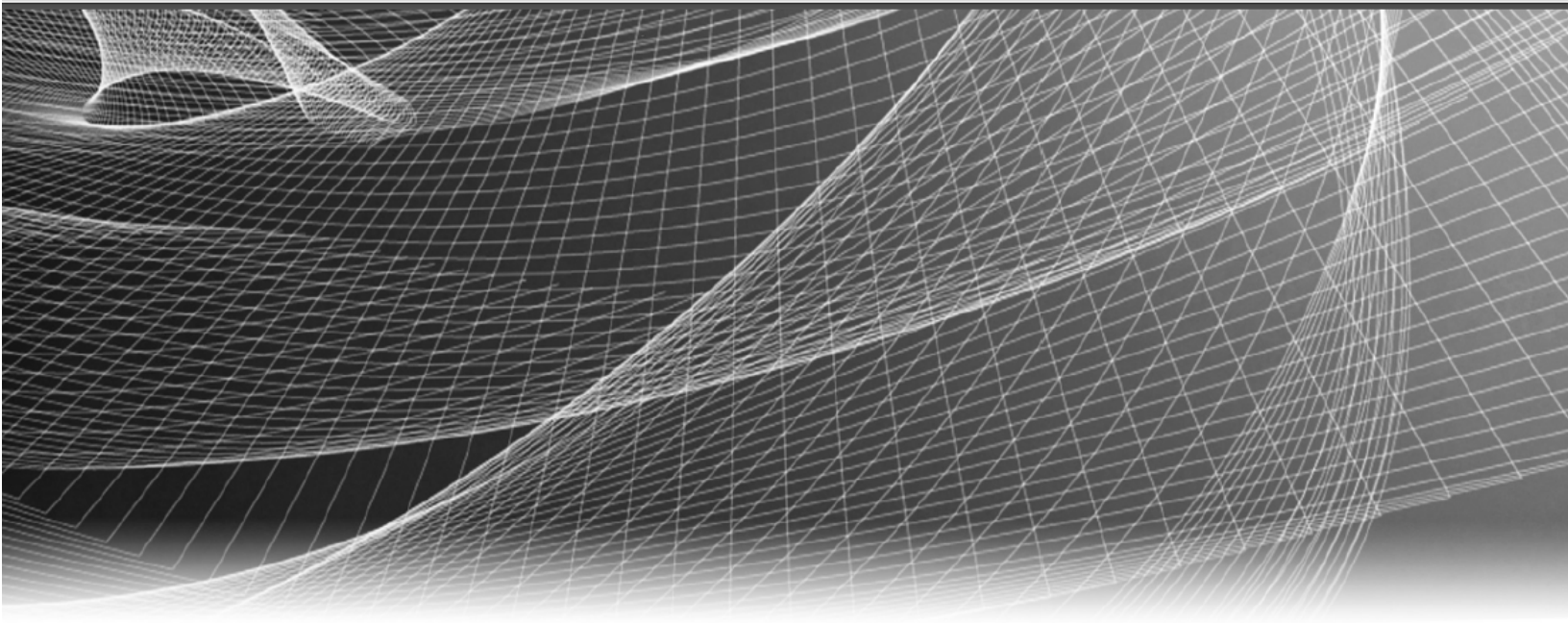


RSA Security Analytics

Context Hub Configuration 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.

October 2017

Contents

Context Hub: Service Overview

Context Hub is a new service in RSA Security Analytics that provides enrichment lookup capability in the Investigation views. This service provides an automated inline enrichment indication as well as an on-demand enrichment lookup capability. Analysts can use the additional insight pulled in by the Context Hub as contextual information and intelligence during investigation. The sources for enrichment data include Incident Management, custom lists, ECAT, and Live Connect.

The Context Hub service:

- Is hosted on Event Stream Analysis (ESA).
- By default supports enrichment lookups for these meta types: IP address, Users, Domains, MAC address, File name, File hash, and Hosts

Purpose

The Context Hub service brings together contextual information from several data sources into Investigation so that analysts can make better decisions during their investigations. Seeing the meta values and contextual information in a single interface helps analysts in prioritizing and identifying the focus areas. For example, recently generated incidents and alerts from Incident Management involving a given meta value will be displayed when the analyst performs context lookup operation for that meta value.

Custom lists such as blacklists, whitelists, or watchlists can be created by analysts. These custom lists may be populated with items either by importing CSV files or by adding meta values by using the option **Add/Remove from List** in Investigation views. The custom lists automatically become data sources for in-line indication of meta values as well as on-demand enrichment lookups.

The lists can also provide better interaction between analysts. For example, a Tier 2 analyst can indicate suspicious items and then Tier 1 analysts can use this knowledge to confirm incidents or create incidents as required.

With context information from ECAT, analysts can get endpoint module and machine indicators.

Workflow for Administrators

In the Services Config view of Context Hub service, an administrator can configure data sources for Context Hub Service. For more information, see Step 2. Configure Data Sources for Context Hub.

An administrator can configure Context Lookups for custom meta keys if required. Also, an administrator can import lists or export lists that can be used by the analyst.

Workflow for Analysts

In the Investigation > Navigate view, meta values having contextual information are highlighted with a gray background. Also, there are inline indicators for the highlighted meta values, which show the sources where the contextual information is available.

Note: Not all highlighted meta values will have context lookup information. This is because the contextual information in the data source might have changed from the time it was marked available.

If the meta values do not have any context indicators, the analyst can initiate an on-demand query to check if context information might be available. To do so, analysts can right-click any meta value that supports context lookup and then choose **Context Lookup** menu option.

The Context Lookup option is also supported in the Investigation > Events view. But inline indicators are not available in this view. So you must initiate an on-demand lookup against the meta values.

After you choose the Context Lookup right-click menu option, a Context Lookup panel opens in the right side of the Investigation views. The panel displays the contextual information from the configured sources relevant to the meta values. If you want additional information on the context, click the corresponding links on the lookup results that appear in the Context Lookup panel. For more information, see the **View Additional Context for a Data Point** topic in the *Investigation and Malware Analysis Guide*.

Analysts can add or remove a meta value to a new or existing list with a right-click on the same meta value and then select **Add/Remove from List** option.

User Roles and Permissions

Analysts using Security Analytics Investigation need to have the appropriate permissions to perform context lookup and use custom lists.

Two new permissions `Context Lookup` and `Manage List from Investigation` are added for Investigation in Security Analytics 10.6. These permissions are added to Analyst, SOC Managers, and Malware Analysts roles by default. However, when upgrading to Security Analytics 10.6 from older versions, an administrator must configure these permissions. For more information about Roles and Permissions, see the topics **Role Permissions** and **Manage Users with Roles and Permissions** in the *System Security and User Management Guide*.

An Analyst with permission `Context Lookup` can perform Context Lookup from the Investigation views. For more information, see the **View Additional Context for a Data Point** topic in the *Investigation and Malware Analysis Guide*.

An Analyst with permission `Manage List from Investigation` can manage lists and list values from the Investigation views. For more information, see the **Manage Lists and List Values in Investigation** topic in the *Investigation and Malware Analysis Guide*.

Example

The following use cases explain some scenarios where Context Hub service is used with data sources like Incident Management, ECAT, and Custom Lists.

Use Case of Incident Management in Context Hub Service

When a Tier 2 analyst searches through meta values hunting for new indicators of compromise, the feedback provided by the Context Enrichment source Incident Management is very useful. The analyst can see if there is an existing incident or alert related to the selected meta value. This ability allows the analysts to ignore meta values for which incidents already exist, and focus on finding new, unique indicators of compromise.

The information becomes available in the same Investigation > Navigate view. The accessibility of this information is efficient because analyst can access enrichment data without jumping between views or different tool.

Use Case of ECAT in Context Hub Service

When a Tier 2 analyst views the lookup results in the investigation views, the analyst will be able to view the IPs, hosts, and Mac address that are running ECAT agents. This makes potential compromises easier than ever, directly in the Security Analytics Investigation views. The context lookup details provide high level information related to the endpoint running the ECAT agent, allowing the analyst to understand if the system is compromised or not. If the analyst needs more information on the risk and IIOC scores to make that determination, they have the ability to see notes and status documented in ECAT as well as the top modules by IOC score. If even further details are necessary, the analyst can click on the details provided in the context lookup panel to jump directly into the ECAT user interface. The analyst can then use the machines indicated as pivot points to their investigations to see what other machines the system has been communicating with to find further compromised hosts.

Use Case of List in Context Hub Service

Use Case 1

A Tier 3 analyst checks Incident Management context for IPs and domains associated to suspicious sessions. If there are no incidents or alerts associated and the ip and domain under investigation needs to be monitored for abnormal behavior.

The analyst can include these meta values into a list. For example, to improve the visibility of the suspicious IP addresses, the analyst can add the same meta values to two lists. One list is for domains suspected of being related to command and control connections, and other list is for IP addresses related to remote access Trojan connections.

Now a Tier 2 analyst can use this context list to spot indicators of compromise. The analyst can also export the lists in CSV format and send to the Tier 1 analyst to create incidents for further tracking and analysis.

Use Case 2

As the Tier 3 analyst has created some custom content to detect certain indicators of compromise, they want to provide further details on that new content to guide the other analysts when they come across the newly generated meta values. They can create three new lists (custom critical, custom suspicious, custom advisory) that categorize the new meta values that an analyst will potentially see when the new content has been triggered. The description provided by the analyst to each list gives some background to the other analysts as what the new meta values are depicting and the necessary action to be taken when when they see them marked in investigation. This is not a replacement for the creation of an incident or alert, but a way to provide further details to the analyst when they first see these new meta values in investigation.

Basic Setup

The Administrator needs to perform each step in the proper sequence to configure the service. After initial setup of the Context Hub service, you can view additional context for a data point from Investigation views. For instructions, see the **View Additional Context for a Data Point** topic in the *Investigation and Malware Analysis Guide*.

Topics:

Step 1. Add the Context Hub Service

This topic provides information on how to add the Context Hub service on a Event Stream Analysis (ESA) host.

In Security Analytics 10.6, Context Hub service is pre-installed on ESA host, but is disabled by default. Use the procedure in this topic to enable Context Hub service.

Note: You can have only one Context Hub service instance enabled in your Security Analytics deployment. If there are multiple ESA service in Security Analytics, you must choose the appropriate ESA host for Context Hub. A minimum of 8GB space is required to configure Context Hub on ESA host.

Prerequisites

Ensure that ESA host with 10.6 is available. In case of older versions, administrator must first upgrade ESA host to 10.6.

Procedure

When you navigate to the Administration > Services panel, if Context Hub service is not enabled, the Enable Context Hub dialog appears. For more information, see Enable Context Hub Dialog.

To add the Context Hub service:

1. In the Security Analytics menu, select **Administration > Services**.

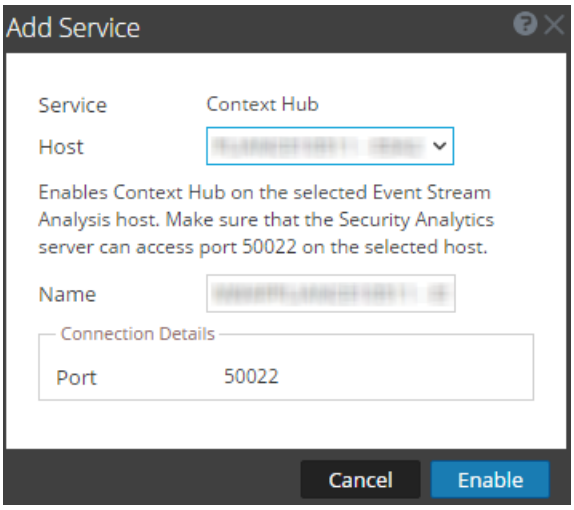
   The services view is displayed.

2. In the Services panel, select + **> Context Hub**.

   The **Add Service** dialog is displayed.

3. Select the ESA host from the list of compatible hosts.

   The other fields like the **Name** and **Port** are entered automatically. The default port is **50022**.



4. Click **Enable**.

   The Context Hub service is added in Security Analytics.

Note: You can have only one Context Hub service instance enabled in your Security Analytics deployment. If you run multiple ESAs and you want to use Context Hub functionality on them, you need to configure them to connect to the ESA that runs the Context Hub service. For instructions, see the **Configure an ESA to Connect to the Context Hub on Another ESA** topic in the *Event Stream Analysis (ESA) Configuration Guide*.

Step 2. Configure Data Sources for Context Hub

This procedure is required to add a data source for Context Hub and configure the response types for the data source. You can add the supported data sources (Incident Management, ECAT, Custom Lists, and Live Connect) to look up the contextual information.

Prerequisites

Ensure that Context Hub is enabled.

Procedures

Perform the following procedures:

- Configure Incident Management as a Data Source for Context Hub
- Configure RSA ECAT as a Data Source for Context Hub
- Configure Lists as a Data Source for Context Hub
- Configure Live Connect Data Source for Context Hub

Configure Incident Management as a Data Source for Context Hub

This topic describes the procedure to configure Incident Management as a data source for Context Hub.

To use the Context Hub service to fetch contextual information from Incident Management service, you must configure Incident Management as a data source for Context Hub. Use the procedures in this topic to add Incident Management as a data source for Context Hub service and configure the responses (if required) for Incident Management.

Responses are different types of context information that are available for a data source. The configuration of these responses for Incident Management source controls what appears in the Context Lookup panel displayed in Investigation views when Context Lookup is performed. The types of responses for Incident Management data source are **Incidents** and **Alerts**.

Responses for each data source is already configured with default values for optimal performance. You can view or edit the default values by using the procedure in this topic.

Prerequisites

Ensure that:

- Context Hub is enabled and the service is available in Administration > Services view of Security Analytics.
- Incident Management service is available and the Incident Management Database password is kept handy.

Procedures

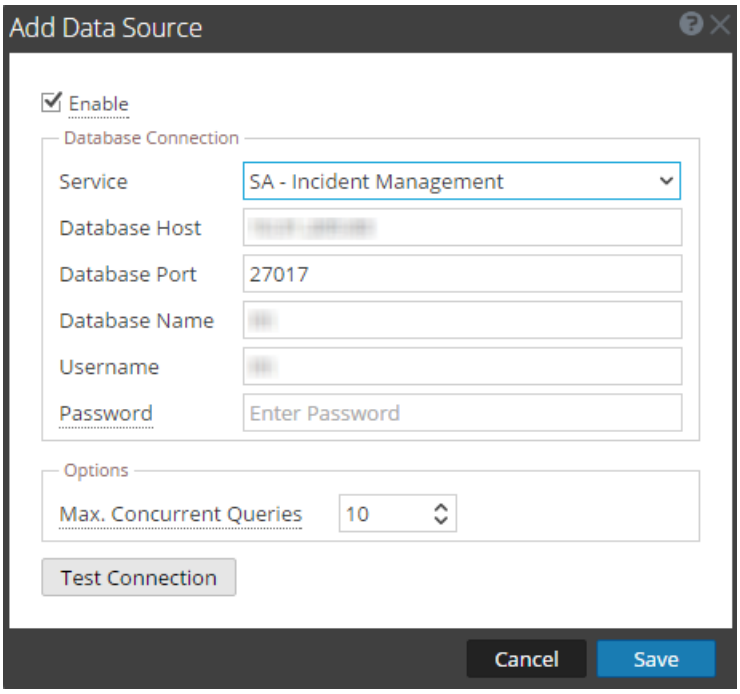
Add Incident Management Data Source

To add incident management as a data source for Context Hub:

1. In the Security Analytics menu, select **Administration** > **Services**.
   The services view is displayed.
2. In the Services panel, select the Context Hub service and click  **> view > Config**.
   The Services Config View of Context Hub is displayed.

3. In the **Data Sources** tab, click  **> Incident Management**.

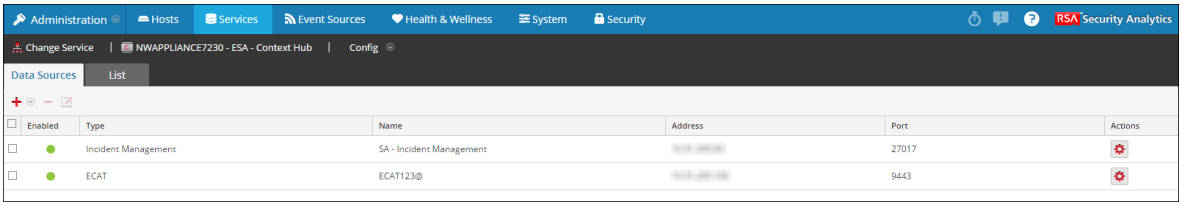
   The **Add Data Source** dialog is displayed.



4. Provide the following database connection details:

   - Enable: Select Enable to enable Incident Management Data Source. This option is enabled by default (checked).
   - Service: Select the Incident Management service that is available.
     The values are populated automatically for the following fields. Change the values if required.
     - **Database Host:** The host name or IP address of the Incident Management database.
     - **Database Port:** The default port is 27017.
     - **Database Name:** The default database name is im.
     - **Username:** The default Username is im.
   - **Password**: Enter the password to connect to the incident management database. The default password is im.
   - **Max. Concurrent Queries**: You can configure the maximum number of concurrent queries defined by the Context Hub service to be run against the configured data sources. The default value is 10.

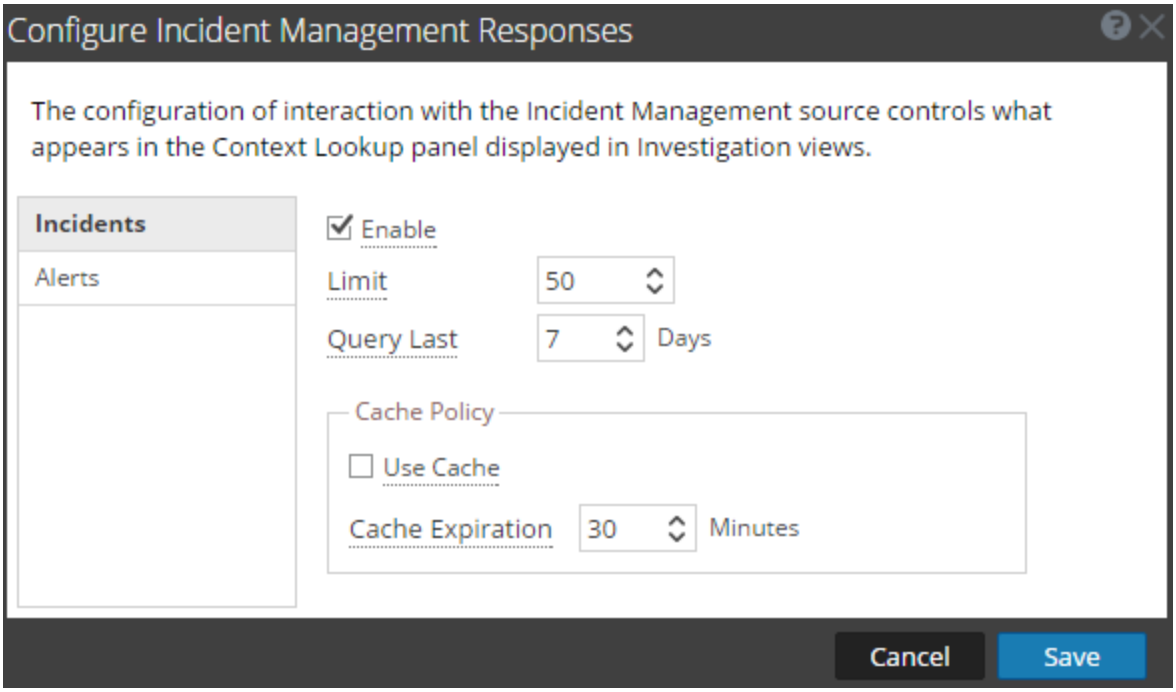
5. Click **Test Connection** to test the connection between Context Hub and the data source.
6. Click **Save** to save the settings.
   Incident Management is added as a data source for the configured Context Hub. The added Incident Management data source is displayed in the **Data Sources** tab.



Configure Responses for Incident Management Data Source

To view/edit responses for Incident Management data source:

1. In the **Data Sources** tab, select the Incident Management source and click  .
   The **Configure Incident Management Responses** dialog is displayed.



2. In the left panel, select each response (Incidents or Alerts) to view and edit the settings.

3. Configure the following fields:

Field	Description
Enable	This option is enabled by default (checked) and can be used to enable or disable the selected response.
Limit	Enter the maximum number of records (incidents or alerts) to be displayed in the **Context Lookup** panel of Investigation views when context lookup is performed. The default value is **50**. For example, if the limit is set to 10, only 10 records are displayed based on the time first and then priority for incidents and severity for alerts.
Query Last	Select the duration (in days) for which the contextual information of the selected response type must be fetched. The default value is **Last 7 Days**.
Use Cache	Select the checkbox to enable response caching. When enabled, Context Hub stores the lookup results in cache. Subsequent requests for the same meta value is served from cache for the configured time (Cache Expiration).
Cache Expiration	The time (in minutes) that the lookup results are stored in cache after Context Lookup is performed. The default value is **30 minutes**.

4. Click **Save**to save the settings for Incident Management data source.

Next steps

After completing the configuration, you can use the Context Lookup option in Investigate > Navigate view or Investigation > Events view to fetch contextual information. For instructions, see the **View Additional Context for a Data Point** topic in the *Investigation and Malware Analysis Guide*.

Configure RSA ECAT as a Data Source for Context Hub

This topic describes the procedure to configure ECAT as a data source for Context Hub.

To use the Context Hub service to fetch contextual information from ECAT, you must configure ECAT as a data source for Context Hub. Use the procedures in this topic to add ECAT as a data source for Context Hub service and configure the responses (if required) for ECAT.

Responses are different types of context information that are available for a data source. The configuration of these responses for ECAT source controls what appears in the Context Lookup panel displayed in Investigation views when Context Lookup is performed. The types of responses for ECAT data source are Machines, Modules, and InstantIOCs

Responses for each data source is already configured with default values for optimal performance. You can view or edit the default values by using the procedure in this topic.

Prerequisites

Ensure that:

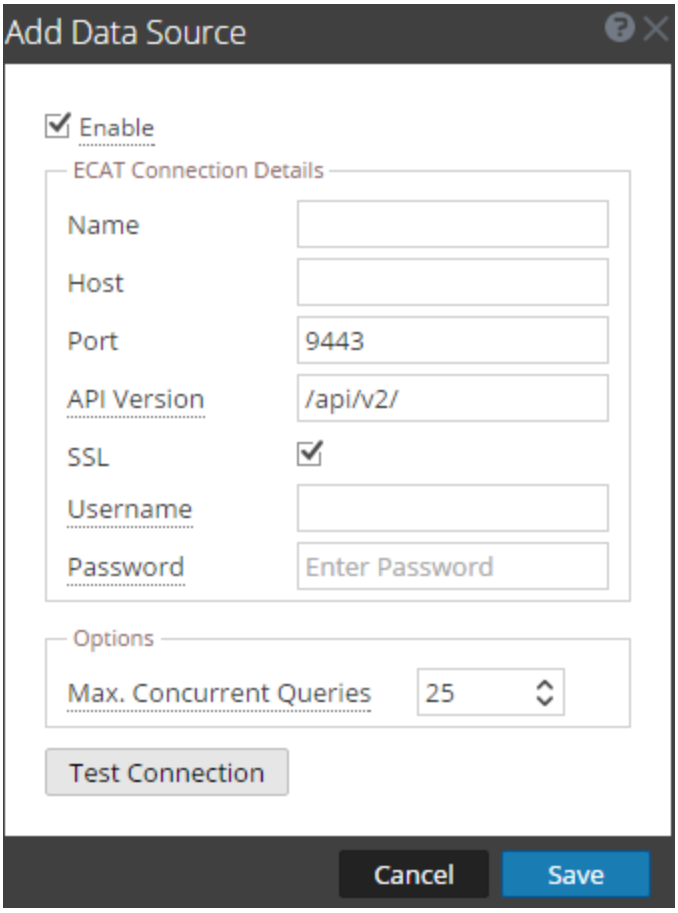
- Context Hub is enabled and the service is available in Administration > Services view of Security Analytics.
- RSA ECAT (v4.1.1 and above) is installed and configured.
  The RSA ECAT 4.1.1 documents provide detailed information about installing and configuring ECAT. Refer the ECAT documents available in https://knowledge.rsasecurity.com.

Procedures

Add RSA ECAT Data Source

To add RSA ECAT as a data source for Context Hub:

1. In the Security Analytics menu, select **Administration > Services**.
   The Services view is displayed.
2. In the **Services** panel, select the Context Hub service, and > **View** > **Config**.
   The Services Config view is displayed.
3. In the **Data Sources** tab, click > **ECAT**.
   The **Add Data Source** dialog is displayed.

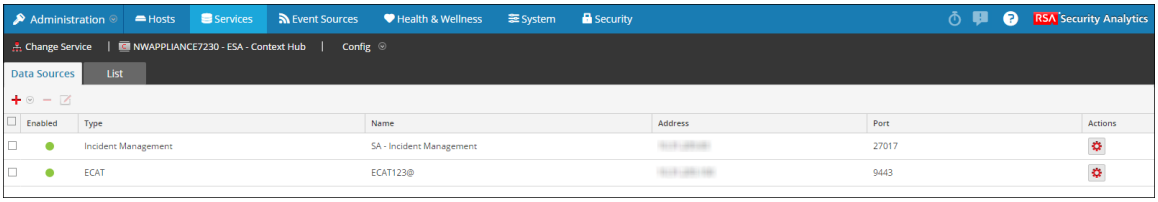


4. Provide the following information:

Field	Description
Enable	Select **Enable** to enable ECAT Data Source. This option is enabled by default (checked).
Name	Provide a name for ECAT data source.
Host	Enter the hostname or IP address where ECAT API server is installed.

Field	Description
Port	Default port is 9443.
API Version	The default API version (/api/v2) supports connection to ECAT 4.1.1 and above.
SSL	Select SSL if you want Security Analytics to communicate with the host using SSL. This is enabled by default.
Username	Enter the ECAT API Server username.
Password	Enter the ECAT API Server password.
Max. Concurrent Queries	You can configure the maximum number of concurrent queries defined by the Context Hub service to be run against the configured data sources. The default value is 25.

5. Click **Test Connection** to test the connection between Context Hub and the ECAT data source.
6. Click **Save** to save the settings.
   ECAT is added as a data source for Context Hub. The added ECAT data source is displayed in the **Data Sources** tab.



Change ECAT Admin Password

The API-Server Admin user assigns the roles and permissions to the new users. The admin user is not created by
default at the time of installation.

ECAT Admin username and password is as given below:

- Username: admin
- Password: This has to be set using the following command:

```
ApiServer.exe /setadminpswd A_Strong_Password
```

After setting the password, restart the server.

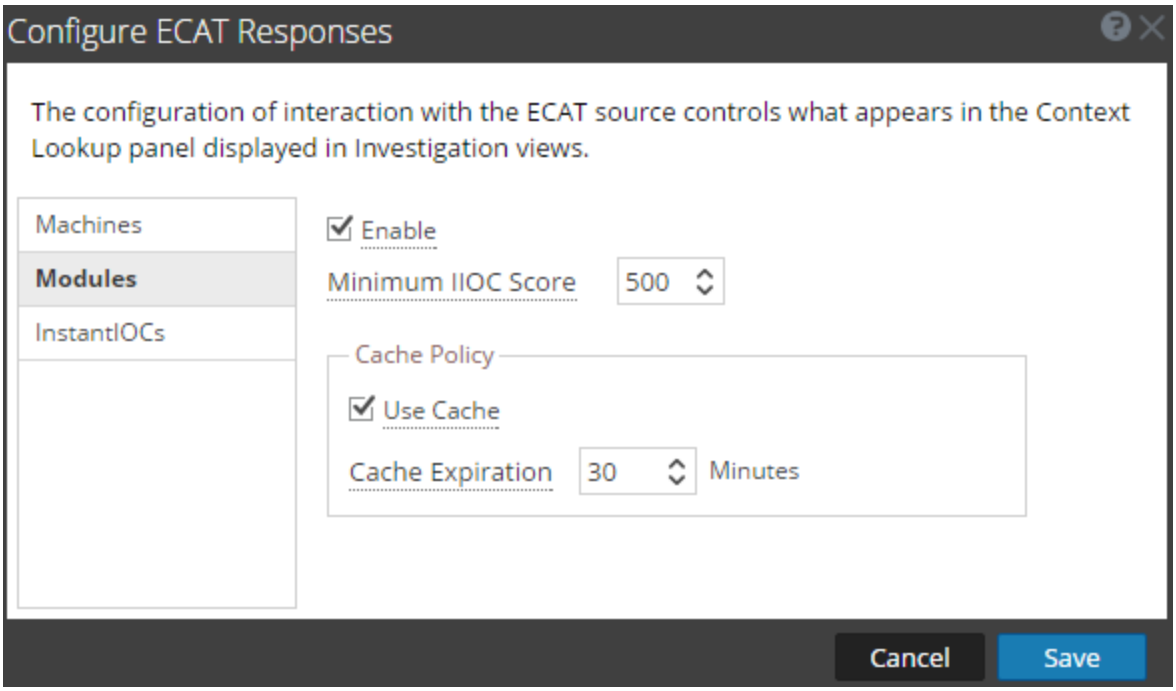
For more information about RSA ECAT REST API Server, refer the ECAT documents available in https://knowledge.rsasecurity.com.

Configure Responses for ECAT Data Source

To view/edit responses for ECAT data source:

1. In the **Data Sources** tab, select the ECAT source and click  .

   The **Configure ECAT Responses** dialog is displayed.



2. In the left panel, select each response (Machines, Modules, and InstantIOCs) to view and edit the settings.

3. Configure the following fields:

Field	Description
Enable	This option is enabled by default (checked) and can be used to enable or disable the selected response.
Use Cache	Select the checkbox to enable response caching. When enabled, Context Hub stores the lookup results in cache. Subsequent requests for the same meta value is served from cache for the configured time (Cache Expiration).
Cache Expiration	The time (in minutes) that the lookup results are stored in cache after Context Lookup is performed. The default value is **30 minutes**.
Minimum IIOC Score (For Modules only)	The minimum IIOC score for fetching contextual information of ECAT modules. The contextual information of ECAT modules having IIOC score greater than or equal to the configured minimum score are fetched. The IIOC score for ECAT modules ranges between 0 to 1024, where 1024 is considered as critical. By default, the minimum IIOC score is set to **500**.

4. Click **Save** to save the changes.

Next steps

After completing the configuration, you can use the Context Lookup option in Investigate > Navigate view or Investigation > Events view to fetch contextual information. For instructions, see the **View Additional Context for a Data Point** topic in the *Investigation and Malware Analysis Guide*.

Configure Lists as a Data Source for Context Hub

This topic describes the procedure to create and configure custom lists for Context Hub. These lists are automatically considered as data sources for Context Hub.

To use the Context Hub service to fetch contextual information from meta types that support context lookup, you can create one or more lists and add relevant list values to the list. Make sure that you create meaningful list such as blacklisted IPs, whitelisted IPs, and so on. These custom lists may be populated with items either by importing CSV files or by adding meta values by using the option Add/Remove from List in Investigation views.

You can also import and export a list. For more information, see Import or Export Lists for Context Hub.

You can also create lists and add list values from Investigation views. For instructions, see the **Manage Lists and List Values in Investigation** topic in the *Investigation and Malware Analysis Guide*

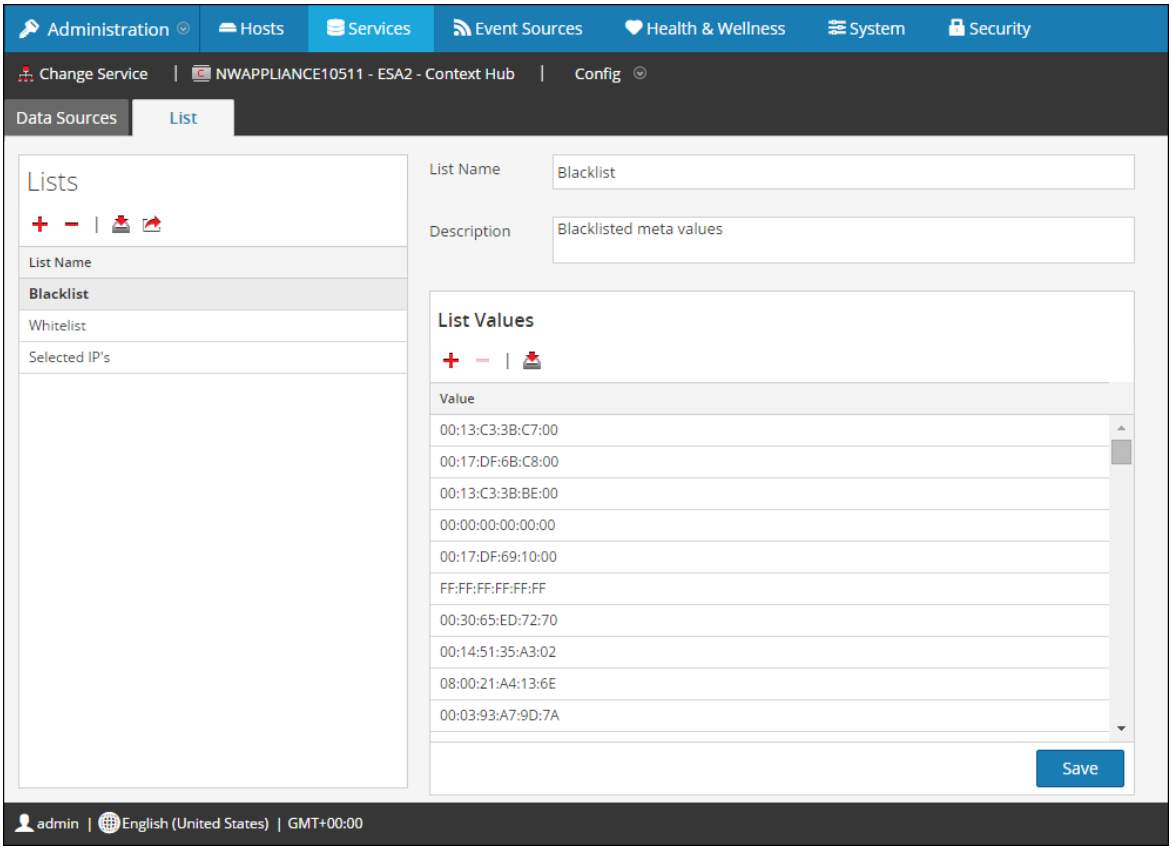
Prerequisites

Ensure that Context Hub is enabled and the service is added in Administration > Services view of Security Analytics.

Procedure

To add a new list for Context Hub:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select the Context Hub service and  **> View > Config**.
   The Services Config view of the selected Context Hub is displayed.
3. Click the **List** tab.
   The **List** tab consists of the **Lists** panel and **List Values** panel.



4. Click + on the **Lists** panel to add a new list and complete the following steps:
   a. In the **List Name** field, enter a unique name for the list.
   b. In the **Description** field, enter the description of the list.
   c. In the **List Values** panel, click + to add unique list values.
   d. To import a list, click on the **Lists** panel.
   e. To import list values for a list, click on the **List Values** panel.
      For more information about importing list and list values, see Import or Export Lists for Context Hub.
5. Click **Save**.
   The list is saved with the values. These lists are considered as data sources for retrieving contextual information.

Next steps

After completing the configuration, you can use the Context Lookup option in Investigate > Navigate view or Investigation > Events view to query and view contextual information. For instructions, see the **View Additional Context for a Data Point** topic in the *Investigation and Malware Analysis Guide*.

Configure Live Connect Data Source for Context Hub

This topic describes the procedure to configure Live Connect data source for Context Hub.

RSA Live Connect is a cloud based threat intelligence service. This service collects, analyzes, and assesses threat intelligence data such as IP addresses, domains, and files collected from various sources including the RSA Security Analytics and RSA ECAT customer community.

RSA Live Connect is a part of Live Services and can be configured from the System View > Live Services Configuration panel. For more information about configuring Live Services, see the **Configure Live Services Settings** topic in the *System Configuration* Guide.

RSA Live Connect Threat Insights provides analysts the opportunity to pull threat intelligence data such as IP related information from the Live Connect service to be leveraged by analysts during the investigation process. By default, **Threat Insights** is enabled in **Additional Live Services**. If Context Hub service is configured, Live Connect is automatically added as a data source for Context Hub.

Procedures

Add Live Connect Data Source

Prerequisites

Ensure that:

- Context Hub is enabled and the service is available in Administration > Services view of Security Analytics.
- RSA Live Account is available.

Note: To create a Live Account, see the **Step 1. Create Live Account** topic in the *Live Services Management Guide*.

By default, **Threat Insights** is enabled in **Additional Live Services** section. Before setting up Live Connect data source, make sure that you have signed in to your Live account with your Live Account Credentials and Context Hub is enabled. Live Connect is automatically added as a data source for context hub.

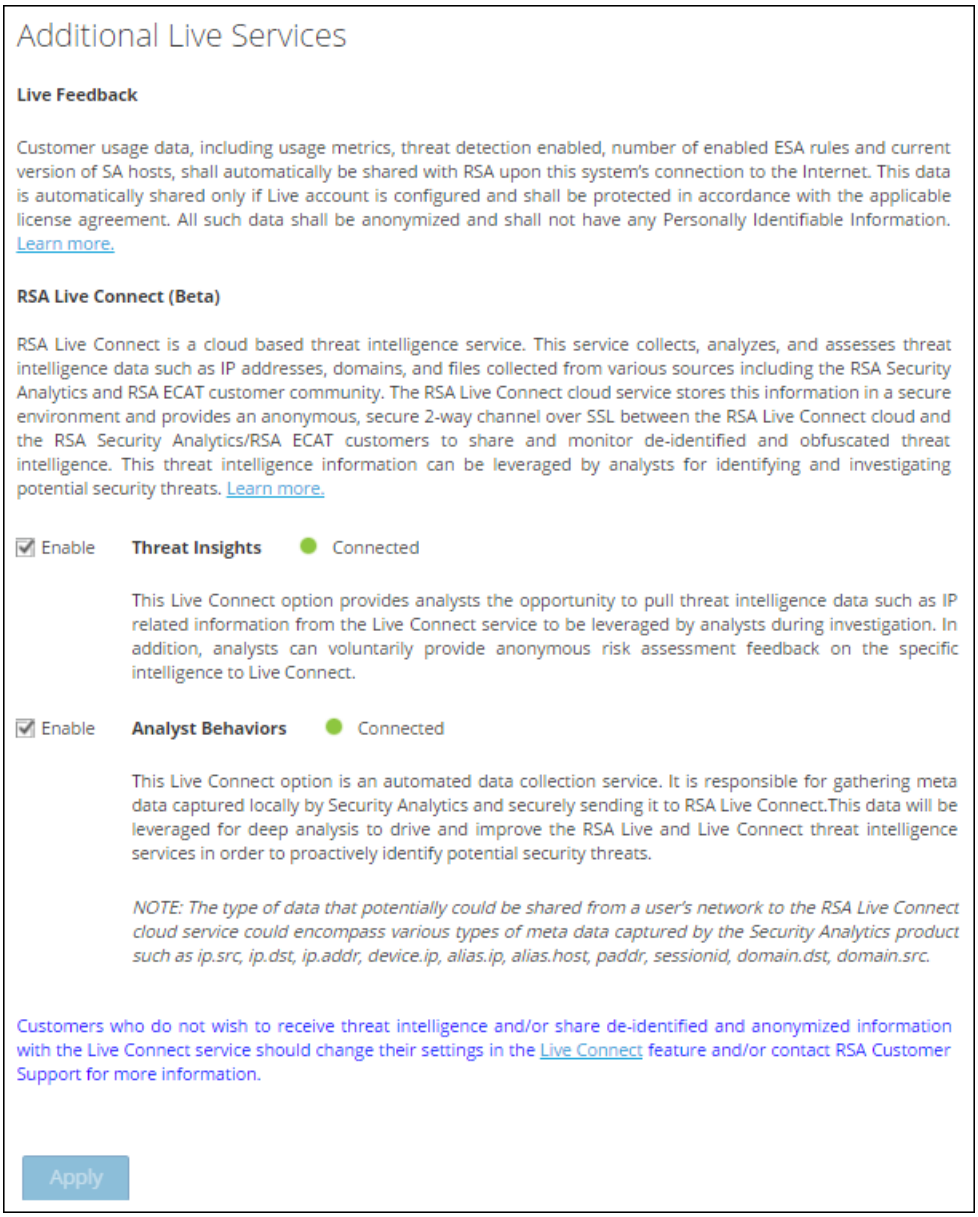
For information about configuring Live Account and Live Services, see the **Configure Live Services Settings** topic in the *System Configuration Guide*.

For information about configuring Context Hub service, see the **Step 1. Add the Context Hub Service** topic in the *Context Hub Configuration Guide*.

Enable/Disable Live Connect Data Source

To enable/disable Live Connect data source for Context Hub:

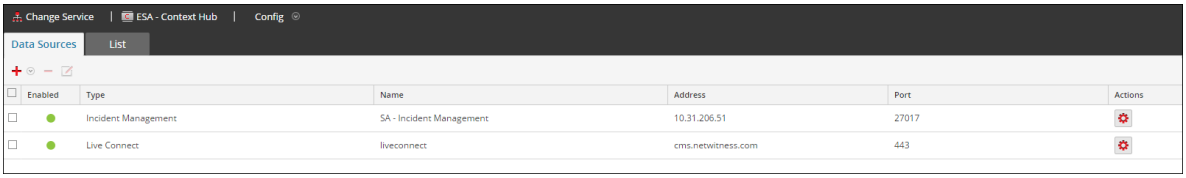
1. In the Security Analytics menu, select **Administration > System**.
2. In the left navigation pane, select **Live Services**.
3. In the **Additional Live Services** section, enable **Threat Insights**.



4. Click **Apply**.

   Live Connect data source is enabled for Context Hub service.

5. To verify, go to the **Data Sources** tab and view the available sources.
   Live Connect source must be added to the list of available sources and the **Enabled** field must be a solid green circle ( ).



6. To disable Live Connect data source, disable **Threat Insights** in Additional Live Services panel and click **Apply**.
   Live Connect data source is disabled for Context Hub service.

> **Note:** If Threat Insights is disabled, the Context Lookup panel for Live Connect (in the Investigation Navigate view and Events view) displays a message to configure the Live Connect data source. To view contextual data for Live Connect, you must enable Threat Insights.

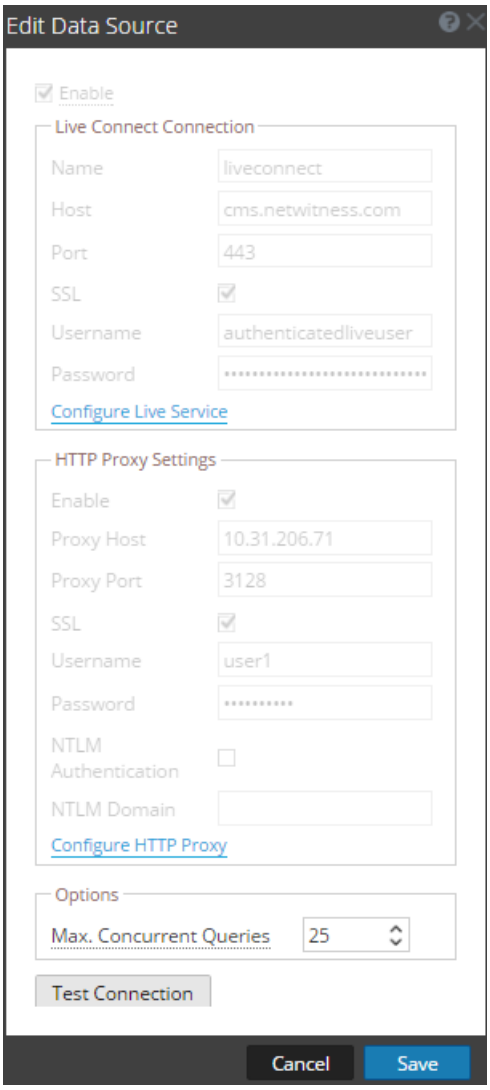
Edit Live Connect Data Source Settings

To edit live connect data source for Context Hub:

1. In the Security Analytics menu, select **Administration** > **Services**.
   The Services view is displayed.
2. In the **Services** panel, select the Context Hub service, and > **View** > **Config**.
   The Services Config view is displayed.

3. In the **Data Sources** tab, select the live connect data source and click .

   The **Edit Data Source** dialog is displayed.



4. Edit the required fields:

Field	Description
Max. Concurrent Queries	You can configure the maximum number of concurrent queries defined by the Context Hub service to be run against the configured data sources. The default value is 25.

5. To edit the Live Connection and Proxy settings, do the following:

   - To edit the Live Connection settings, see the **Live Services Configuration Panel** topic in the *System Configuration Guide*.

- To edit the proxy settings, see **the HTTP Proxy Settings Panel** topic in the *System Configuration Guide*.

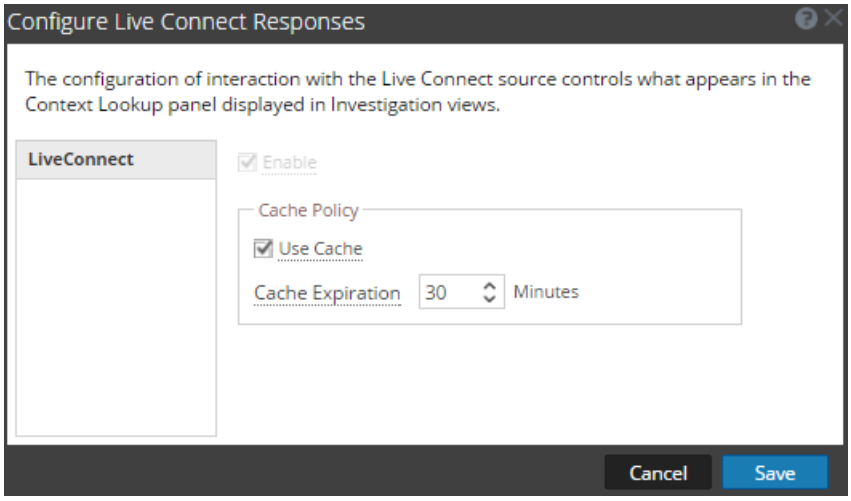
6. Click **Test Connection** to test the connection between Context Hub and the data source.
7. Click **Save** to save the settings.

Configure Responses for Live Connect Data Source

To view/edit responses for Live Connect data source:

1. In the **Data Sources** tab, select the Live Connect source and click  .

   The **Configure Live Connect Responses** dialog is displayed.



2. Configure the following fields:

Field	Description
Enable	This option is enabled by default (checked) and cannot be modified.
Use Cache	Select the checkbox to enable response caching. When enabled, Context Hub stores the lookup results in cache. Subsequent requests for the same meta value is served from cache for the configured time (Cache Expiration). This option is enabled by default (checked).
Cache Expiration	The time (in minutes) that the lookup results are stored in cache after Context Lookup is performed. The default value is **30 minutes**.

3. Click **Save** to save the settings for Live Connect data source.

Next steps

After completing the configuration, you can use the Context Lookup option in Investigate > Navigate view or Investigation > Events view to fetch contextual information. For instructions, see the **View Additional Context for a Data Point** topic in the *Investigation and Malware Analysis Guide*.

Additional Procedures

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

Topics:

Change Context Hub Storage Password

In Security Analytics, this procedure is optional. However, it is always a best practice for administrators to change any default password for added security. Some organizations do not allow default passwords and make this procedure mandatory.

Prerequisites

You must have Administrator role privileges.

Procedures

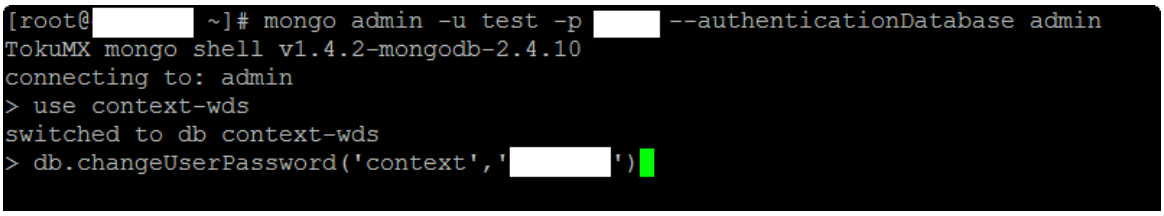
Change Password for Context Hub Database

1. Log on to ESA host that runs the Context Hub service:
   a. SSH to the ESA host.
   b. Log on as **root**.
2. Log on to the MongoDB as the admin user:

   ```
   mongo admin -u admin -p <current_admin_password> --
   authenticationDatabase admin
   ```

3. Switch to Context Hub database.

   ```
   use context-wds
   ```

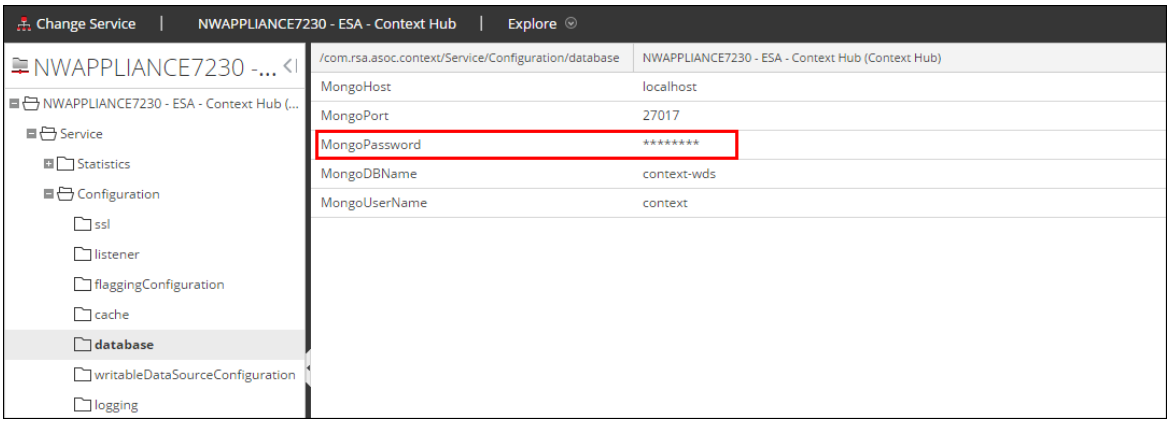
   

4. Type the following command to change the Context Hub account password. The default pasword is `context`.

   ```
   db.changeUserPassword('context','<new_password>')
   ```

Update Context Hub Database Configuration with the new Password

1. Log on to Security Analytics as admin.
2. In the **Security Analytics** menu, select **Administration > Services**.
3. Select the Context Hub service, then > **View** > **Explore**.
4. In the Explore view on the left, select **Configuration** > **database**.



5. In the right panel, type the updated database password in the **MongoPassword** field.
6. Restart the Context Hub service to accept the password change and force the session to start using the new password.
   a. Select **Administration > Services**.
   b. Select the Context Hub service, and click > **Restart**.
7. To validate the password change, go to the Config view of Context Hub service and check the configured data sources, and lists.
   - If content appears in the Data Sources and Lists tab, the passwords match and were changed successfully.
   - If you do not see the required content in the Data Sources and Lists tab, revise the service password to match the MongoDB password.

Import or Export Lists for Context Hub

This topic provides instructions for administrators to import or export a list that is configured in the Context Hub service. The file to be imported or exported must be a CSV file.

Users with administrator role can import or export lists that can be used by the analyst.

Note: The CSV file that you are importing as a list must be a single column file.

Prerequisites

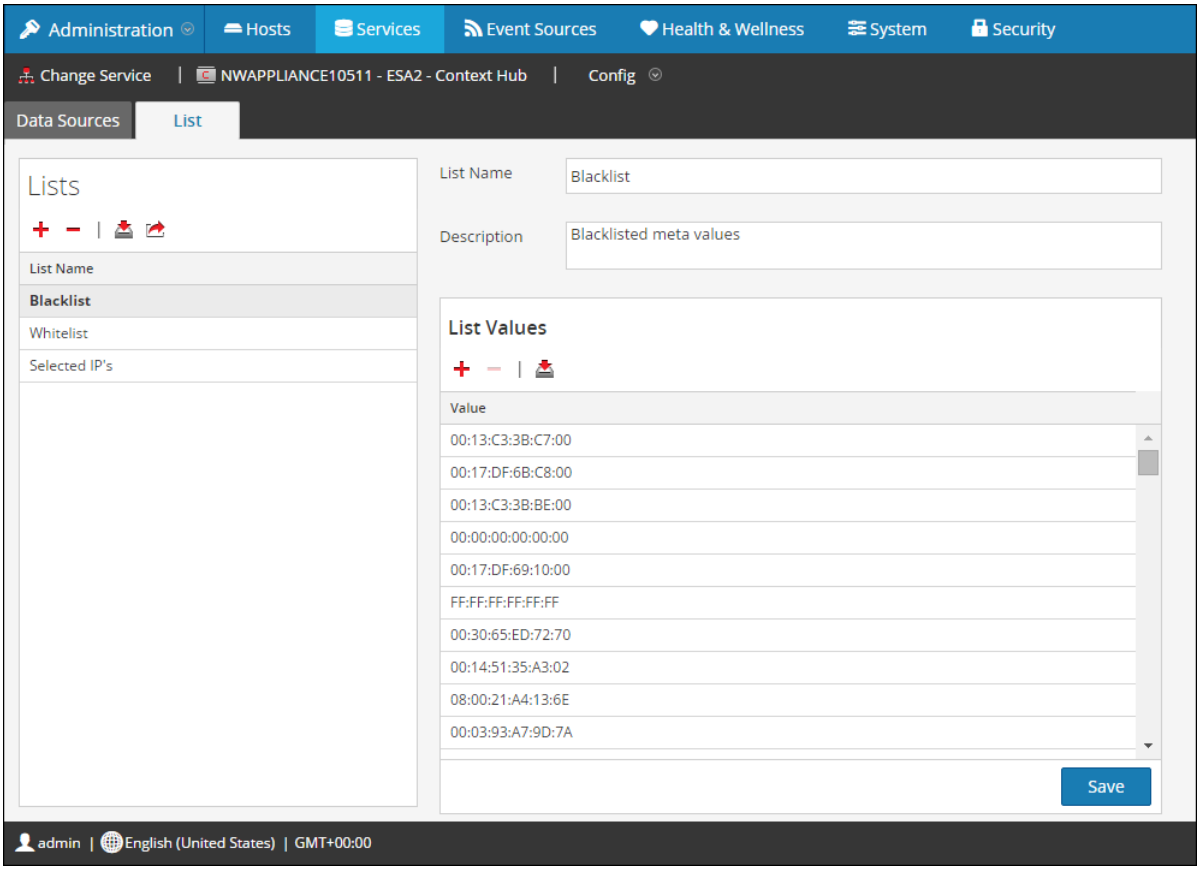
Ensure that Context Hub is enabled and the service is available in Administration > Services view of Security Analytics.

Procedures

Import List for Context Hub

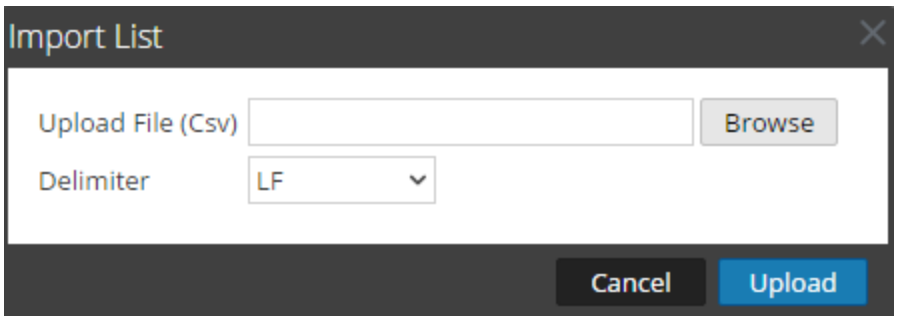
To import a list:

1. In the Security Analytics menu, select **Administration > Services**.
   The services view is displayed.
2. In the **Services** panel, select the Context Hub service and click  **> View > Config**.
   The Services Config View of the Context Hub service is displayed.
3. Click the **List** tab.
   The List tab consists of the **Lists** panel and **List Values** panel.



4. Click on the **Lists** panel.

   The **Import List** dialog is displayed.



5. In the **Import List** dialog, complete the following steps:

   a. In the **Upload File (Csv)** field, browse and select the `CSV` file.

   b. In the **Delimiter** field, select the delimiter to separate the values in a list from the options—**Comma**, **CR** (Carriage Return), and **LF** (Line Feed).

6. Click **Upload** to upload the CSV file to Security Analytics.

The list is imported to Security Analytics. These lists are considered as data sources for retrieving contextual information.

Import List Values for a List

To import List Values for a list:

1. In the Security Analytics menu, select **Administration > Services**.
   The services view is displayed.
2. In the **Services** panel, select the Context Hub service and click  **> View > Config**.
   The Services Config View of the Context Hub service is displayed.
3. Click the **List** tab.
   The List tab consists of the **Lists** panel and **List Values** panel.
4. In the Lists panel, select a list for which you want to import the values.
5. Click  on the **List Values** panel.
   The **Import List** dialog is displayed.
6. In the **Import List** dialog, complete the following steps:
   a. In the **Upload File (Csv)** field, browse and select the `CSV` file.
   b. In the **Delimiter** field, select the delimiter to separate the values in a list from the options—**Comma**, **CR** (Carriage Return), and **LF** (Line Feed).

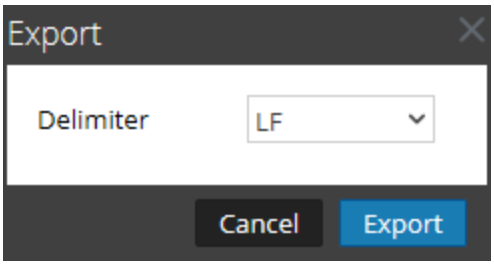
   Note: You can import list values to a list only after saving the list. The import button () on the **List Values** panel is disabled if the list is not saved.
7. Click **Upload** to upload the CSV file to Security Analytics.

The list values are imported to the selected list. These lists are considered as data sources for retrieving contextual information.

Export List for Context Hub

To export a list:

1. On the **List** tab of the Services Config view of the Context Hub service, click .
   The **Export** dialog is displayed.



2. In the **Delimiter** field, select the delimiter to separate the values in an exported list from the options—**Comma**, **CR** (Carriage Return), and **LF** (Line Feed).
3. Click **Export**.

The list is exported as a CSV file to the local machine.

Manage Meta Type and Meta Key Mapping

This topic provides instructions for an administrator to manage mapping of Context Hub meta types with Investigation meta keys.

The Context Hub service provides context lookup for meta values in the Investigation views. These meta values are grouped into meta types based on the category they belong to. For example, meta keys of Security Analytics Investigation like `ip.src` and `ip.dst` are grouped into the meta type `IP` in Context Hub. The meta type `IP` is in turn mapped to metas like `alert.events.source.device.ip_address` and `alert.events.destination.device.ip_address` in the Incident Management database.

In the Administration > System > Investigation view, the Context Lookup tab enables the administrator to configure the Investigation meta keys and meta type mapping. The administrator can add or remove investigation meta keys to the list of meta types supported by Context Hub.

The Context Hub service is pre-configured with default meta type and meta key mapping, which is expected to work with most deployments, unless there are some custom mappings created for your specific deployment.

Note: You cannot add a new Meta Type.

The default mapping is given below:

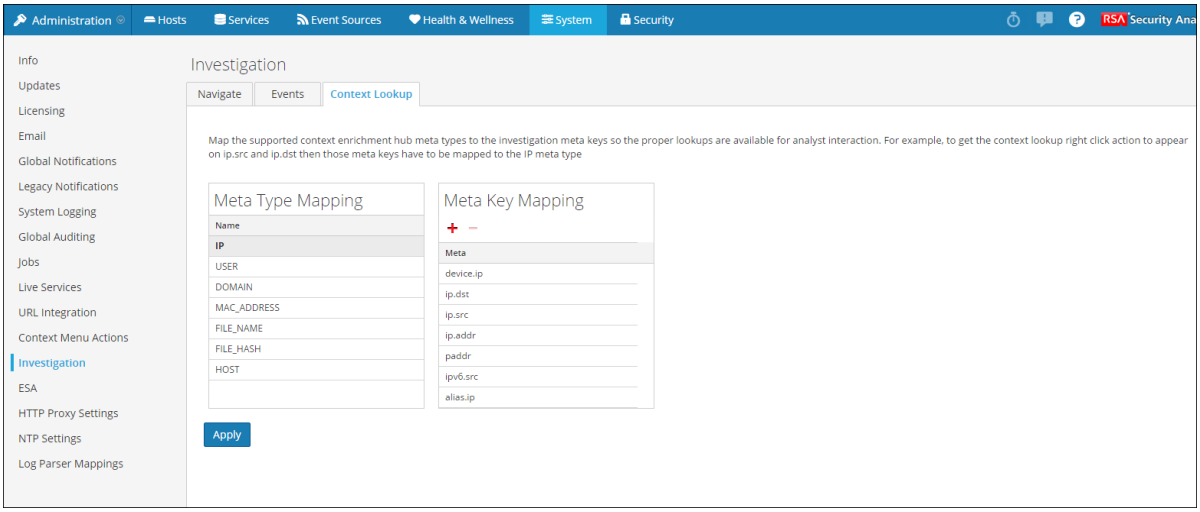
Meta Type Name	Meta Keys
IP	device.ip, ip.src, ip.dst, paddr, ip.addr, alias.ip
USER	user.src, user.dst, username
DOMAIN	domain.src, domain.dst
MAC_ADDRESS	eth.dst, eth.src, alias.mac
FILE_NAME	filename, sourcefile
FILE_HASH	checksum
HOST	device.host, alias.host

Procedure

To manage Investigation meta keys mapping:

1. In the **Security Analytics** menu, select **Administration > System**.
2. In the options panel, select **Investigation**.

   The Investigation Configuration panel is displayed.
3. Select the **Context Lookup** tab.



4. Select a meta type to view the default meta keys that are mapped with this meta type.
5. To add a meta key, click + and enter the meta key.
6. To remove a meta key, select the meta key and click − .
7. To save the changes, click **Apply**.

In case a new meta key is added, the Context Lookup menu option is enabled for the meta values under that meta key in the Investigation views.

For more information about Investigation Configuration Panel, see the **Investigation Configuration Panel** topic in the *System Configuration Guide*.

Context Hub Service References

The reference topics in this section are presented in alphabetical order.

Topics:

Configure Responses Dialog

This topic describes the functions and features of the Configure Responses dialog for Incident Management, ECAT, and Live Connect data sources.

In the Context Hub Services Config view > Data Sources tab, you can configure the responses for Incident Management, ECAT, and Live Connect data sources.

Related procedures are available in the following topics:

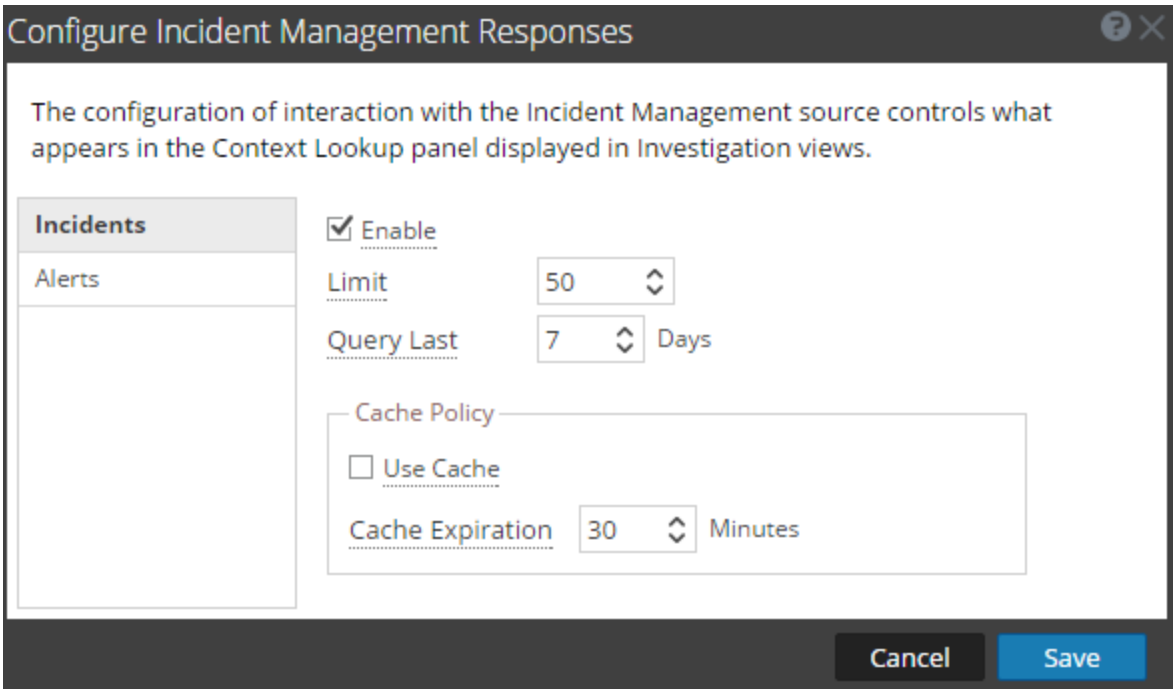
- Configure Responses for Incident Management Source. See Configure Incident Management as a Data Source for Context Hub.
- Configure Responses for ECAT Data Source. See Configure RSA ECAT as a Data Source for Context Hub.

To access this dialog:

1. In the Security Analytics menu, select **Administration > Services**.
   The services view is displayed.
2. In the Services panel, select the Context Hub service and click  **> View > Config**.
   The Services Config view of Context Hub is displayed.
3. Select the data source (Incident Management, ECAT, or Live Connect) for which you want to configure the responses and click  in the **Actions** column.

Configure Incident Management Responses Dialog

The types of responses for Incident Management data source are **Incidents** and **Alerts**. The following figure shows the Configure Incident Management Responses dialog.



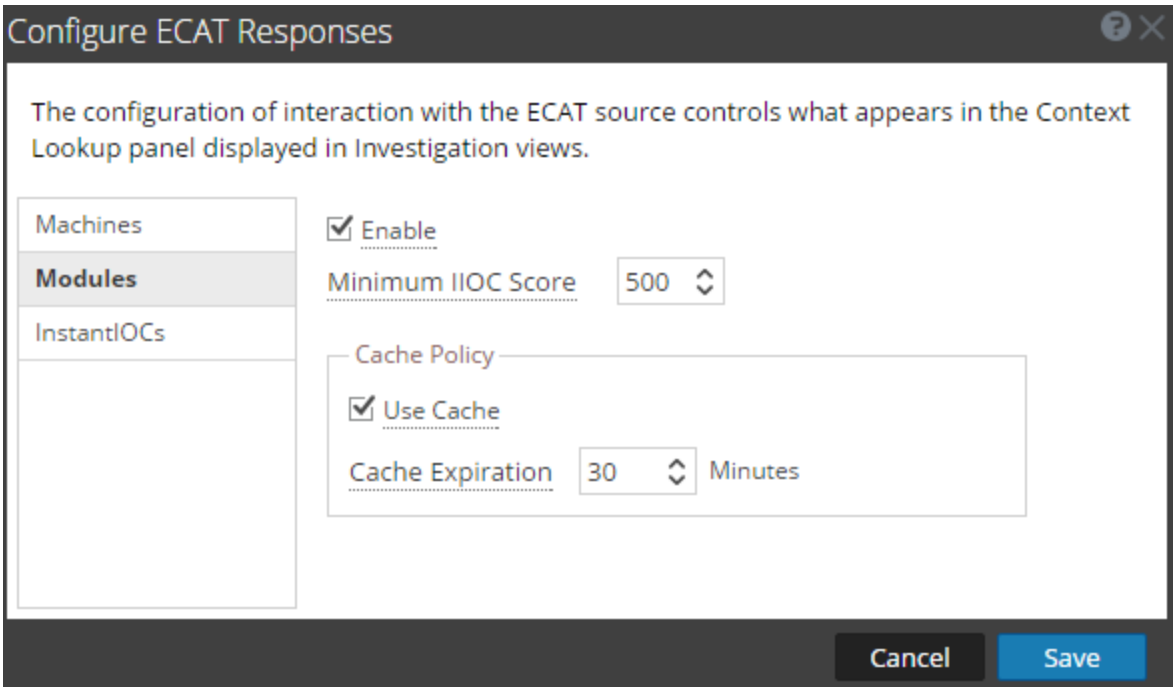
The following table describes the features of Configure Incident Management Responses dialog.

Feature	Description
Enable	This option determines if the selected response type must be enabled for the data source and the lookup results must appear in the Context Lookup panel displayed in Investigation views. The default setting is enabled.
Limit	The maximum number of records (incidents or alerts) to be displayed in the Context Lookup panel of Investigation views when context lookup is performed. The default value is 50.
Query Last	The duration (in days) for which the contextual information of the selected response type must be fetched. The default value is Last 7 Days.

Feature	Description
Use Cache	This option determines if response caching is enabled. When enabled, Context Hub stores the lookup results in cache. Subsequent requests for the same meta value is served from cache for the configured time (Cache Expiration).
Cache Expiration	The time (in minutes) that the lookup results are stored in cache after Context Lookup is performed. The default value is 30 minutes.

Configure ECAT Responses Dialog

The types of responses for ECAT data source are Modules, Machines, and InstantIOCs. The following figure shows the Configure ECAT Responses dialog.



The following table describes the features of Configure ECAT Responses dialog.

Feature	Description
Enable	This option determines if the selected response type must be enabled for the data source and the lookup results must appear in the Context Lookup panel displayed in Investigation views. The default setting is enabled.

Feature	Description
Minimum IIOC Score [For Modules only]	The minimum IIOC score for fetching contextual information of ECAT modules. The contextual information of ECAT modules having IIOC score greater than or equal to the configured minimum score are fetched. The IIOC score for ECAT modules ranges between 0 to 1024, where 1024 is considered as critical. By default, the minimum IIOC score is set to **500**.
Use Cache	This option determines if response caching is enabled. When enabled, Context Hub stores the lookup results in cache. Subsequent requests for the same meta value is served from cache for the configured time (Cache Expiration).
Cache Expiration	The time (in minutes) that the lookup results are stored in cache after Context Lookup is performed. The default value is **30 minutes**.

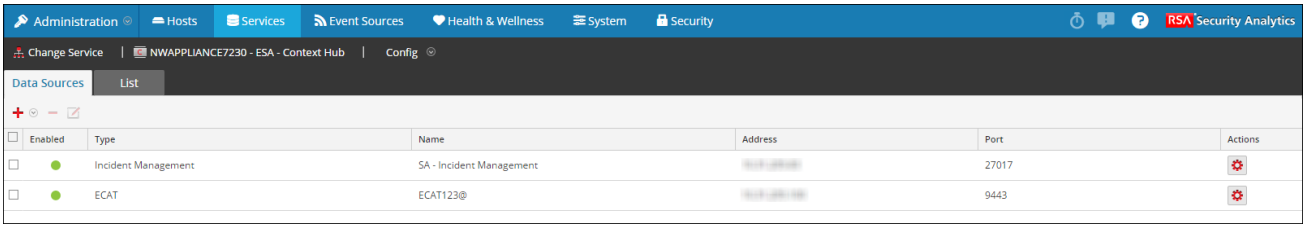
Context Hub Data Sources Tab

This topic describes the features of Data Sources tab in Services Config view of Context Hub service.

The Context Hub Services Config view > Data Sources tab is used to configure data sources for Context Hub service.

To access this tab:

1. In the Security Analytics menu, select **Administration > Services**.
   The services view is displayed.
2. In the Services panel, select the Context Hub service and click  **> View > Config**.
   The Services Config view of Context Hub is displayed with the Data Sources tab selected.



Features

The following table describes the features of Data Sources tab.

Feature	Description
	Opens the Add Data Source dialog so that you can add a data source. You can add only one data source of each type. For detailed instructions to add a data source, see Step 2. Configure Data Sources for Context Hub.
	Delete a data source. If you delete a data source, Context Hub does not consider the deleted service as a data source. All contextual information fetched previously will not be available.
	Opens the Edit Data Source dialog. For description of each field in Edit Data Source panel, see Step 2. Configure Data Sources for Context Hub.

Feature	Description
	Opens the Configure Responses dialog. You can view and edit the responses for the data sources. For example, alerts and incidents are responses that can be retrieved when context information is fetched from Incident Management data source. For description of each field in Configure Responses dialog, see Step 2. Configure Data Sources for Context Hub.
Enabled	Indicates whether the data source is enabled or disabled. A solid colored green circle indicates that data source is enabled ( ). An blank white circle indicates that data source is disabled.
Type	The type of data source. For example, Incident Management or ECAT.
Name	The unique name to identify the data source. For example, Incident Management.
Address	The IP address or hostname of the data source.
Port	The connection port for the data source.

Context Hub List Tab

This topic describes the features of Context Hub Services Config view > Lists tab.

The List tab of the Context Hub service allows you to create one or more lists and add relevant list values to the list. These lists are automatically considered as data sources for the Context Hub service.

Note: You can also create lists and add list values from Investigation views. For instructions, see the **Manage Lists and List Values in Investigation** topic in the *Investigation and Malware Analysis Guide*.

To access this tab:

1. In the Security Analytics menu, select Administration > Services.

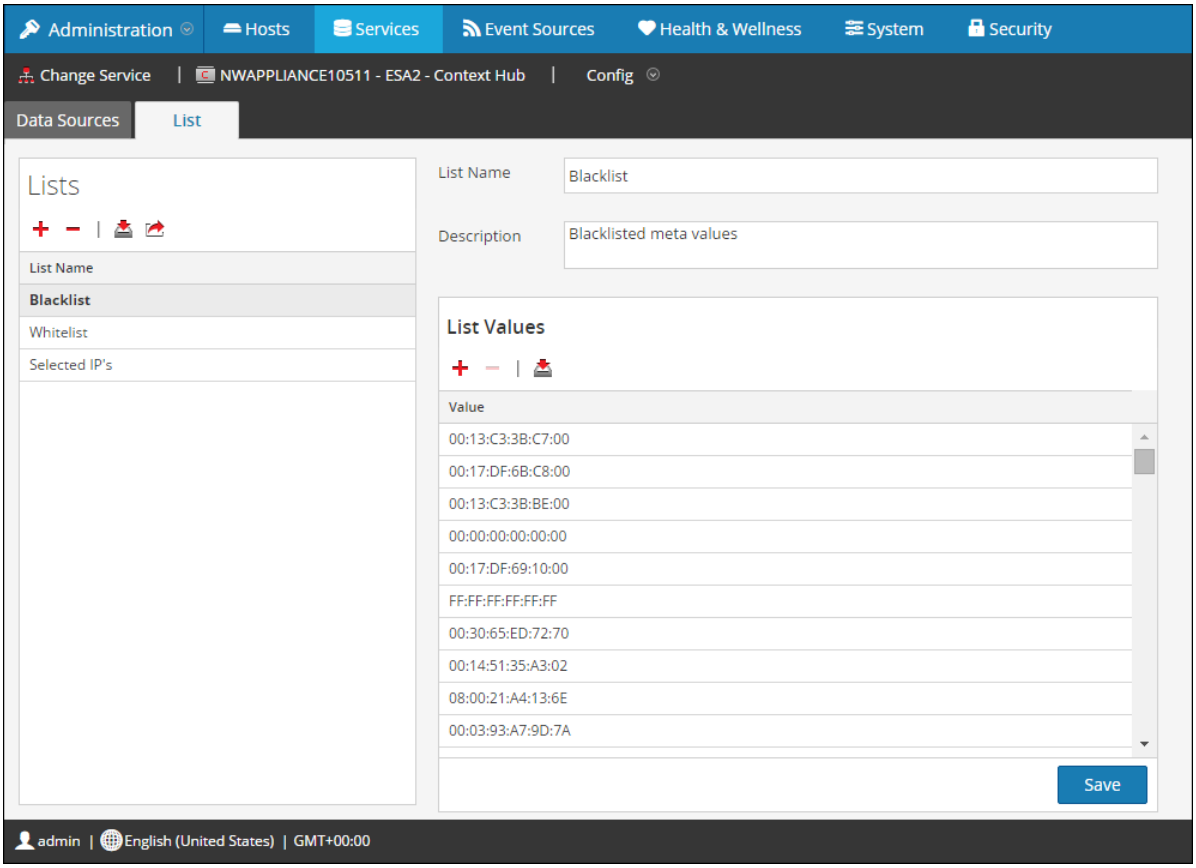
   The services view is displayed.

2. In the Services panel, select the Context Hub service and click  **> View > Config**.

   The Services Config view of Context Hub is displayed.

3. Click the **List** tab.

The List panel is displayed.



Features

The List tab consists of the **Lists** panel and **List Values** panel. The **Lists** panel has a toolbar with options to add, delete, import, and export lists. The entries under **List Name** are lists that are added or imported for the Context Hub service.

The **List Values** panel has a toolbar with options to add, delete, and import list values to the selected list. The entries under **Value** identify each list entry included in the list.

The following table describes the features of the List tab in the Services Config View for Context Service.

Feature	Description
+	Add a new list. For more information, see Configure Lists as a Data Source for Context Hub.

Feature	Description
	Delete a list. If you delete a list from Context Hub, the list is no longer considered as a data source for retrieving contextual information.
	Import lists to Context Hub. For more information, see Import or Export Lists for Context Hub.
	Export a list to the local machine. For more information, see Import or Export Lists for Context Hub.
List Name	Unique name to identify the list.
Description	Description of the list.
Save	Saves and closes the dialog.

The following table describes the features of the **List Values** section on the **List** tab.

Parameter	Description
	Add a new list value to the selected list.
	Delete one or more list values from the list.
	Import list values to the selected list.
Save	Saves and closes the dialog.

Context Lookup Panel

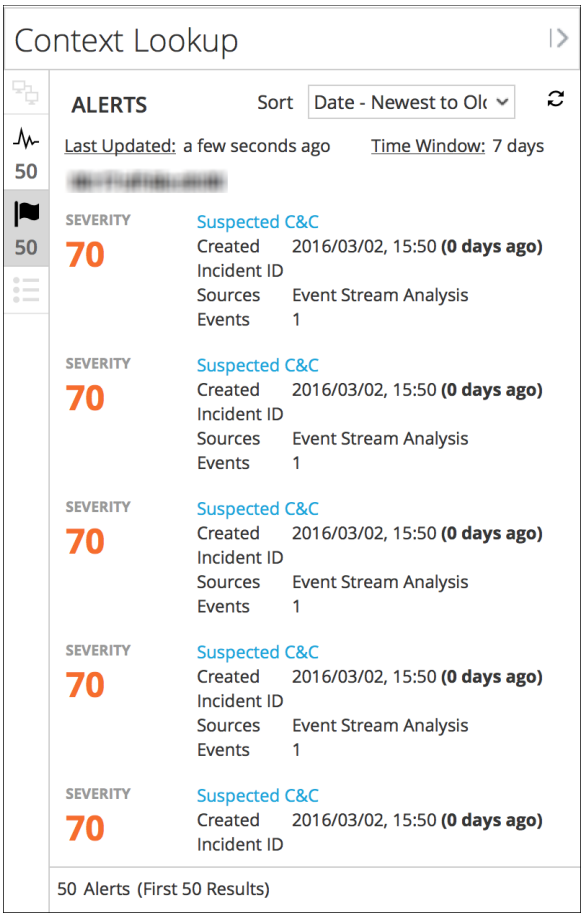
After you configure the Context Hub service, you can view the Context Lookup panel in the Navigate view and Events view of the Investigation module. For the first time when you view this panel, it displays the instructions for performing the Context Lookup. Later on, this panel gets minimized and can be expanded if required.

The Context Lookup panel does not display any data until you perform a Context Lookup on a meta value. Meta values that have associated context information are highlighted with a gray color background. The lookup results are displayed in the Context Lookup panel for different configured sources for the selected meta value. Procedures related to this panel are described in the **View Additional Context for a Data Point** topic of *Investigation and Malware Analysis Guide*.

To access this panel:

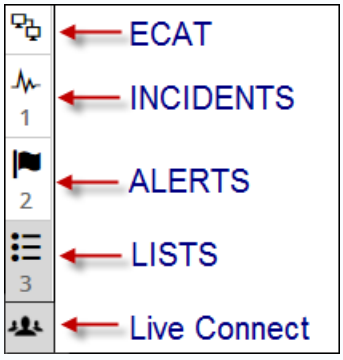
1. In the Security Analytics menu, select Investigation > Navigate or Events.
2. Right-click a meta value and select Context Lookup in the context menu.
   The Context Lookup panel displays the contextual information.
3. From the Icon bar, select the source for which you want to view the contextual information by clicking the corresponding icon.

The following figure is an example of the Lookup panel.



Features

The Context Lookup Panel has the following controls and features:

Feature	Description
Source Options Bar 	Displays the icons for the available sources: ECAT, Incidents, Alerts, Lists, and Live Connect.

Feature	Description
Source Name	Displays the source name based on the selected icon: • ECAT • INCIDENTS • ALERTS • LISTS • LIVE CONNECT
Sort	Provides a drop-down of sort options for the listed context information. Possible sort options are Severity - High to Low, Severity Low to High, Date - Oldest to Newest. and Date - Newest to Oldest. The sorting options vary by source type.
	Refreshes the lookup results.
n items (First n Results)	The footer provides a count of the total number of results, and the count of results currently displayed. For example, 50 Alerts (First 50 Alerts).

Lookup Results

The Context Lookup panel displays the following information when retrieving the context data from different configured sources:

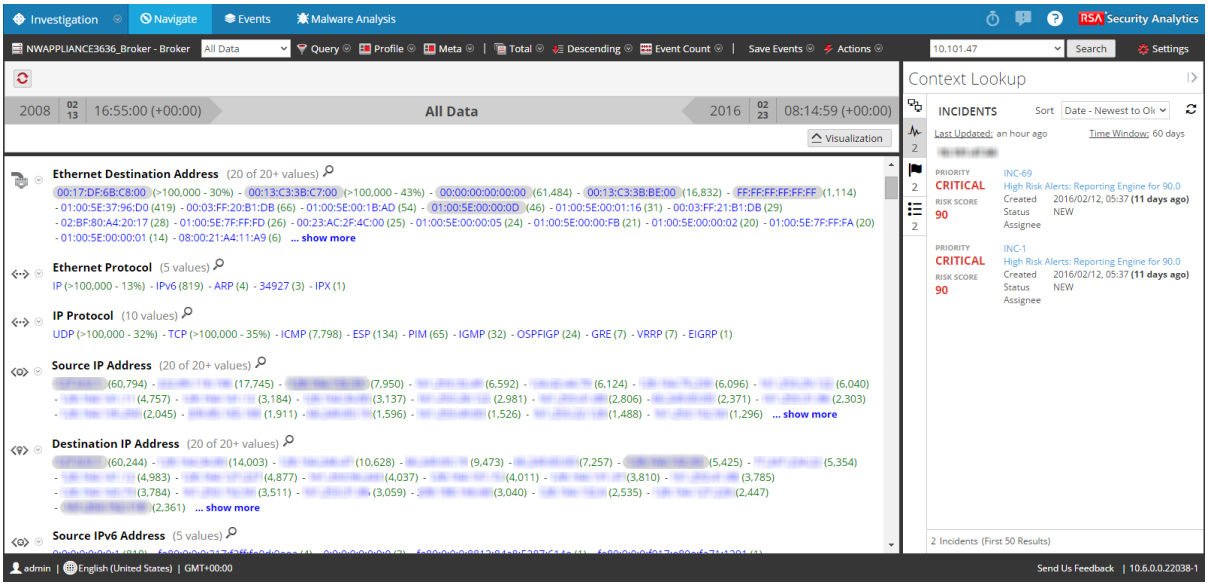
Incidents

Incidents are displayed based on time first (Newest to Oldest) and then priority status. The following information is displayed for incident lookups:

- Incident Name and ID
- Priority status of the incidents
- Risk Score value of the incidents
- Date when the incident was created
- Status of the incident
- Assignee for the incident

- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Time window: This is based on the value that is set for the "Query Last" field in the Configure Responses Dialog.
- Sort: This drop-down field provides option to change the sorting of result based on time or priority.

The following figure is an example of lookup results for Incidents.



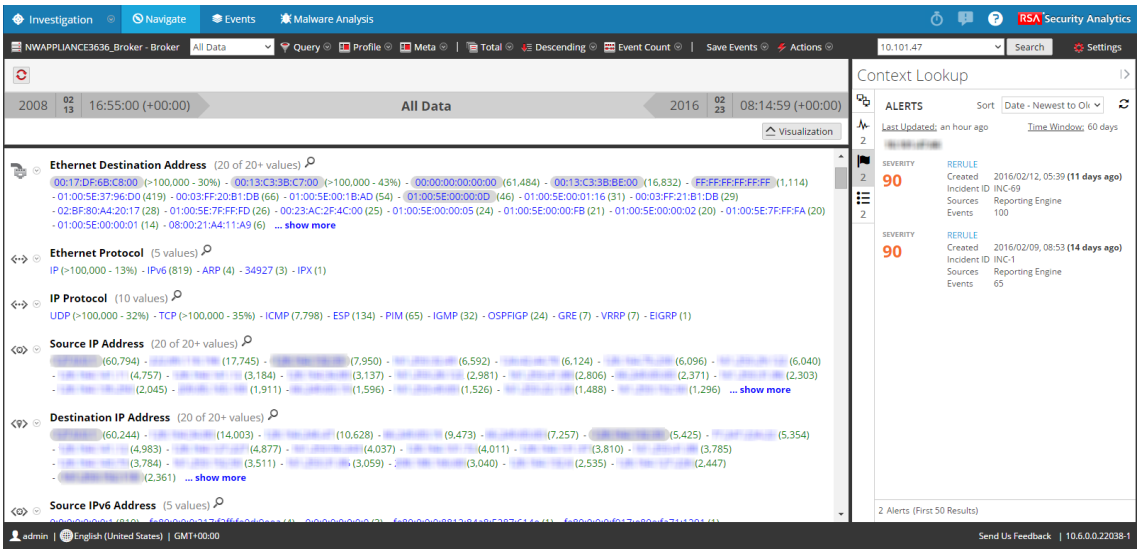
Alerts

Alerts are displayed based on the Severity. The following information is displayed for alert lookups:

- Alert Name
- Severity value of the alerts
- Date when the alert was created
- Incident ID: This is the ID of the incident that the alert is associated with (If any).
- Sources: Event source name
- Number of events associated with the alert.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.

- Time window: This is based on the value that is set for the "Query Last" field in the Configure Responses Dialog.
- Sort: This drop-down field provides option to change the sorting of result based on time or priority.

The following figure is an example of lookup results for Alerts.

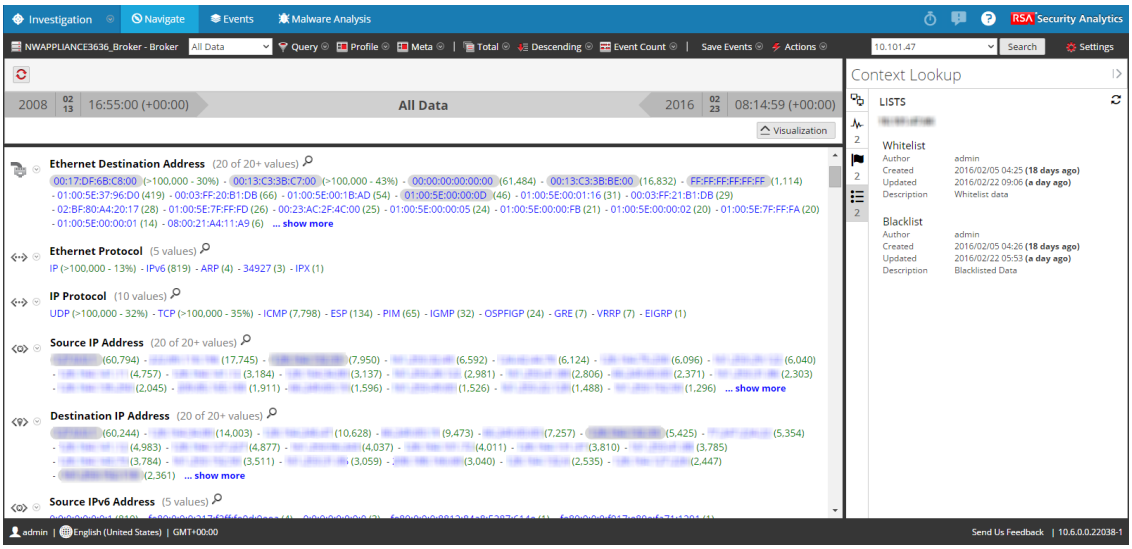


Lists

The following information is displayed for list lookups.

- List Name
- Owner who created the list
- Created Date
- Last Updated Date
- Description of the list

The following figure is an example of lookup results for Lists data source.



ECAT

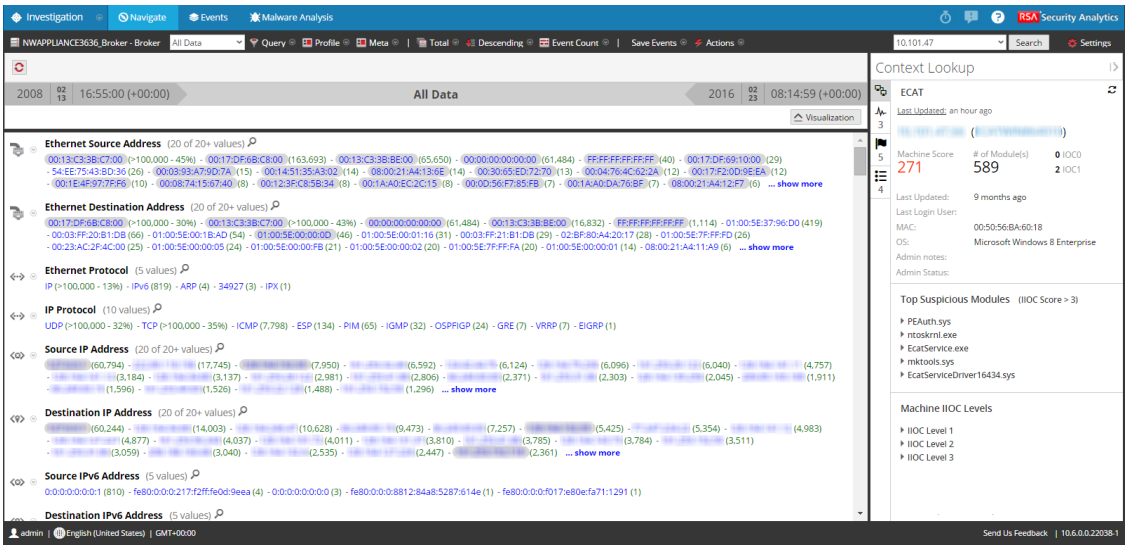
The following information is displayed for ECAT lookups.

- Machine name and IP address of the machine.
  By clicking on the IP or ECAT machine name, you will be navigated to ECAT UI to perform further investigation.
- Last Updated: Indicates when contextual data was last fetched from data source and updated to cache.
- Machine Score: A machine IIOC score is aggregated based on the module scores.
- Number of modules: Number of active files for the selected machine.
- Last Updated: Indicates when the scan results were last updated in ECAT database.
- Last Login User
- Machine MAC Address
- Operating System Version
- Admin Notes (if any)
- Admin Status (if any)
- Top Suspicious Modules (Modules that has IIOC score > 500). This is based on the value set for "Minimum IIOC Score" field in the Configure Responses Dialog. The default value for

"Minimum IIOC Score" is 500.

- Machine IIOC Levels

  The following figure is an example of lookup results for ECAT data source.

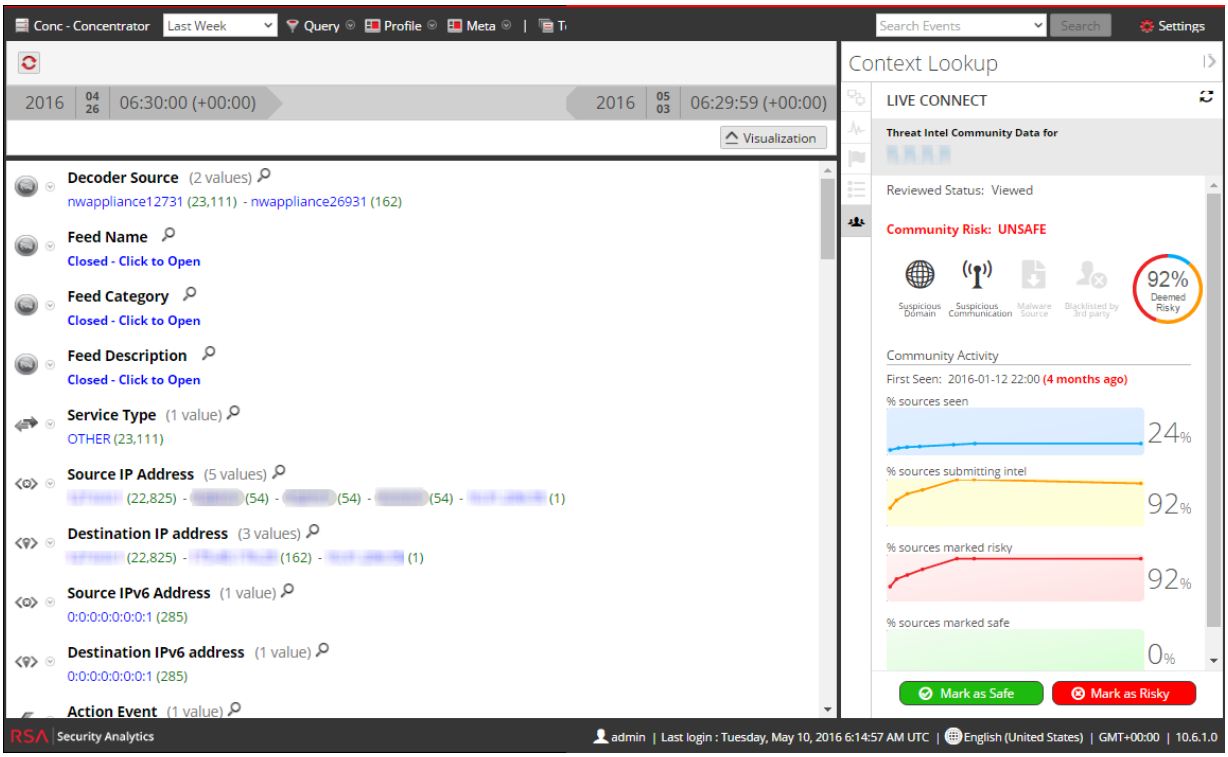


Live Connect

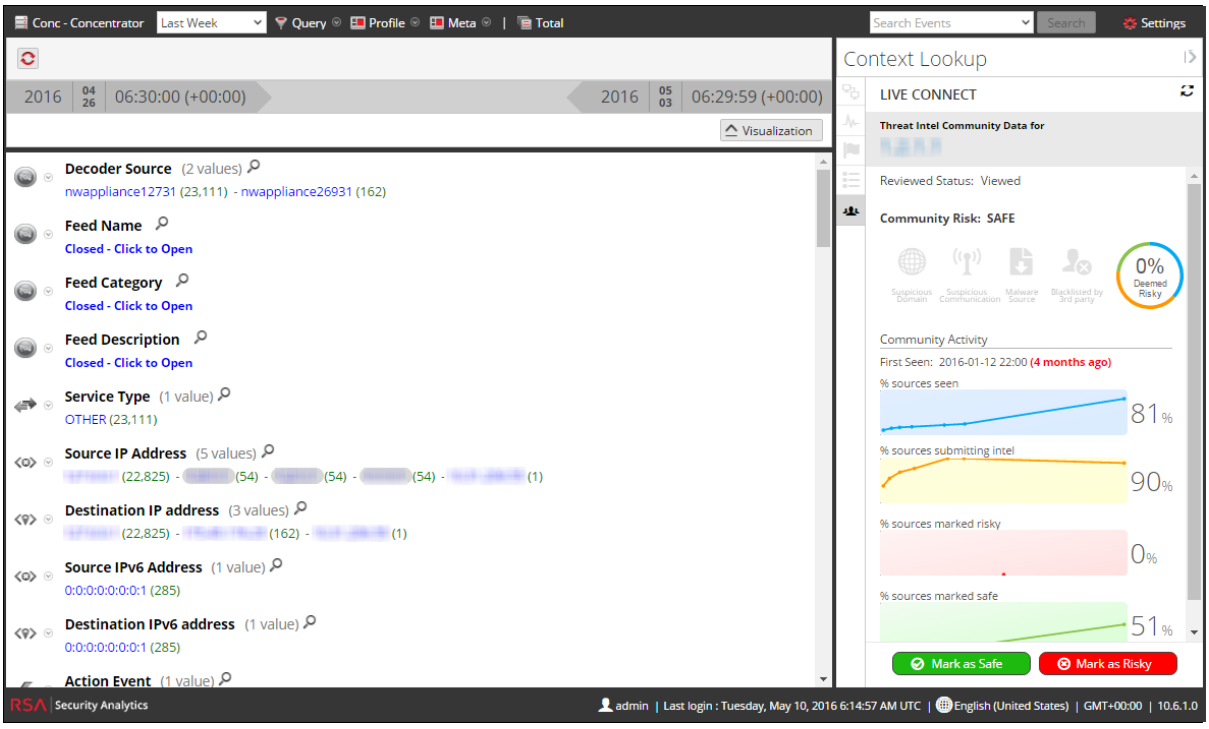
For Live Connect, context lookup is supported only for IP meta type (device.ip, ip.src, ip.dst, paddr, ip.addr, alias.ip). The IP addresses that has live connect data can be identified by using the in-line indicator when you hover the mouse over highlighted IP addresses.

The following figures are examples of lookup results for IP address with live connect data.

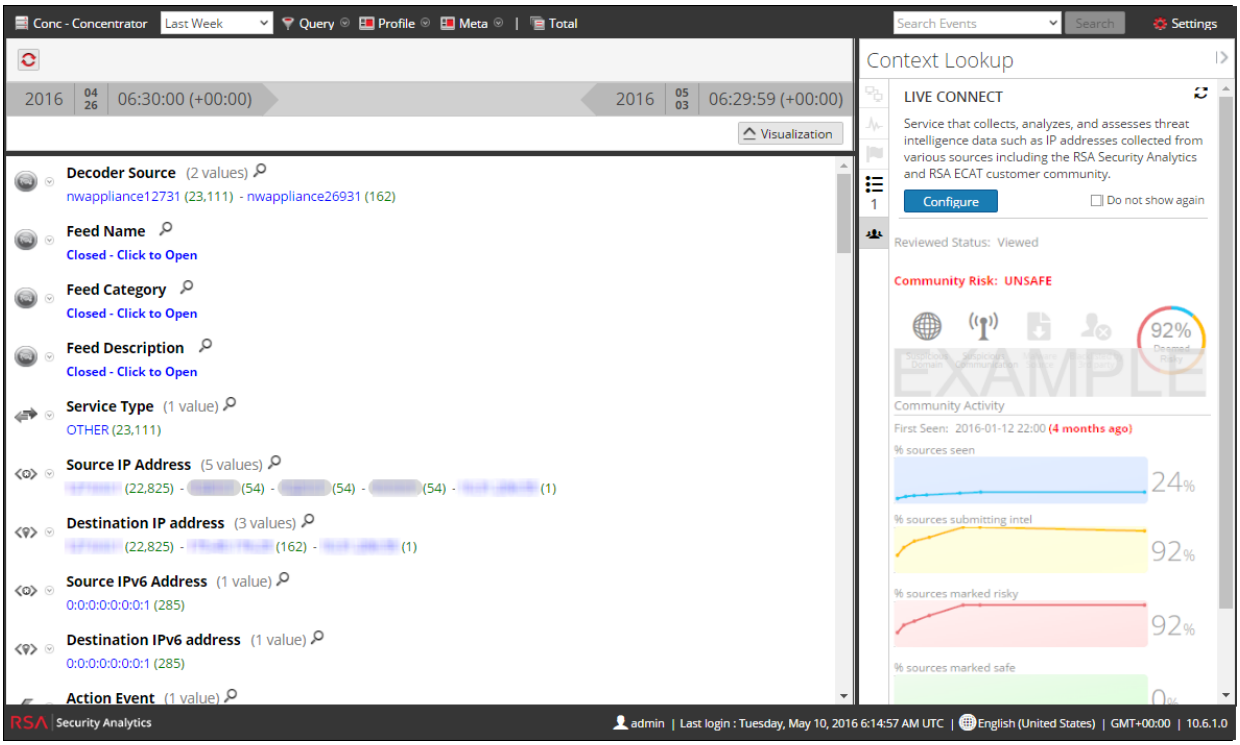
Sample 1:



Sample 2:



Sample 3:



Sample 3 is an example of Context Lookup panel when Live Connect is disabled. To enable Live Connect data source, go to **Administration > Systems > Live Services** and enable **Threat Insights** in **Additional Live Services** section. For more information, see Configure Live Connect Data Source for Context Hub.

Features

The Context Lookup panel has the following controls and features for Live Connect:

Field	Description
IP Address	Displays the IP address for which the lookup results are displayed.

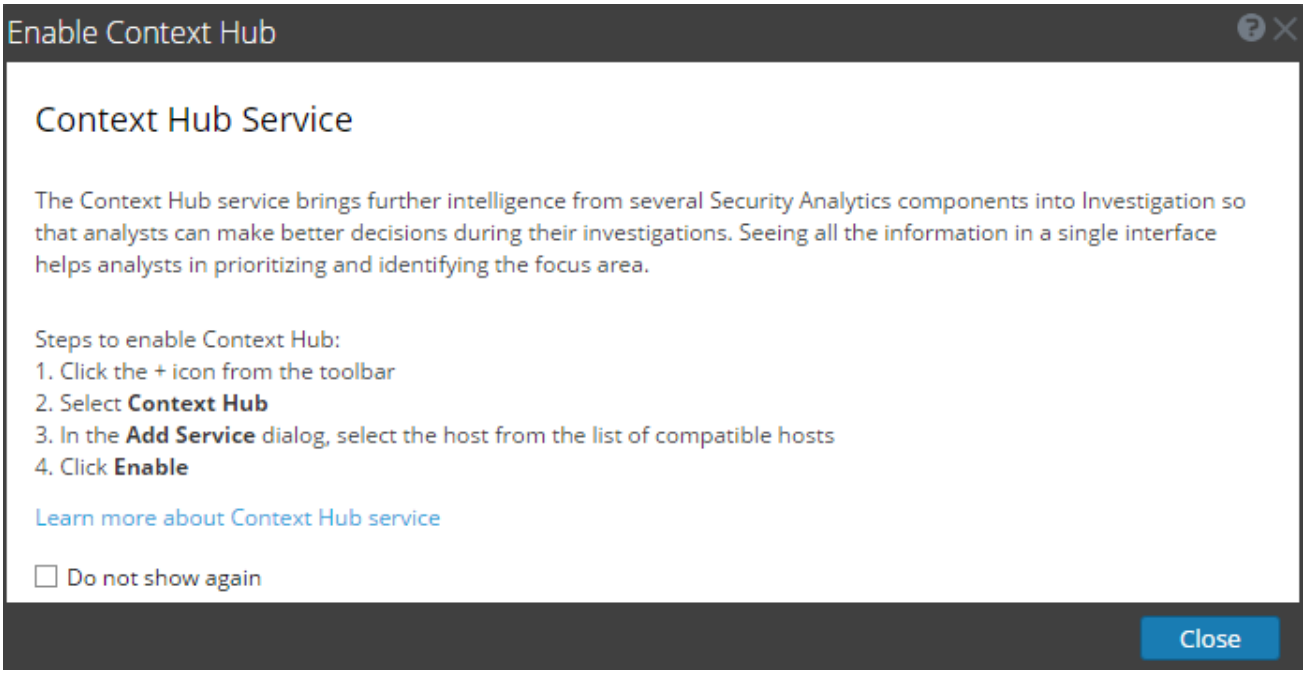
Field	Description
Reviewed Status	Displays the reviewed status of the IP address based on the analyst activity. This gives the visibility of the analyst activity within an organization. Below are the types of status: • **New:** If lookup results for an IP address is viewed for the first time within the organization. • **Viewed:** If any analyst within the organization has already viewed the lookup results for an IP address. • **Marked as Safe:** If any analyst within the organization has already viewed the lookup results and marked the IP address as safe. • **Marked as Risky:** If any analyst within the organization has already viewed the lookup results and marked the IP address as risky.
Community Risk Rating and Reasons	Displays the community risk rating for an IP address such as: • **Safe:** An IP address is marked as "Safe" if it is considered safe based on the Live Connect analysis and analyst feedback. • **Unknown:** The risk rating for an IP address is displayed as "Unknown" if there is no enough information to calculate the risk rating. • **Unsafe:** An IP is rated unsafe if it is associated with one or more of the following community risk reasons: ◦ Suspicious Domain ◦ Suspicious Communication ◦ Malware Source ◦ Blacklisted by 3rd Party The risk reasons are represented by appropriate icons. The icons appear normal if it is matched with the IP, else its grayed out.

Field	Description
Community Activity	If the IP address is known within the RSA community, a graphical representation of the community activity trend is displayed for the following: • Users (in %) who have viewed the IP address in the Live Connect community over time. • Users (in %) who submitted feedback for the IP address. • Users (in %) who marked the IP address as risky over time. • Users (in %) who marked the IP address as safe over time.
Community Activity Statistics	Community activities such as: • Date first seen in the community. • Time since the IP was seen for the first time (Current time - First seen time). • A Pie chart based on the community activity trend graph. The pie chart shows the correct breakdown of the % of Live Connect customers that have seen the IP (blue), the % who have submitted feedback (yellow), the % who marked risky (red), and the % who have marked safe (green). The number in the middle of the chart reflects the percent who have marked the IP as risky.
IP Rating Feedback	Provides an option for the analyst to give feedback on the IP address if the IP address was already known within the RSA Community. The options are: • Mark as Safe • Mark as Risky Based on the feedback, the "Reviewed Status" changes to "Marked as Safe" or "Marked as Risky".

Enable Context Hub Dialog

This topic provides technical details of **Enable Context Hub** dialog.

When you navigate to the **Administration > Services panel**, if Context Hub service is not enabled, the **Enable Context Hub** dialog appears.



To enable Context Hub service, follow the steps provided in the **Enable Context Hub** dialog or see Step 1. Add the Context Hub Service.

If you do not want this dialog to appear without enabling Context Hub service, click **Do not show again**.

Troubleshooting

This topic provides information about possible issues that Security Analytics users may encounter when setting up their Context Hub service in Security Analytics.

Possible Issues

Problem	Solutions
Creation of database fails during installation or DB gets corrupted.	Manually run the script `mongoDbConfig.sh` located at **/opt/rsa/context/bin**
With ECAT 4.1.1, ECAT feed does not work for Security Analytics.	You must use ECAT 4.1.1.1 for the feed to work.