RSA NetWitness Platform

Event Source Log Configuration Guide

Salesforce

Last Modified: Tuesday, November 5, 2019

Event Source Product Information:

Vendor: Salesforce
Event Source: CRM
Versions: API v1.0

RSA Product Information:

Supported On: Security Analytics 10.6.2 and later
Event Source Log Parser: cef

Note: The CEF parser parses this event source as **device.type=salesforce**

Collection Method: Plugin Framework
Event Source Class.Subclass: Host.Cloud

This document contains the following sections:

- Getting Started with NetWitness and Salesforce Integration
- Configure the Salesforce Event Source
- Set Up the Salesforce Event Source in RSA NetWitness
- Salesforce Collection Configuration Parameters

Getting Started with NetWitness and Salesforce Integration

The Salesforce event monitoring product gathers information about your Salesforce organization's operational events. You can use this information to analyze usage trends and user behavior. You can interact with event monitoring data by querying fields on the **EventLogFile** object (such as **Event Type** and **LogDate**). To view the underlying event data, query the **LogFile** field. The Event Type determines the schema of this field. For more information, see EventLogFile Supported Event Types on the Salesforce Developers Website.

Configure the Salesforce Event Source

This document describes how to configure the Salesforce event source using either the Classic View or the Lightning Experience View:

- Configure the Salesforce Event Source using Classic View or,
- Configure the Salesforce Event Source using Lightning Experience View

Configure the Salesforce Event Source using Classic View

To configure Salesforce, you must complete these tasks:

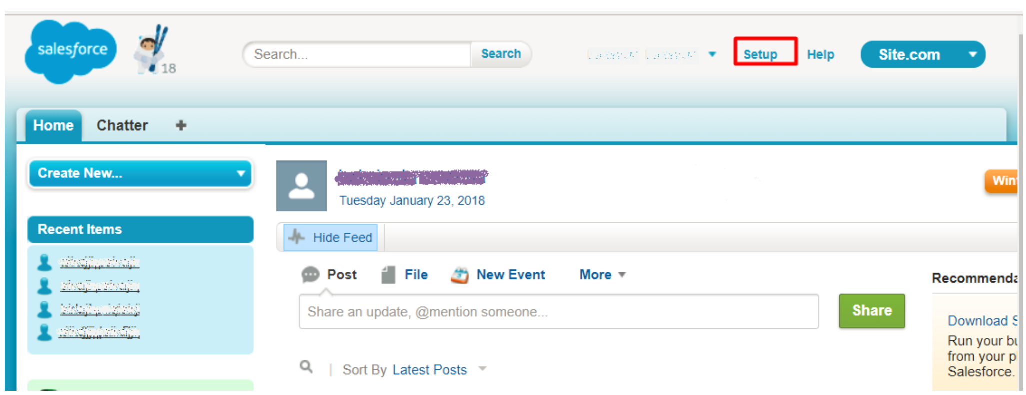
I. Create a Salesforce connected app (Classic)

II. Create a custom read-only profile (Classic)

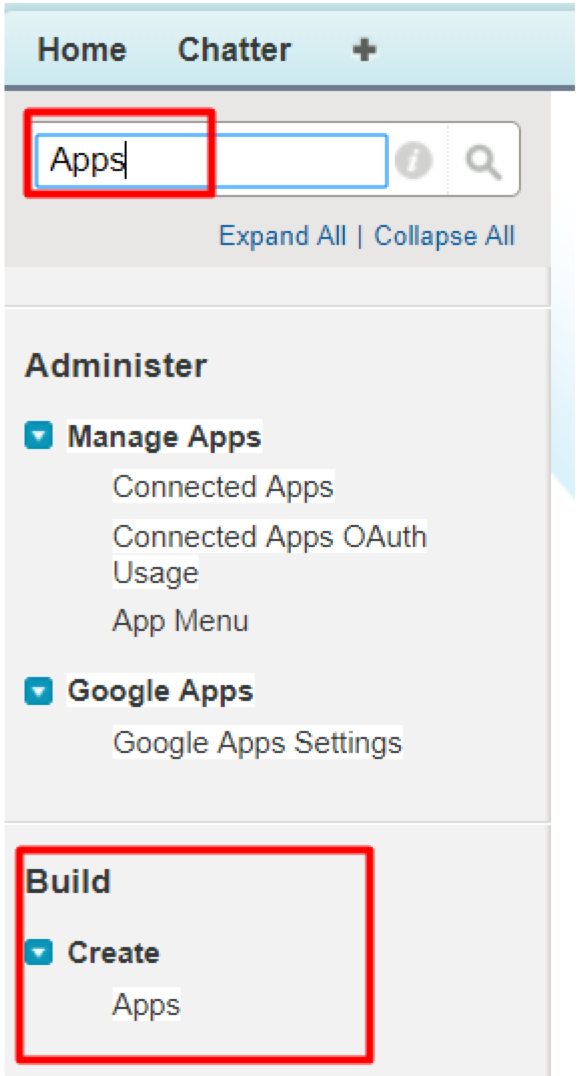
III. Create a user under Salesforce admin account (Classic)

Create a Salesforce connected app (Classic)

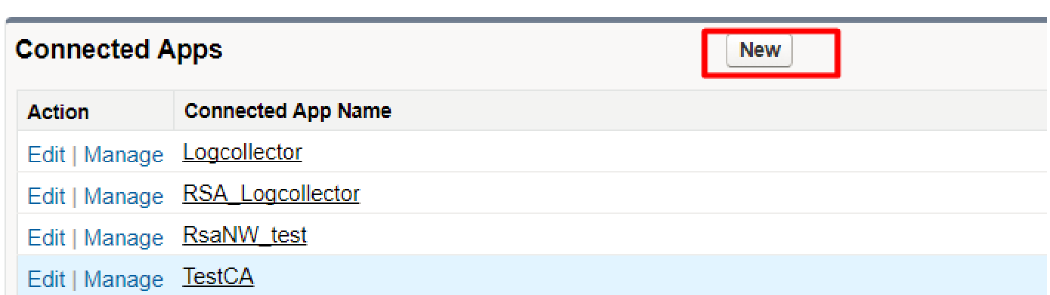
1. Log into to your Salesforce account through Salesforce portal: login.salesforce.com
2. In Salesforce Classic view, click on the Setup tab as shown here:



3. In **Quick Find/ Search** box enter **Apps**, then select **Apps** (under **Build | Create**).



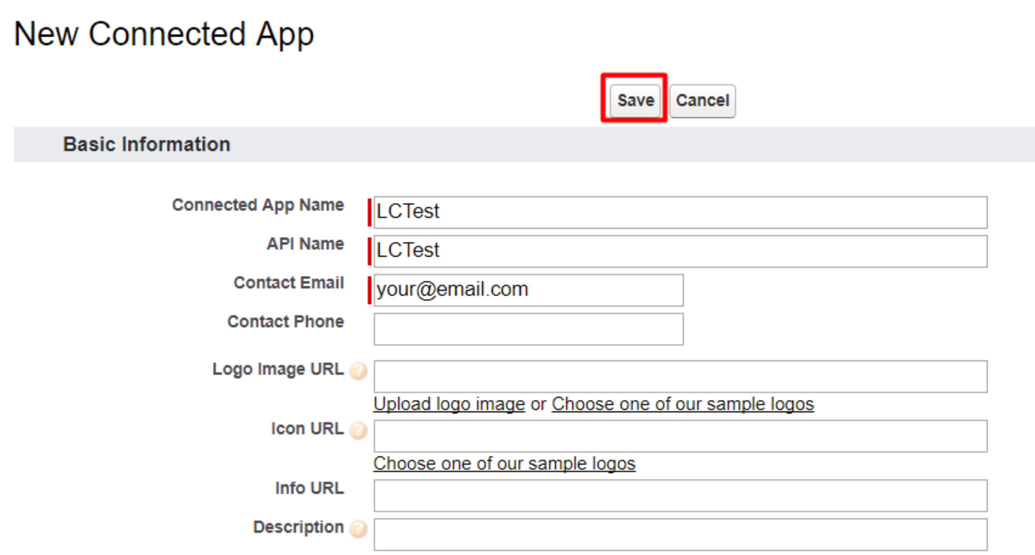
4. In the Connected Apps section, click **New**.

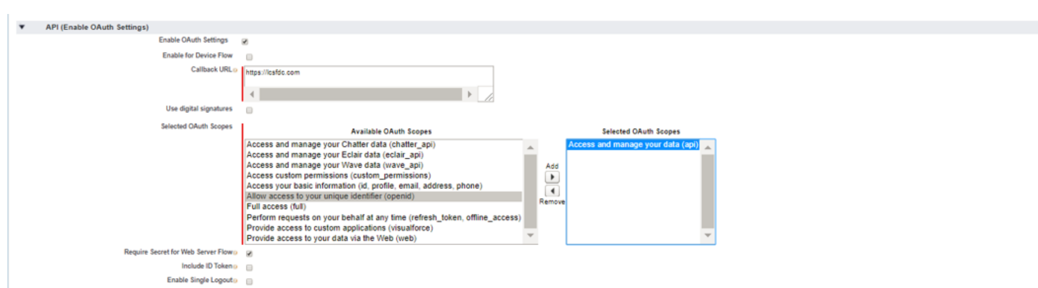


5. Make sure the following settings are defined in Salesforce to enable your new app:

Setting	Value
Connected App Name	Enter a name for the app, for example **Logcollector**.
API Name	This setting is populated automatically with the Connected App Name you enter.
Contact Email	Enter a valid email address.
Enable OAuth Settings	Make sure this is selected.
Callback URL	Enter the callback URL (endpoint) that Salesforce calls back to your application during OAuth. This is the OAuth redirect URI. Depending on which OAuth flow you use, the URL is typically the one that a user's browser is redirected to after successful authentication. Because this URL is used for some OAuth flows to pass an access token, the URL must use secure HTTPS or a custom URI scheme.
Selected OAuth Scopes	Select **Access and manage your data (api)**.

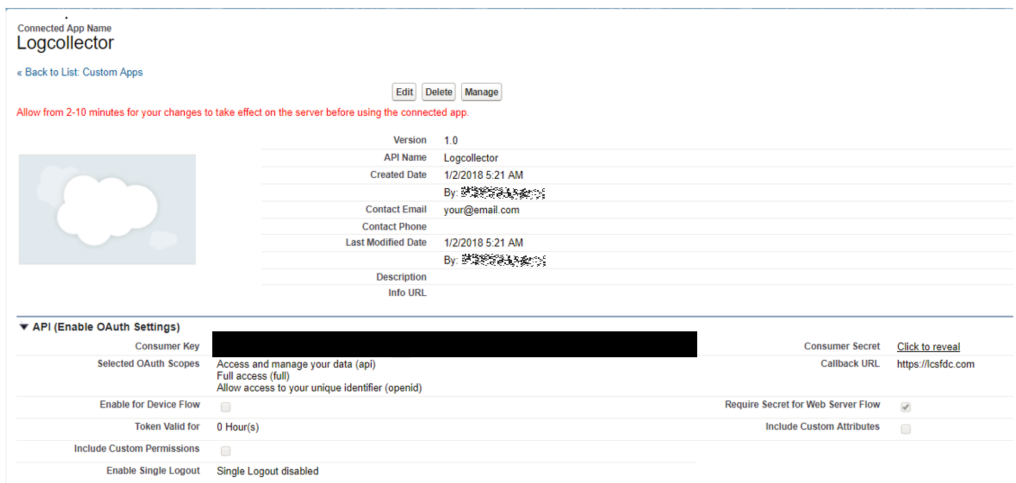
6. Click **Save** to complete your Connected App setup.





7. After you save the connected app, you are redirected to a new page. Click **Continue**.
8. From this page, you can copy your Consumer Key. Select **Click to reveal** to see your Consumer Secret, and copy that as well.

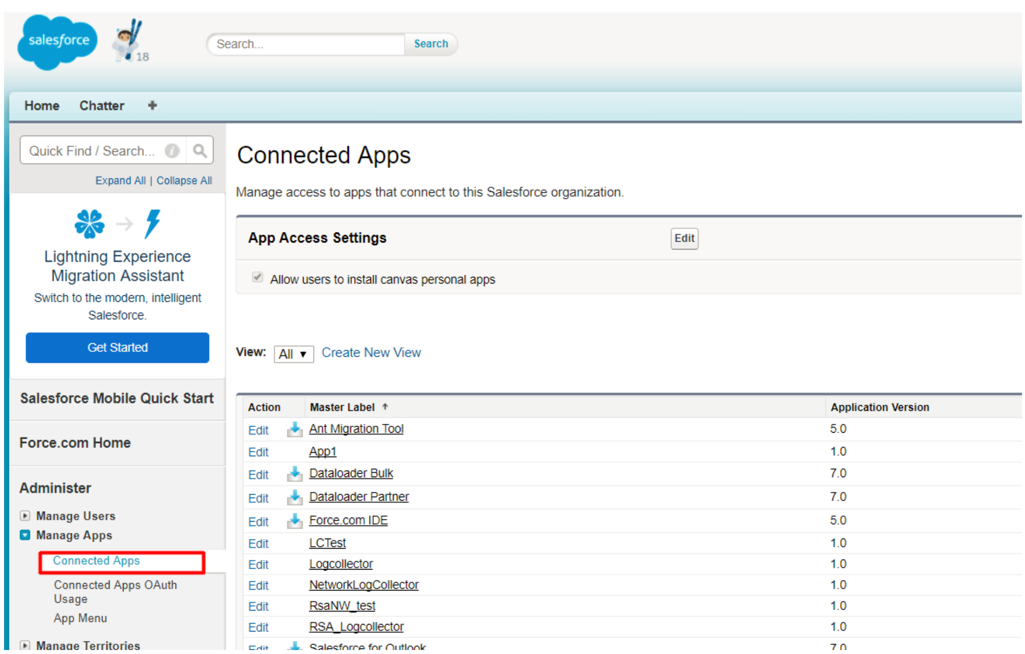
> **Note:** You need the Consumer Key and Consumer Secret values later, while configuring **Client ID** and **Client Secret** values in RSA NetWitness.



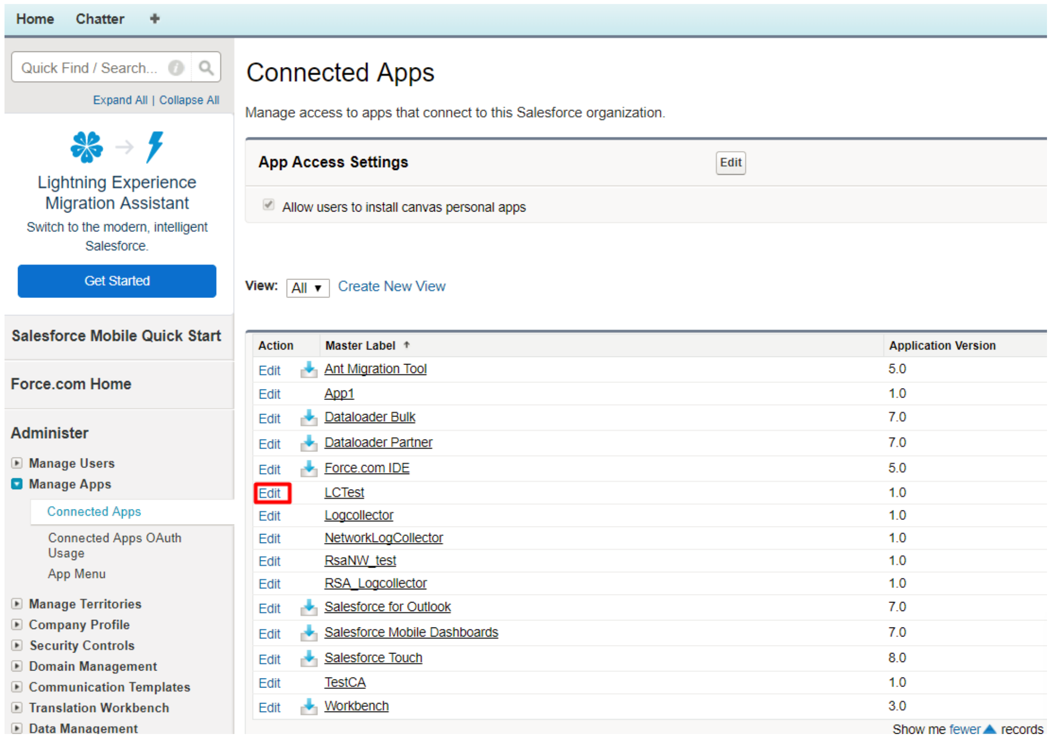
After you create the connected app, you need to edit its policies, as described in the following procedure.

To edit the policies for a connected app:

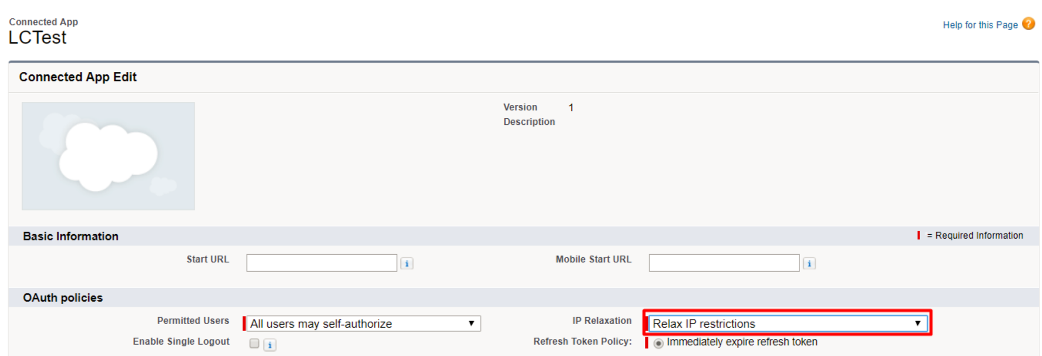
1. Click on **Connected Apps** under Manage Apps tab as shown below:



2. Click the **Edit** button for the connected app you created, as shown below:



3. In the **OAuth policies** section, from the **IP Relaxation** drop-down menu, select **Relax IP restrictions**.

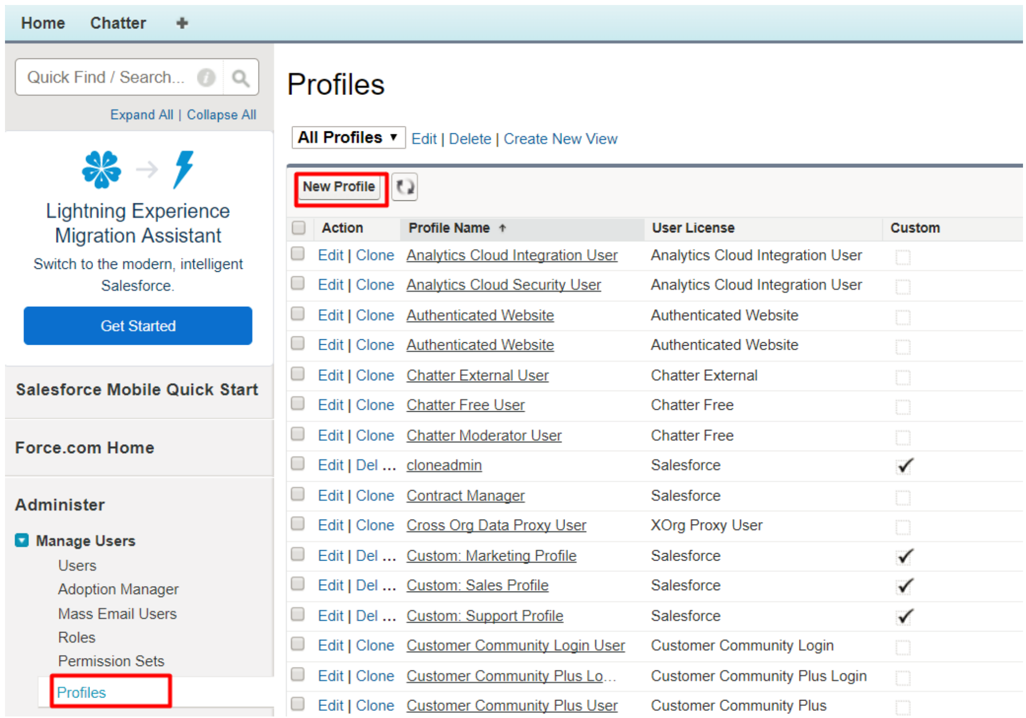


4. Save your changes.

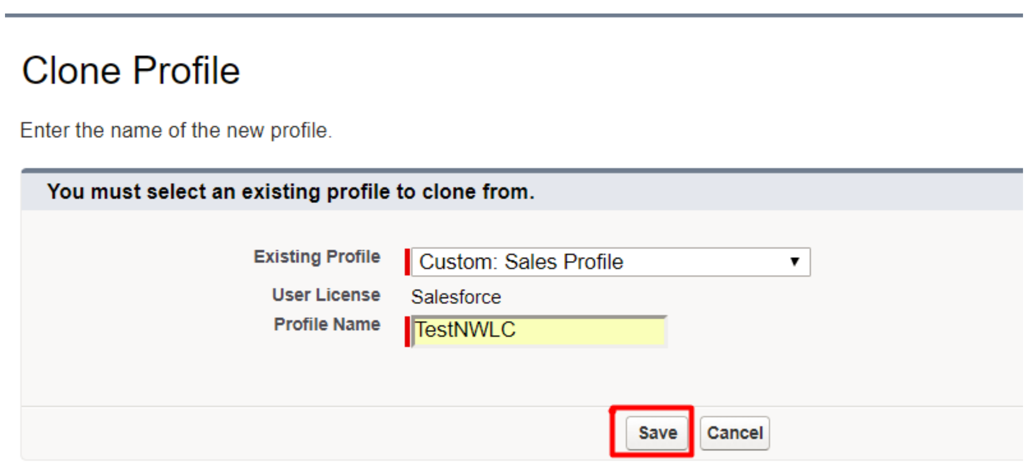
Create a custom read-only profile (Classic)

RSA NetWitness uses OAuth Username-password flow to authenticate between a Connected App and the Salesforce API. Creating a read-only custom profile restricts the users to have read-only access to Salesforce API logs.

1. In the Salesforce UI, go to **Manage Users > Profiles**, then click **New Profile**.



2. Choose the **Custom-Profile Name** option for the **existing profile** field. This existing profile should have **Salesforce** in the **User License** field, as shown below.



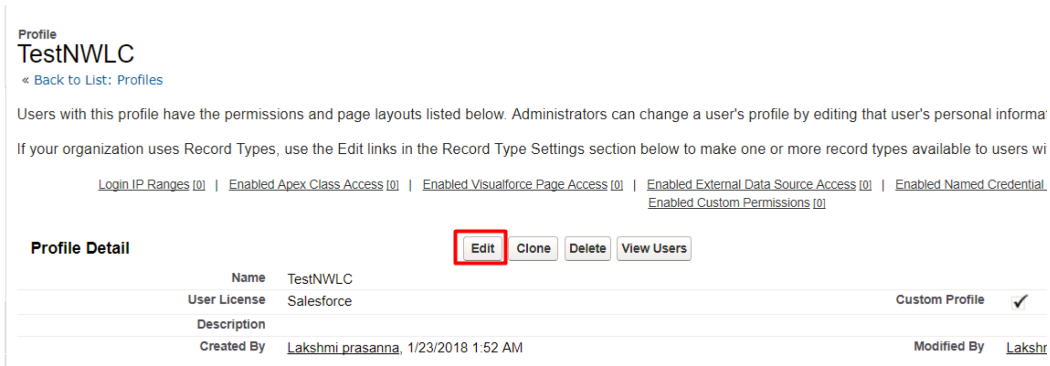
For more details about User Licenses, see .

see the User Licenses article in the Salesforce online help.

3. Click **Save**.

4. After you save the profile, you are redirected to a new page where you can view the new custom profile. Click **Edit** to change settings to minimize user access to

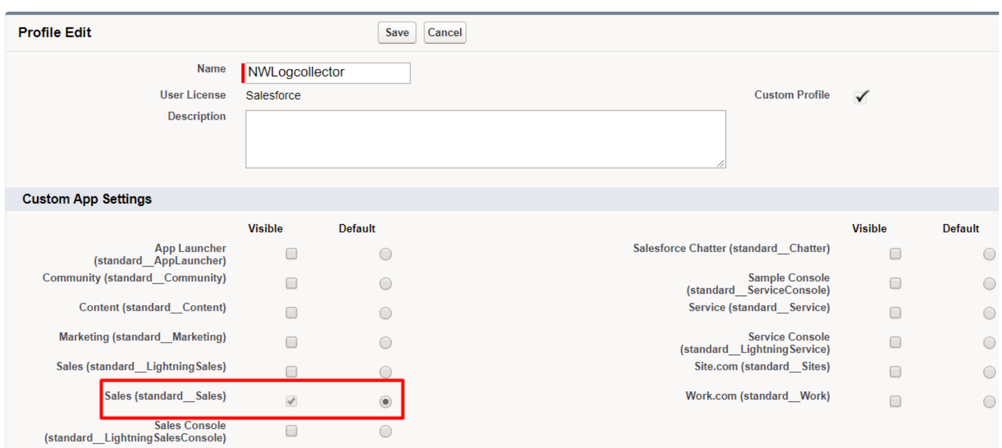
Salesforce event logs.



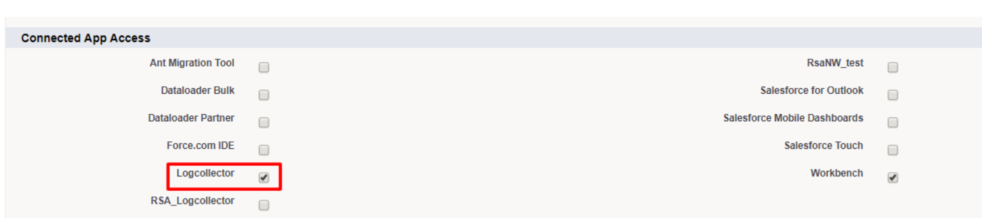
Note: Copy the custom profile name: you need to use this profile later, while creating a new user under the Salesforce admin account.

5. Assign permission sets and enable the connected app for this profile, as follows:

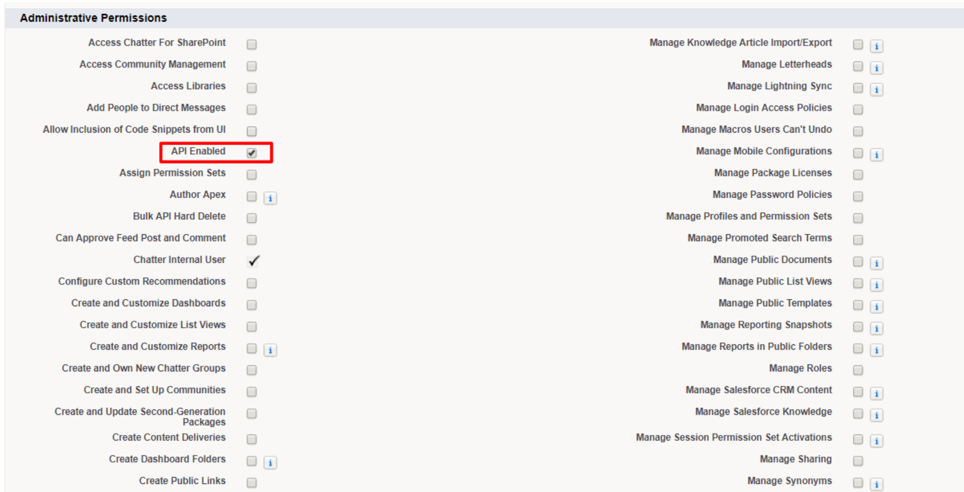
   a. In the **Custom App Settings** section, select and enable the **Sales (standard_Sales)** option as shown below.



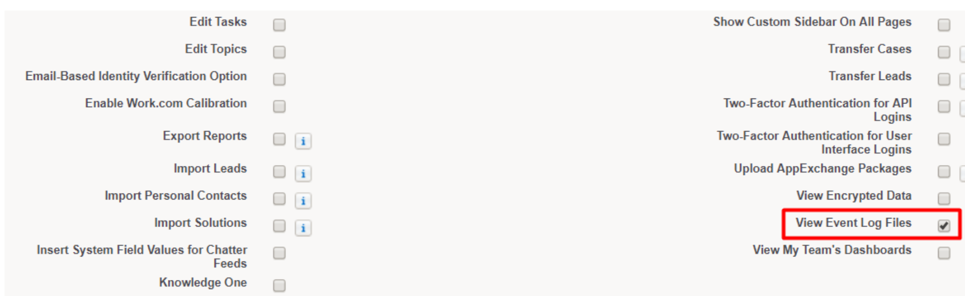
   b. In the **Connected App Access** section, select the connected app that you created in [Create a Salesforce connected app (Classic)](). Optionally, select **Workbench** to use the UI for querying the data using the REST API.



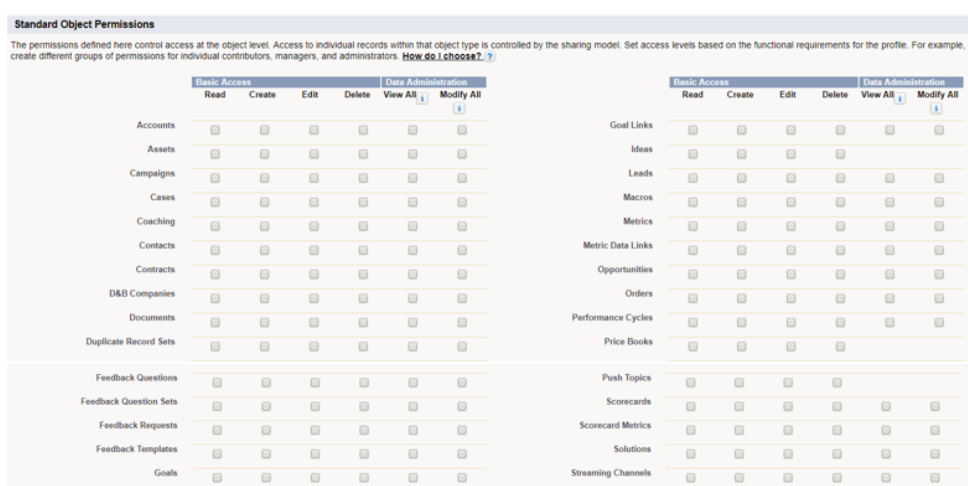
   c. In the **Administrative Permissions** section, select the **API Enabled** option as shown below.



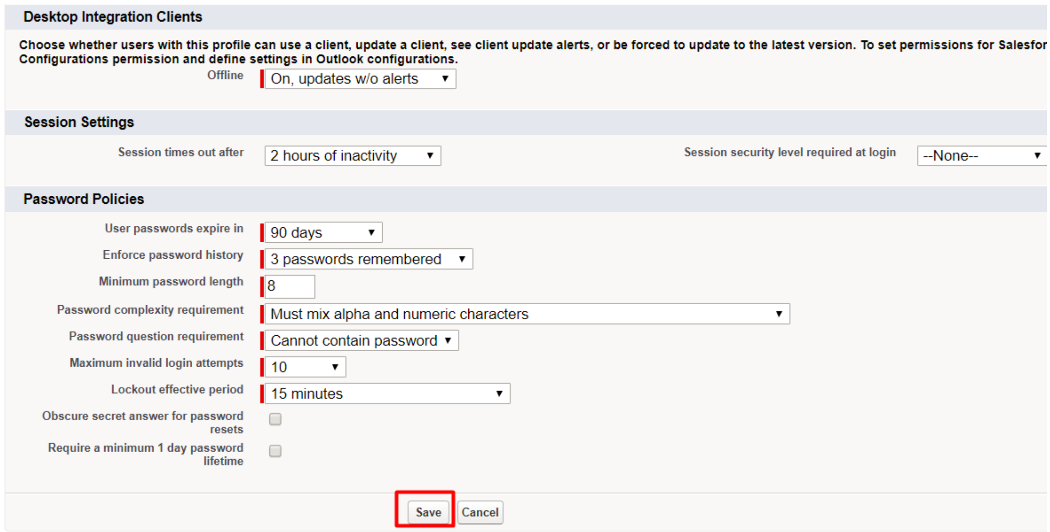
d. In the **General User Permissions** section, select the **View Event Log File** option as shown below.



e. In the **Standard Object Permissions** section, make sure to uncheck all available options.



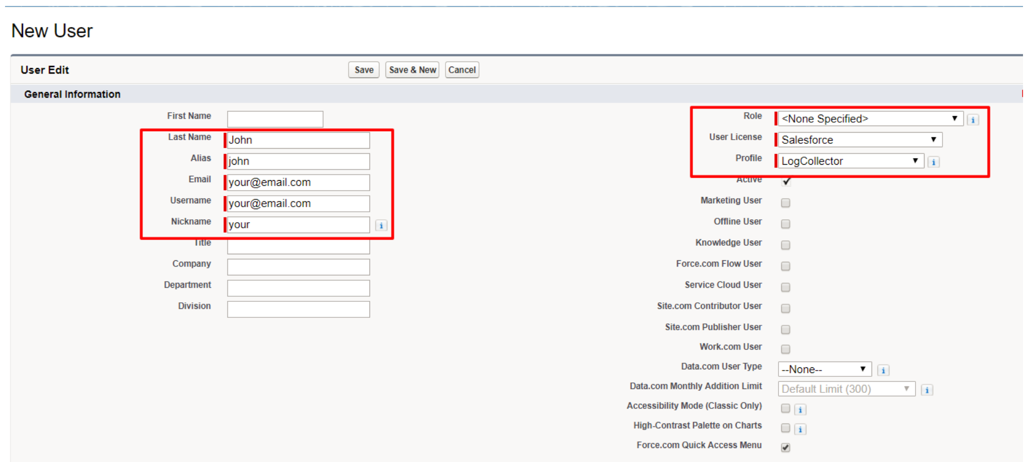
6. Click **Save** to save your changes to the profile.



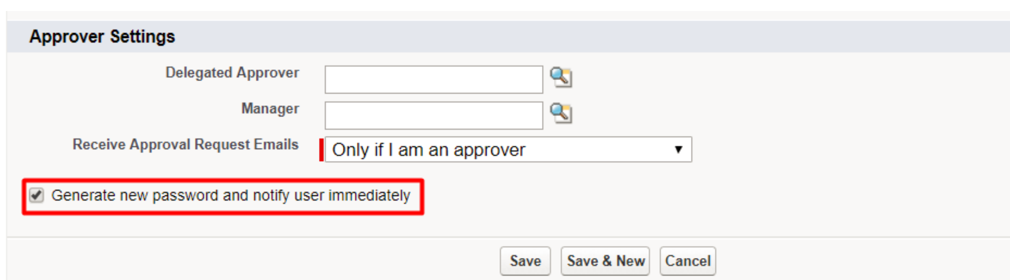
Create a user under Salesforce Admin account (Classic)

1. In the Salesforce UI, go to **Home** > **Manage Users** > **Users**, then click the **New User** tab.
2. Define the settings as described in the following table.

Setting	Value
Last Name	Enter user's last name
Alias	Enter an alias for the new user
Email	Enter a valid email address where the new user can be contacted
Username	This setting is automatically populated, based on the email address
Nickname	This setting is automatically populated, based on the email address
Role	Select **<None Specified>** from the drop-down menu
User License	Select **Salesforce** from the drop-down menu
Profile	From the drop-down menu, select the custom profile you created in [Create a custom read-only profile (Classic)]



3. In the **Approver Settings** section, make sure to select **Generate new password and notify user immediately**.



4. Click **Save**.

   Salesforce sends a message to the email account entered for the user account, with the subject **Verify your account**.

5. From the email message, click the verify account hyperlink, then change the password.

6. Save the username and password, since you need them later when you are configuring the Salesforce event source in RSA NetWitness.

Configure the Salesforce Event Source using Lightning Experience View

To configure Salesforce, you must complete these tasks:

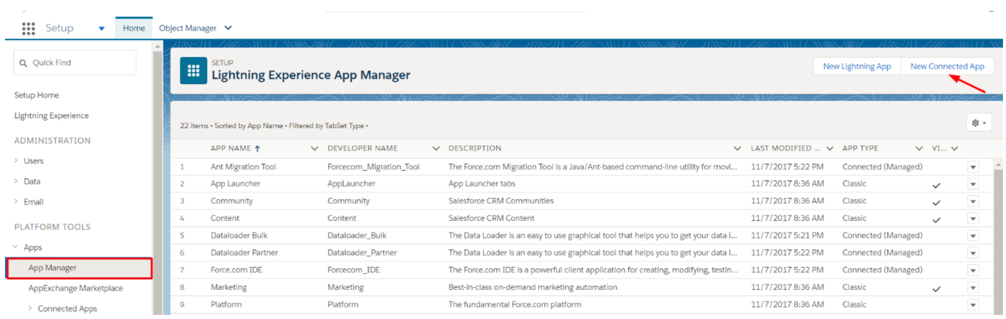
I. Create a Salesforce connected app (Lightning)

II. Create a custom read-only profile (Lightning)

III. Create a user under Salesforce admin account (Lightning)

Create a Salesforce Connected App (Lightning)

1. Log into to your Salesforce account through Salesforce portal: login.salesforce.com
2. In Lightning Experience view, you can use the App Manager to create a connected app.
   a. On the Setup page, type the keyword **App** in the Quick Find box.
   b. Select **App Manager**.
   c. Click **New Connected App**.

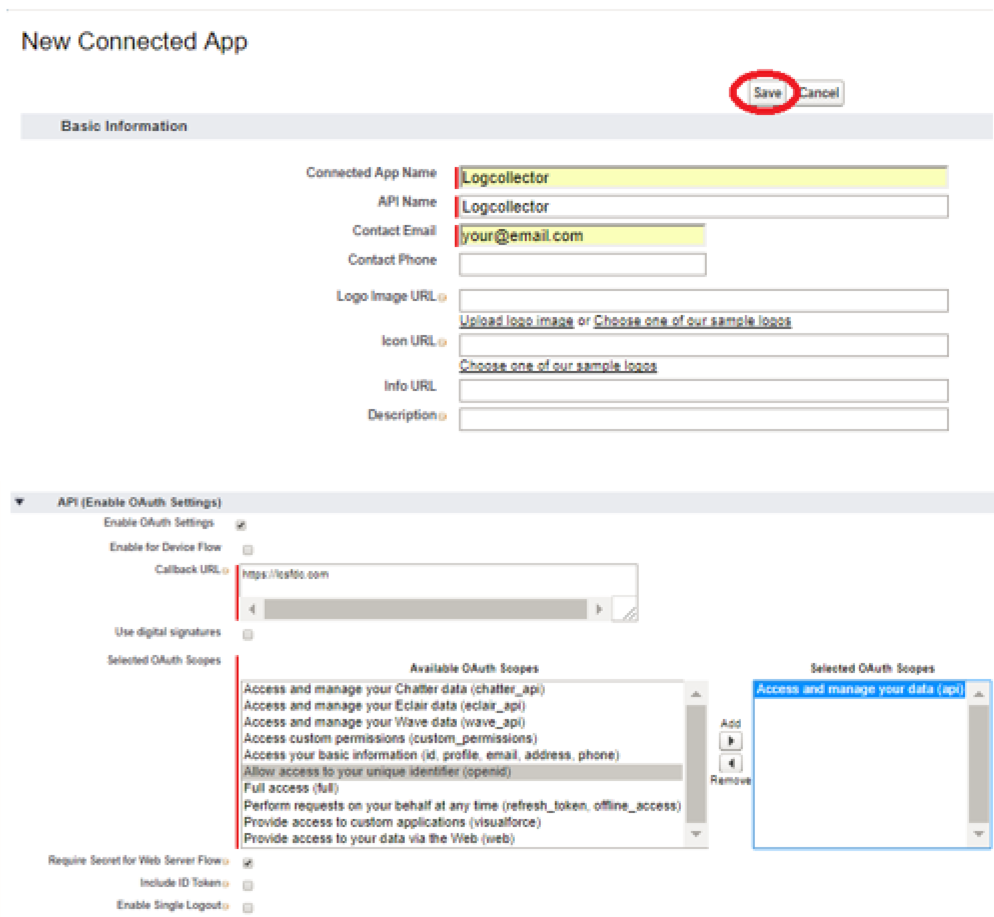


3. Make sure the following settings are defined in Salesforce to enable your new app:

Setting	Value
Connected App Name	Enter a name for the app, for example **Logcollector**.
API Name	This setting is populated automatically with the Connected App Name you enter.
Contact Email	Enter a valid email address.
Enable OAuth Settings	Make sure this is selected.
Callback URL	Enter the callback URL (endpoint) that Salesforce calls back to your application during OAuth. This is the OAuth redirect URI. Depending on which OAuth flow you use, the URL is typically the one

Setting	Value
	that a user’s browser is redirected to after successful authentication. Because this URL is used for some OAuth flows to pass an access token, the URL must use secure HTTPS or a custom URI scheme.
Selected OAuth Scopes	Select **Access and manage your data (api)**.

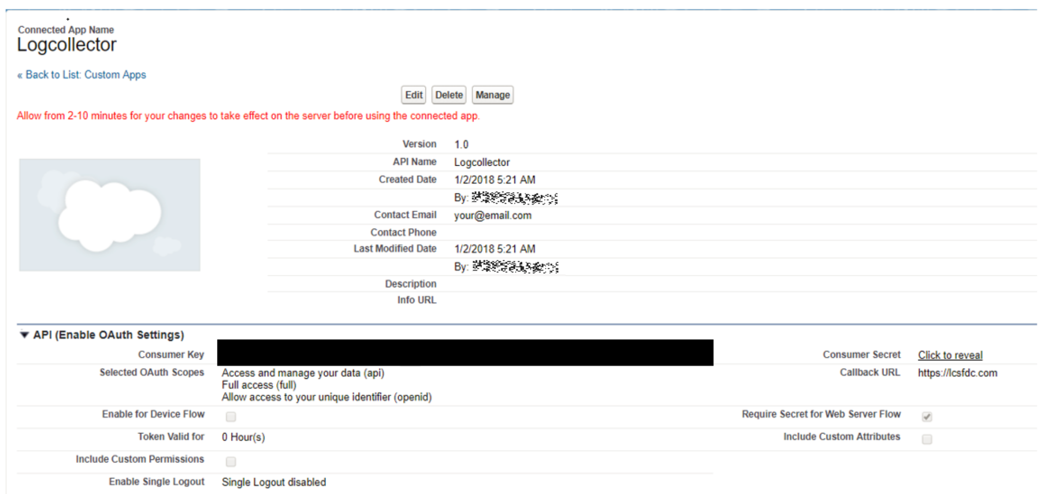
4. Click **Save** to complete your Connected App setup.



5. After you save the connected app, you are redirected to a new page. Click **Continue**.

6. From this page, you can copy your Consumer Key. Select **Click to reveal** to see your Consumer Secret, and copy that as well.

> **Note:** You need the Consumer Key and Consumer Secret values later, while configuring Client ID and Client Secret values in RSA NetWitness.

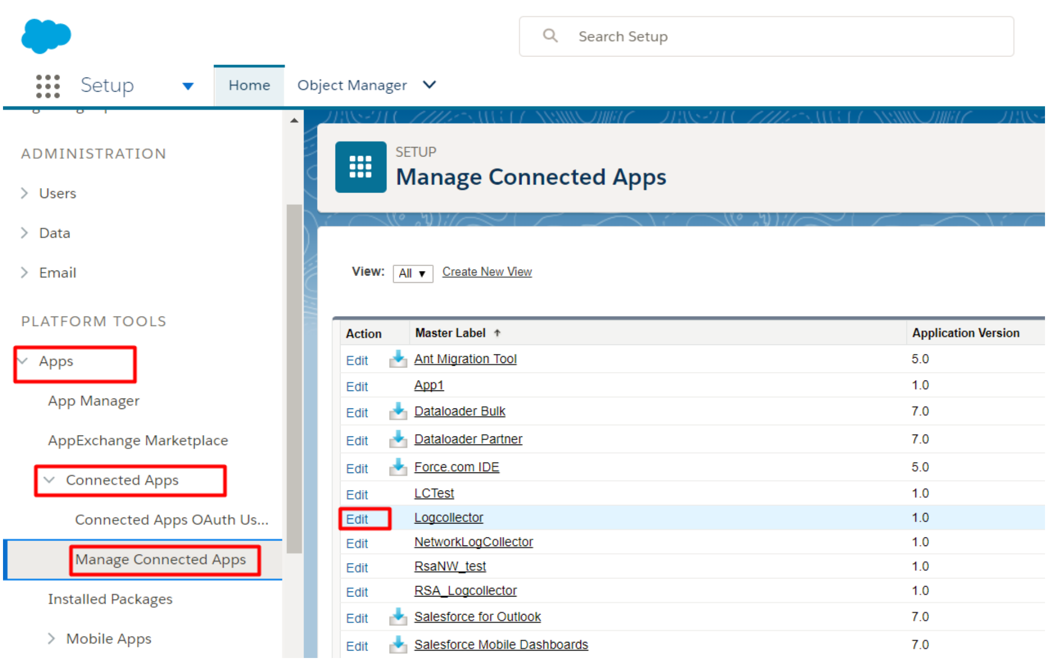


For more details about creating a Connected App, see the Create a Connected App article in the Salesforce online help.

After you create the connected app, you need to edit its policies, as described in the following procedure.

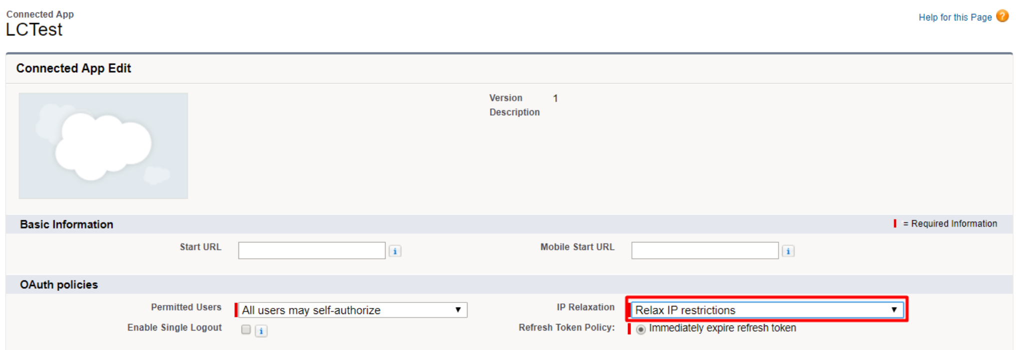
To edit the policies for a connected app:

1. Click on **Manage Connected Apps** under the Connected Apps tab.
2. Click the **Edit** button for the connected app you created, as shown below:



3. In the **OAuth policies** section, from the **IP Relaxation** drop-down menu, select **Relax**

IP restrictions.

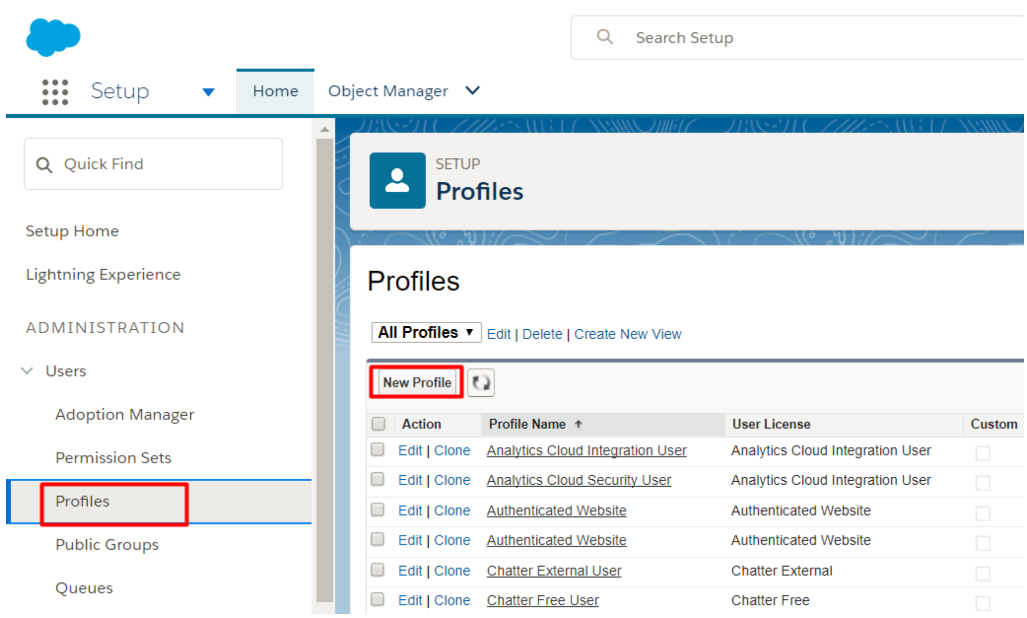


4. Save your changes.

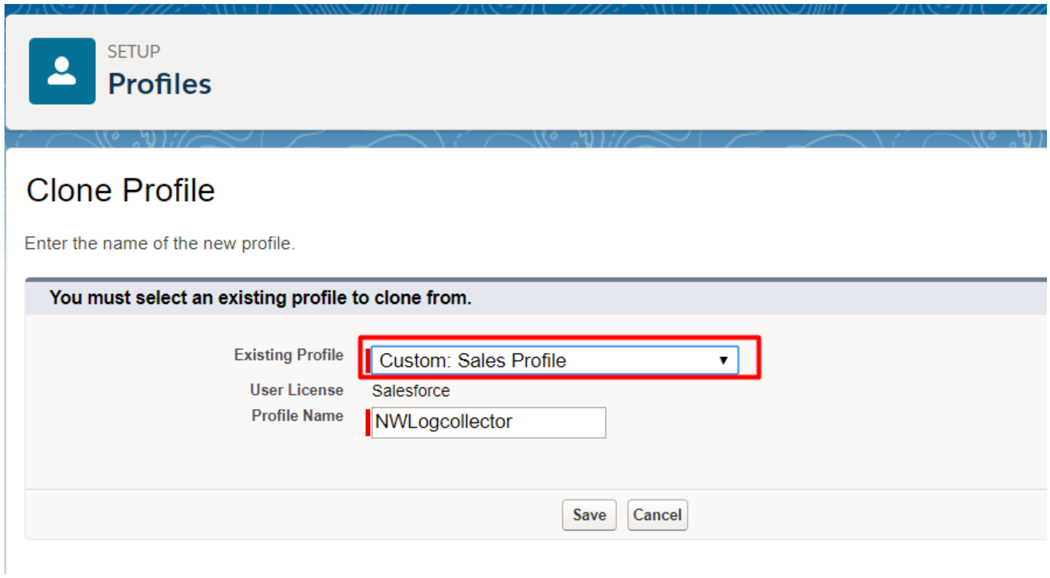
Create a Custom Read-Only Profile (Lightning)

RSA NetWitness uses OAuth Username-password flow to authenticate between a Connected App and the Salesforce API. Creating a read-only custom profile restricts the users to have read-only access to Salesforce API logs.

1. In the Salesforce UI, go to **Home** > **Users** > **Profiles**, then click **New Profile**.



2. Choose the **Custom-Profile Name** option for the **existing profile** field. This existing profile should have **Salesforce** in the **User License** field, as shown below.

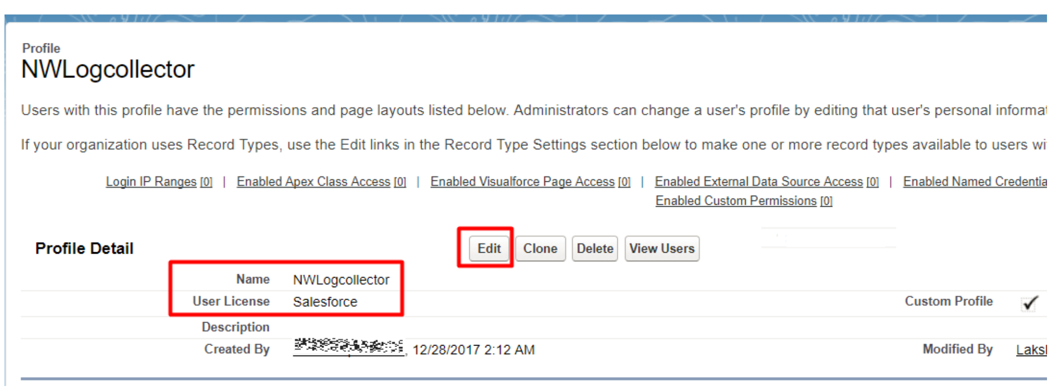


For more details about User Licenses, see .

see the User Licenses article in the Salesforce online help.

3. Click **Save**.

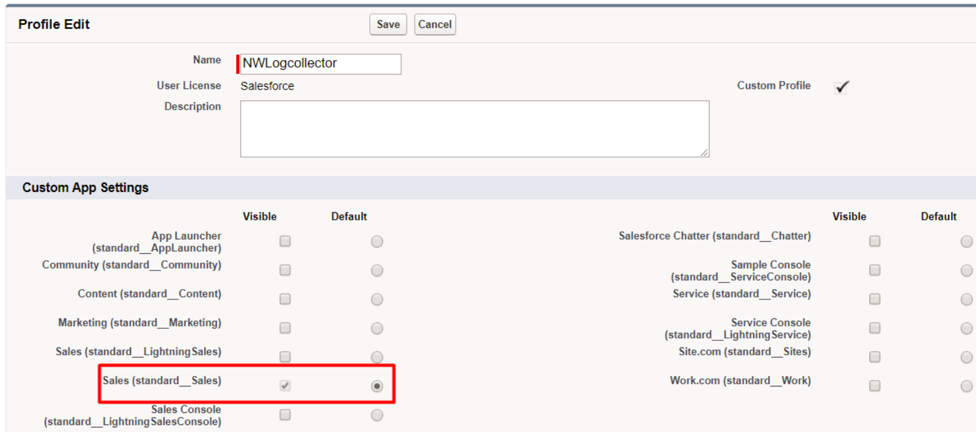
4. After you save the profile, you are redirected to a new page where you can view the new custom profile. Click **Edit** to change settings to minimize user access to Salesforce event logs.



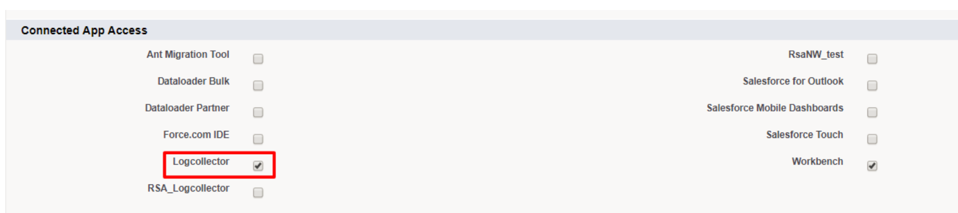
Note: Copy the custom profile name: you need to use this profile later, while creating a new user under the Salesforce admin account.

5. Assign permission sets and enable the connected app for this profile, as follows:

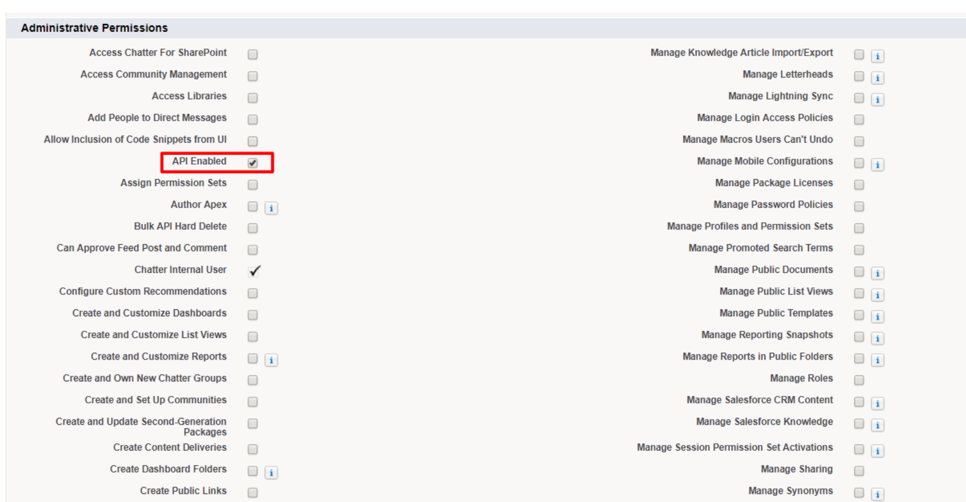
   a. In the **Custom App Settings** section, select and enable the **Sales (standard_Sales)** option as shown below.



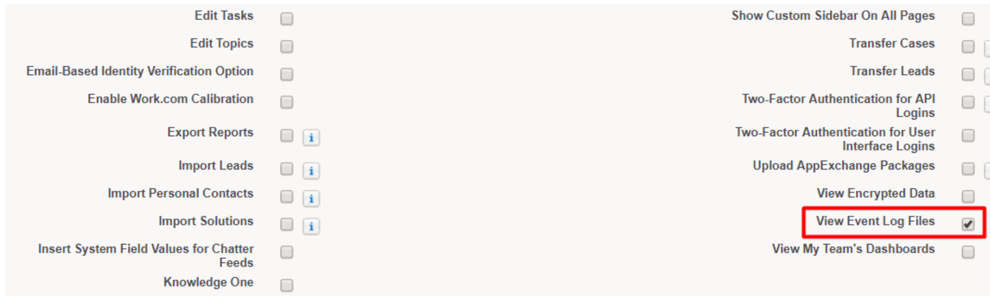
b. In the **Connected App Access** section, select the connected app that you created in [Create a Salesforce Connected App (Lightning)](). Optionally, select **Workbench** to use the UI for querying the data using the REST API.



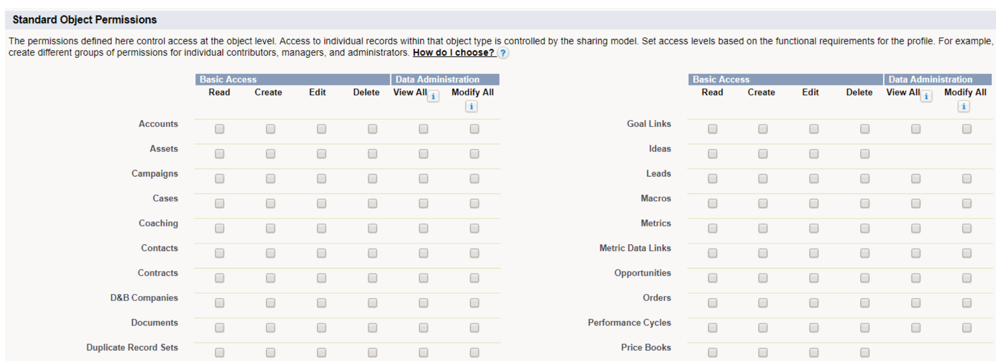
c. In the **Administrative Permissions** section, select the **API Enabled** option as shown below.



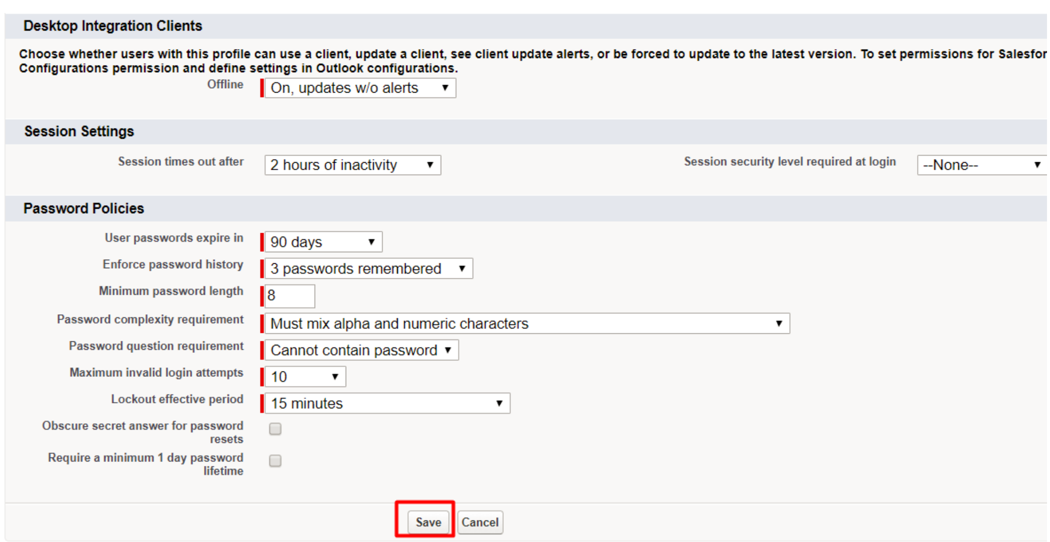
d. In the **General User Permissions** section, select the **View Event Log File** option as shown below.



e. In the **Standard Object Permissions** section, make sure to uncheck all available options.



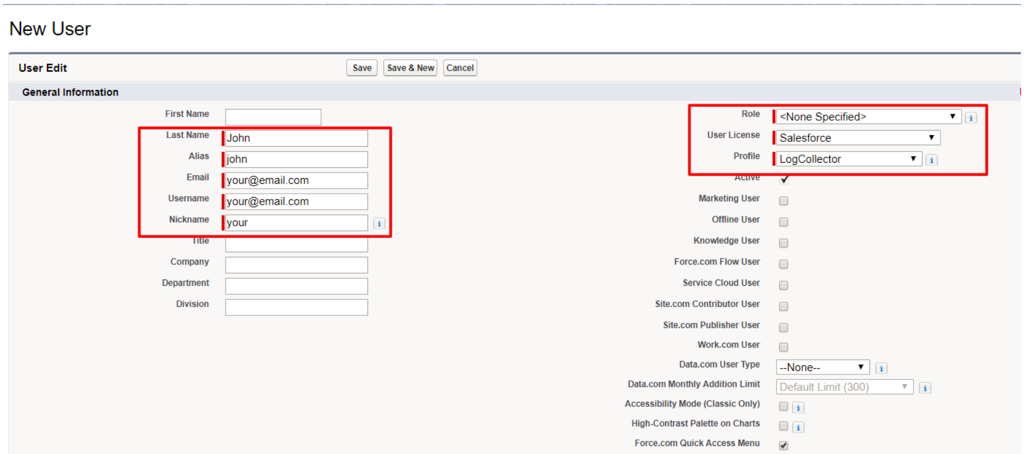
6. Click **Save** to save your changes to the profile.



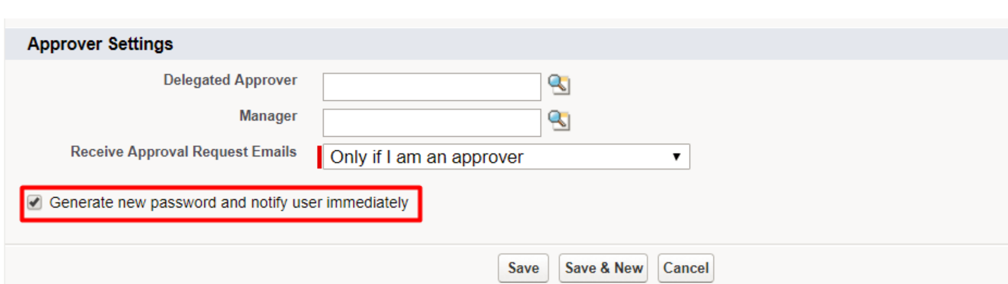
Create a User under Salesforce Admin Account (Lightning)

1. In the Salesforce UI, go to **Home** > **Users** > **Users**, then click the **New User** tab.
2. Define the settings as described in the following table.

Setting	Value
Last Name	Enter user's last name
Alias	Enter an alias for the new user
Email	Enter a valid email address where the new user can be contacted
Username	This setting is automatically populated, based on the email address
Nickname	This setting is automatically populated, based on the email address
Role	Select **<None Specified>** from the drop-down menu
User License	Select **Salesforce** from the drop-down menu
Profile	From the drop-down menu, select the custom profile you created in [Create a Custom Read-Only Profile (Lightning)](#)



3. In the **Approver Settings** section, make sure to select **Generate new password and notify user immediately**.



4. Click **Save**.

   Salesforce sends a message to the email account entered for the user account, with the subject **Verify your account**.

5. From the email message, click the verify account hyperlink, then change the password.

6. Save the username and password, since you need them later when you are configuring the Salesforce event source in RSA NetWitness.

Set Up Salesforce Event Source in RSA NetWitness

In RSA NetWitness Suite, perform the following tasks:

1. Deploy the CEF parser from Live
2. Configure the event source

Deploy the Salesforce Files from Live

Salesforce requires resources available in Live in order to collect logs.

To deploy the Salesforce content from Live:

1. In the RSA NetWitness Platform menu, select **Live**.
2. Browse Live for the **Common Event Format** (cef) parser, using **RSA Log Device** as the **Resource Type**.
3. Select the cef parser from the list and click **Deploy** to start the Deployment Wizard. The wizard deploys the parser to the appropriate the Log Decoders.
4. You also need to deploy the Salesforce package. Browse Live for Salesforce EventLogs content, typing "Salesforce" into the Keywords text box, then click **Search**.
5. Select the item returned from the search and click **Deploy** to deploy to the appropriate Log Collectors.

   Note: On a hybrid installation, you need to deploy the package on both the VLC and the LC.

6. Restart the **nwlogcollector** service.

For more details, see the Add or Update Supported Event Source Log Parsers topic, or the *Live Resource Guide* on RSA Link.

Configure the Salesforce Event Source in NetWitness

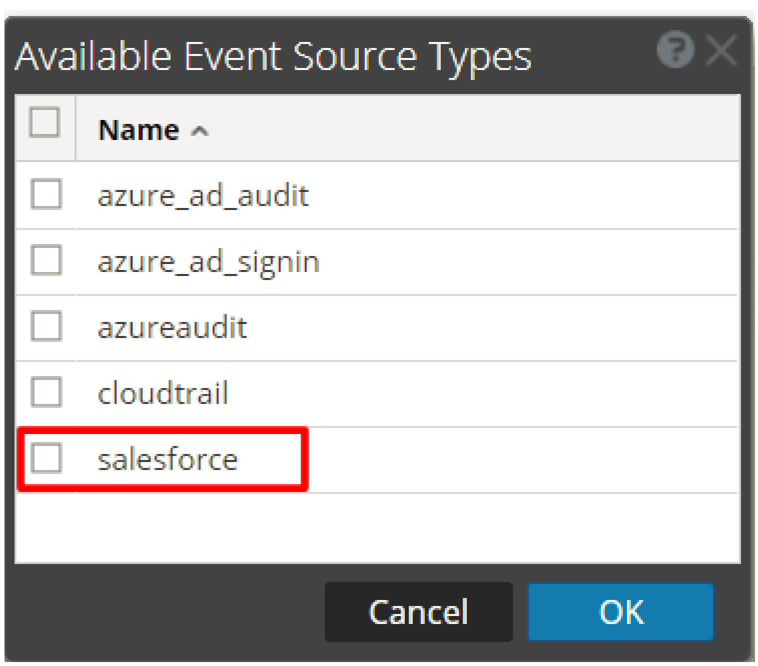
This section contains details on setting up the event source in RSA NetWitness Suite. In addition to the procedure, the Salesforce Collection Configuration Parameters are described.

To configure the Salesforce Event Source:

1. In the RSA NetWitness Platform menu, select **Administration > Services**.
2. In the Services grid, select a Log Collector service, and from the Actions menu, choose **View** > **Config**.
3. In the **Event Sources** tab, select **Plugins/Config** from the drop-down menu.

   The Event Categories panel displays the File event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.

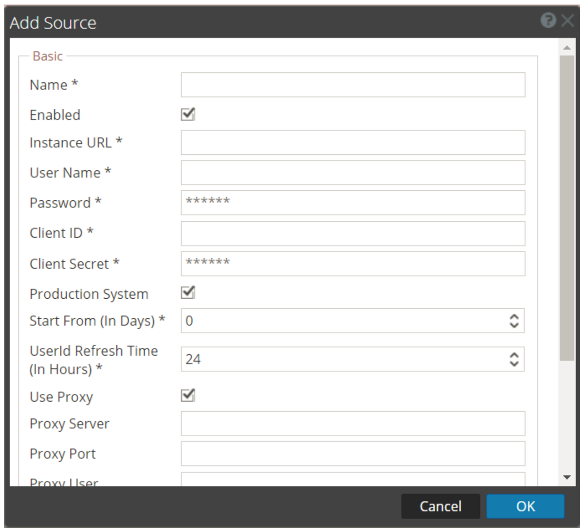


5. Select **salesforce** from the list, and click **OK**.

   The newly added event source type is displayed in the Event Categories panel.

6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.



7. Define parameter values, as described in [Salesforce Collection Configuration Parameters].

8. Click **Test Connection**.

   The result of the test is displayed in the dialog box. If the test is unsuccessful, edit the device or service information and retry.

   Note: The Log Collector takes approximately 60 seconds to return the test results. If it exceeds the time limit, the test times out and RSA NetWitness Platform displays an error message.

9. If the test is successful, click **OK**.

   The new event source is displayed in the Sources panel.

10. Repeat steps 4–9 to add another Salesforce plugin type.

Salesforce Collection Configuration Parameters

The following tables describe the configuration parameter for the Salesforce integration with RSA NetWitness Platform. Fields marked with an asterisk (*) are required.

The Add Source dialog is divided into **Basic** and **Advanced** sections.

Basic Parameters

The following table describes the Basic parameters.

Parameter	Description
Name *	Enter an alpha-numeric, descriptive name for the source. This value is only used for displaying the name on this screen.
Enabled	Select the checkbox to enable the event source configuration to start collection. The checkbox is selected by default.
Instance URL *	To view instance details in Company Information: • In Salesforce Lightning Experience UI (LEX): **Setup > Company Settings > Company Information** • In Salesforce Classic UI (Aloha): **Setup > Company Profile > Company Information** The URL should be **https://*{instance}*.salesforce.com**, where ***{instance}*** is the name of your organization instance.
User Name *	Enter the user name you created, which has permissions to view the logs.
Password *	Enter the password that matches the **User Name**.
Client ID *	Enter your connected application Consumer key.
Client Secret *	Enter your connected application Consumer Secret.
Production System	By default, the environment type is set to **Production**. Clear this checkbox to use the sandbox instead. • For Production environment, Oauth uses **https://login.salesforce.com/services/oauth2/token** for the Token URL. • For Sandbox environment, Oauth uses **https://test.salesforce.com/services/oauth2/token** for the Token URL.
Start From (In Days) *	Enter the number of days, between 0 and 30. This represents the number of days in the past (using the current timestamp) from which to start collection. The default is **0** (current day).
UserId Refresh Time * (In Hours)	The time interval, in hours, to update the mapped **userid** (the username information stored in RSA NetWitness Suite from the User Salesforce API Object). By default, refresh time is set to 24 hours.
Use Proxy	Select to enable a proxy.
Proxy Server	If you are using a proxy, enter the proxy server address.
Proxy Port	Enter the proxy port.

Parameter	Description
Proxy User	Username for the proxy (leave empty if using anonymous proxy).
Proxy Password	Password for the proxy (leave empty if using anonymous proxy).
Source Address	A custom value chosen to represent the IP address for the Salesforce Event Source in the customer environment. The value of this parameter is captured by the **device.ip** meta key. This value can help you to query or group events collected by a particular instance of the plugin.
Test Connection	Checks the configuration parameters you set to verify they are correct.

Advanced Parameters

Click next to **Advanced** to view and edit the advanced parameters, if necessary.

Name	Description
Polling Interval	Interval (amount of time in seconds) between each poll. The default value is **180**. For example, if you specify 180, the collector schedules a polling of the event source every 180 seconds. If the previous polling cycle is still underway, the collector waits for that cycle to finish. If you have a large number of event sources that you are polling, it may take longer than 180 seconds for the polling to start because the threads are busy. **Note:** The Salesforce event source generates events every 24 hours, and max polling interval can be set to 24 hours as well in RSA NetWitness. Therefore, RSA recommends setting the Polling Interval to 60 minutes, and then change as necessary, depending on the number of events, bandwidth and load of the system.
Max Duration Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit. RSA recommends that you do not set this value to zero (0), since logs are collected every 24 hours. The collection of logs depends on the polling time + polling interval time set. The following factors contribute to how you should set these values: 1. Load on the system 2. Number of events generated by the event source 3. Bandwidth for data transfer from the event source to Log Collector or Remote/Virtual Log Collector.
Max Events Poll	The maximum number of events per polling cycle (how many events collected per polling cycle).

Name	Description
Max Idle Time Poll	Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.
Command Args	Optional arguments to be added to the script invocation.
Debug	**Caution:** Only enable debugging (set this parameter to On or Verbose) if you have a problem with an event source and you need to investigate this problem. Enabling debugging will adversely affect the performance of the Log Collector. **Caution:** Enables or disables debug logging for the event source. Valid values are: • **Off** = (default) disabled • **On** = enabled • **Verbose** = enabled in verbose mode - adds thread information and source context information to the messages. This parameter is designed to debug and monitor isolated event source collection issues. If you change this value, the change takes effect immediately (no restart required). The debug logging is verbose, so limit the number of event sources to minimize performance impact.
SSL Enable	The check box is selected by default. Uncheck this box to disable SSL certificate verification.

Trademarks

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