



Context Hub Configuration Guide

for Version 11.0



Copyright © 1994-2017 Dell Inc. or its subsidiaries. All Rights Reserved.

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

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

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

	7
How Context Hub Works	8
Overview of Context Hub Configuration	9
Configure Data Sources for Context Hub	10
Configure Lists as a Data Source	11
Configure Archer as Data Source	16
Configure Active Directory as a Data Source	20
Configure Netwitness Endpoint as a Data Source	24
Configure Respond as a Data Source	28
Configure Live Connect as a Data Source for Context Hub	30
Configure Context Hub Data Source Settings	35
Import or Export Lists for Context Hub	40
Import a List	40
Import Single-Column List	40
Import Values to an existing List	42
Export List for Context Hub	42
Configure Meta Type Mapping for Context Hub	44
Context Hub References	47
Context Hub Data Sources Tab	48
Workflow	48
What do you want to do?	48
Related Topics	49
Quick Look	49
Context Hub Lists Tab	52
Workflow	52
What do you want to do?	52
Related Topics	53
Quick Look	53

Troubleshooting **57**

 Possible Issues 57

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 Suite 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.

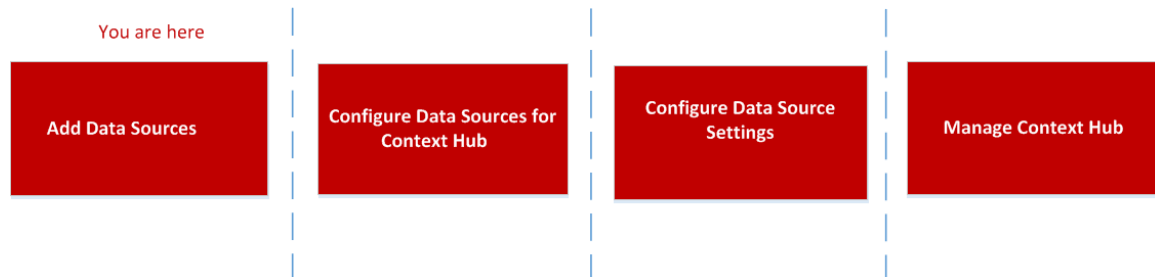
Respond- Provides contextual information of a specific meta available in respond and enables analyst to respond faster based on context data.

Live Connect - Provides contextual information for IP addresses, Domains and File Hashes from RSA Live Connect Threat intelligence community server.

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 Suite.

Note: You can have only one Context Hub service instance enabled in your NetWitness Suite deployment. If there are multiple ESA service in NetWitness Suite, 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 Data Sources for Context Hub

To use the enrichment lookup capability and to view the related contextual information, you must configure the data sources for the Context Hub service. You can add the supported data sources such as Lists, RSA Archer, Active Directory, NetWitness Endpoint, Respond, and Live Connect.

Prerequisites

- Ensure that ESA host is available. In case of older versions, administrator must first upgrade ESA host to 11.0
- Ensure Context Hub is automatically added to the NetWitness Suite through orchestration and is enabled.
- Ensure to add the Data Sources.

Configure Lists as a Data Source

Lists as a Data Source uses 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 list 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.

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 Suite.
- 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.

Add List data source using Local File Store

To add 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  > **LISTS**.
The **Add Data Source** dialog is displayed

4. By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, view the list in the list tab and view the contextual information.
5. Select the **Local File Store** Connection Type.

Add Data Source

☒ **Enable**

List Connection Details

Connections: ☐ HTTP(S) ☒ Local File Store

Name:

Path:

Description:

With Column Headers: ☒

Validate

Validation successful

Cancel **Next**

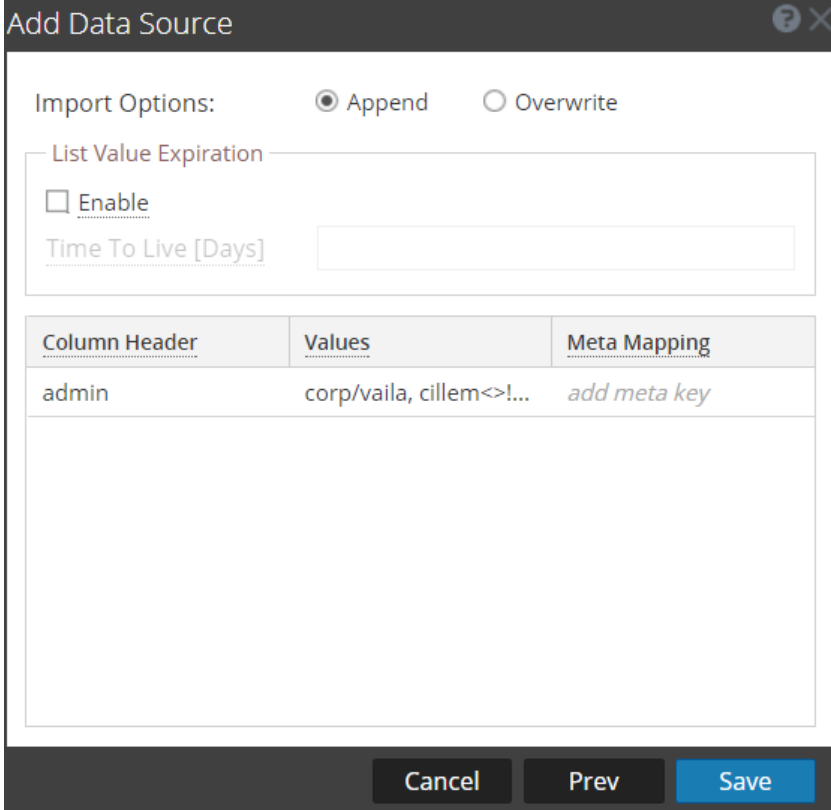
6. Provide the following database connection details:
 - Enter the following fields for Local File Store Connection Type:
 - **Name:** Provide a name for the list data source.
 - **Path:** This field displays all the data files available in the data folder `/var/lib/netwitness/contexthub-server/data`, 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.

Note: For Local File Store connection type, the file can be mounted or copied to the local drive. Also, the user must have read permission to the `/var/lib/netwitness/contexthub-server/data` folder located on the Context Hub machine.

5. Click **Validate**.
If the validation fails, you cannot add the data source.

6. Click **Next**.

The next dialog is displayed.



The dialog box titled "Add Data Source" contains the following elements:

- Import Options:** Two radio buttons, "Append" (selected) and "Overwrite".
- List Value Expiration:** A section containing an unchecked "Enable" checkbox and a "Time To Live [Days]" text input field.
- Table:** A table with three columns: "Column Header", "Values", and "Meta Mapping".

Column Header	Values	Meta Mapping
admin	corp/vaila, cillem<>!...	add meta key
- Buttons:** "Cancel", "Prev", and "Save" buttons at the bottom right.



7. 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.
8. 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.
9. 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.

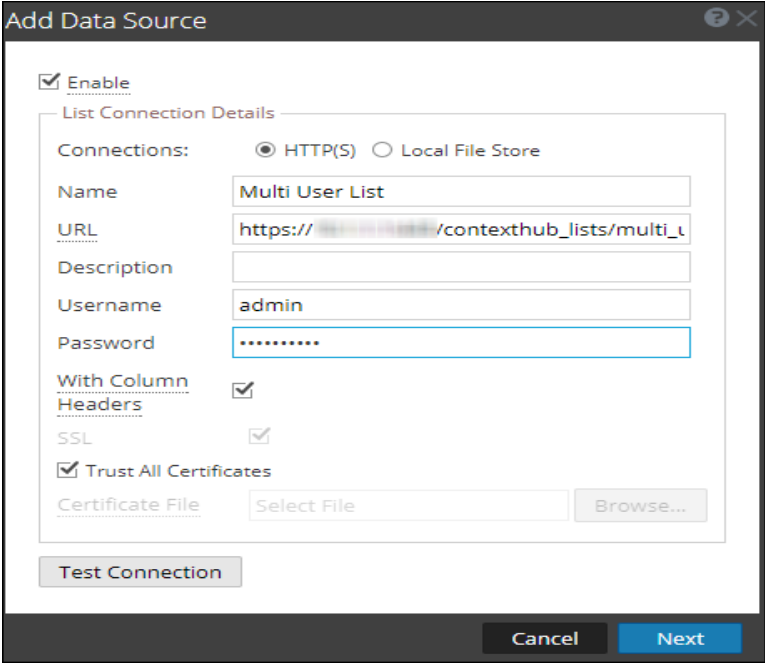
- **Meta Mapping:** Maps a column header field to a meta type.
- **Values:** Displays the first three values from the imported list.

9. 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  > **LISTS**.
The **Add Data Source** dialog is displayed.
4. Select the HTTP(S) Connection Type.

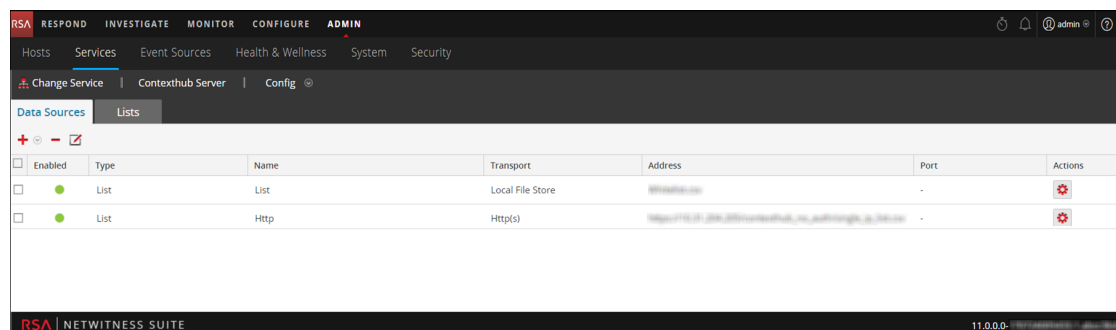


- Enter the following fields for HTTP(S) Connection Type:
 - **Name:** Provide a name for the list data source.
 - **URL:** Enter the path of the CSV file available on the HTTP(S) location along with the host name or IP address of the remote machine where the list is stored. The URL must be of the format: `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 Investigation and Malware Analysis 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.

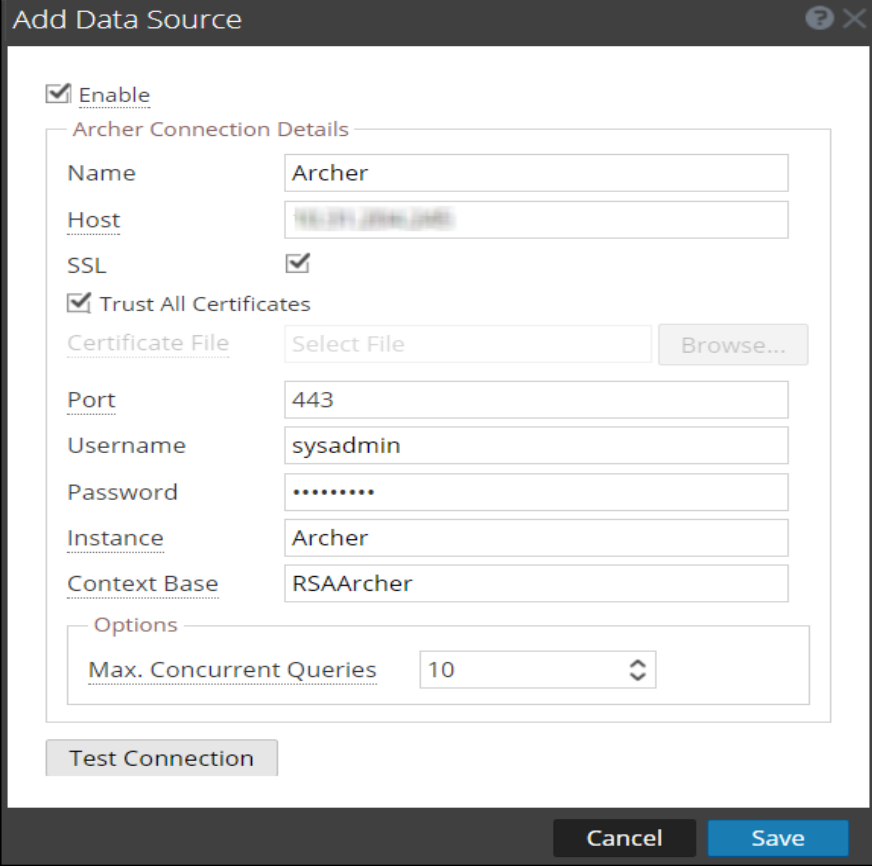
Prerequisites

Before you configure Archer data source, ensure that:

- Context Hub service is available in **ADMIN>Services** view of NetWitness Suite.
- 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  > **Archer**.
The **Add Data Source** dialog is displayed.



The image shows a screenshot of the 'Add Data Source' dialog box for the Archer service. The dialog has a title bar with a question mark and a close button. It contains several sections: 'Enable' with a checked checkbox, 'Archer Connection Details' with fields for Name (Archer), Host (192.168.1.100), SSL (checked), Trust All Certificates (checked), Certificate File (Select File with a Browse... button), Port (443), Username (sysadmin), Password (masked with dots), Instance (Archer), and Context Base (RSAArcher). There is also an 'Options' section with 'Max. Concurrent Queries' set to 10. At the bottom, there is a 'Test Connection' button and a 'Cancel' button, and a 'Save' button in the bottom right corner.

Add Data Source

☒ **Enable**

Archer Connection Details

Name: Archer

Host: 192.168.1.100

SSL: ☒

☒ **Trust All Certificates**

Certificate File: Select File Browse...

Port: 443

Username: sysadmin

Password:

Instance: Archer

Context Base: RSAArcher

Options

Max. Concurrent Queries: 10

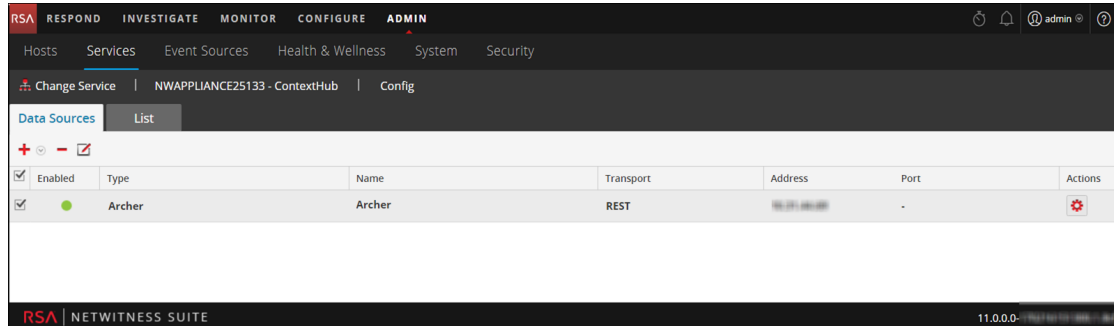
Test Connection Cancel Save

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:
 - **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 Endpoint 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 *Investigation and Malware Analysis User Guide*.

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 Suite.
- 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 **+> AD**.

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

The screenshot shows the 'Add Data Source' dialog box with the following fields and options:

- ☒ **Enable**
- Active Directory Connection Details**
 - Name**: AD Data Source
 - Host**: [IP Address]
 - SSL**: ☒
 - ☒ **Trust All Certificates**
 - Certificate File**: Select File Browse...
 - Port**: 636
 - Bind User DN**: cn=Administrator,cn=Users,dc=sub,dc=sas
 - Password**: [Masked]
 - Search Base DN**: cn=Administrator,cn=Users,dc=sub,dc=sas
- Options**
 - Max. Concurrent Queries**: 10
- Test Connection** button
- Cancel** and **Save** buttons at the bottom right.

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.

6. Provide the following database connection details:

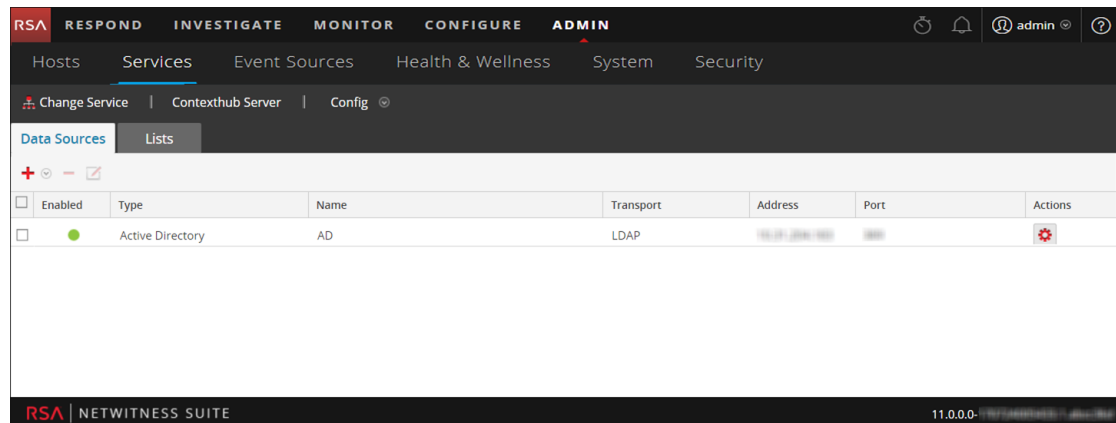
- By default, the **Enable** checkbox is selected. If this option is unchecked, the save button is disabled, you cannot add the data source, and cannot view the contextual information.
- Enter the following fields.
 - **Name:** Enter a name for the AD data source.
 - **Host:** Enter the host name or 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.

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

8. 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 *Investigation and Malware Analysis 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 Suite.
- 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 [RSA Link](#).

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

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

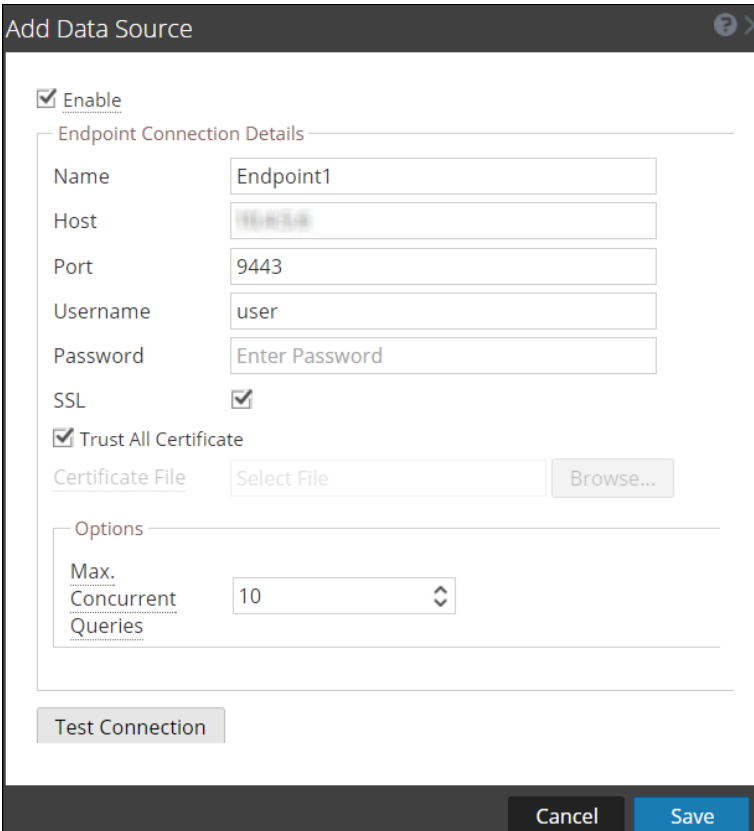
The Services view is displayed.

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.



The "Add Data Source" dialog box is shown. It has a title bar with a question mark and a close button. The dialog is divided into sections. The first section has a checkbox labeled "Enable" which is checked. Below this is a section titled "Endpoint Connection Details" with fields for Name (Endpoint1), Host (192.168.1.100), Port (9443), Username (user), and Password (Enter Password). There is also a checkbox for "SSL" which is checked, and a checkbox for "Trust All Certificate" which is checked. Below these is a "Certificate File" section with a "Select File" button and a "Browse..." button. The next section is titled "Options" and contains a "Max. Concurrent Queries" field with a value of 10 and a spinner. At the bottom of the dialog is a "Test Connection" button. The footer of the dialog has "Cancel" and "Save" buttons.

Add Data Source

☒ Enable

Endpoint Connection Details

Name: Endpoint1

Host: 192.168.1.100

Port: 9443

Username: user

Password: Enter Password

SSL: ☒

☒ Trust All Certificate

Certificate File: Select File Browse...

Options

Max. Concurrent Queries: 10

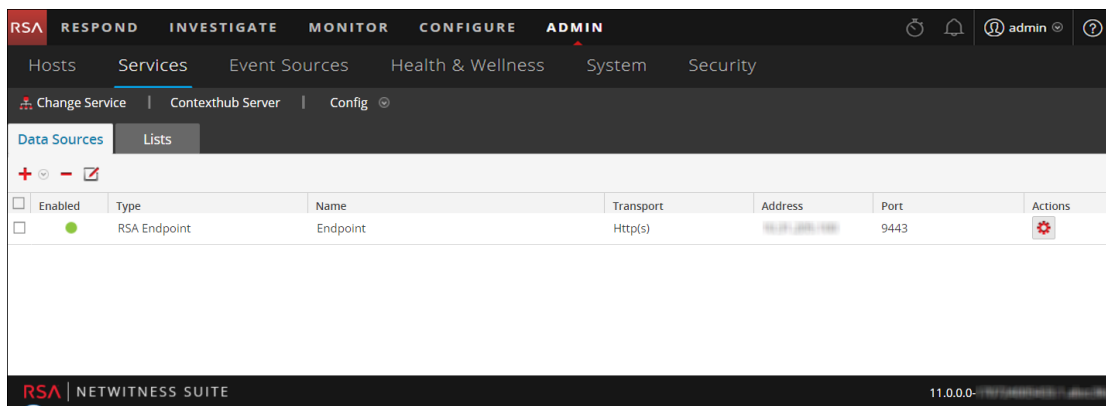
Test Connection

Cancel Save

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:
 - **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 Suite 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 Investigation and Malware Analysis 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

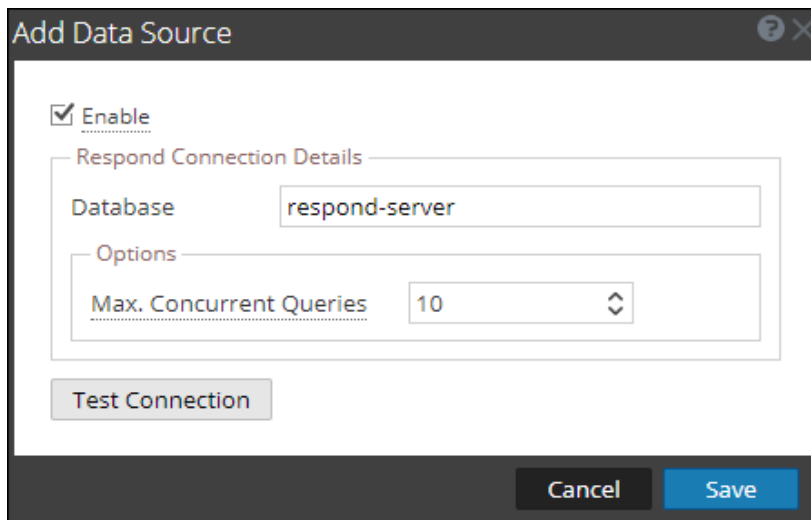
Before you configure Respond data source, ensure that:

- Context Hub service is available in **ADMIN > Services** view of NetWitness Suite.
- 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.

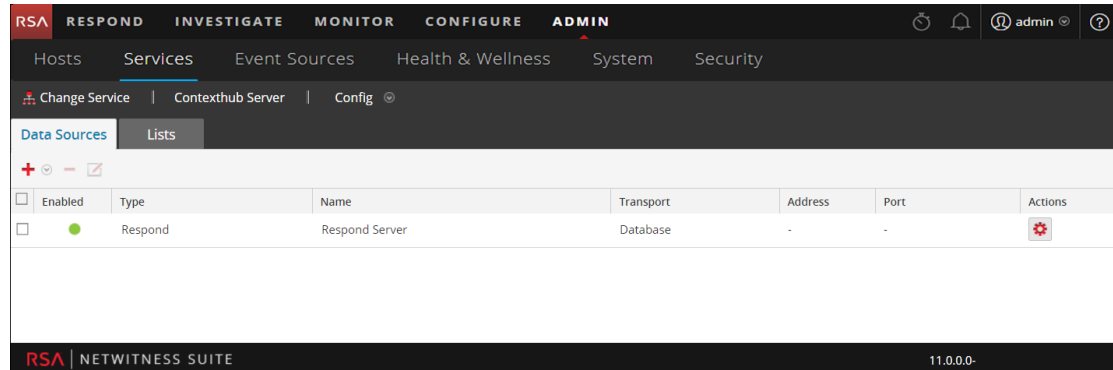


The image shows a screenshot of the 'Add Data Source' dialog box in the NetWitness Suite. The dialog has a title bar with a question mark and a close button. Inside, there is a section for 'Respond Connection Details'. At the top, there is a checkbox labeled 'Enable' which is checked. Below this, there is a 'Database' field with the value 'respond-server'. Underneath the database field is an 'Options' section containing a 'Max. Concurrent Queries' field with the value '10' and a dropdown arrow. At the bottom of the dialog, there is a 'Test Connection' button. The bottom of the dialog features a dark bar with 'Cancel' and 'Save' buttons.

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

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 Investigation and Malware Analysis Guide*.

Configure Live Connect as a 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 NetWitness® Suite and RSA NetWitness® Endpoint 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.

Prerequisites

Ensure that:

- Context Hub is enabled and the service is available in Admin > Services view of NetWitness Suite.
- 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 or Disable Live Connect Data Source

To enable or disable Live Connect 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 **Threat Insights**.

Additional Live Services


Live Feedback

Customer usage data, including usage metrics, threat detection enabled, number of enabled ESA rules and current version of NetWitness Suite hosts, shall automatically be shared with RSA upon this system's connection to the Internet. This data is automatically shared only if Live account is configured and shall be protected in accordance with the applicable license agreement. All such data shall be anonymized and shall not have any Personally Identifiable Information. [Learn more.](#)


☒ **Share Live Content Usage Details** -  Show More

RSA Live Connect (Beta)

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 NetWitness Suite and RSA NetWitness Endpoint customer community. The RSA Live Connect cloud service stores this information in a secure environment and provides an anonymous, secure 2-way channel over SSL between the RSA Live Connect cloud and the RSA NetWitness Suite/RSA NetWitness Endpoint customers to share and monitor de-identified and obfuscated threat intelligence. This threat intelligence information can be leveraged by analysts for identifying and investigating potential security threats. [Learn more.](#)

☒ **Enable Threat Insights**  Connected

This Live Connect option 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 investigation. In addition, analysts can voluntarily provide anonymous risk assessment feedback on the specific intelligence to Live Connect.

☒ **Enable Analyst Behaviors**  Connected

This Live Connect option is an automated data collection service. It is responsible for gathering meta data captured locally by NetWitness Suite and securely sending it to RSA Live Connect. This data will be leveraged for deep analysis to drive and improve the RSA Live and Live Connect threat intelligence services in order to proactively identify potential security threats.

NOTE: The type of data that potentially could be shared from a user's network to the RSA Live Connect cloud service could encompass various types of meta data captured by the NetWitness Suite product such as ip.src, ip.dst, ip.addr, device.ip, alias.ip, alias.host, paddr, sessionid, domain.dst, domain.src.

Customers who do not wish to receive threat intelligence and/or share de-identified and anonymized information with the Live Connect service should change their settings in the [Live Connect](#) feature and/or contact RSA Customer Support for more information.

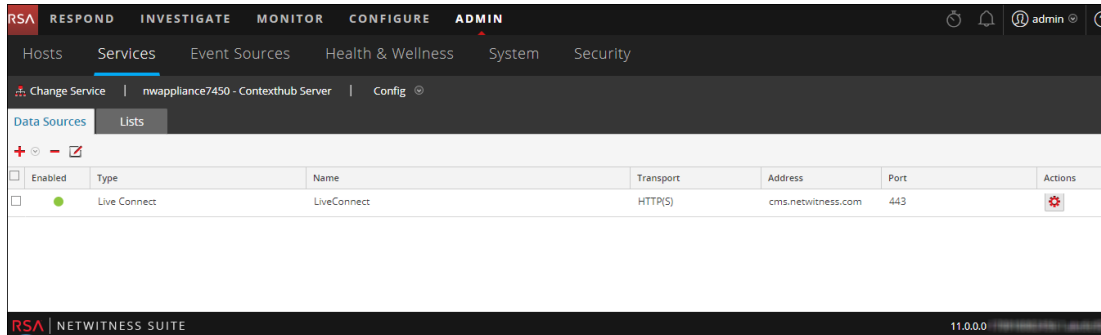
[Apply](#)

4. Click **Apply**.

Live Connect data source is enabled for Context Hub service.

- 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 (●).



- 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:

- In the main menu, select **Admin > Services**.
The Services view is displayed.
 - In the **Services** panel, select the Context Hub service, and > **View > Config**.
The Services Config view is displayed.
 - 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.

To configure responses and meta mapping for Live Connect data source, see [Step 3. Configure Responses for Context Hub Data Sources](#).


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 NetwitnessRespond User Guide* and the *RSA Netwitness Investigation and Malware Analysis Guide*.

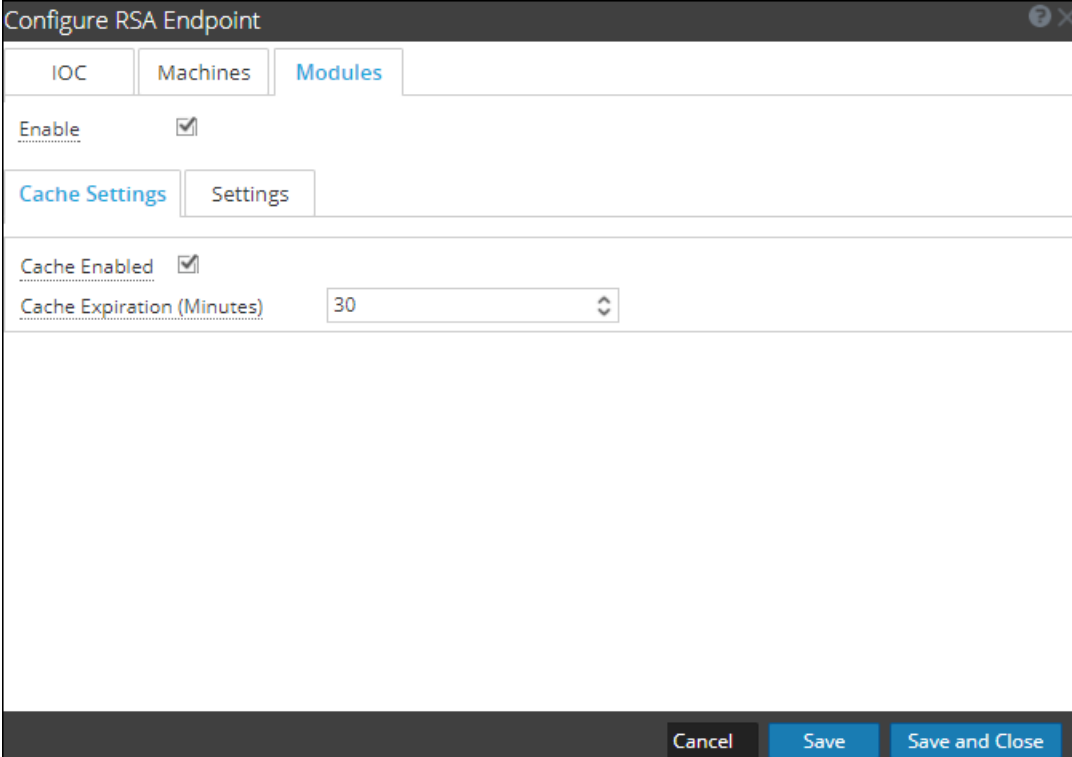
Configure Context Hub Data Source Settings

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 screenshot shows a dialog box titled "Configure RSA Endpoint". It has three tabs: "IOC", "Machines", and "Modules". The "Enable" checkbox is checked. Below the tabs are two sub-tabs: "Cache Settings" and "Settings". Under "Cache Settings", the "Cache Enabled" checkbox is checked, and the "Cache Expiration (Minutes)" is set to 30. At the bottom of the dialog are three buttons: "Cancel", "Save", and "Save and Close".



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.
Cache Settings	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Time to Live (Days): Enter the number of days you want to the list values to be retained.</p>
Meta Mapping	<p>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.</p> <p>Meta Type: Entities available in Context Hub.</p> <p>Context Hub Fields: Column headers from CSV file you have added when adding List Data Source.</p>
Minimum IIOC Score	The minimum IIOC score to be considered for fetching contextual information of Netwitness Endpoint modules.
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.

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]
 RSA Archer	Archer	Cache Settings Cache Enabled Cache Expiration (Minutes)

Data Source (Connection)	Response Supported Groups	Field Settings
 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]
 RSA 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

Data Source (Connection)	Response Supported Groups	Field Settings
Respond	 Alerts	Context Panel Settings Data Prefetch Settings Query Last [Days]
	 Incidents	Cache Settings Cache Enabled Cache Expiration (Minutes)
 Live Connect	Domain	Cache Settings Cache Enabled Cache Expiration (Minutes)
	File	Settings Context Panel Settings
	IP	

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 Suite.

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 the next the schedule recurs.

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.


The screenshot shows the RSA NetWitness Admin console. The top navigation bar includes tabs for RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. Under the CONFIGURE tab, there are sub-tabs for HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, and SYSTEM. The 'List' tab is selected. The main content area is divided into two panels. The left panel, titled 'Lists', contains a table with the following data:

List Name	Whitelist
test list1	
list2	

The right panel, titled 'List Values', contains a table with the following data:

Value	Whitelist
10.10.10.10	
2.2.2.2	
xyz.com	
1.1.1.1	

A 'Save' button is located at the bottom right of the right panel.

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

The **Import List** dialog is displayed.

The 'Import List' dialog box is shown. It has a title bar with a close button. The main area contains two fields: 'Upload File (Csv)' with a 'Browse' button, and 'Delimiter' with a dropdown menu showing 'LF'. At the bottom, there are 'Cancel' and 'Upload' buttons.

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 importing. For information on how to import multi-column list, see [Configure List Data Source for Context Hub](#).

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:

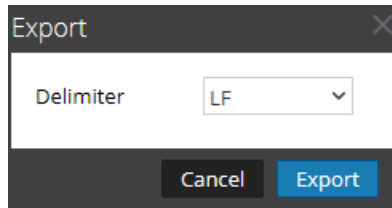
1. Go to **ADMIN > Services**.
The services view is displayed.
2. Service and click  > **View > Config**.
The Services Config View of the Context Hub service is displayed.
3. Click the **Lists** tab.
The Lists tab consists of the **Lists** panel and **List Values** panel.
4. In the Lists panel, select 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 Suite.

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.

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 Suite 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:

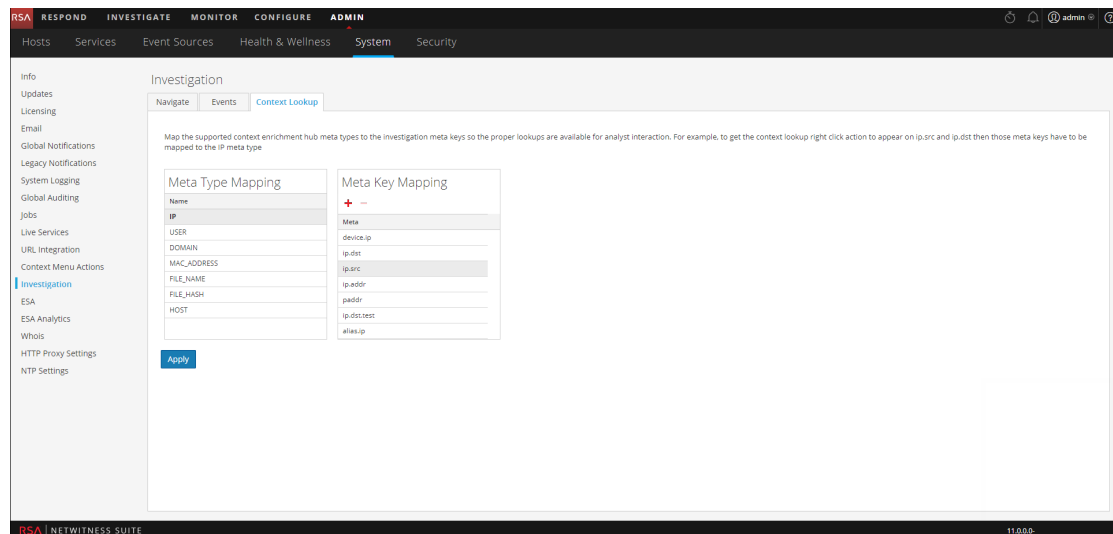
Meta Type Name	Meta Keys
IP	device.ip, ip.src, ip.dst, ip.addr, ipv6.src, alias.ip, ipv6.addr, device.ipv6, forward.ip, forward.ipv6, ipv6.dst, ipv6.addr, stransaddr, transaddr
USER	user.src, user.dst, username, event user
DOMAIN	domain.src, domain.dst, fqdn, web.domain, domain, sdomain, ddomain
MAC_ADDRESS	eth.dst, eth.src, alias.mac
FILE_NAME	filename, sourcefile
FILE_HASH	checksum

Meta Type Name	Meta Keys
HOST	device.host, alias.host, host.src, host.dst

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" format="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 References

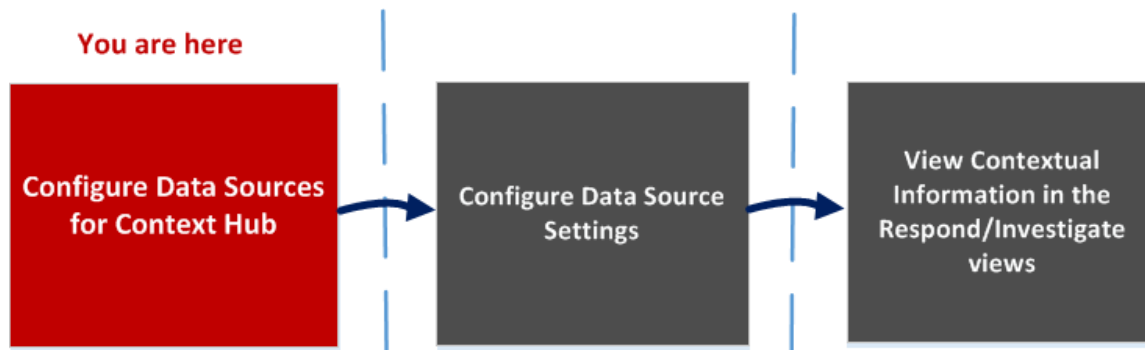
After you have configured the Context Hub service and the required data source, you can manage the settings for each data source. This will help in optimizing and customizing the lookup results.

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 Data Sources for Context Hub
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 <i>NetWitness Respond User Guide</i> .
Analyst	Add, create and delete list from the Respond or Investigate View	See the <i>NetWitness Respond User Guide</i> . See the <i>Investigation and Malware Analysis User Guide</i> .
Analyst	Add or delete an entry from an existing list	See the <i>NetWitness Respond User Guide</i> .

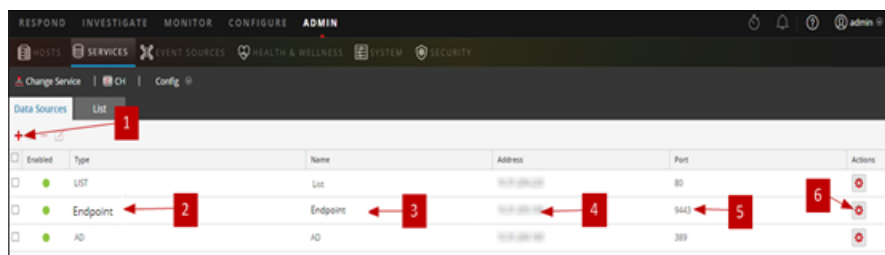
*You can complete this task here (that is in the Context Hub Data Sources Tab.)

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 Live Connect as a Data Source for Context Hub](#)

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 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 Configure Data Sources for Context Hub .
	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 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, or Live Connect.
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.

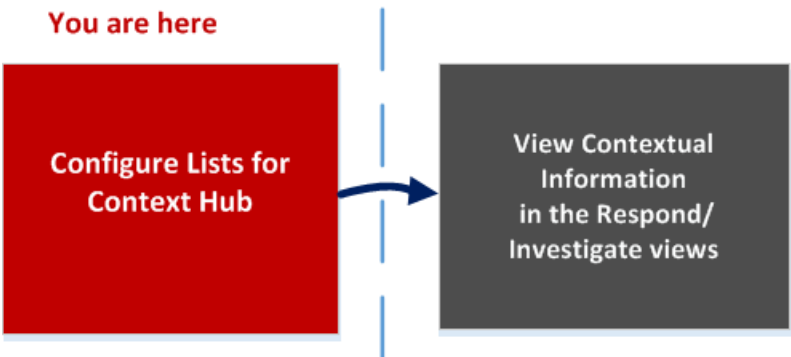
The Lists tab of the Context Hub service allows you to create one or more lists and add relevant list values to the list. These lists are automatically considered as data sources for the Context Hub service.

These lists may be populated with items either by importing 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 *RSA NetWitness Respond User Guide* and the *RSA NetWitness Investigation and Malware Analysis 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

Role	I want to ...	Show me how
Administrator/ Analyst	View Contextual Information in Respond View	See the <i>NetWitness Respond User Guide</i> .
Administrator/ Analyst	"Manage Lists and List Values in Investigation	See the <i>Investigation and Malware Analysis User Guide</i> .
Administrator/ Analyst	Create a list	See the <i>NetWitness Respond User Guide</i> and <i>Investigation and Malware Analysis User Guide</i>
Administrator/ Analyst	Update a list	See the <i>NetWitness Respond User Guide</i> and <i>Investigation and Malware Analysis User Guide</i>
Administrator/ Analyst	Delete list	See the <i>NetWitness Respond User Guide</i> and <i>Investigation and Malware Analysis User Guide</i>
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

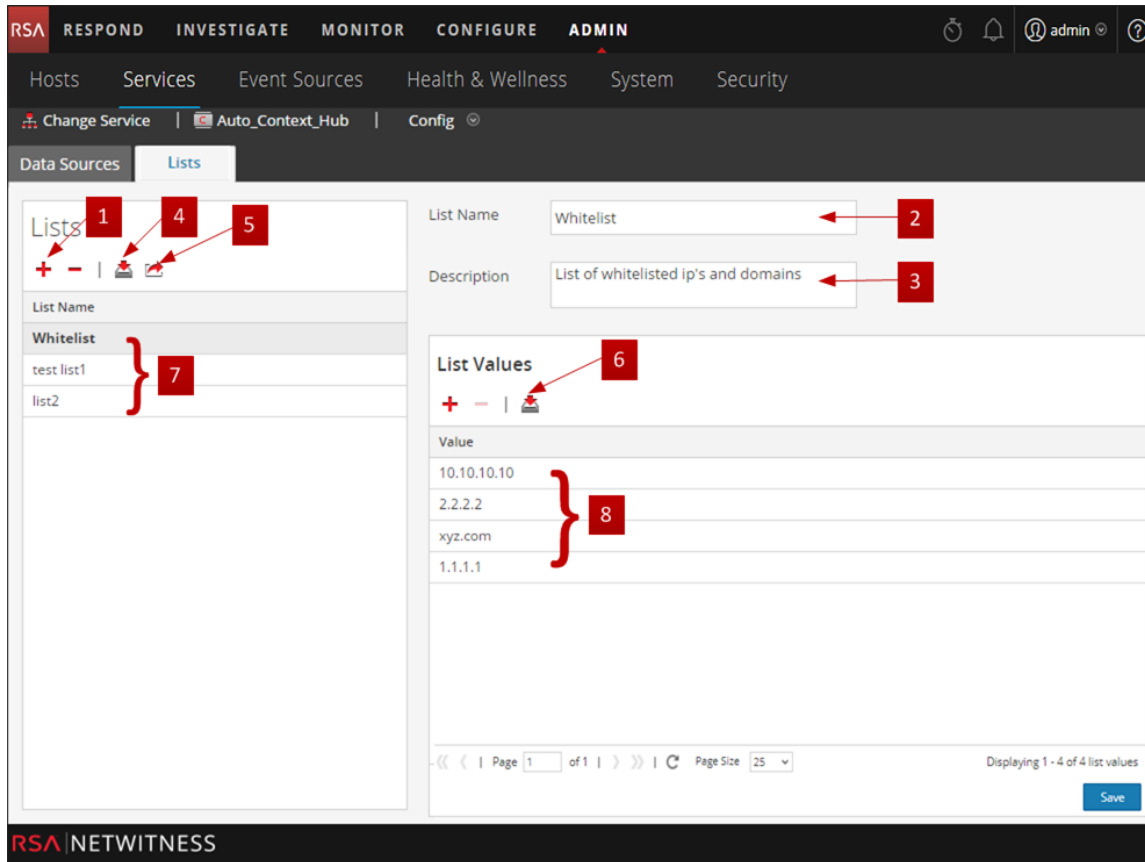
- [Context Hub Data Sources Tab](#)

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.





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 Displays the custom list(s) that are added to Context Hub.
- 8 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 for Context Hub .
	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 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 *Investigation and Malware Analysis User Guide*.

Troubleshooting

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

Possible Issues

Problem	Solutions
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.
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.

