NetWitness® Platform XDR

Version 12.3.0.0

Context Hub Configuration Guide

NETWITNESS
Platform XDR

Contact Information

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

Trademarks

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

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

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

Note on Encryption Technologies

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

Distribution

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

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

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

Miscellaneous

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

September, 2023

Contents

How Context Hub Works

Context Hub service provides enrichment lookup capability in the Respond and Investigate views. An Administrator can configure the Context Hub service and the data sources to enable an Analyst to perform the context lookup for the required data sources.

By default, the Context Hub service supports enrichment lookups for meta types such as IP address, User, Domain, MAC address, File Name, File Hash, and Host.

The following data sources are supported by NetWitness and provide enriched data when configured.

Lists- Provides contextual information from a list of blacklists, whitelists, or watchlists.

RSA Archer- Provides Criticality information of a device or specific asset based on the IP or Host which needs constant monitoring.

Active Directory - Provides contextual information of a user to help determine if the user is suspicious or not.

RSA NetWitness Endpoint - Provides context information for endpoint module and machine indicators and to help determine if any of the Endpoint devices are compromised.

Respond- Provides contextual information of a specific meta available in respond and enables analyst to respond faster based on context data.

File Reputation Server - Provides contextual information for reputation status of files.

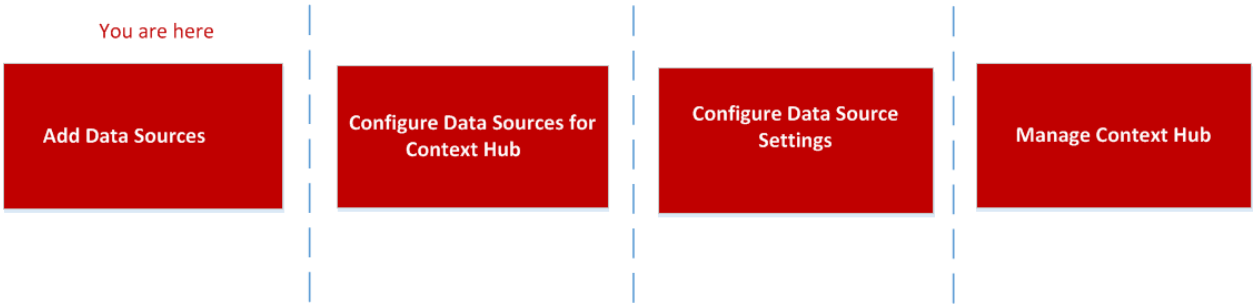
STIX - Provides contextual information on IP address, email address, domain, filename, URL, and file hash from STIX sources.

REST API - Provides contextual information for any accessible web service with an exposed REST API.

Overview of Context Hub Configuration

The Administrator needs to perform each step in the proper sequence to configure the services to perform the context lookup effectively. In the **(Admin) > Services**. Services Config view of Context Hub service, an administrator can configure data sources for Context Hub Service. The administrator can also configure Context Lookups for custom meta keys, if required and also import lists or export lists.

The workflow below describes how the Context Hub service can be configured:



Context Hub service is pre-installed on primary ESA host, and automatically added to the NetWitness.

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

Configure Lists as a Data Source

Lists as a Data Source use the Context Hub service to fetch contextual information for 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 lists such as blacklisted IPs, whitelisted IPs, and so on. The lists can contain supported entities such as IP address, MAC address, User name, Host name, Domain name, File name or File hash. You can import a single-column list or a multi-column list from the Data Source tab. Additionally, all feeds (except STIX feeds) that are created are converted to lists and displayed on the context lookup. If Context Hub is not configured or the service is down, then the feeds will be made available whenever Context Hub is up and running. For more information on creating feeds, see the *Live Services Management Guide*.

Note: When you create a feed, a list is automatically generated with the same name as the feed. If the list name already exists, then the name of the new list is suffixed with the number '2". For example if the existing feed name is test1.csv, then the new list will be named as test2.csv.

List values are in CSV format available in an external location and can be accessed through the following two methods:

- **Local File Store**: You can share a file from a local location.
- **HTTP(S)**: You can share a file using a web server location.

Note: You can also set up recurring job to fetch data on regular intervals by using the Prefetch settings while configuring meta mapping.

Prerequisites

Before you configure Lists data source, ensure that:

- User should have admin permissions.
- Context Hub service is available in  **(Admin) > Services** view of NetWitness.
- If you are using Local File Store or HTTP(S) server, the path mentioned should contain the CSV file In case of remote Local File Store, the file must be mounted or placed on the local drive location `/var/lib/netwitness/contexthub-server/data`.
- The NetWitness user must have read permission to access the file.

Caution: If you are creating a Context Hub list for use as an enrichment source in ESA, the list name cannot include any spaces or special characters, or start with a number. If you do not follow this naming convention, when you attempt to add the list as an enrichment source in ESA, an error message will be displayed and you will not be allowed to add the list.

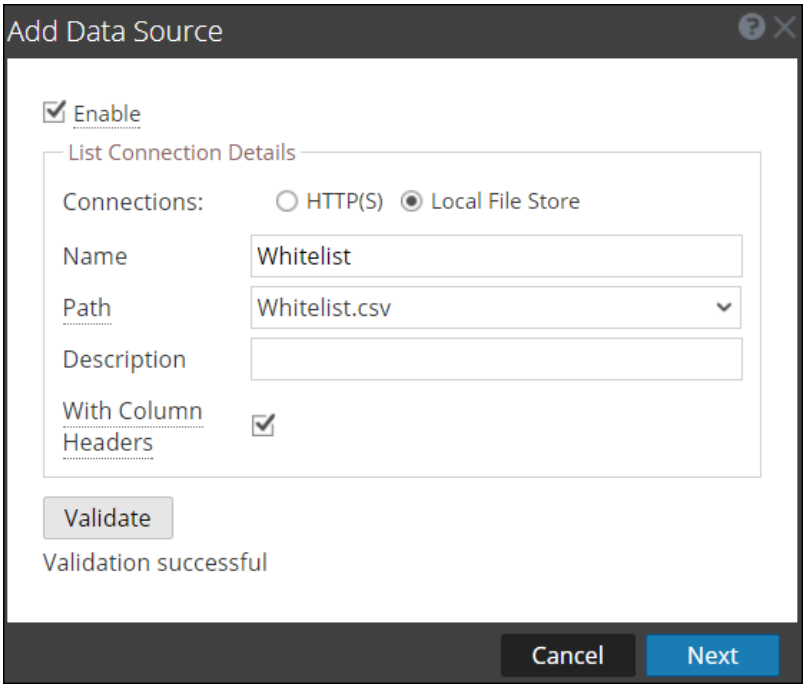
Add List data source using Local File Store

To add a List as a data source:

1. Go to **(Admin) > Services**.
   The services view is displayed.
2. 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 > **LIST**.
   The **Add Data Source** dialog is displayed.
4. By default, the **Enable** checkbox is selected. If this option is unchecked, the Next button is disabled, you cannot add the data source, view the list in the list tab and view the contextual information.
5. By default, the Context Highlighting checkbox is enabled. This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub.

Note: You can disable the context highlighting globally in the Context Hub explorer view. After you disable this option, the entity values for all the data sources configured will not be highlighted if there are any contextual information.

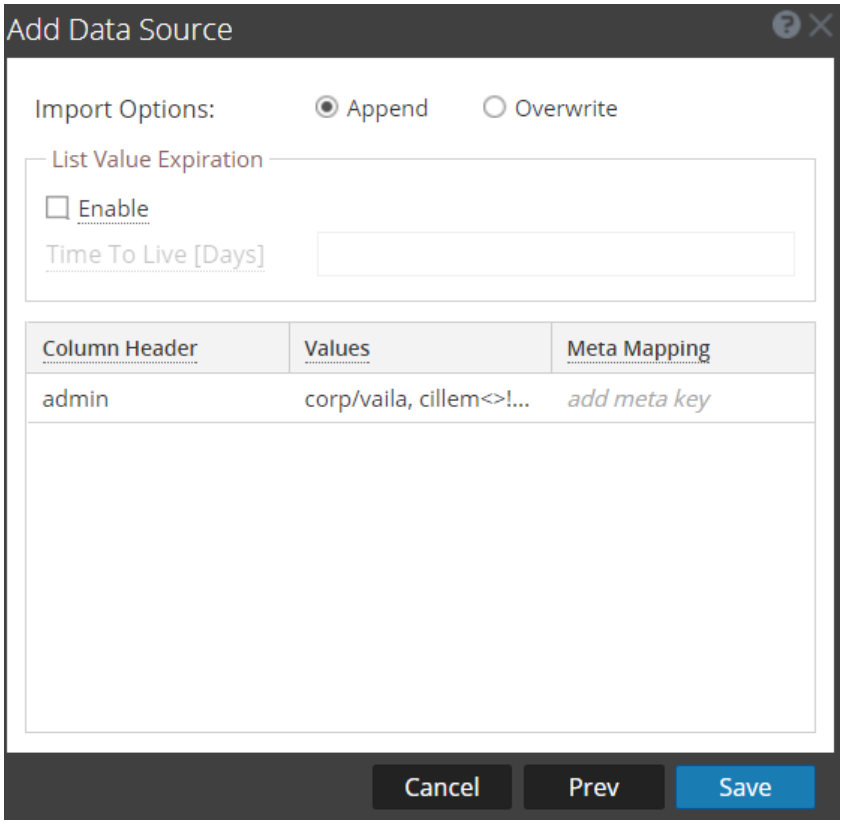
6. Select the **Local File Store** Connection Type.



7. Provide the following database connection details. Enter the following fields for Local File Store Connection Type:
   - **Name:** Provide a name for the list data source.
   - **Path:** This field displays all the data files available in the data folder `/var/lib/netwitness/contexthub-server/data`, where context hub service is running. Select the file name from the drop-down.
     A maximum of 32 columns of CSV file are supported that adhere to the RFC1480 standards.
   - (Optional) **Description**: Add a description for the selected file.
   - **With Column Headers**: Select this option to consider the first row as column headers from the CSV file. If you don't select this option, you need to enter the column headers in the next screen.
8. Click **Validate**.

   If the validation fails, you cannot add the data source.
9. Click **Next**.

   The next dialog is displayed.



10. Select any one of the following options:
    - **Append** - Select this option to add the imported values to an existing list.
    - **Overwrite** - Select this option to replace the values in an existing list with the imported values.
11. In the **List Value Expiration** section, the **Enable** option is unchecked, by default. If you want to store the looked up list values in the cache for a specified number of days then select the **Enable**

checkbox and enter the number of days in the **Time to Live (days)** field for the list values to be retained.

12. In the next screen, map at least one meta key with one or more meta types by mapping a column header with a meta. The description for each field is as follows:
    - **Column Header**: Display headers of the CSV file which must be mapped to a meta type.
    - **Meta Mapping**: Maps a column header field to a meta type.
    - **Values**: Displays the first three values from the imported list.
13. Click **Save**.

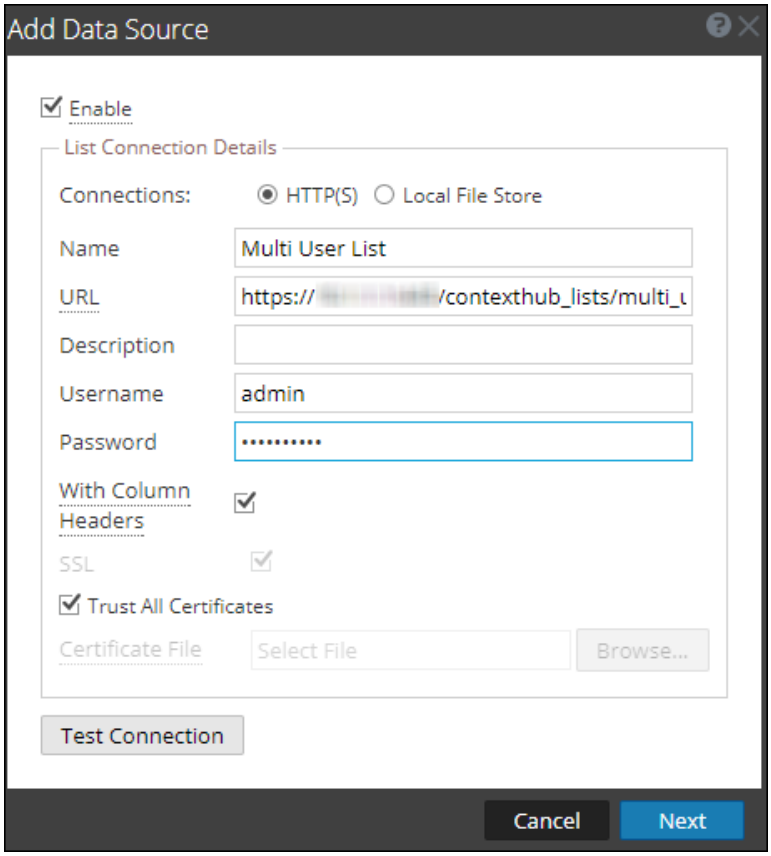
Add List data source using HTTP(S)

To add List as a data source:

1. Select  **(Admin) > Services**.
   The services view is displayed.
2. 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  > **LIST**.
   The **Add Data Source** dialog is displayed.
4. By default, the **Enable** checkbox is selected. If this option is unchecked, the Next button is disabled, you cannot add the data source, view the list in the list tab and view the contextual information.
5. By default, the Context Highlighting checkbox is enabled. This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled.

Note: You can disable the context highlighting globally in the Context Hub explorer view. After you disable this option, the entity values for all the data sources configured will not be highlighted if there are any contextual information.

6. Select the HTTP(S) Connection Type.

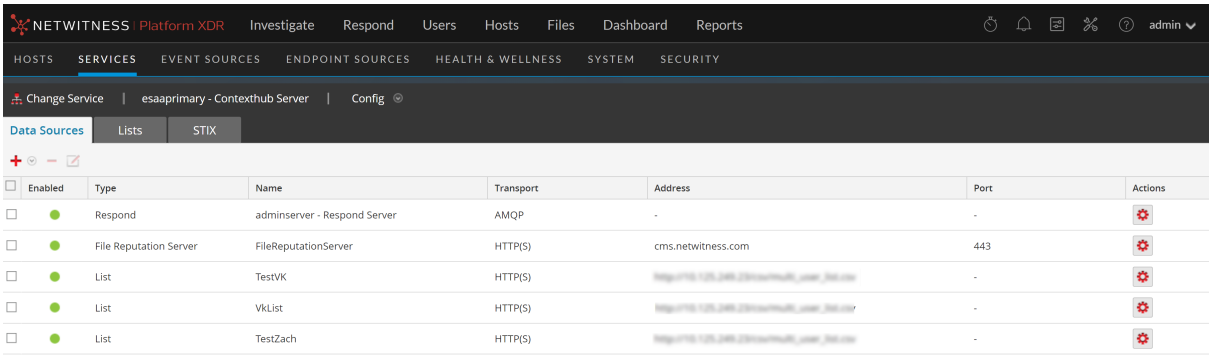


- Enter the following fields for HTTP(S) Connection Type:
  - **Name:** Provide a name for the list data source.
  - **URL**: Enter the path of the CSV file available on the HTTP(S) location along with the host name or IP address of the remote machine where the list is stored. The URL must be of the format: `https://<Hostname or IP-address of the HTTP(S)server>:<Port on which the HTTP(S) server is hosted>/<Absolute path of CSV file>`. For example, `https://10.1.1.1:443/contexthub_lists/multi_user_list.csv`
  - (Optional) **Description**: Add a description for the selected file.
  - (Optional) **Username:** Enter the username to connect to the HTTP(S) server requires basic authentication.
  - (Optional) **Password:** Enter the password to connect to the HTTP(S) server requires basic authentication.
  - **With Column Headers**: Select this option if you want to import a CSV file with headers. If this option is selected and you import the CSV without headers, the first row will be considered as a header which can be edited.
  - **SSL:** If you enter a URL with HTTPS in this field, then this is selected automatically. If you enter a URL with HTTP, then this checkbox is unselected.

- **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid .cer or .crt format HTTP (S)server certificate for the connection to be successful.

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

   List is added as a data source for the configured Context Hub and is displayed in the **Data Sources** tab.



Next Steps

- Add, edit, or remove values from a specific list.
- Configure the data source settings to determine the data source fields to be displayed in the Context panel. For instructions, see Configure Context Hub Data Source Settings .
- Import and export a list. For more information, see Import or Export Lists for Context Hub.
- View the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *RSA NetWitness Respond User Guide* and *RSA NetWitness Investigate User Guide*.

Configure Archer as Data Source

You can configure Archer as a data source for Context Hub and use the Context Hub service to fetch contextual information from Archer. Use the procedures in this topic to add Archer as a data source for Context Hub service and configure the settings (if required) for Archer.

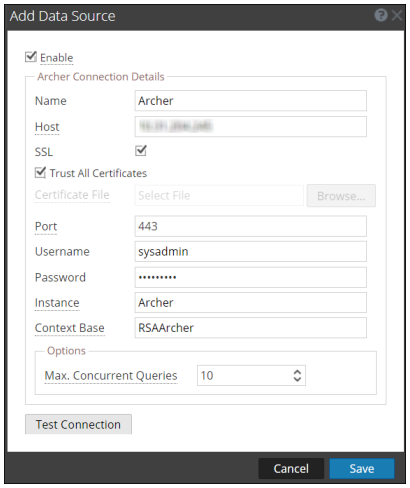
Prerequisites

Before you configure Archer data source, ensure that:

- Context Hub service is available in **(Admin) > Services** view of NetWitness.
- Archer is installed with Licensed Devices application.

To add Archer as a data source for Context Hub:

1. Go to **(Admin) > Services**.
   The Services view is displayed.
2. Select the Context Hub service, and click > **View** > **Config**.
   The Services Config view is displayed.
3. In the **Data Sources** tab, click > **RSA Archer**.
   The **Add Data Source** dialog is displayed.



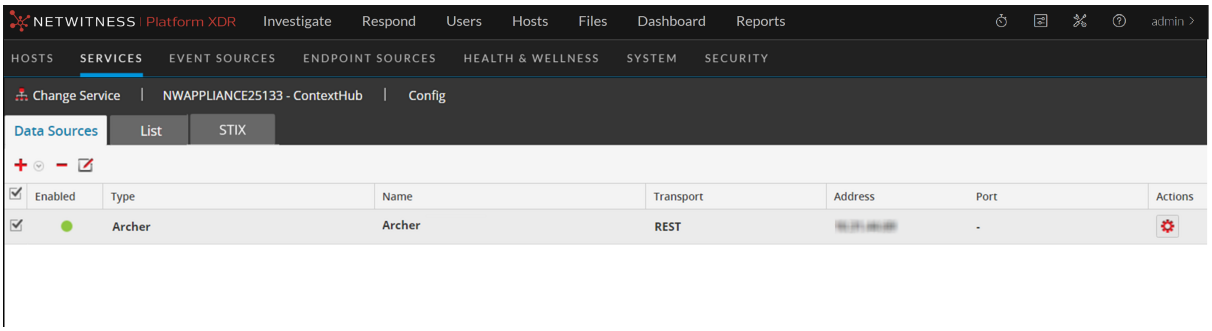
4. Provide the following information:
   - By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
   - **Context Highlighting**: This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled.

Note: You can disable the context highlighting globally in the Context Hub explorer view. After you disable this option, the entity values for all the data sources configured will not be highlighted if there are any contextual information.

- Enter the following fields:
  - **Name**: Enter a name for Archer data source.
  - **Host**: Enter the hostname or IP address where Archer server is installed.
  - **SSL**: By default this option is selected and enables SSL communication to Archer .
  - **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid Archer server certificate for the connection to be successful.
  - **Port**: The default port is 443.
  - **Username**: Enter the Archer Server username.
  - **Password**: Enter the Archer Server password.
  - **Instance**: Enter the Instance name from which you want to extract data. An RSA Archer instance is a single set up that includes unique content in a database, the connection to the database, the interface, and log-in. You might have individual instances for each office location or region or for development, test, and production environments. The Instance Database stores the RSA Archer content for a specific instance.
  - **Context Base**: Enter the virtual directory name where the files are stored. For example, rsaarcher located at the RSA Archer web address https://archer.company.com/**rsaarcher**/default.aspx. If the files are stored in the IIS default web address https://archer.company.com/default.aspx, then this field must be empty.
  - **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 Archer data source.
6. Click **Save**.

   Archer is added as a data source for Context Hub and is displayed in the **Data Sources** tab.



After adding the data source, you can configure data source settings. For instructions, see Configure Context Hub Data Source Settings . And View the contextual data in the Context Summary Panel of the Respond view or Investigate view. For instructions, see the *NetWitness Respond User Guide* and *Investigate User Guide*.

Configure Archer Data Source

After you have configured the required data sources you can customize the settings for the data sources based on your requirement.

To access and configure settings:

1. Go to **(Admin) > Services**.

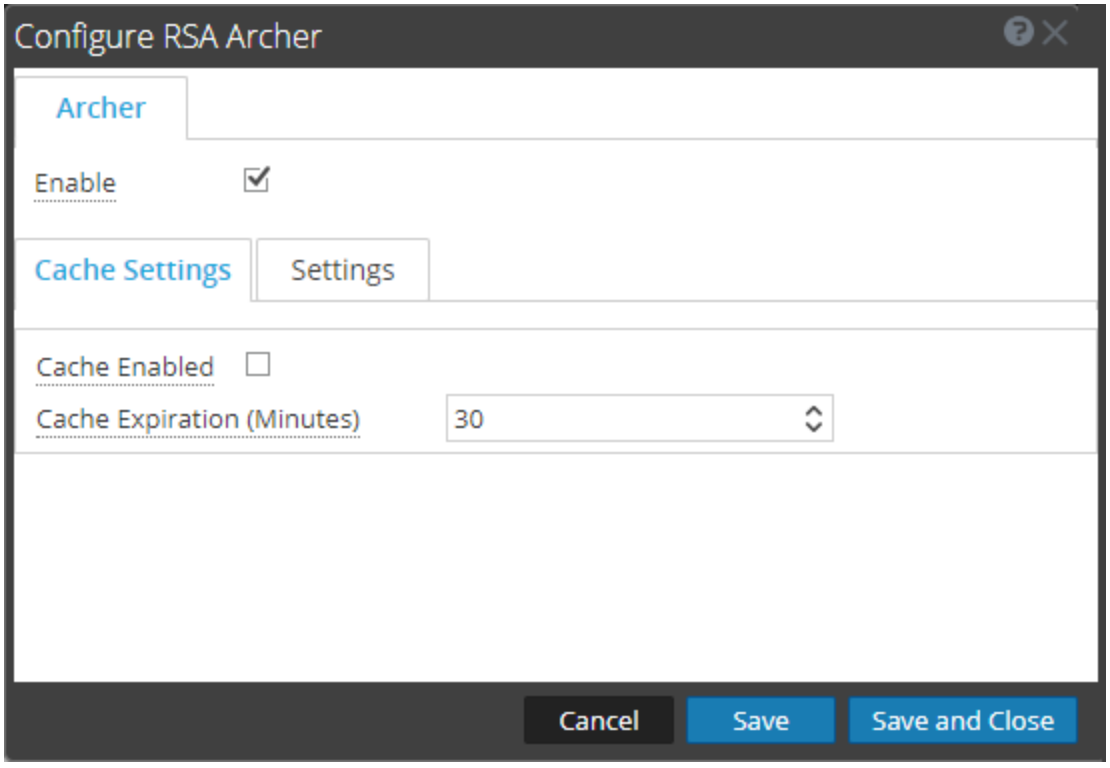
   The services view is displayed.

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 for which you want to configure the settings and click in the Actions column.

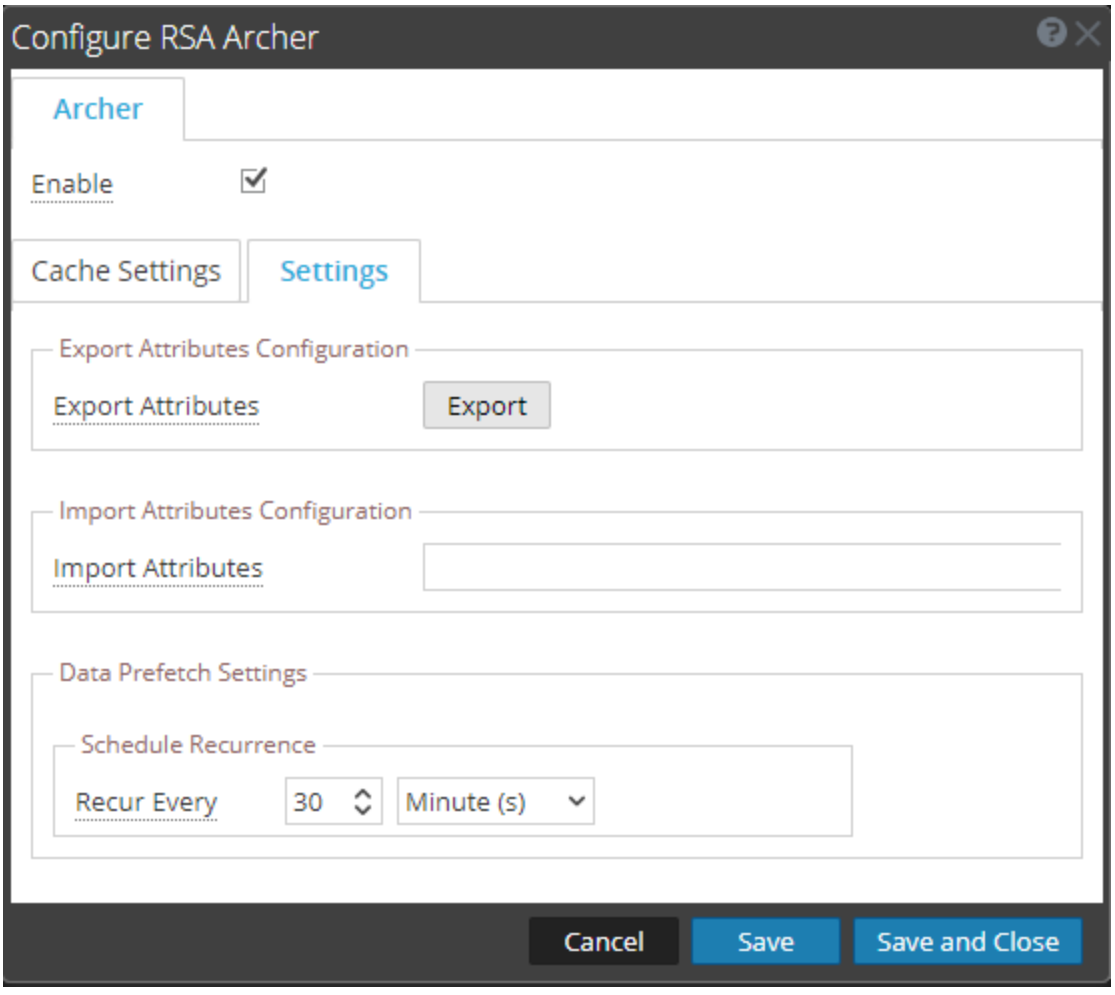
   The following screenshot is an example of the Configure RSA Archer dialog:



4. In the **Settings** tab. Configure the following fields:

Field	Description
Enable	This option is enabled by default (checked) and can be used to enable or disable the response from the selected data source.
Cache Settings	Any lookup from Context Hub can be stored in the Context Hub cache for a configured time. Response to any subsequent matching request will be fetched from the Context Hub cache. Use this section to define the following cache settings for query lookup: • **Cache Enabled**: By default, this checkbox is selected and the query response is cached. • **Cache Expiration (Minutes)**: The maximum time the query lookup is retained in cache. The default time is 30 minutes and maximum is 7200 minutes that you can configure.

5. Click **Cache Settings**. Configure the following fields.



Field	Description
Export Attributes Configuration	In **Settings**, **Export Attributes Configuration**, click **Export** to export the Archer Attributes Configuration. These are the attributes visible in Context Lookup while viewing Archer details for a IP, Host, or Mac. A JSON configuration file gets downloaded and the order of the attributes in sync with the listing in the context panel is maintained in the JSON file.
Import Attributes Configuration	If you want to update or edit the configuration settings, in **Settings**, **Import Attributes Configuration**, click **Browse**. Select the JSON file containing the configuration attributes. The attributes appear in the Context Lookup panel when a user views the context, in the order which they were imported. **Note:** You can backup the previous attributes before importing any changes made to existing attributes.
Data Prefetch Settings	In **Settings**, **Data Prefetch Settings** helps prefetch the data. Configure the **Schedule Recurrence** to provide data faster when you hover over the intended entity in Respond.
Schedule Recurrence	In the **Recur Every** field, enter a value or use the drop-down to configure the recurrence for prefetch. The default time duration can be selected from the drop-down list for configuring the duration of recurrence. Available values are minutes, hours, days, or weeks.

6. Click any one of the following options:

- **Cancel** - select this option to cancel the changes.
- **Save** - select this option to save the changes.
- **Save and Close** - select this option to save and close the dialog.

Note: After you configure the data source settings, you can configure the Context Hub configuration parameters by navigating to  **(Admin) > Services**> **View** > **Explore** view. Make sure you restart the Context Hub service if you make any configuration changes in the Explore view.

Configure Active Directory as a Data Source

You can configure Active Directory (AD) as a data source for Context Hub using LDAP and use the Context Hub service to fetch contextual information from AD. Use the procedures in this topic to add AD as a data source for Context Hub service and configure the settings(if required) for AD.

Prerequisites

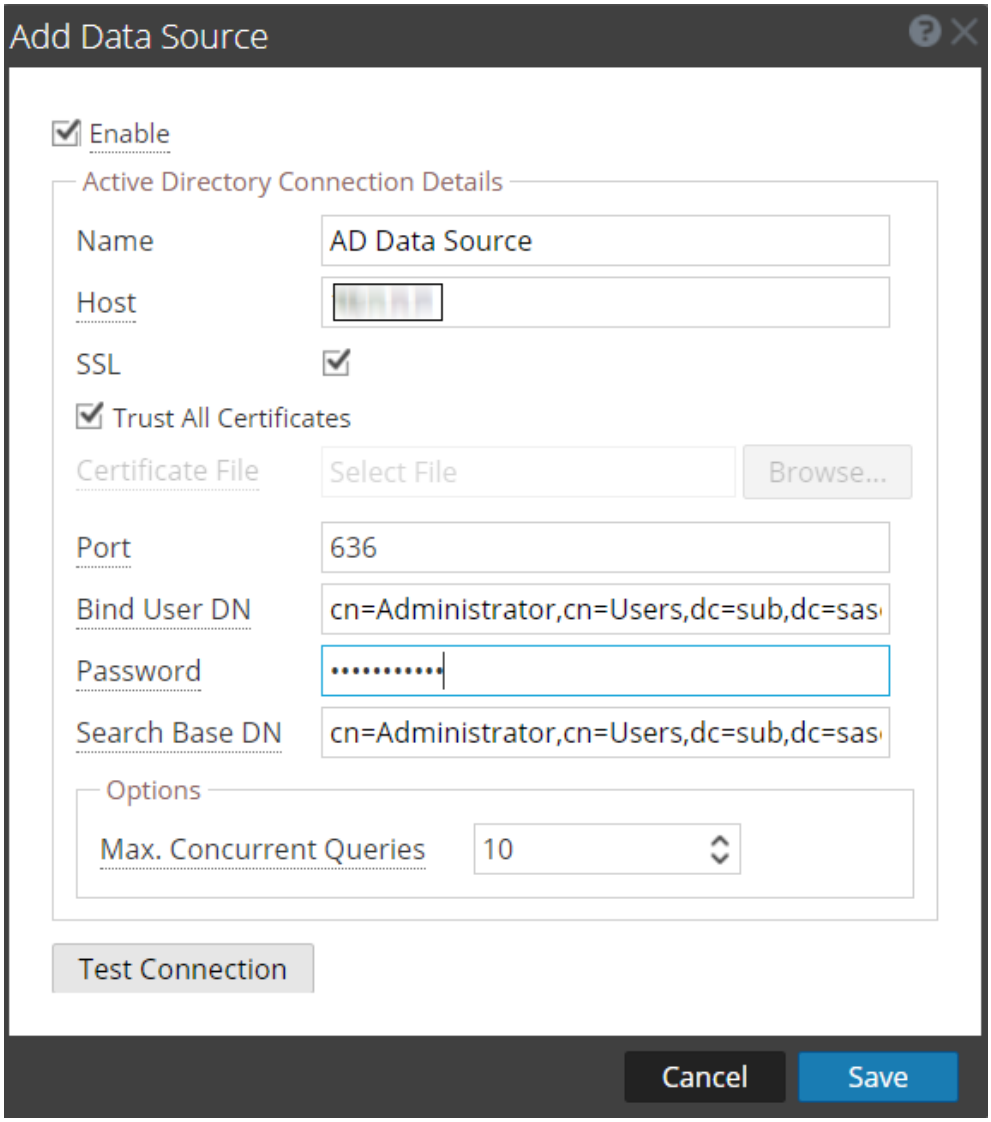
Before you configure Active Directory data source, ensure that:

- Context Hub service is available in **(Admin) > Services** view of NetWitness.
- AD is available and is running on Windows versions 2003, 2008, and 2012 are supported.

To add AD as a data source for Context Hub:

1. Go to **(Admin) > Services**.
   The services view is displayed.
2. 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 + **> Active Directory**.
   The **Add Data Source** dialog is displayed.



You need to configure the Active Directory schema to replicate the following attributes to view the data in the Respond page:

- Employee ID
- Department
- Company
- Title
- Postal Code

All the other attributes replicate automatically.

4. Provide the following database connection details:

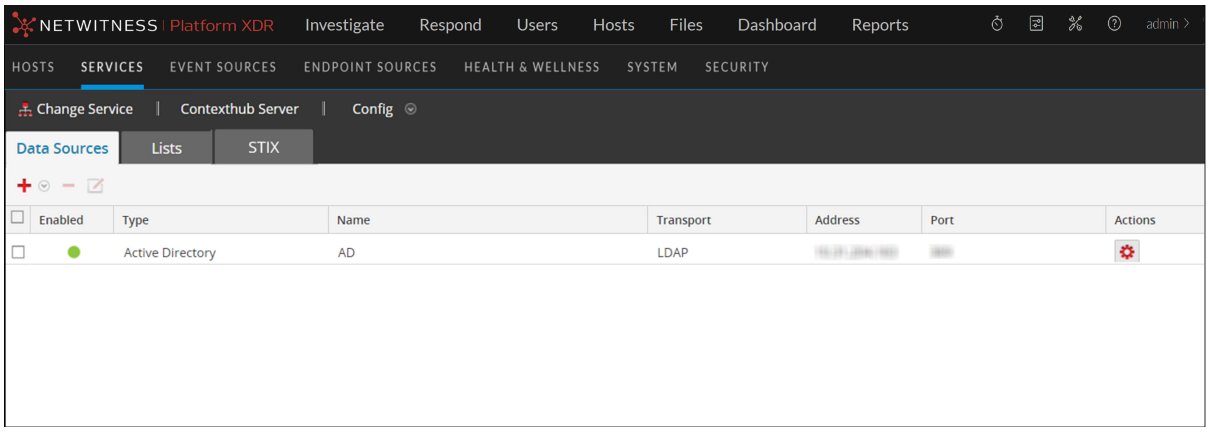
- By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
- Enter the following fields.
  - **Name:** Enter a name for the AD data source.
  - **Host:** Enter the host name or IP address of the AD.
  - **SSL:** By default this will be checked with 636 port number which will connect to the data source using Secure Sockets Layer (SSL) connection.
  - **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid .cer or .crt format Active Directory server certificate for the connection to be successful. If you add multiple AD data sources with ssl, you should configure all the data sources with either a valid certificate or a Trust All Certificates.
  - **Port:** The default port is 636 with SSL and 389 without SSL.
    If you want to fetch data from multi-domains you can configure a single data source with the Global catalog port (3269 with SSL or 3268 without SSL).

    Alternately, for multi-domain, you can configure a single data source for each domain with the default port (389 with SSL or 636 without SSL).

    Multi-forest is a collection of multi-domains. If you want to fetch data from multi-forest you need to configure each forest with the Global catalog port (3269 with SSL or 3268 without SSL).
  - **Password:** Enter password of the user DN used to bind with AD.
  - **Bind User DN:** The distinguished name of the user that will authenticate to the search directory. For example, cn=Administrator,cn=Users,dc=sub,dc=saserver,dc=local.
  - **Search Base DN:** The base distinguished name, or base DN, identifies the entry in the directory from which searches are initiated; the base DN is often referred to as the search base. For example, dc=sub,dc=saserver,dc=local.

5. Click **Test Connection** to test the connection between Context Hub and the data source.
6. Click **Save**.
   AD is added as a data source for the configured Context Hub. The added AD data source is displayed

in the **Data Sources** tab.



After adding the data source, you can configure the data source settings. For instructions, see Configure Context Hub Data Source Settings .

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For instructions, see the **Navigate to Context Summary Panel and View Additional Context** topic in the *Investigate User Guide*.

Configure NetWitness Endpoint as a Data Source

You can configure NetWitness Endpoint as a data source for Context Hub and use the Context Hub server to fetch contextual information from NetWitness Endpoint. Use the procedures in this topic to add NetWitness Endpoint as a data source for Context Hub service and configure the settings (if required) for NetWitness Endpoint.

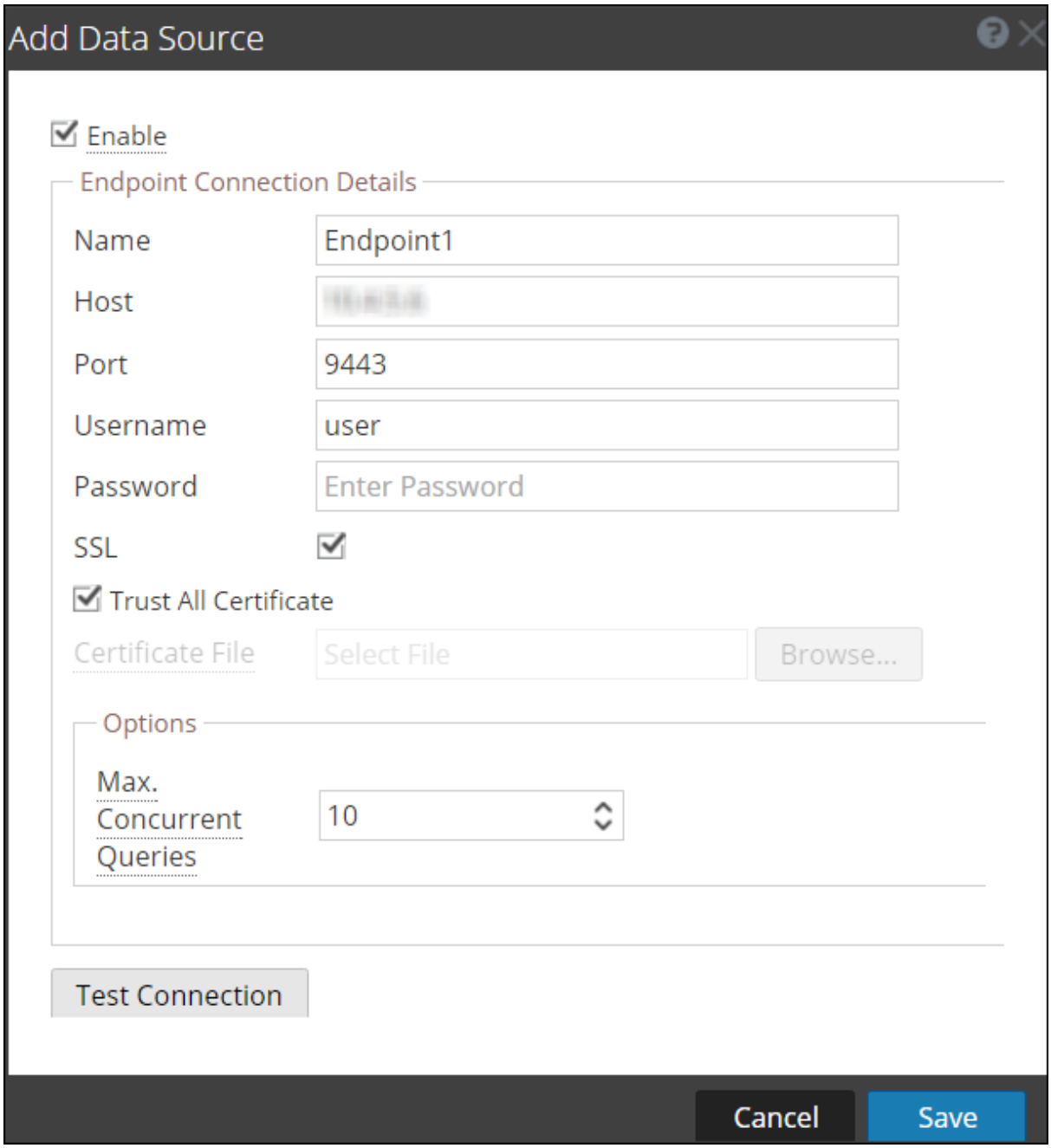
Prerequisites

Before you configure NetWitness Endpoint data source, ensure that:

- Context Hub service is available in  **(Admin) > Services**.view of NetWitness.
- NetWitness Endpoint (v4.1.1 to 4.3.0.5) is installed and configured.
  For more information on how to install, configure and for detailed information on NetWitness Endpoint, see the NetWitness Endpoint documents available at NetWitness Community.

To add NetWitness Endpoint as a data source for Context Hub:

1. Go to **(Admin) > Services**.
   The Services view is displayed.
2. Select the Context Hub service, and click > **View** > **Config**.
   The Services Config view is displayed.
3. In the **Data Sources** tab, click > **RSA Endpoint**.
   The **Add Data Source** dialog is displayed.



4. Provide the following information:

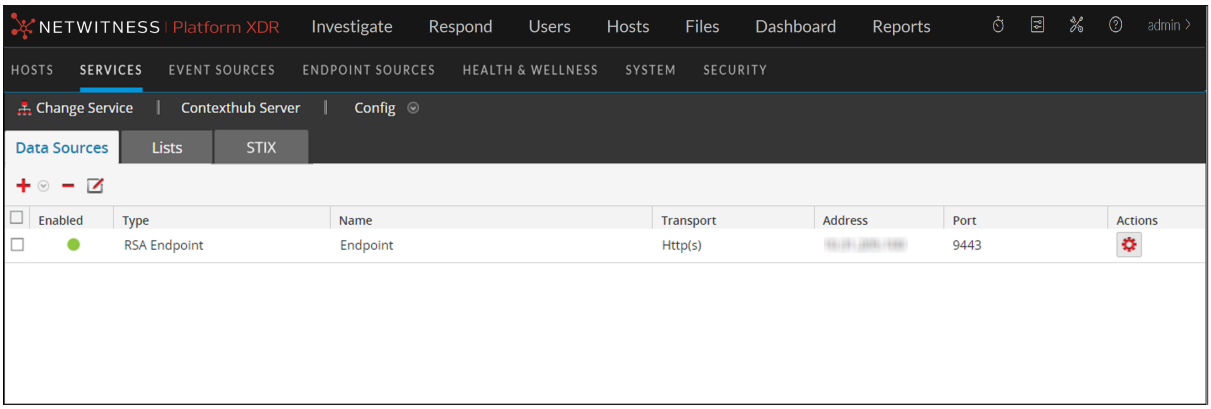
   - By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
   - **Context Highlighting** – This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled.

   Note: You can disable the context highlighting globally in the Context Hub explorer view. After you disable this option, the entity values for all the data sources configured will not be highlighted if there are any contextual information.

   - Enter the following fields:
     - **Name**: Enter a name for NetWitness Endpoint data source.
     - **Host**: Enter the hostname or IP address where NetWitness Endpoint API server is installed.
     - **Port**: The default port is 9443.
     - **SSL**: Select SSL if you want NetWitness to communicate with the host using SSL. This is enabled by default.
     - **Username**: Enter the NetWitness Endpoint API Server username.
     - **Password**: Enter the NetWitness Endpoint API Server password.
     - **Trust All Certificates**: Select this checkbox to add the data source without validating the certificate. If you uncheck this option, you need to upload a valid server generated or CA certificate to authenticate the connection with the supported formats of .cer or .crt of Base64 [PEM] encoded or DER encoded.
     - **Max. Concurrent Queries**: You can configure the maximum number of concurrent queries 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 NetWitness Endpoint.

6. Click **Save**.
   NetWitness Endpoint is added as a data source for Context Hub and is displayed in the **Data Sources** tab.



Next steps

After adding the data source, you can configure the settings. For more information, see Configure Context Hub Data Source Settings .

Also you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *RSA NetWitness Respond User Guide* and the *RSA NetWitness Investigate User Guide*

Configure Respond as a Data Source

You can configure Respond as a data source for Context Hub and use the Context Hub service to fetch contextual information from Respond service. If Respond service is already configured, the configuration details are pre-populated while adding Respond as a data source. Use the procedures in this topic to add Respond as a data source for Context Hub service and configure the settings.

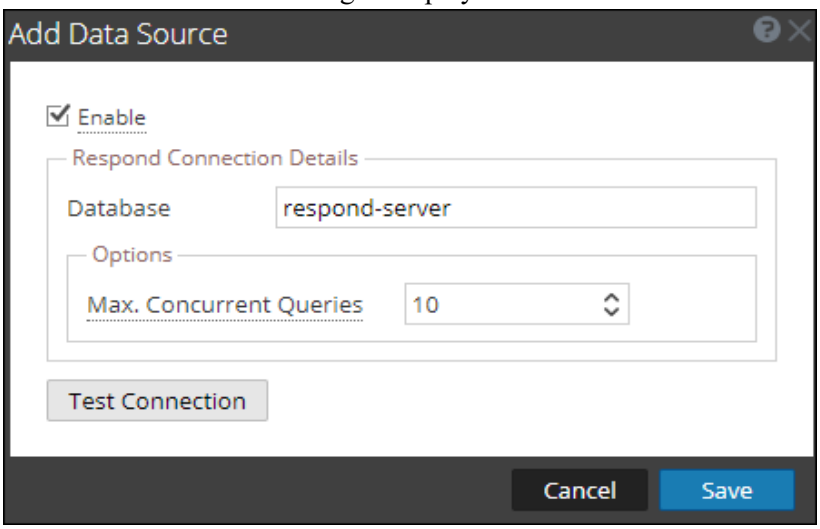
Prerequisites

Before you configure Respond data source, ensure that:

- Context Hub service is available in **(Admin) > Services** view of NetWitness.
- Respond service is available.

To add Respond as a data source for Context Hub:

1. Go to **(Admin) Services**.
   The services view is displayed.
2. 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 > **Respond**.
   The **Add Data Source** dialog is displayed.

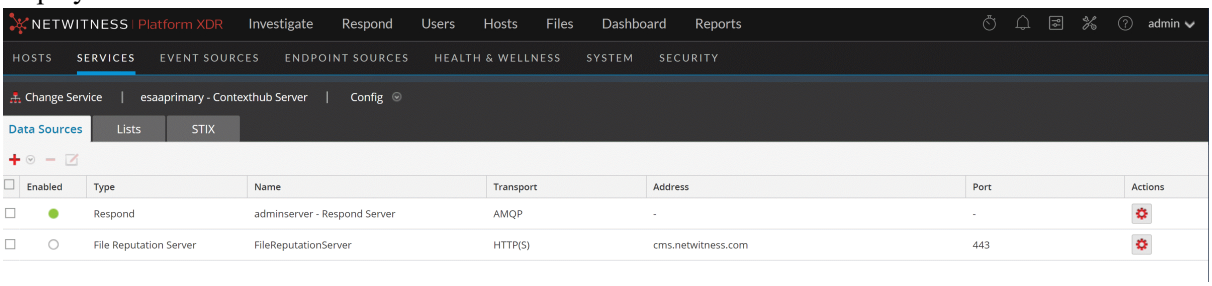


The required fields to configure the Respond data source are automatically updated.

You can enable or disable Context Highlighting. This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled.

> **Note:** You can disable the context highlighting globally in the Context Hub explorer view. After you disable this option, the entity values for all the data sources configured will not be highlighted if there are any contextual information.

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



After adding the data source, you can configure the settings. For more information, see Configure Context Hub Data Source Settings .

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *RSA NetWitness Respond User Guide* and the *RSA NetWitness Investigate User Guide*.

Configure File Reputation Server as a Data Source

File Reputation Server provides analysts the opportunity to view reputation status of files. By default, File Reputation is enabled in Additional Live Services section.

If Context Hub service is configured, File Reputation Server is automatically added as data source for Context Hub.

Prerequisites

Ensure the followings:

- Context Hub is enabled and the service is available in  **(Admin) > Services** view of NetWitness.
- NetWitness 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, **File Reputation** is enabled in **Additional Live Services** section. Before setting up File Reputation data source, make sure that you have signed in to your Live account with your Live Account Credentials and Context Hub is enabled. File Reputation is automatically added as a data source for context hub.

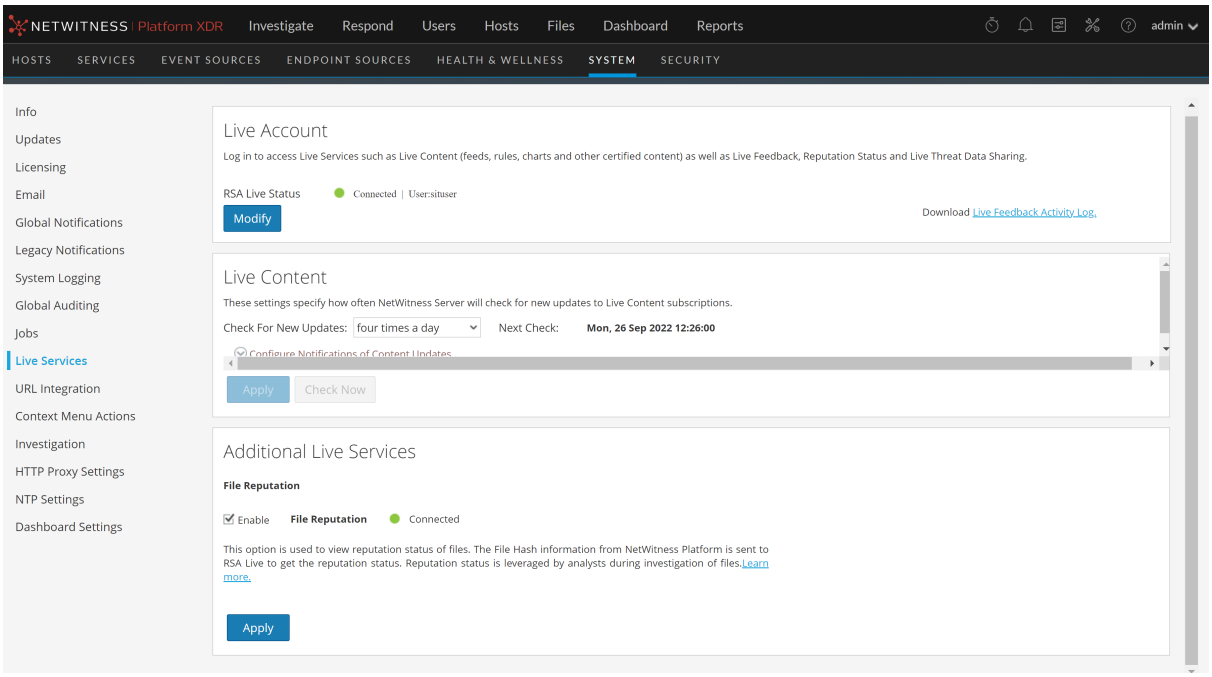
For information about configuring Live Account and Live Services, see the **Configure Live Services Settings** topic in the *System Configuration Guide*.

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

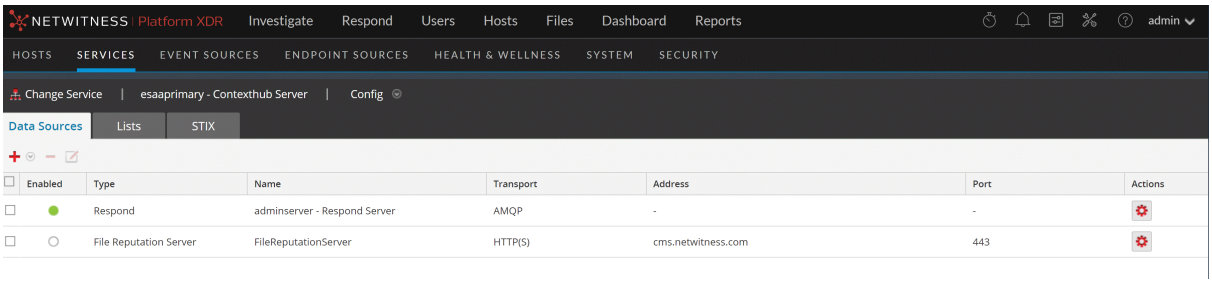
Enable or Disable File Reputation Data Source

To enable or disable File Reputation data source for Context Hub:

1. Go to  **(Admin) > System**.
2. In the left navigation pane, select **Live Services**.
3. In the **Additional Live Services** section, enable **File Reputation**.



4. Click **Apply**.
   File Reputation Server data source is enabled for Context Hub service.
5. To verify, go to the **Data Sources** tab and view the available sources.
   File Reputation source must be added to the list of available sources and the **Enabled** field must be a solid green circle ( ).



6. To disable File Reputation data source, disable **File Reputation** in Additional Live Services panel and click **Apply**.

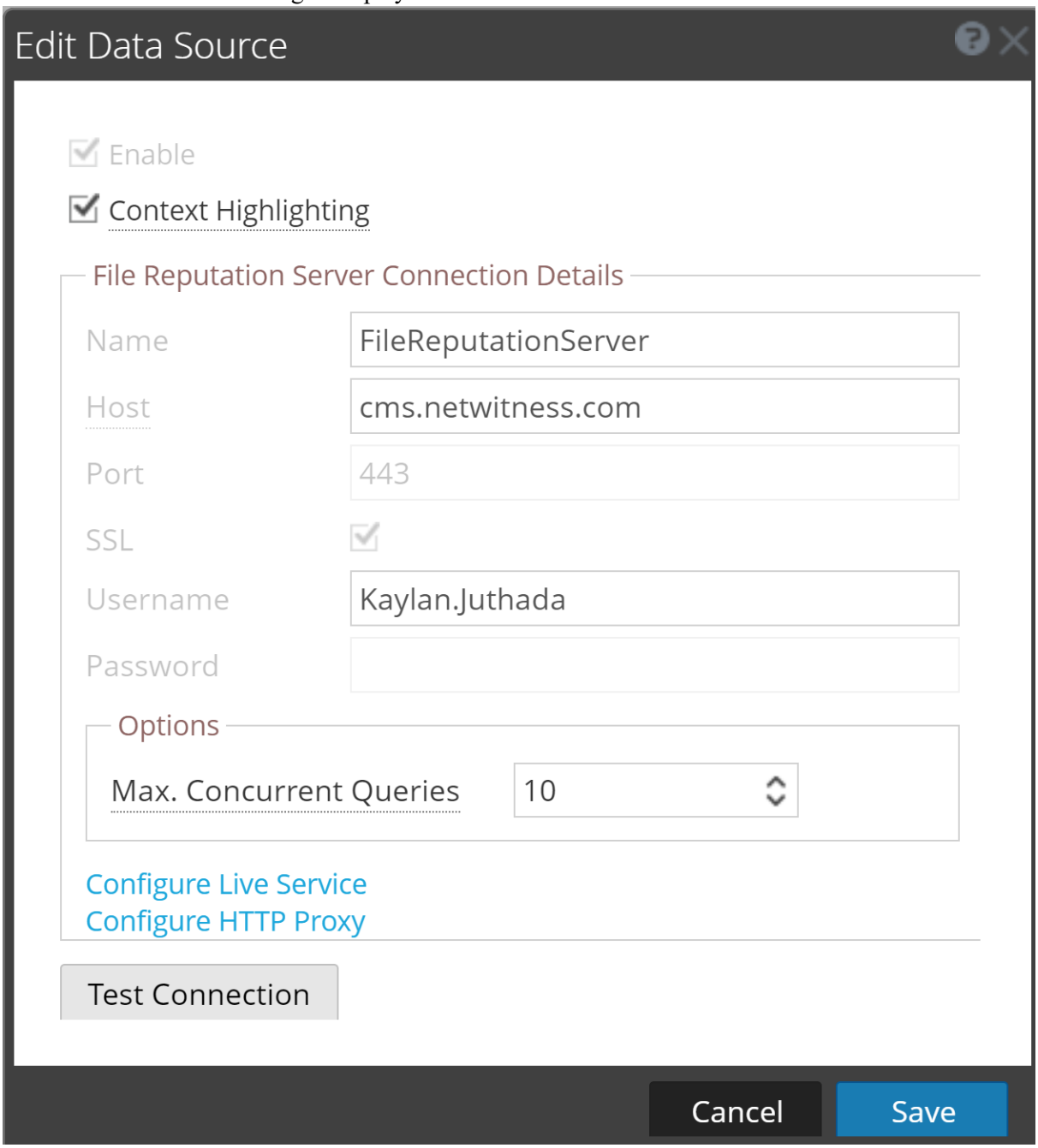
   File Reputation data source is disabled for Context Hub service.

Edit File Reputation Server Data Source Settings

To edit File Reputation Server data source for Context Hub:

1. Select **(Admin) > 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 File Reputation Server source and click .
   The **Edit Data Source** dialog is displayed.



4. Edit the required fields:

Field	Description
Context Highlighting	This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled. **Note:** You can disable the context highlighting globally in the Context Hub explorer view. After you disable this option, the entity values for all the data sources configured will not be highlighted if there are any contextual information.
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 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.

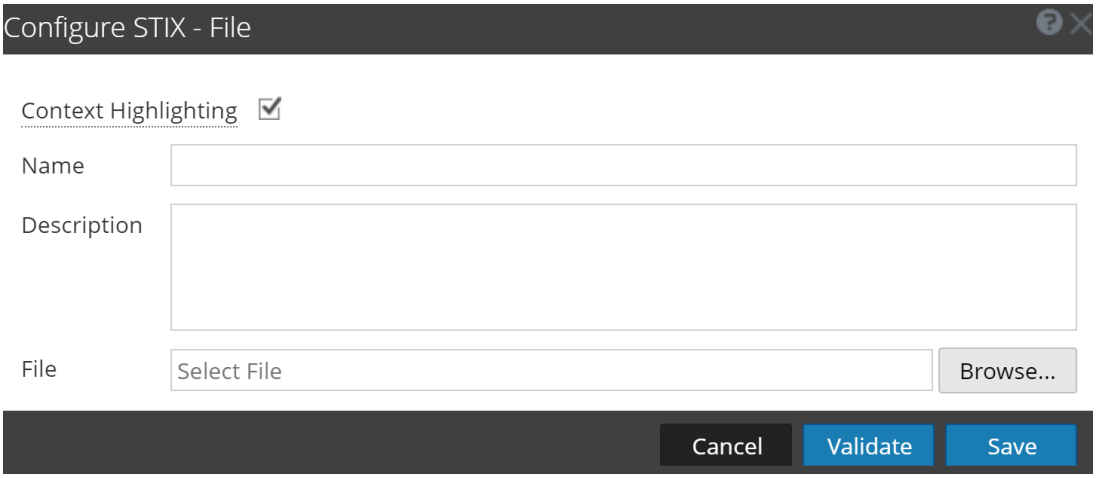
Configure STIX as a Data Source

You can configure Structured Threat Information eXpression (STIX) as a data source for Context Hub and use the Context Hub service to fetch contextual threat intelligence information from a STIX source.

Configure STIX File

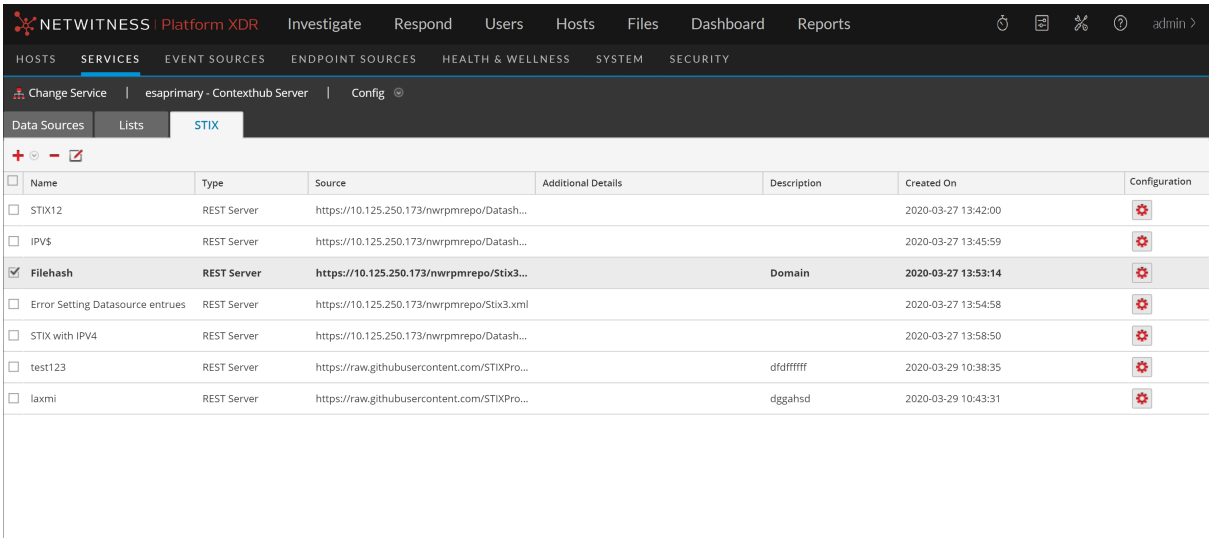
To add STIX as a data source for Context Hub:

1. Go to **(Admin) > Services** .
   The Services view is displayed.
2. Select the Context Hub service and click > **View** > **Config**.
   The Services config view of Context Hub is displayed.
3. Click the **STIX** tab, and click .
4. Select **File** as data source.



4. Provide the following details:
   a. **Context Highlighting**: This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled.
   b. **Name**: Provide a name for the STIX file data source.
   c. **Description**: Provide description of the data source.
   d. **File**: Browse for the file you want to add as a data source.
5. Click **Validate** to verify the format of the file.

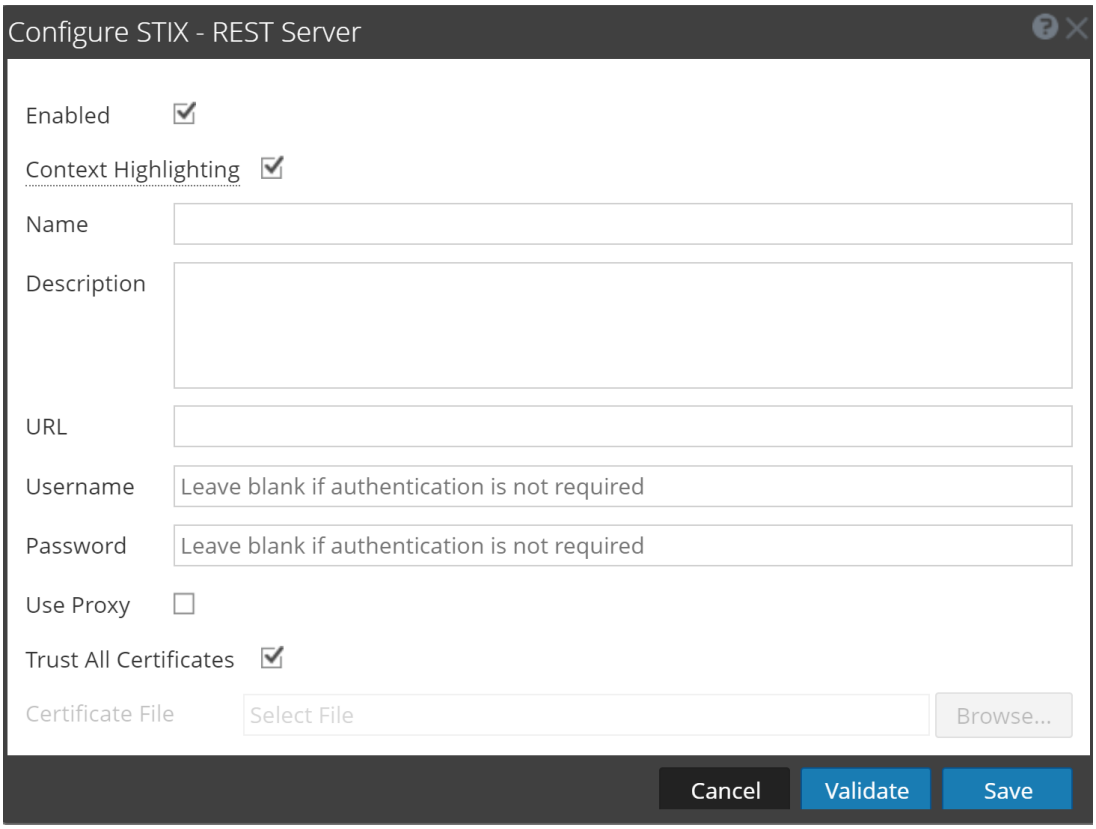
6. Click **Save** to configure the data source.
   The File is added as a data source for the configured Context Hub and is displayed in the **STIX** tab.



Configure REST Server

To add REST as a data source for Context Hub:

1. Go to **(Admin) > Services**.
   The Services view is displayed.
2. Select the Context Hub service and click > **View** > **Config**.
   The Services config view of Context Hub is displayed.
3. Click the **STIX** tab, and click .
4. Select **REST Server** as data source.



4. Provide the following details:
   a. **Enabled**: Select this checkbox to enable the connection.
   b. **Context Highlighting**: This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled.
   c. **Name**: Provide a name for the REST Server data source.
   d. **Description**: Provide a description for the data source.
   e. **URL**: Specify the URL to the STIX file to be hosted on the server.
   f. (Optional) **Username**: Enter the username for the REST server.
   g. (Optional) **Password**: Enter the password for the REST server.
   h. **Use Proxy**: Select this checkbox to use proxy.
   i. (Optional) **Trust All Certificates**: Select this checkbox if you want to trust all certificates and do not have a custom certificate.
   j. (Optional) **Certificate File**: Browse for the certificate file if you have not selected the Trust All certificates checkbox.
5. Click **Validate** to verify the connection parameters to the REST Server.

6. Click **Save** to configure the data source.
   The REST Server is added as a data source for the configured Context Hub and is displayed in the **STIX** tab.

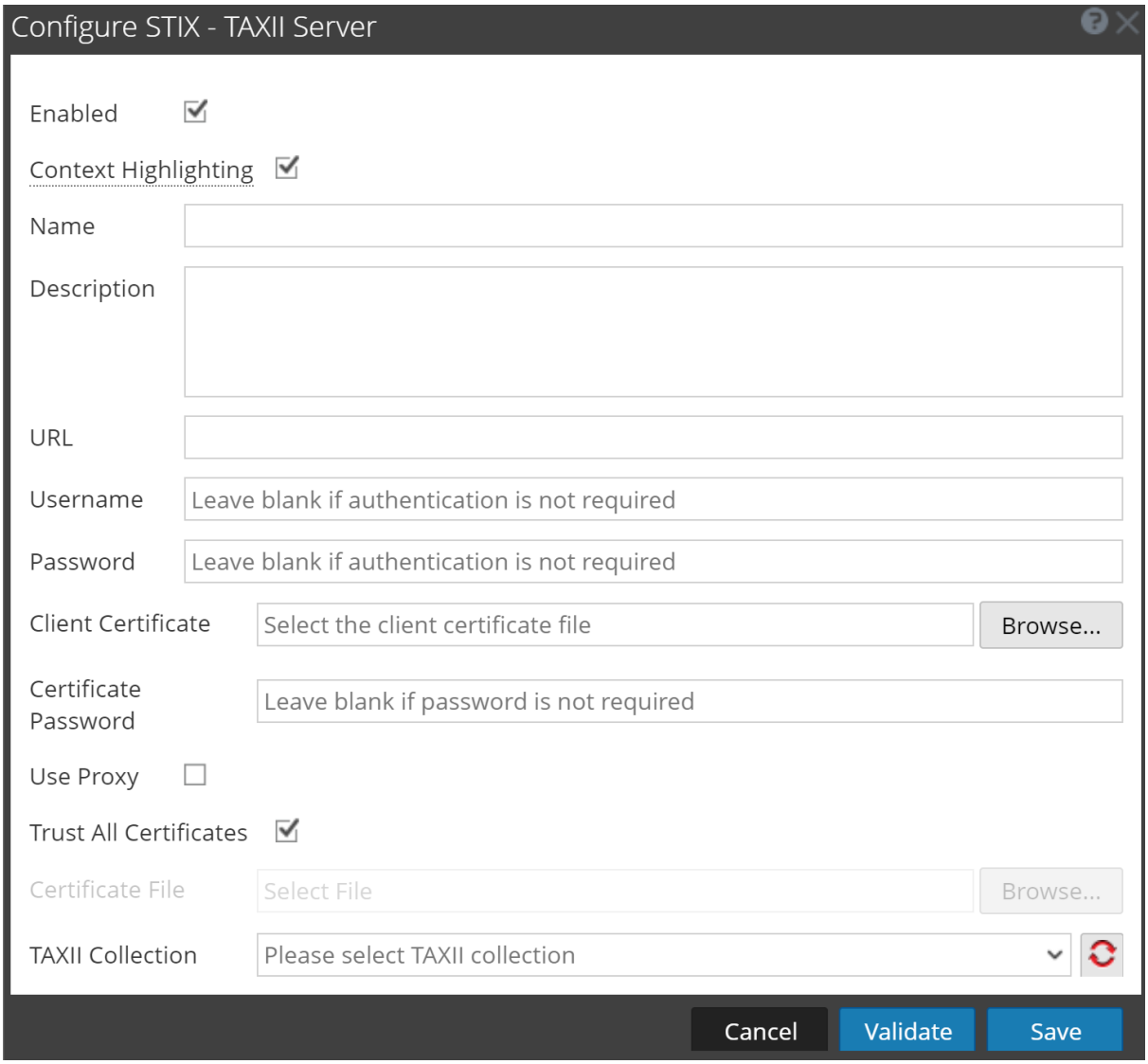
After adding the data source, you can configure additional settings. For more information, see Configure Context Hub Data Source Settings .

Configure TAXII Server

To add TAXII Server as a data source for Context Hub:

1. Go to  **(Admin) > Services**.
   The Services view is displayed.
2. Select the Context Hub service and click  > **View** > **Config**.
   The Services config view of Context Hub is displayed.
3. Click the **STIX** tab, and click  .

4. Select **TAXII Server** as data source.



5. Provide the following details:
   a. **Enabled**: Select this checkbox to enable the connection.
   b. **Context Highlighting**: This highlights the meta values (in the **Investigate** > **Navigate**, **Events**, **Event details** and **Nodal graph**) for which the contextual information is available for this data source in the Context Hub. By default, this option is enabled.
   c. **Name**: Provide a name for the TAXII Server data source.
   d. **Description**: Provide a description for the data source.
   e. **URL**: Specify the discovery URL to the TAXII Server.
   f. (Optional) **Username**: Enter the username for the TAXII server.
   g. (Optional) **Password**: Enter the password for the TAXII server.

h. (Optional) **Client Certificate**: Browse to upload a pkcs12 format client certificate available on your local system.

i. (Optional) **Certificate Password**: Enter the password to the certificate, if it is password-protected.

j. (Optional) **User Proxy**: Select this checkbox to use proxy.

k. (Optional) **Trust All Certificates**: Select this checkbox if yoenabu want to trust all certificates and do not have a custom certificate.

l. (Optional) **Certificate File**: Browse for the certificate file if you have not selected the Trust All certificates checkbox.

m. **TAXII Collection**: Select the TAXII Collection name from the drop-down to automatically download the collection.

6. (Optional) Click  to manually retrieve the list of collections available in the TAXII server , if the collections are not downloaded automatically.
7. Click **Validate** to verify the connection parameters to the TAXII Server.
8. Click **Save** to configure the data source.
   The TAXII Server is added as a data source and is displayed in the **STIX** tab.

After adding the data source, you can configure additional settings. For more information, see Configure Context Hub Data Source Settings .

Note: You can disable the context highlighting globally in the Context Hub explorer view. After you disable this option, the entity values for all the data sources configured will not be highlighted if there are any contextual information.

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *NetWitness Respond User Guide* and the *NetWitness Investigate User Guide*.

Configure REST API as a Data Source

You can configure REST API as a data source for Context Hub which allows analysts to use the Context Hub during an investigation to fetch contextual information from any accessible web service with an exposed REST API. Use the procedures in this topic to add REST API as a data source for Context Hub service and configure the settings (if required) for REST API. The maximum number of REST APIs supported by default is ten.

Prerequisites

Before you configure REST API data source, ensure that:

• Context Hub service is available in  (Admin) > **Services** view of NetWitness Platform.

• Third-party REST API web server is reachable.

To add REST API as a data source for Context Hub:

1. Go to  (**Admin**) > **Services**.
   The Services view is displayed.

2. Select the Context Hub service and click  > **View** > **Config**.
   The Services Config view is displayed.

3. In the **Data Sources** tab, click  > **REST API**.
   The Add Data Source dialog is displayed.

4. Provide the following information:
   - By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
   - Enter the following fields.
     a. **Name** - Enter a name for the REST API data source.
     b. **URL** - Specify the REST API URL with the query parameters.
     The following table lists some examples of URL and associated parameters:

URL	Parameters
https://www.virustotal.com/vtapi/v2/file/report?apikey=<API Key>&resource=$metaValue	• **API key** – Specify your API key • **$metaValue** - You must specify the Test meta value in step 7 to test the REST API connection. For example, C5D0065B594A4775E26FA9875B21189F

URL	Parameters
https://www.virustotal.com/vtapi/v2/url/report?apikey= 1bfdf66f3b0f1875381830ec933f7151f5b48c1cbaa54ac625f2d5a74312e9a2&resource=$metaValue	• **API key** – Specify your API key • **$metaValue** - You must specify the Test meta value in step 7 to test the REST API connection. For example, textspeier.de

c. **Description** – Enter the description of the REST API data source.

d. **User name**: Enter the username of the REST API if it needs to be authenticated.

e. **Password**: Enter the password of the RSET API if it needs to be authenticated.

f. **Response Type**: Select the REST API response type. Possible values are:

- HTML
- JSON

g. **Test Meta value**: Enter the meta value to test the REST API connection.

Note:
- The meta value you specify will be replaced with `$metavalue` in the URL mentioned in step 2 for test connection.
- During context lookup, the `$metavalue` variable is replaced with meta value in the REST API call.

h. **SSL** - Enables SSL communication to REST API. By default, this option is selected.

i. (Optional) **Trust All Certificates**: Select this checkbox if you want to trust all certificates and do not have a custom certificate. By default, this option is enabled.

j. (Optional) **Certificate File**: Browse for the certificate file if you have not selected the Trust All certificates checkbox.

5. Click **Test Connection** to test the connection between Context Hub and the REST API data source.
6. Click **Next**.
7. In the **Response Preview** section, you can view the live response for the REST API configured, using the test meta value as a placeholder.
8. In the **Meta Mapping** section, select one or more meta type supported by the REST API to view context lookup (for meta values) in the Respond and Investigation views.
9. In the **Field Mapping** section, you can add friendly display name for the response field for which you want to perform context lookup. Do the following:

a. Click  .

b. In the **Field** drop-down, enter the path for which you want to add a friendly name. As you type the path, the auto-suggest function looks for the matches in the JSON path returned in the response preview. You can also add the path that is not available in the response preview but available for other meta values.

c. **Value (from Preview)** field is filled automatically when you select the path.

d. In the **Display Name** field, enter the friendly name.

> **Note:** After configuration, only the fields that are mapped with friendly names are displayed during context lookup. If you do not map any fields, all fields in the JSON will be available during context lookup.

10. Click **Save** to configure the data source.

> **Note:** After you configure the data source settings, you can configure the Context Hub configuration parameters by navigating to  (**ADMIN**) > **Services**> **View** > **Explore** view.

Edit REST API Data Source

To edit REST API data source for Context Hub:

1. Go to  (**Admin**) > **Services**.
2. Select the Context Hub service and click  > **View** > **Config**.
3. In the Data Sources tab, click  > **REST API**.
4. Edit the required fields.
5. Click **Test Connection** to test the connection between Context Hub and the data source.
6. In the **Meta and Field Mapping** and **Cache settings**, edit the required fields.
7. Click **Save** to save the settings.

> **Note:** In 12.3 and later versions, field mapping and Data Preview are enabled for authenticated REST API without providing the username and password.

Delete REST API Data Source

To edit REST API data source for Context Hub:

1. Go to  (**Admin**) > **Services**.
2. Select the Context Hub service and click  > **View** > **Config**.
3. In the **Data Sources** tab, select the data source you want to delete.
4. Click .

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For more information, see the *NetWitness Respond User Guide* and the *NetWitness Investigate User Guide*.

Configure Context Hub Data Source Settings

After you have configured the required data sources you can customize the settings for the data sources based on your requirement.

To access and configure settings:

1. Go to  **(Admin) > Services**.

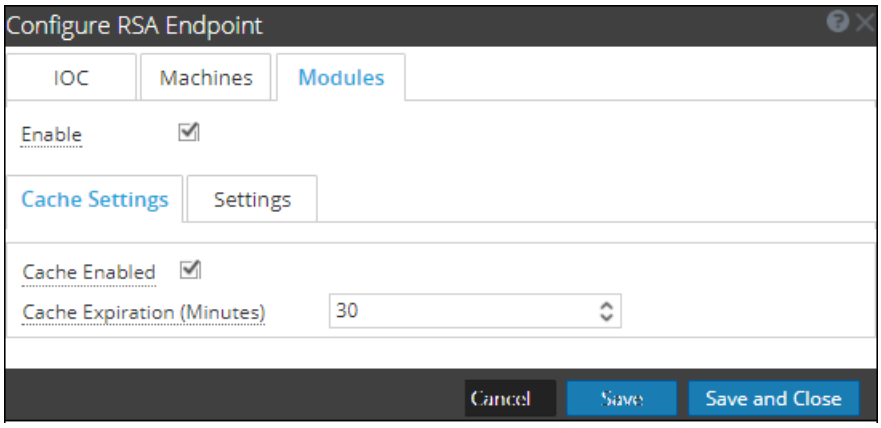
   The services view is displayed.

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

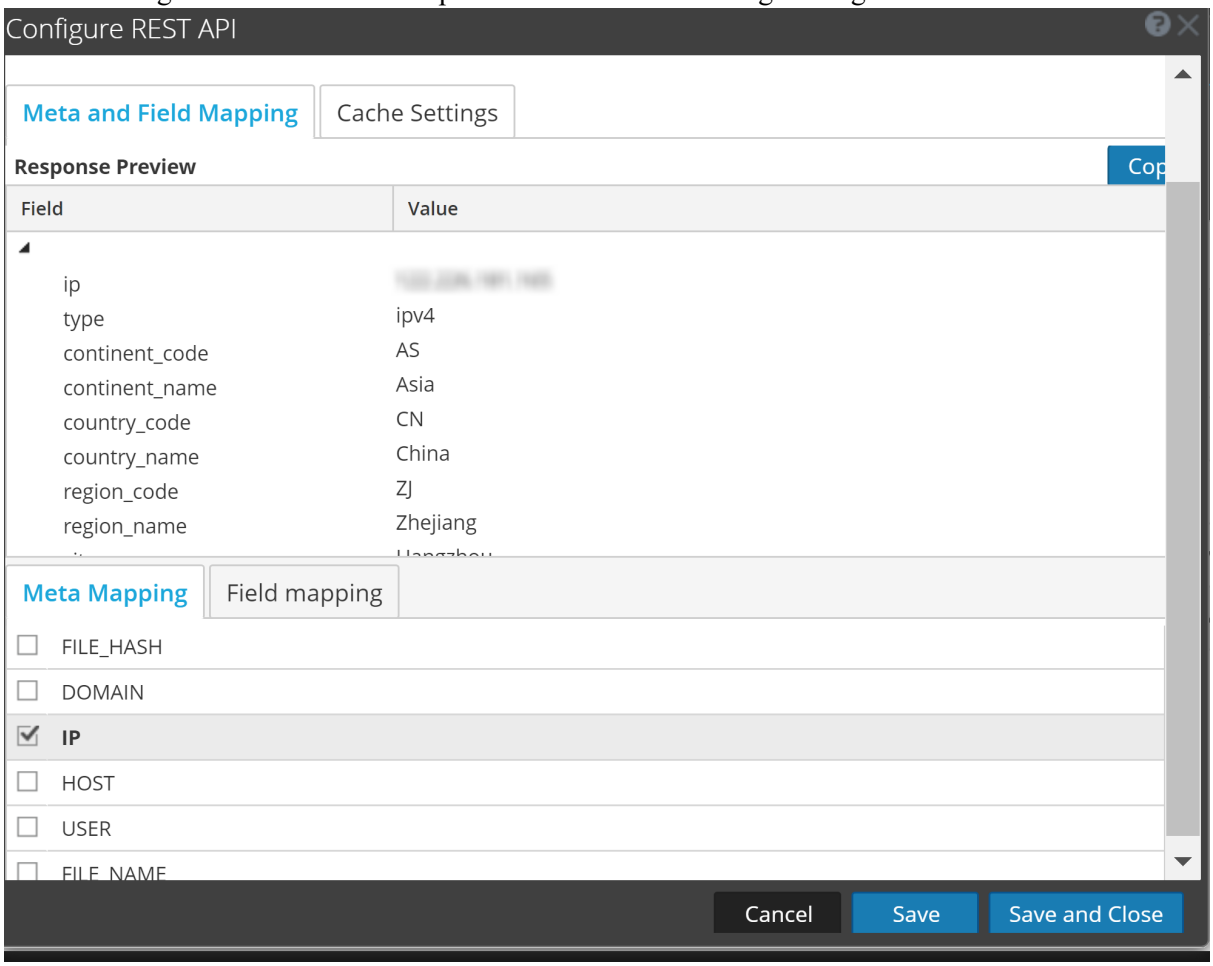
   The Services Config view of Context Hub is displayed.

3. Select the data source for which you want to configure the settings and click  in the Actions column.

   The following screenshot is an example of the NetWitness Endpoint settings dialog:



The following screenshot is an example of the REST API settings dialog:



4. Configure the following fields:

Field	Description
Enable	This option is enabled by default (checked) and can be used to enable or disable the response from the selected data source.

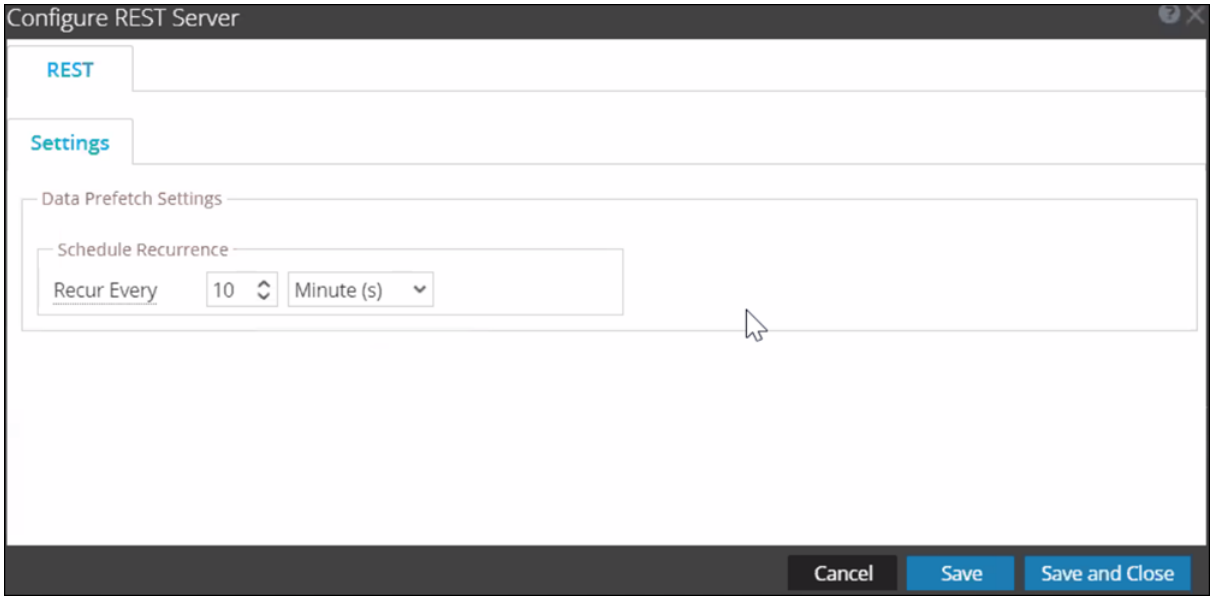
Field	Description
Cache Settings	Any lookup from Context Hub can be stored in the Context Hub cache for a configured time. Response to any subsequent matching request will be fetched from the Context Hub cache. Use this section to define the following cache settings for query lookup: • **Cache Enabled**: By default, this checkbox is selected and the query response is cached. • **Cache Expiration (Minutes)**: The maximum time the query lookup is retained in cache. The default time is 30 minutes and maximum is 7200 minutes that you can configure.
List value Expiration	**Enable**: Select Enable to define the number of days the list values must be available. By default, this option is disabled and the values are retained. **Time to Live (Days)**: Enter the number of days you want to the list values to be retained.
Meta Mapping	Any list stored in Context Hub should be made available for a lookup. The lookup in Context Hub is performed based on meta type or entities. Examples IP, HOST, MAC ADDRESS, DOMAIN, FILE_NAME, FILE_HASH, USER. **Meta Type**: Entities available in Context Hub. **Context Hub Fields**: Column headers from CSV file you have added when creating a list.
Meta and Field Mapping	**Response Preview**: You can view the live response for the REST API configured, using the test meta value as a placeholder. **Copy**: Copies the response preview. **Meta Mapping**: Any REST API stored in Context Hub should be made available for a lookup. The lookup in Context Hub is performed based on meta type or entities selected. Examples IP, HOST, MAC ADDRESS, DOMAIN, FILE_NAME, FILE_HASH, USER. **Meta Type**: Entities available in Context Hub. **Field Mapping**: Add friendly display name for the response field which is displayed during the context lookup.  - Add a field mapping. - Delete a field mapping. **Field**- Enter the path for which you want to add a friendly name. **Value (from Preview)**- The value is filled automatically based on the path. **Display Name**- Enter friendly name.
Minimum IIOC Score	The minimum IIOC score to be considered for fetching contextual information of NetWitness Endpoint modules.

Field	Description
Query Last (Days)	The duration (in days) for which the Context Data must be queried.
Limit	The maximum number of records to be displayed when Context Lookup is performed.
Recur Every	Configure recurring schedule to fetch and store contextual data for the required intervals.

5. Click any one of the following options:
   - **Cancel** - select this option to cancel the changes.
   - **Save** - select this option to save the changes.
   - **Save and Close** - select this option to save and close the dialog.

To access and configure settings for STIX data sources

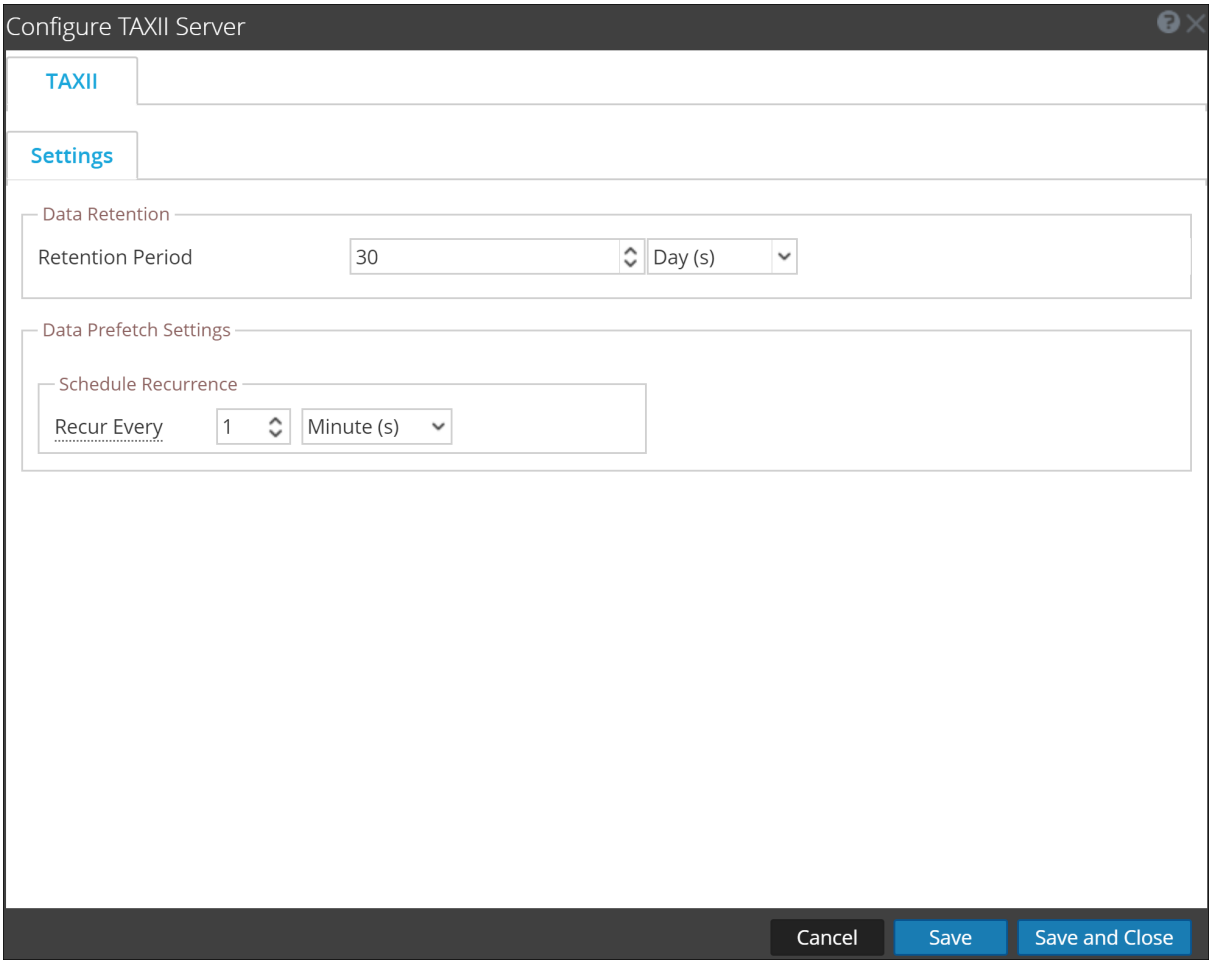
1. Go to **(Admin) > Services** and select Context Hub service.
2. Click > **View** > **Config** > **STIX** tab.
3. Select the data source for which you want to configure the settings and click in the Configurations column.
   a. For REST Server, the following fields are displayed.



Configure the following fields for REST Server.

Field	Description
Recur Every	Specify the time frequency in minutes, hours, days or weeks to retrieve the content from the data source.

b. For TAXII Server, the following fields are displayed.



Configure the following fields for TAXII Server.

Field	Description
Retention Period	Specify the number of days the content retrieved from the taxi data source must be retained before it is automatically deleted.
Recur Every	Specify the time frequency in minutes, hours, days or weeks to retrieve the content from the data source .

Based on the data source you select, the Response Groups differ. The following table describes the response groups for every data source.

Data Source (Connection)	Response Supported Groups	Field Settings
List	List	Meta Mapping Meta Type Context Hub Fields Settings Data Prefetch Settings Schedule Recurrence List Value Expiration Cache Settings Cache Enabled Cache Expiration (Minutes) [Min is 30 minutes Max is 7200 minutes]
Archer	Archer	Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Export Attributes Configuration Export Attributes Data Prefetch Settings Schedule Recurrence
Active Directory	Users	Meta Mapping Meta Type Context Hub Fields Settings Data Prefetch Settings Schedule Recurrence List Value Expiration Cache Settings Cache Enabled Cache Expiration (Minutes)[Min is 30 minutes Max is 7200 minutes]

Data Source (Connection)	Response Supported Groups	Field Settings
NetWitness Endpoint	IOC Machines Modules	Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Context Panel Settings Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Context Panel Settings Cache Settings Cache Enabled Cache Expiration (Minutes) Settings Minimum IIOC Score Context Panel Settings
Respond	Alerts Incidents	Context Panel Settings Data Prefetch Settings Query Last [Days Cache Settings Cache Enabled Cache Expiration (Minutes)
File Reputation Server	File Reputation Server	Cache Settings Cache Enabled Cache Expiration (Minutes)
TI	Displays information for STIX data sources.	IP address, email address, domain, filename, URL's, and file hash. **Note:** The context lookup for email address and URL will be displayed only if these metas are mapped. To map the metas, navigate to (Configure) > **System** > **Investigation** > **Context Lookup**.

Data Source (Connection)	Response Supported Groups	Field Settings
REST API	REST API	• Meta and Field Mapping • Meta Type • Field • Value (from Preview) • Display Name • Cache Settings • Cache Enabled • Cache Expiration (Minutes)

Note: After you configure the data source settings, you can configure the Context Hub configuration parameters by navigating to **(Admin) > Services**> **View** > **Explore** view. Make sure you restart the Context Hub service if you make any configuration changes in the Explore view.

Import or Export Lists for Context Hub

As an administrator you can import or export a list that is configured in the Context Hub service which can be used by an analyst. The file to be imported or exported is a CSV file and you can add multiple lists as Data Sources.

Prerequisites

Ensure that Context Hub is enabled and the service is available in  **(Admin) > Services** view of NetWitness.

Import a List

After you have imported a list, you can perform the following tasks:

- Import values to an existing list
- Add row to a list
- Edit a list name and description
- Edit a value from a list
- Delete a list
- Delete row from a list

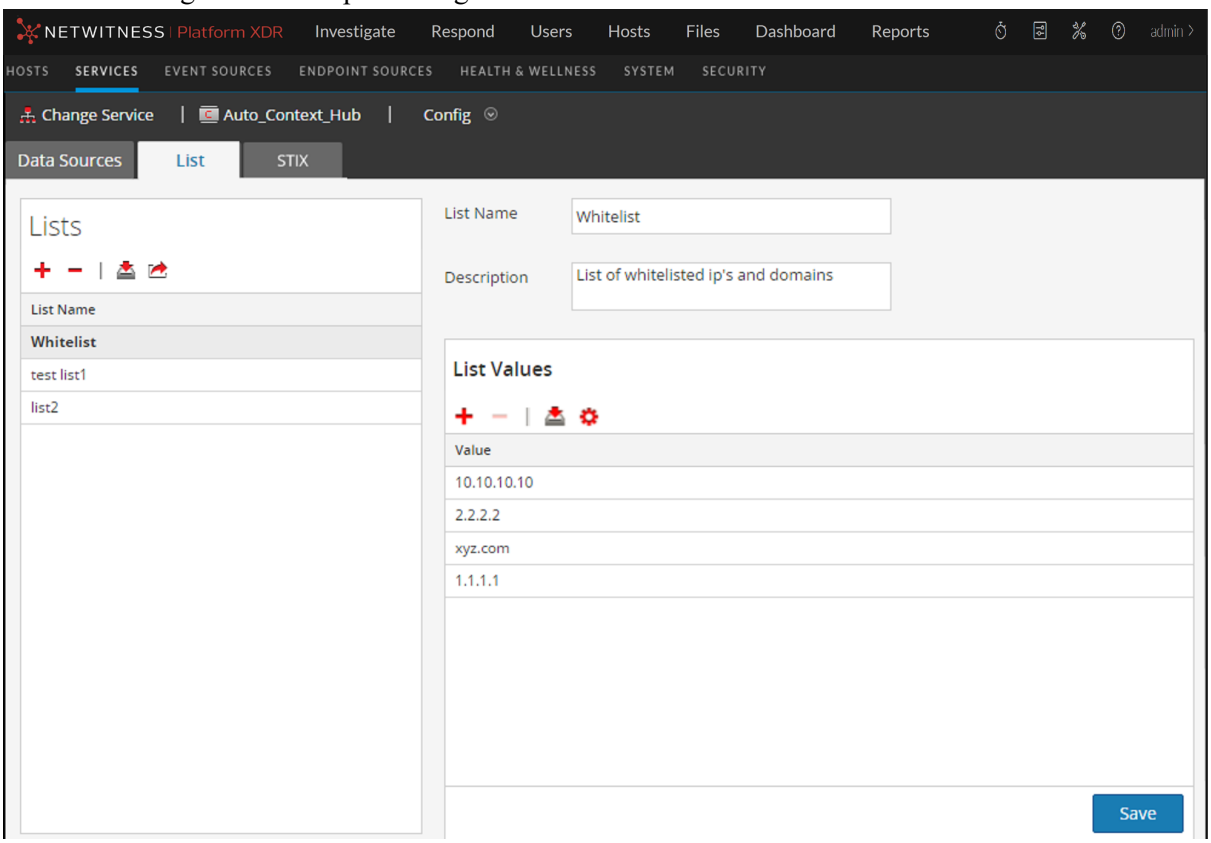
Note: You have to make the same changes to the relevant .CSV file, so that the changes get reflected the next time the schedule recurs. Otherwise, when you import values into an existing single-column or multi-column list, the data is overwritten from the source file when the schedule recurs. In case of a custom feed list, if the feed is edited or deleted, the corresponding Context Hub list also gets edited or deleted.

Import Single-Column List

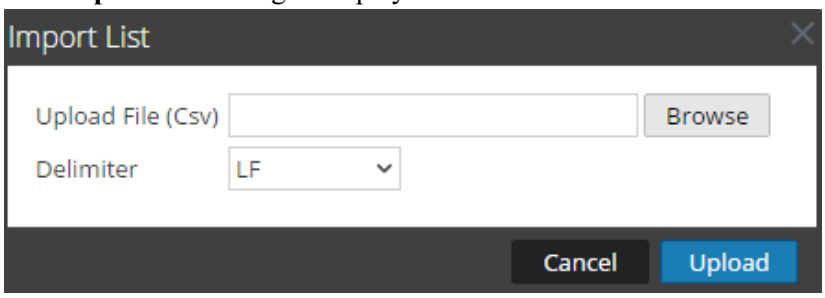
To import a list:

1. Select  **(Admin) > 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 **Lists** tab.
   The Lists tab consists of the **Lists** panel and **List Values** panel.

The below image is an example of single-column list.



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 Context Hub.

These lists are considered as data sources for retrieving contextual information. But you can append to an existing multi-column list. The data will be appended only if the number of columns match.

Note: You cannot create a new multi column list by directly importing a CSV file. However, all the feeds that are converted into multi-colum lists will be displayed in the List tab. For information on how to import multi-column list, see Configure Lists as a Data Source

Import Values to an existing List

When you are importing into existing multi- column list the data is overwritten from the source file when the schedule recurs.

To import values to a list:

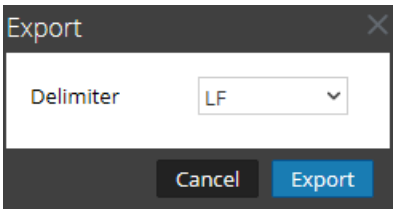
1. Go to  **(Admin) > Services**.
   The services view is displayed.
2. Service and click  > **View** > **Config**.
   The Services Config View of the Context Hub service is displayed.
3. Click the **Lists** tab.
   The Lists tab consists of the **Lists** panel and **List Values** panel.
4. In the Lists 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).
7. Click **Upload** to upload the CSV file to NetWitness.

The list values are imported to the selected list. These lists are considered as data sources for retrieving contextual information. But you can append an existing multi column list. The data will be appended only if the number of column match.

Export List for Context Hub

To export a list:

1. On the **Lists** 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 drop-down [**Comma**, **CR** (Carriage Return), and **LF** (Line Feed)].
3. Click **Export**.

In case of a single-column list, you can select the delimiter. And, in case of a multi-column list, the list is exported as CSV file to the local machine.

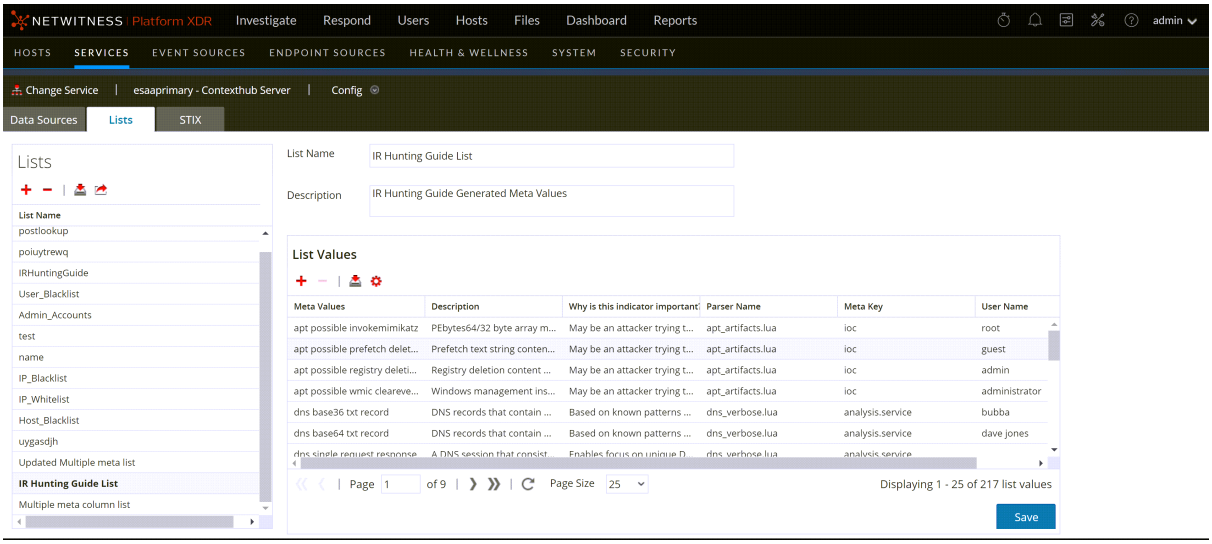
Note: When a custom feed is converted into a Context Hub list, you must map at least one meta key with one or more entity mapping for a column header with a meta. However, if you want to add or edit more entities you can do so by clicking ⚙.

Manage Meta values for Context Hub Lists

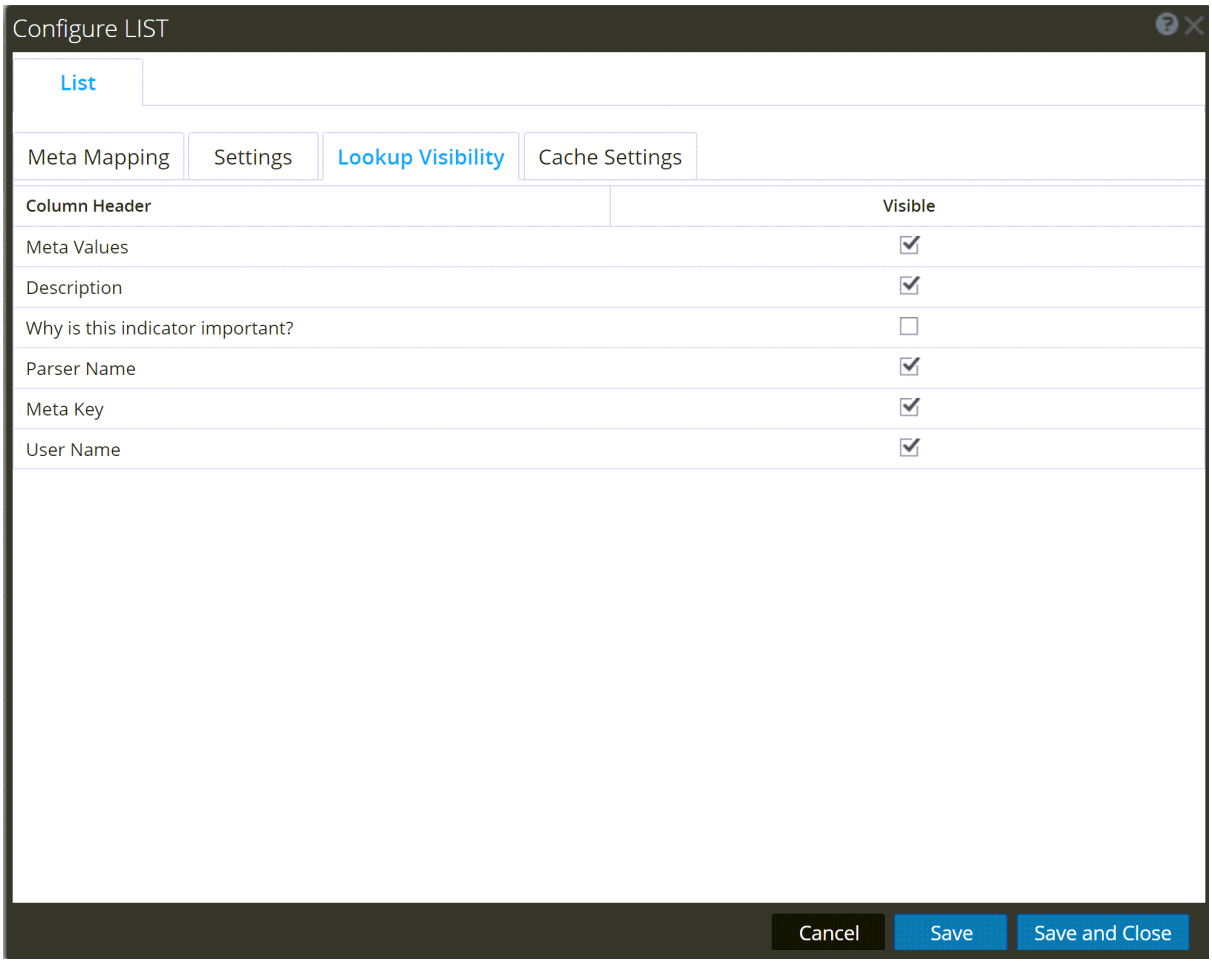
From NetWitness Platform XDR 12.3 version or later, administrators can view and manage headers and values in the context Hub lists panel's newly added **List Details** tab. This enhancement helps administrators with more flexibility in enabling and disabling required meta values and helps analysts to have better visibility in the **Investigate** and **Respond** Context lookup Lists Panel for further analysis and investigation.

To view and manage context hub lists Meta keys

1. Go to **(Admin) > 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 **Lists** tab.
   The Lists tab consists of the **Lists** panel and **List Values** panel.
   The below image is an example of multi-column lists.



4. In the Lists panel, select a list name for which you want to configure the settings and click on the **Actions** column.
   The Configure List dialog is displayed.
5. Click the **List Details** tab.
   The available configured meta key for the lists is displayed.



6. By default, five meta keys will be enabled. You can deselect the required meta keys from the lists and select the required ones.

   Note:
   - The List Details tab must have at least one meta key enabled.
   - You can enable a maximum of only five meta keys in the Lists Details tab.

7. Click **Save**.

   You can now navigate to **Investigate** > **Events** or **Respond** view and click on the selected meta key or entity associated with the lists, the context look-up panel opens with the details of the selected meta keys on the Lists tab for further analysis. For more information, see topic Context Lookup Panel Lists Tab in the *NetWitness Investigate User Guide*.

Configure Meta Type Mapping for Context Hub

As an administrator you manage the mapping of Context Hub meta types with NetWitness meta keys.

The Context Hub service provides context lookup for meta values in the Respond and Investigation views. These meta values are grouped into meta types based on the category they belong to. For example, meta keys of NetWitness Respond and 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 Respond database.

In the  (Admin) **> System > Investigation** view, the Context Lookup tab enables the administrator to configure the NetWitness meta keys and meta type mapping. The administrator can add or remove 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:

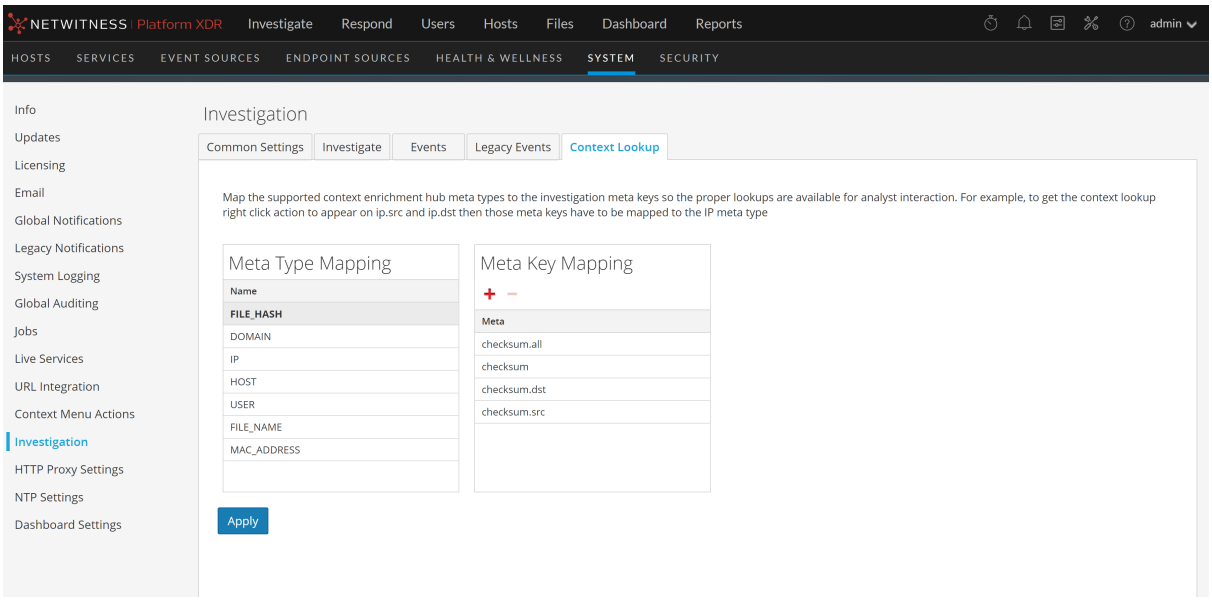
Meta Type Name	Meta Keys
IP	device.ip, ip.dst, ip.src, ip.addr, paddr, ip.all, alias.ip
USER	user.all, user.src, user.dst, username
DOMAIN	domain.src, domain.all, domain.dst
MAC_ADDRESS	eth.dst, eth.src, eth.all
FILE_NAME	filename, filename.all, filename.src, filename.dst, sourcefile
FILE_HASH	checksum.all,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

Procedure

To manage Investigation meta keys mapping:

1. Go to  **(Admin) > 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**.
8. In order to add a new meta, they need to be included in the Concentrator's custom index file. For example, if you want to add a meta "**fqdn**" then you need to add an new entry: **<key name="fqdn" description="Fully Qualified Domain Name="IndexValues" form-at="Text" valueMax="100" />** in the index file. For more information on how to include a new meta in the index file, see Index Customization topic in the *Core Database Tuning Guide*. After you add the new meta, you can view the contextual information on clicking the Pivot to investigate option in the Respond view.

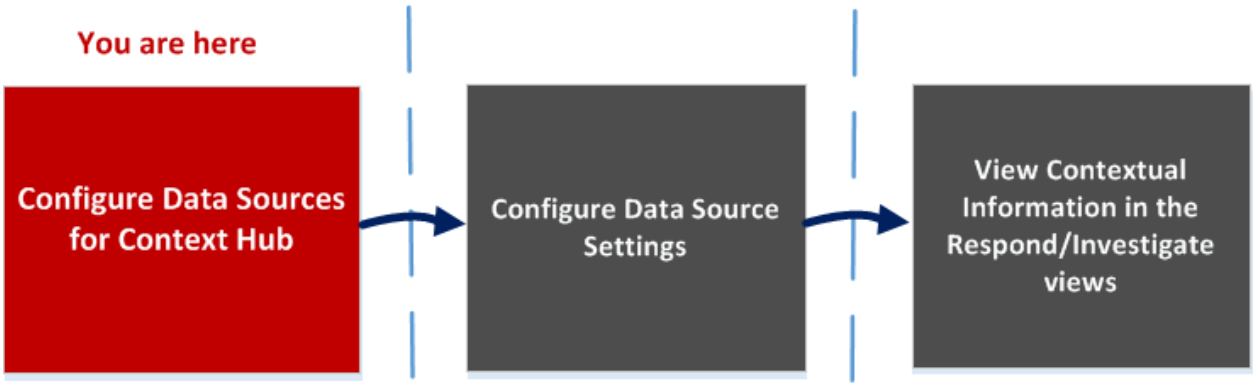
In case a new meta key is added, the Context Lookup menu option is enabled for the meta values under that meta key. For more information, see the "Investigation Configuration Panel" topic in the *System Configuration Guide*

Context Hub Data Sources Tab

In the **Data Sources** tab, you can configure one or more data sources for Context Hub service. Navigate to **(Admin) > Services** > Select Context Hub service > **View** > **Config** > **Data Sources** tab.

Workflow

This workflow shows the procedure to configure data sources for Context Hub service to view contextual information in the Respond / Investigate views.



- The first task is to add a data source
- The second task is to configure data sources settings to enhance your deployment. This task is optional as the settings for each data source is already configured with default values for optimal performance.
- And the third task is to view and analyze the contextual information in the Context Summary panel of the Respond or Investigate views.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure Data Sources for Context Hub*	Configure Lists as a Data Source Configure Archer as Data Source Configure Active Directory as a Data Source Configure NetWitness Endpoint as a Data Source Configure REST API as a Data Source Configure File Reputation Server as a Data Source Configure STIX as a Data Source
Administrator	Configure Hub Data Settings*	Configure Context Hub Data Source Settings

Role	I want to ...	Show me how
Analyst	View Contextual Information in Respond View	See the *NetWitness Respond User Guide*.
Analyst	Add, create and delete list from the Respond or Investigate View	See the *NetWitness Respond User Guide*. See the *Investigate User Guide*.
Analyst	Add or delete an entry from an existing list	See the *NetWitness Respond User Guide*.

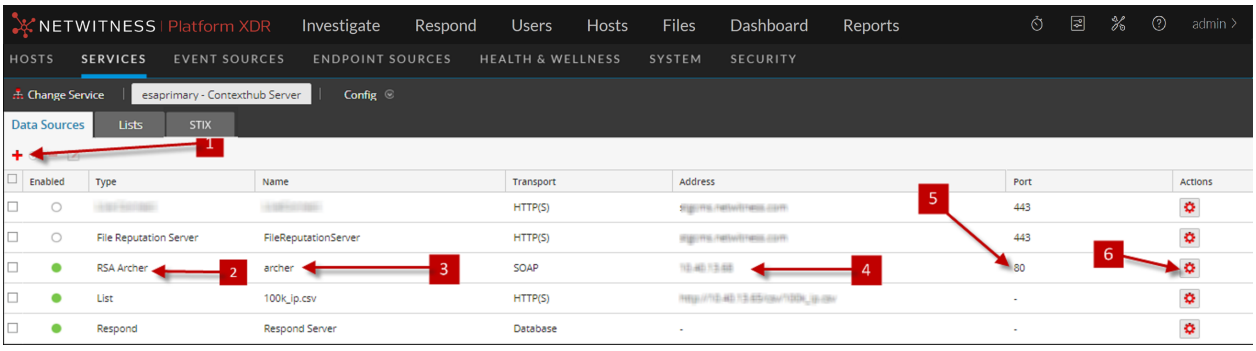
*You can complete this task here (that is in the Context Hub Data Sources Tab.)

Related Topics

- Configure Lists as a Data Source
- Configure Archer as Data Source
- Configure Active Directory as a Data Source
- Configure NetWitness Endpoint as a Data Source
- Configure Respond as a Data Source
- Configure REST API as a Data Source
- Configure File Reputation Server as a Data Source
- Configure STIX as a Data Source
- Configure REST API as a Data Source

Quick Look

The following example illustrates how to add a data source for Context Hub service.



1 Click + to display the **Add Data Source** dialog.
2 Displays the type of Data Source.
3 Name that identifies the Data Source.
4 The IP address or hostname of the data source.
5 The connection port for the data source.

6 Opens the **Configure Settings** dialog. You can view and edit the settings to be displayed on the Context Summary panel in the Respond or Investigate views.

7 Click **Test Connection** to verify that the host is connected to the Context Hub service.

Toolbar

The following table describes the toolbar actions.

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. Except in case of Lists and Active Directory data sources which can be added in multiples. For detailed instructions to add a data source, see Configure Lists as a Data Source.
	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.
	Opens the Configure Settings dialog. You can view and edit the settings for the data sources. For description of each field in Configure Responses dialog, see Configure Context Hub Data Source Settings .

Data Source Configurations

The following table describes the listed configurations.

Feature	Description
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, Lists, Archer, Active Directory, Endpoint, Respond, REST API or File Reputation server.
Name	The unique name to identify the data source. For example, Respond.
Address	The IP address or hostname of the data source.
Port	The connection port for the data source and vary based on the data source being added. For example, for Endpoint the port is 9443, for Lists the port is 80 and so on.

Context Hub Lists Tab

In the **Lists** tab, you can create and configure lists for Context Hub. Navigate to **(Admin) > Services** > Select Context Hub service > **View** > **Config** > **Lists** tab.

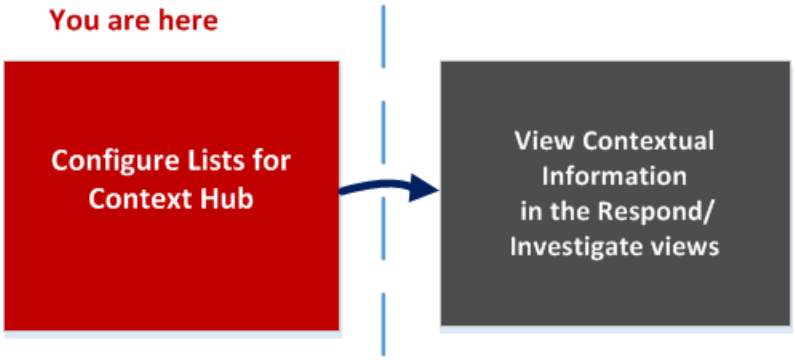
The Lists tab of the Context Hub service allows you to create one or more lists and add relevant list values to the list. These lists are automatically considered as data sources for the Context Hub service.

These lists may be populated with items either by importing external or custom feed CSV files or by adding meta values by using the option Add/Remove from List in Investigation and Respond views.

Note: You can also create lists and add list values from Respond and Investigation views. For more information, see the *NetWitness Respond User Guide* and the *NetWitness Investigate User Guide*.

Workflow

This workflow shows the procedure to configure lists for Context Hub service and to view contextual information in the Respond and Investigate views.



Creating one or more list is the first task in this workflow. The lists can contain supported metas such as an IP address, User, Host, Domain, MAC address, File Name or File Hash. The next task is to analyze or use the list data to view contextual data in Respond and Investigate views.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure List Data Source for Context Hub*	Configure Lists as a Data Source
Administrator/ Analyst	View Contextual Information in Respond View	See the *NetWitness Respond User Guide*.

Role	I want to ...	Show me how
Administrator/ Analyst	"Manage Lists and List Values in Investigation	See the *Investigate User Guide*.
Administrator/ Analyst	Create a list	See the *NetWitness Respond User Guide* and *Investigate User Guide*
Administrator/ Analyst	Update a list	See the *NetWitness Respond User Guide* and *Investigate User Guide*
Administrator/ Analyst	Delete list	See the *NetWitness Respond User Guide* and *Investigate User Guide*
Administrator/ Analyst	Import a list	Import or Export Lists for Context Hub
Administrator/ Analyst	Export list	Import or Export Lists for Context Hub

*You can complete this task here (that is in the Context Hub Lists Tab).

Related Topics

- Context Hub Data Sources Tab
- "Troubleshooting NetWitness Investigate" in the *NetWitness Investigate User Guide*

Quick Look

The following example illustrates how to add lists for Context Hub service.

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.

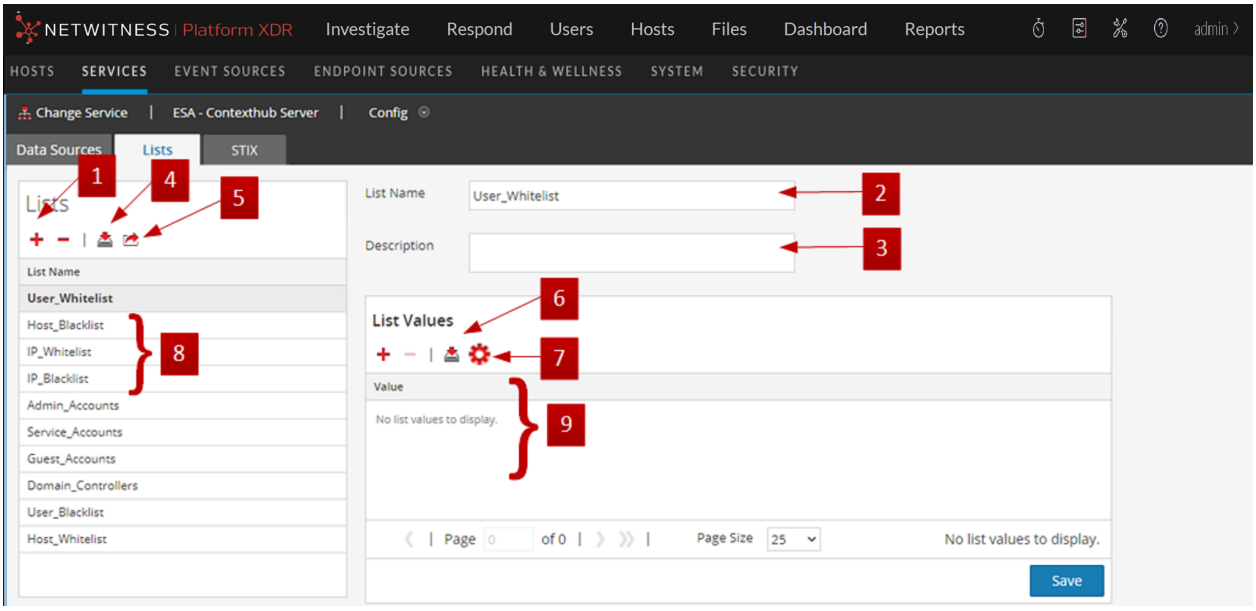
By default, 10 empty single-column lists are available in NetWitness11.1. These lists are empty and you need to add information to these lists. The out of the box 10 list names are used in ESA rules, for more information on ESA rules, see the *Alerting with ESA Correlation Rules User Guide*. For users upgrading from previous versions, they will be able to view these new lists in addition to their previously created lists. The lists available by default are:

- Admin_Accounts
- Guest_Accounts
- Service_Accounts
- User_Blacklist
- User_Whitelist
- Host_Whitelist

- Domain_Controllers
- IP_Blacklist
- IP_Whitelist
- Host_Blacklist

Note: If a list with the same name already exists prior to updating to or installing NetWitness12.3.0.0, then that list will be retained. Either rename that list before updating to 11.1 or update the contents in such a way that it can be used in ESA rules.

The lists are available in ESA rules tab in CONFIGURE > ESA Rules > Settings > Enrichment Sources. For more information on ESA rules, see the *Alerting with ESA Correlation Rules User Guide for Version 11.1*.
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.



1	Click + to add a new list.
2	Name that identifies the list.
3	Description of the list.
4	Click to import list(s) to Context Hub.
5	Click to export a list to the local machine.
6	Click to import list values to selected list.
7	Click to add or edit entity mapping.

8	Displays the custom list(s) that are added to Context Hub.
9	Displays the list values that are added to the selected list.

Toolbar

The following table describes the toolbar actions.

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

Note: You can select multiple lists at a time. Do one of the following:
1. Select a list, press and hold Ctrl key, and click the lists to be selected.
2. Select a list, press and hold Shift Key, and use arrow keys to select other lists.

List View Options

The following table describes the Lists configurations.

Feature	Description
List Name	Unique name to identify the list.
Description	Description of the list.
Save	Saves the changes made to the list.

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For instructions, **Navigate to Context Summary Panel and View Additional Context** topic in the *Investigate User Guide*.

Context Hub STIX Tab

In the **STIX** tab, you can create and configure Structured Threat Information eXpression (STIX) data source for Context Hub. Navigate to  **(Admin) > Services**> Select Context Hub service > **View** > **Config** > **STIX** tab.

The STIX tab of the Context Hub service allows you to create one or more STIX, REST URLs, or TAXII data sources and edit them whenever required. When STIX is configured, Context Hub service automatically considers it as a data source.

What do you want to do?

Role	I want to ...	Show me how
Administrator	Configure STIX Data Source for Context Hub*	Configure STIX as a Data Source
Administrator/ Analyst	View Contextual Information in Respond View	See the *NetWitness Respond User Guide*.

*You can complete this task here (that is in the Context Hub Lists Tab).

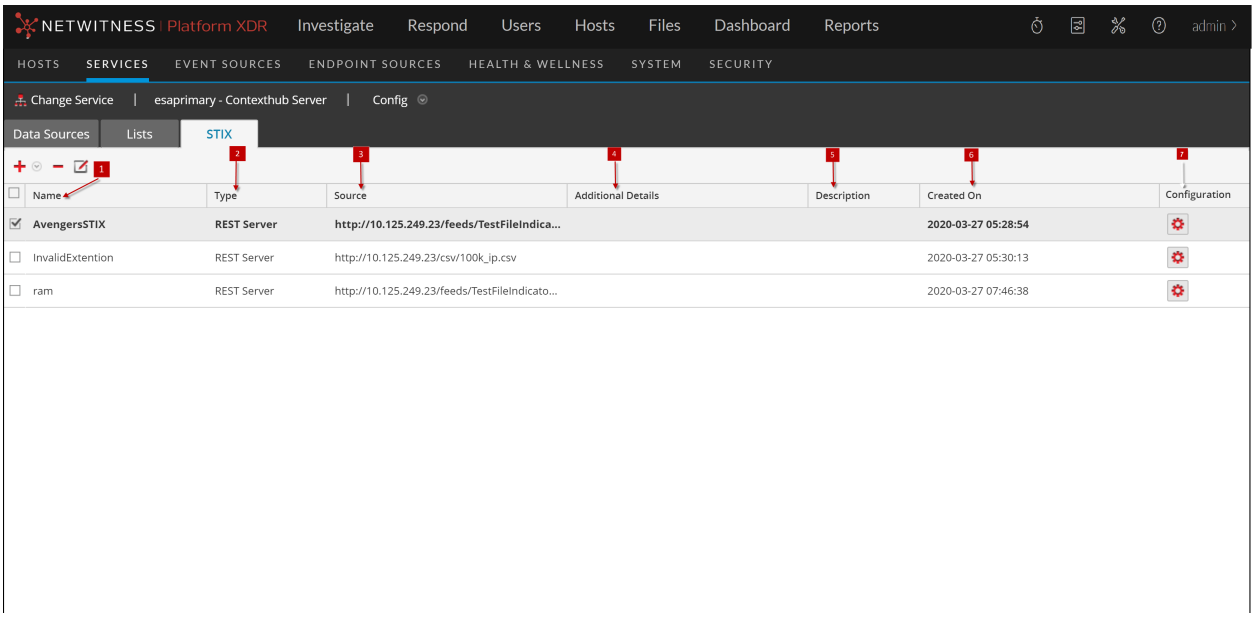
Related Topics

- Configure STIX as a Data Source

Quick Look

The following example illustrates how to add STIX to Context Hub service.

The STIX tab consists of add, delete and edit data sources options.



1	Name that identifies the added STIX source.
2	Type of data source - REST server, STIX or TAXII server.
3	The path of the source from which the STIX files are obtained.
4	Additional details related to the data source being added.
5	Description of the data source.
6	Date when the data source was created.
7	Click to edit the selected data source and configure advanced settings.

Toolbar

The following table describes the toolbar actions.

Feature	Description
	Add a new data source such as File, REST Server, or TAXII Server. For more information, see Configure STIX as a Data Source .
	Delete the selected data source.
	Edit the selected data source.

The following table describes the all the data source server configuration options.

Field	Description
Common Configuration Options	

Field	Description
Enabled	Select this checkbox to enable the configuration.
Name	Provide a name to the data source you want to add.
Description	Description of the data source.
Cancel	Click to revert the data source addition.
Validate	Click to verify the URL path to the Server.
Save	Click to save the configuration and add the required server as a data source.
REST Server Configuration Options	
URL	URL of the REST server.
Username (Optional)	Provide the username of the REST server if it needs to be authenticated.
Password (Optional)	Provide the password of REST server if it needs to be authenticated.
Trust All Certificates	Select this checkbox to trust all certificates.
Certificate File	Click browse to navigate to the location of the certificate file.
TAXII Server Configuration Options	
URL	URL of the TAXII server.
Username (Optional)	Provide the username of TAXII server if it needs to be authenticated.
Password (Optional)	Provide the password of REST server if it needs to be authenticated.
Client Certificate	Browse to upload a pkcs12 format client certificate available on your local system.
Certificate Password	Enter the password to the certificate, if it is password-protected.
UserProxy	Select this checkbox to enable proxy.
Trust All Certificates	Select this checkbox to trust all certificates.
Certificate File	Browse and select the certificate file.
TAXII Collections	Select the TAXII Collection name from the drop-down to automatically download the collection.
	Click to manually retrieve the list of available TAXII Servers, if the collections are not downloaded automatically.

Field	Description
STIX File Configuration Options	
File	Browse and select the STIX file.

Next steps

After completing the configuration, you can view the contextual data in the Context Summary Panel of the Respond view or Investigate view. For instructions, **Navigate to Context Summary Panel and View Additional Context** topic in the *Investigate User Guide*.

Troubleshooting

This topic provides information about possible issues that NetWitness users may encounter when setting up their ContextHub service in NetWitness.

Problem	Solutions
Prefetch for list fails if the list is created in append mode.	**Details:** The following error message is displayed in logs indicating that, entries in list exceeds the max allowed. `Error setting data source entries com.rsa.asoc.contexthub.exception.ContextHubException: total.entries.exceed.max` Also, Health & Wellness sets the stat - `Contexthub.Datasource.Health.Data-Sources-Health` to `Unhealthy` and displays the names of the lists for which prefetch has failed. For example, number of entries in the list are 50001 and number of records in the CSV file are 50001 (user did not change the csv since last prefetch.). Upper limit on number of entries in list is 100,000. Now on prefetch, Context Hub will try to append 50001 entries to the list but since 50001 + 50001 > 100,000, prefetch fails. **Solutions:** You should add only those entries in the .csv file which they wish to append to the existing .csv file. If, you do not want to append any entries to the list then perform one of the options, as applicable: • If you created the list with headers: remove all rows from the csv except the header. • If you created list without headers: you should have 0 rows in csv.
The Respond service is not able to send incidents to Archer with third party signed certificates.	As a workaround, you need to run a command to add a PEM certificate to the Respond trust store Run the following command on the Respond host: `security-cli-client --add-trusts -s respond-server -x <pem_certfilename> -u <username> -k <password>` Where: • `<pem_certfilename>` is the name of the certificate file. • `<username>` and `<password>` are your NetWitness administrator credentials.
SSL handshake with Archer certificate fails while adding it as a data source.	Use an archer generated certificate with the Trust All Certificates option configured.

Problem	Solutions
Pivot to Investigate option on the Respond page does not navigate to the correct link.	When you stop and restart the RabbitMQ server, the Pivot to Investigate option available on the respond screen is not visible. And the context panel for Pivot to Investigate reopens the same page. You need to restart the jetty service on the NetWitness Server, login to the NetWitness Server Host and enter the service jetty restart command.
When you import a list with missing quotes such as "172.16.0.0, the list is saved without any data to display.	This is because of the Apache bug (CSV-141), which does not parse CSV files with incorrect formats. To fix, import a list with correct quotes to avoid displaying an empty file. For example, “172.16.0.0”, “host.mycompany.com” and so on.
Increasing the limit settings for Alerts and Incidents leads to lookup error.	By default, the limit settings to view number of Alerts and Incidents is set to 50. If the limit is increased, the looked-up meta for alerts and incidents may lead to lookup error. This happens due to an internal database restriction. Make sure to keep the limit for viewing number of Alerts and Incidents to 50 or less.
Multiple incident and alert tabs are displayed while editing advanced configuration of Respond datasource.	You must delete duplicate entries in the Context Hub MongoDB and restart the MongoDB Context Hub Server. Perform the following: 1. Log in to control MongoDB on Admin Server. 2. Go to contexthub-server > ds_meta collection. **Note:** Make a note of '_id' value of duplicate entries for the incident and alerts documents that you want to delete. 3. In the ds_meta collection, delete 1 Incident and 1 Alert document. Once the duplicate entries are deleted only 1 Incident and 1 Alert type document will be available in the ds_meta collection. 4. Log in to application MongoDB on ESA Primary. 5. Go to contexthub-server, locate and delete the below collections: • ds_entries*_*<id-of-incident-doc-deleted-in-step 3> • ds_entries*_*<id-of-alert-doc-deleted-in-step 3> 6. Under bookmark_store collection, locate and delete documents with id same as _id of Incident and Alert from ds_meta collection. 7. Restart Context Hub Server.