hostname of the Windows server on which ECAT is installed:
      - For RSA ECAT version 4.0, use the URL **`https://<EcatServerHostname>:9443/ext/feed/machines.csv`**.
      - For RSA ECAT version 4.1, use the URL **`https://<EcatServerExported>:9443/api/v2/feed/machines.csv`**.
4. Enable the checkbox **Authenticated** and enter the username and password as noted in *Enable the ECAT Feed* above.
5. Select **Verify** to check that Security Analytics can reach the web resource.

6. Define the schedule. Click **Next**.



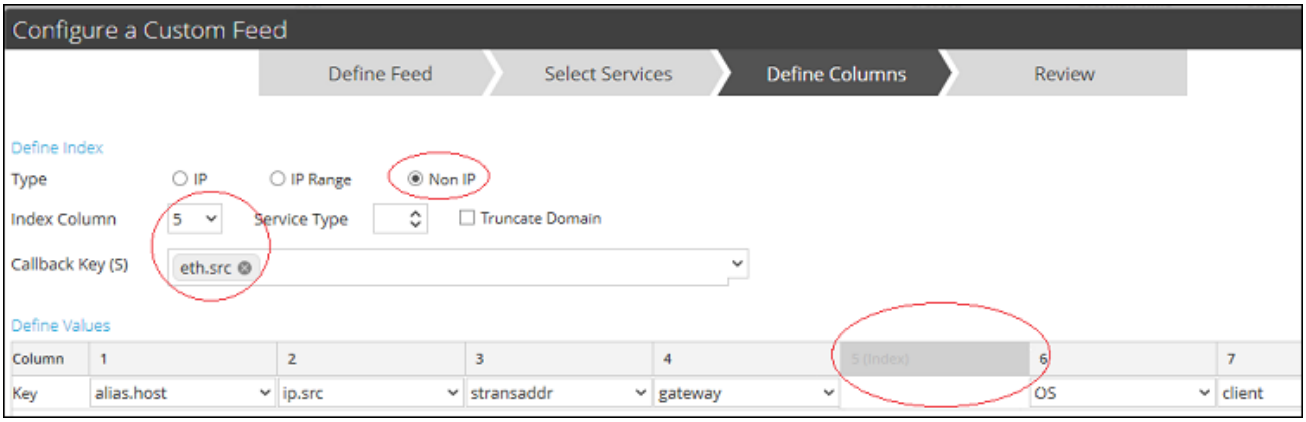
7. In the **Select Services** tab, select the Decoder or groups to consume the feed. Click **Next**.
8. In the **Define Columns** tab, enter the column names as shown in the table below and save the feed.



The following table shows the columns in the CSV file for the ECAT feed.

Column	Name	Description	Column Name in Security Analytics (Meta Key Name)
1	MachineName	Host name of the Windows agent	alias.host
2	LocalIp	IPv4 address	index
3	RemoteIp	Far end IP as seen by the router	stransaddr
4	GatewayIp	IP of the gateway	gateway
5	MacAddress	MAC address	eth.src
6	OperatingSystem	Operating system used by the Windows Agent	OS
7	AgentID	Agent ID of the host (unique ID assigned to the agent)	cllient
8	ConnectionUTCTime	Last time when the agent connected to ECAT server	ecat.ctime
9	Source Domain	Domain	domain.src
10	ScanUTC time	Last time when the agent was scanned	ecat.stime
11	Machine Score	Score of the agent indicating the suspicious level	risk.num

Note: In the table, the recommended index setting is LocalIp. However, if the LocalIp for ECAT Agent PC is allocated by a DHCP Server and the DHCP lease has expired, and if the IP is then re-allocated to another PC, the metadata created by the feed will be incorrect. To avoid this risk, use the machine name or the Mac address instead of the localIP address as the Feed's index. For example, to use a Mac address, you could enter the values as shown in the following figure.



Result

When viewing feed data in Security Analytics, upon match of the indexed value (ip.src), meta data is populated in Investigation, Reporting and Alerting Interfaces.

Troubleshooting

This section suggests how to resolve problems you may encounter when working with recurring feeds.

Known Issues	Solutions
With ECAT 4.1.0.2 and ECAT 4.1.1, ECAT feed integration does not work for Security Analytics.	You must use ECAT 4.1.1.1 for the feed to work.

Configure ECAT Alerts via Syslog into a Log Decoder

This topic provides instructions for configuring the use of RSA ECAT data in Security Analytics to provide ECAT alerts via Syslog into Log Decoder sessions. This generates meta data that is used by Security Analytics Investigation, Alerts, and Reporting Engine.

For Security Analytics networks that are consuming logs, this integration of ECAT with Security Analytics pushes ECAT events to the Log Decoder via common event format (CEF) syslog messages and generates meta data that is used by Security Analytics Investigation, Alerts, and Reporting Engine. The use case for this integration is SIEM Integration to allow centralized event management, correlation of ECAT events with other Log Decoder data, Security Analytics reporting on ECAT events, and Security Analytics alerting of ECAT events.

Prerequisites

The following are required for this integration:

- Version 4.0 or later ECAT UI
- Security Analytics Server Version 10.4 or above is installed.
- Version 10.4 or later RSA Log Decoder and Concentrator connected to the Security Analytics Server in the network.
- Port 514 open from ECAT server to Log Decoder in the firewall.

Procedure

Perform the following steps to configure this integration:

1. Deploy the required parser (CEF or ECAT) to the Log Decoder as described in the **Manage Live Resources** topic in *Live Services Management*. After you deploy the parser, make sure the parser is enabled. For more information, See **Services Config View - General Tab** topic in *Decoder and Log Decoder Configuration Guide*.

Note: Use only use one of these parsers. When the CEF parser is deployed, it supersedes the ECAT parser, and all CEF messages into Security Analytics are processed by the CEF parser. Enabling both parsers is an unnecessary burden on performance.

2. Configure ECAT to send syslog output to Security Analytics and generate eCAT alerts to the Log Decoder.

3. (Optional) Edit the table mapping in `table-map-custom.xml` and the `index-concentrator-custom.xml` to add fields based on user preferences for metadata to be mapped to Security Analytics.

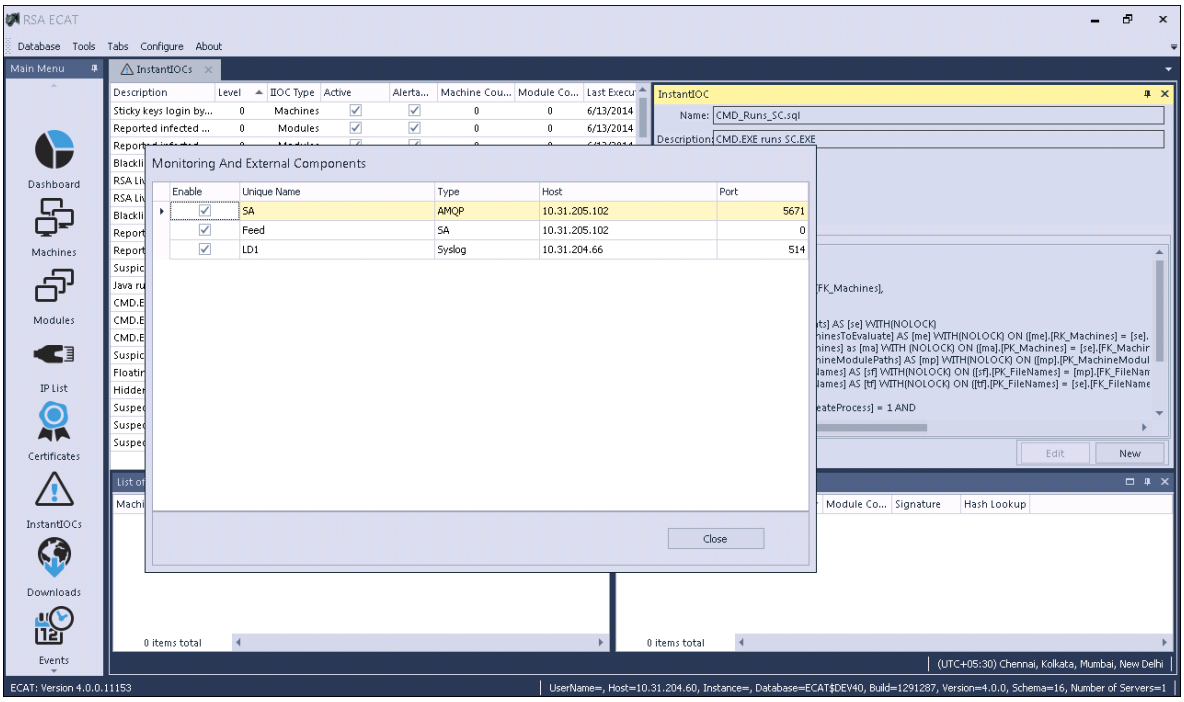
Configure ECAT to Send Syslog Output to Security Analytics

To add the Log Decoder as a Syslog external component and generate ECAT alerts to the Log Decoder:

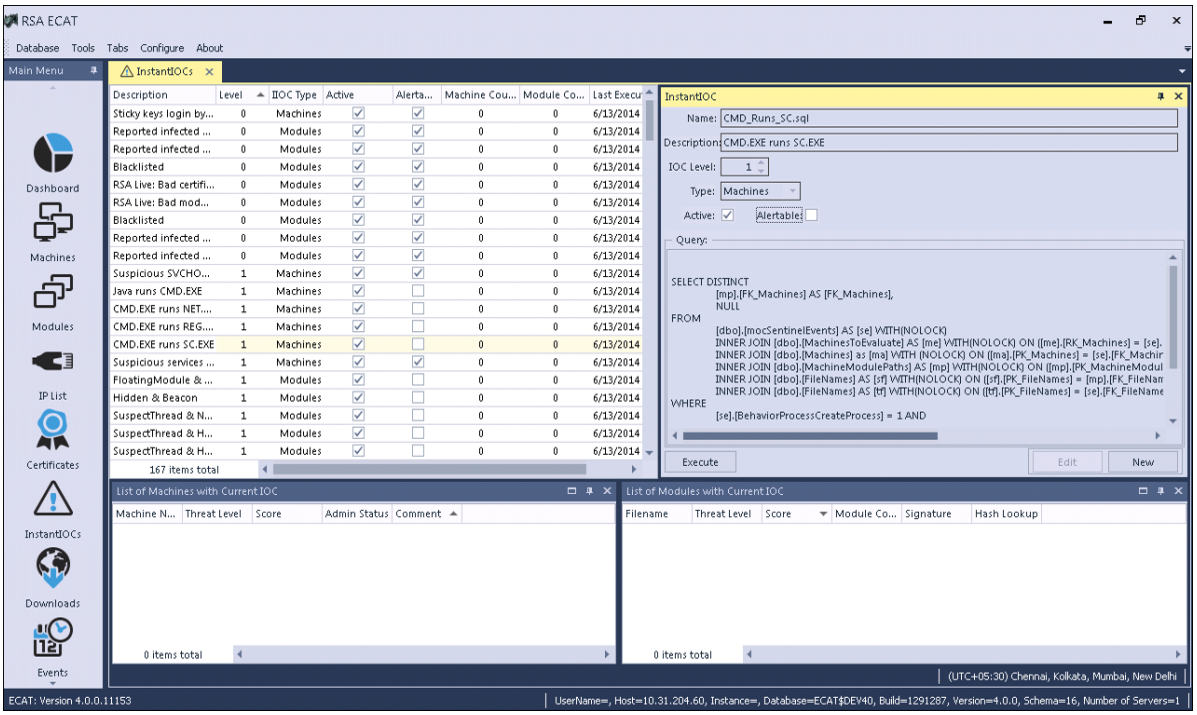
For ECAT version 4.0

1. Open the ECAT user interface and log on using the proper credentials.
2. From the menu bar select **Configure > Monitoring and External Components**.
3. Right-click in the dialog box, and then select **Add Component.** In the dialog box, complete the fields required to enable Syslog messaging:

   Component Type = Syslog
   Unique Name = A descriptive name for the Log Decoder
   IP = The IP address of the RSA Log Decoder
   Port = 514
4. Click **Settings.**
5. In the **Configure Syslog** dialog box, select **UDP** or **TCP** as appropriate for your syslog serverfor the transport protocol.
6. Click **Save** twice, to close the dialog boxes.
7. Click the **Enable** check box to enable the component.
8. Click **Close** to finish.



9. Click **Instant IOCs** and change the settings to make them alertable.



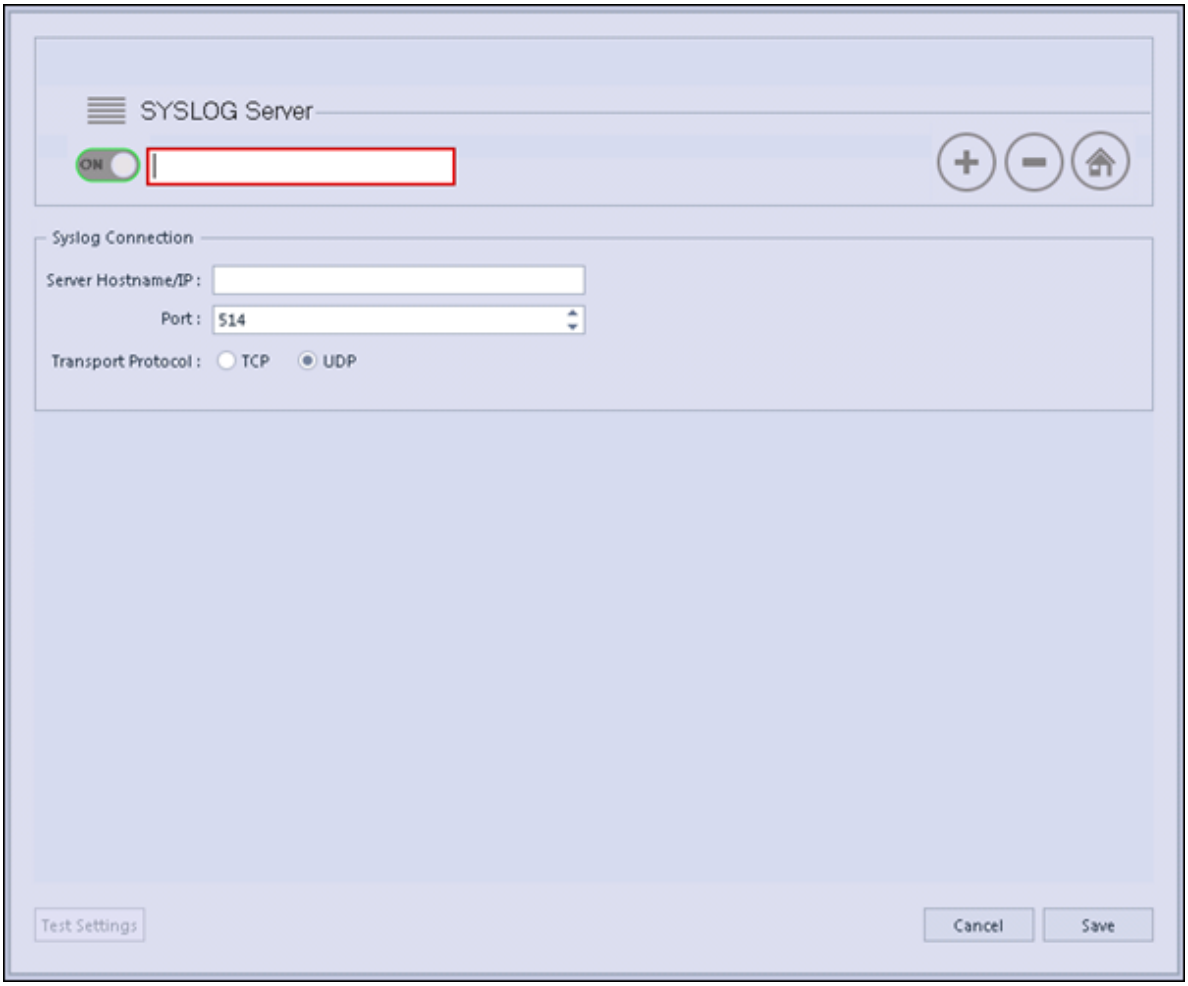
When the instant IOCs are triggered, Syslog alerts from the ECAT server are sent to the Log Decoder. Log Decoder alerts are then aggregated to the Concentrator. These events are injected into the Concentrator as metadata.

For ECAT version 4.1

1. Open the ECAT user interface and log on using the proper credentials.
2. From the menu bar select **Configure > Monitoring and External Components**.

   The External Components Configuration dialog is displayed.
3. In **SYSLOG Server**, click +.

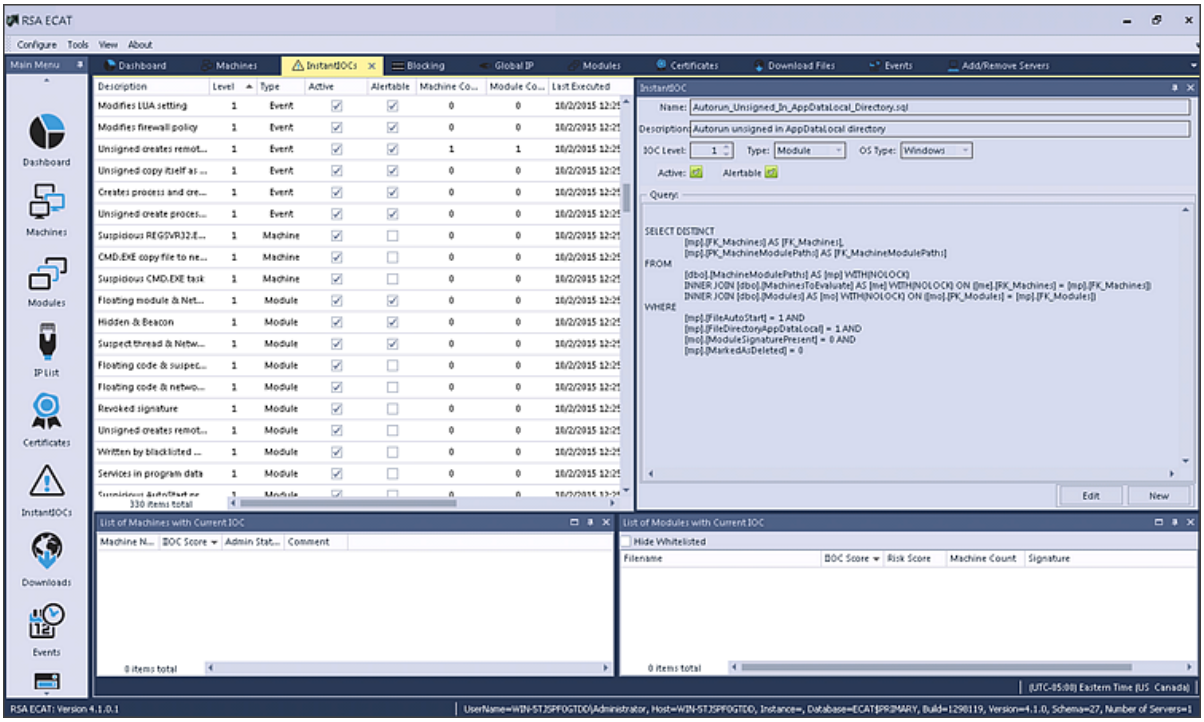
   The SYSLOG Server dialog is displayed.



4. Complete the fields required to enable Syslog messaging:

   On = A descriptive name for the Log Decoder
   Server Hostname/IP = The hostname DNS orIP address of the RSA Log Decoder
   Port = 514
   Transport Protocol = Select **UDP** or **TCP** as appropriate for your Syslogserverfor the transport protocol.
5. Click **Save**.

6. Click **Instant IOCs** and change the settings to make them alertable.



When the instant IOCs are triggered, Syslog alerts from the ECAT server are sent to the Log Decoder. Log Decoder alerts are then aggregated to the Concentrator. These events are injected into the Concentrator as metadata.

Edit the Table Mapping in table-map-custom.xml

In the default RSA table-map.xml provided by RSA, the meta keys in the table-map.xml file are set to `Transient`. In order to view the meta keys in Investigation, the keys must be set to `None`. To make changes to the mapping, you must add the entries to the `table-map-custom.xml`on the Log Decoder.

This is the list of meta keys in `table-map.xml`.

ECAT Fields	Security Analytics Mapping	Transient in Security Analytics
agentid	client	No
CEF Header Hostname Field	alias.host	No

ECAT Fields	Security Analytics Mapping	Transient in Security Analytics
CEF Header Product Version	version	Yes
CEF Header Product Name	Product	Yes
CEF Header Severity	severity	Yes
CEF Header Signature ID	event.type	No
CEF Header Signature Name	event.desc	No
destinationDnsDomain	ddomain	Yes
deviceDnsDomain	domain	Yes
dhost	host.dst	No
dst	ip.dst	No
end	endtime	Yes
fileHash	checksum	Yes
fname	filename	No
fsize	filename.size	Yes
gatewayip	gateway	Yes
instantIOCLevel	threat.desc	No
instantIOCName	threat.category	No
machineOU	dn	Yes

ECAT Fields	Security Analytics Mapping	Transient in Security Analytics
machineScore	risk.num	No
md5sum	checksum	Yes
os	OS	Yes
port	ip.dstport	No
protocol	protocol	Yes
Raw Message	msg	Yes
remoteip	stransaddr	Yes
rt	alias.host	No
sha256sum	checksum	Yes
shost	host.src	No
smac	eth.src	Yes
src	ip.src	No
start	starttime	Yes
suser	user.dst	No
timezone	timezone	Yes
totalreceived	rbytes	Yes
totalsent	bytes.src	No
useragent	user.agent	Yes
userOU	org	Yes

These seven keys are not in `table-map.xml`; to use these keys in Security Analytics you need to add them to `table-map-custom.xml`, and set the flags to `None`.

ECAT Fields	Security Analytics Mapping	Transient in Security Analytics
moduleScore	cs.modulescore	Yes
moduleSignature	cs.modulesign	Yes
Target module	cs.targetmodule	Yes
YARA result	cs.yararesult	Yes
Source module	cs.sourcemodule	Yes
OPSWATResult	cs.opswatresult	Yes
ReputationResult	cs.represult	Yes

Note: Get the latest version of the enVision configuration file from RSA Live.

Here are the entries to be added to the table-map-custom.xml if required.

```
<mapping envisionName="cs_represult" nwName="cs.represult" flags="None"
envisionDisplayName="ReputationResult"/>
 <mapping envisionName="cs_modulescore" nwName="cs.modulescore" format="Int32"
flags="None" envisionDisplayName="ModuleScore"/>
 <mapping envisionName="cs_modulesign" nwName="cs.modulesign" flags="None"
envisionDisplayName="ModuleSignature"/>
 <mapping envisionName="cs_opswatresult" nwName="cs.opswatresult" flags="None"
envisionDisplayName="OpswatResult"/>
 <mapping envisionName="cs_sourcemodule" nwName="cs.sourcemodule" flags="None"
envisionDisplayName="SourceModule"/>
 <mapping envisionName="cs_targetmodule" nwName="cs.targetmodule" flags="None"
envisionDisplayName="TargetModule"/>
 <mapping envisionName="cs_yararesult" nwName="cs.yararesult" flags="None"
envisionDisplayName="YaraResult"/>
```

Note: Restart the Log Decoder or reload the log parsers for the changes to take effect.

Configure the Security Analytics Concentrator Service

1. Log on to Security Analytics and navigate to **Administration > Services**.
2. Select a concentrator from the list, and select **View > Config.**
3. Select the **Files** tab, and from the **Files to Edit** pull-down menu, select **index-concentrator-custom.xml**.

4. Add the ECAT meta keys to the file and click **Apply**. Make sure that this file contains the XML sections already; if the lines are not included, add them.
5. Restart the Concentrator.
6. To add the Concentrator as a data source in the Reporting Engine, in the Administration > Services view, select the Reporting Engine and **RE > View> Config > Sources.**
   ECAT meta is populated in Reporting Engine, and you can run reports by selecting the appropriate meta keys.

Example

Note: The following lines are examples; make sure the values match your configuration and the column names you included in the feed definition, where:
description is the name of the meta key you want to display in Security Analytics Investigation.
level is "IndexValues"
name is the ECAT meta key name from the table below

```
<language>
<key description="Product" format="Text" level="IndexValues" name="product"
valueMax="250000" defaultAction="Open"/>
 <key description="Severity" format="Text" level="IndexValues" name="severity"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Dns Domain" format="Text" level="IndexValues"
name="ddomain" valueMax="250000" defaultAction="Open"/>
 <key description="Domain" format="Text" level="IndexValues" name="domain"
valueMax="250000" defaultAction="Open"/>
 <key description="Destination Host" format="Text" level="IndexValues"
name="host.dst" valueMax="250000" defaultAction="Open"/>
 <key description="End Time" format="TimeT" level="IndexValues" name="endtime"
valueMax="250000" defaultAction="Open"/>
 <key description="Checksum" format="Text" level="IndexValues" name="checksum"
valueMax="250000" defaultAction="Open"/>
 <key description="Filename Size" format="Int64" level="IndexValues"
name="filename.size" valueMax="250000" defaultAction="Open"/>
 <key description="Gateway" format="Text" level="IndexValues" name="gateway"
valueMax="250000" defaultAction="Open"/>
 <key description="Distinguished Name" format="Text" level="IndexValues" name="dn"
valueMax="250000" defaultAction="Open"/>
 <key description="Risk Number" format="Float64" level="IndexValues"
name="risk.num" valueMax="250000" defaultAction="Open"/>
 <key description="ReputationResult" format="Text" level="IndexValues"
name="cs.represult" valueMax="250000" defaultAction="Open"/>
 <key description="Module Score" format="Text" level="IndexValues"
name="cs.modulescore" valueMax="250000" defaultAction="Open"/>
 <key description="Module Sign" format="Text" level="IndexValues"
name="cs.modulesign" valueMax="250000" defaultAction="Open"/>
 <key description="opswat result" format="Text" level="IndexValues"
```

```
name="cs.opswatresult" valueMax="250000" defaultAction="Open"/>
 <key description="source module" format="Text" level="IndexValues"
name="cs.sourcemodule" valueMax="250000" defaultAction="Open"/>
 <key description="Target Module" format="Text" level="IndexValues"
name="cs.targetmodule" valueMax="250000" defaultAction="Open"/>
 <key description="yara result" format="Text" level="IndexValues"
name="cs.yararesult" valueMax="250000" defaultAction="Open"/>
 <key description="Protocol" format="Text" level="IndexValues" name="protocol"
valueMax="250000" defaultAction="Open"/>
 <key description="Event Time" format="TimeT" level="IndexValues"
name="event.time" valueMax="250000" defaultAction="Open"/>
 <key description="Source Host" format="Text" level="IndexValues" name="host.src"
valueMax="250000" defaultAction="Open"/>
 <key description="Start Time" format="TimeT" level="IndexValues" name="starttime"
valueMax="250000" defaultAction="Open"/>
 <key description="Timezone" format="Text" level="IndexValues" name="timezone"
valueMax="250000" defaultAction="Open"/>
 <key description="Received Bytes" format="UInt64" level="IndexValues"
name="rbytes" valueMax="250000" defaultAction="Open"/>
 <key description="Agent User" format="Text" level="IndexValues" name="user.agent"
valueMax="250000" defaultAction="Open"/>
 <key description="Source Bytes" format="UInt64" level="IndexValues"
name="bytes.src" valueMax="250000" defaultAction="Open"/>
 <key description="Strans Address" format="Text" level="IndexValues"
name="stransaddr" valueMax="250000" defaultAction="Open"/>
 </language>
```

Result

Analysts can:

- Create Security Analytics alerts based on ECAT events by configuring ECAT events as an enrichment source.
- Create ESA rules using ECAT meta as described in the **Add Rules to the Rules Library** topic in *Alerting Using ESA*.
- Report on ECAT events using ECAT meta as described in the **Working with Reporting Rules** topic in *Reporting*.
- View ECAT alerts in Incident Management as described in the **Alerts View** topic in *Incident Management*.
- View ECAT meta keys in Investigation along with standard SA core meta keys as described in the **Conduct an Investigation** topic in *Investigation and Malware Analysis*.