

NetWitness[®] Platform

Salesforce Event Source Log Configuration Guide

Salesforce

Last Modified: Tuesday, July 9, 2024

Event Source Product Information:

Vendor: [Salesforce](#)

Event Source: CRM

Versions: API v1.0

RSA Product Information:

Supported On: NetWitness Platform 12.2 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

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 and 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/>.

© 2024 RSA Security LLC or its affiliates. All Rights Reserved.

February, 2024

Contents

Getting Started with NetWitness Platform and Salesforce Integration	6
Configure the Salesforce Event Source	7
Configure the Salesforce Event Source using Classic View	7
Create a Salesforce connected app (Classic)	7
Create a custom read-only profile (Classic)	12
Create a user under Salesforce Admin account (Classic)	16
Configure the Salesforce Event Source using Lightning Experience View	18
Create a Salesforce Connected App (Lightning)	18
Create a Custom Read-Only Profile (Lightning)	21
Create a User under Salesforce Admin Account (Lightning)	25
Set Up Salesforce Event Source in RSA NetWitness	27
Deploy the Salesforce Files from Live	27
Configure the Salesforce Event Source in NetWitness Platform	27
Salesforce Collection Configuration Parameters	29
Basic Parameters	29
Advanced Parameters	30
Getting Help with NetWitness Platform	32
Self-Help Resources	32
Contact NetWitness Support	32
Feedback on Product Documentation	33

This document contains the following sections:

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

Getting Started with NetWitness Platform 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](#)

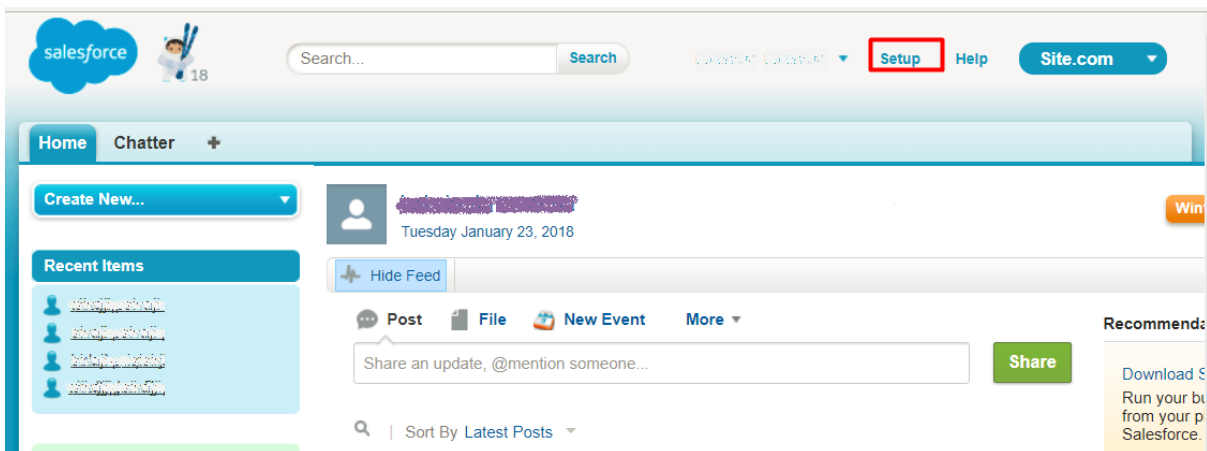
Configure the Salesforce Event Source using Classic View

To configure Salesforce, you must complete these tasks:

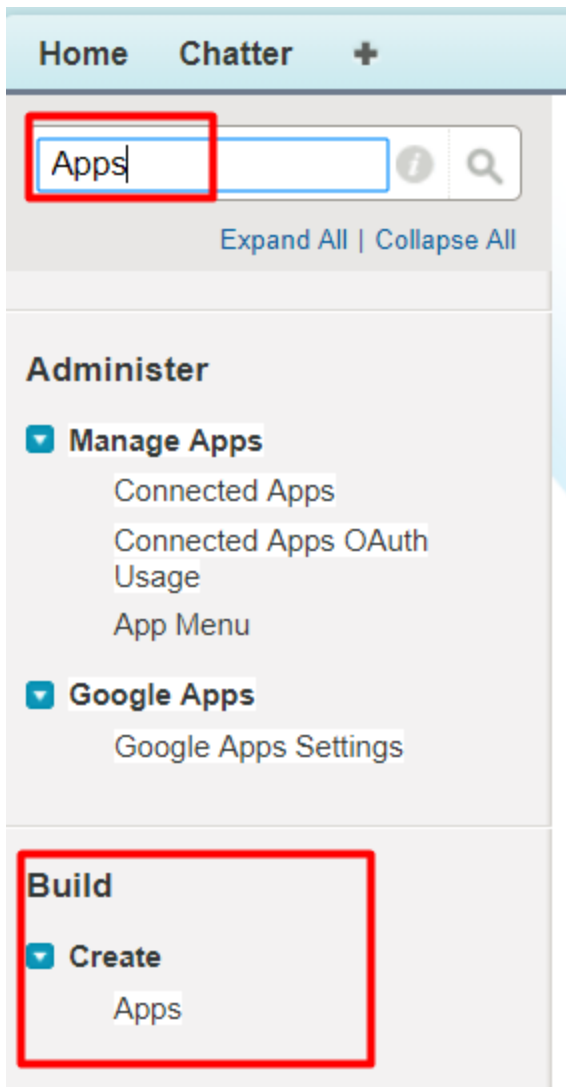
- I. Create a Salesforce connected app (Classic)
- II. Create a custom read-only profile (Classic)
- III. Create a user under Salesforce admin account (Classic)

Create a Salesforce connected app (Classic)

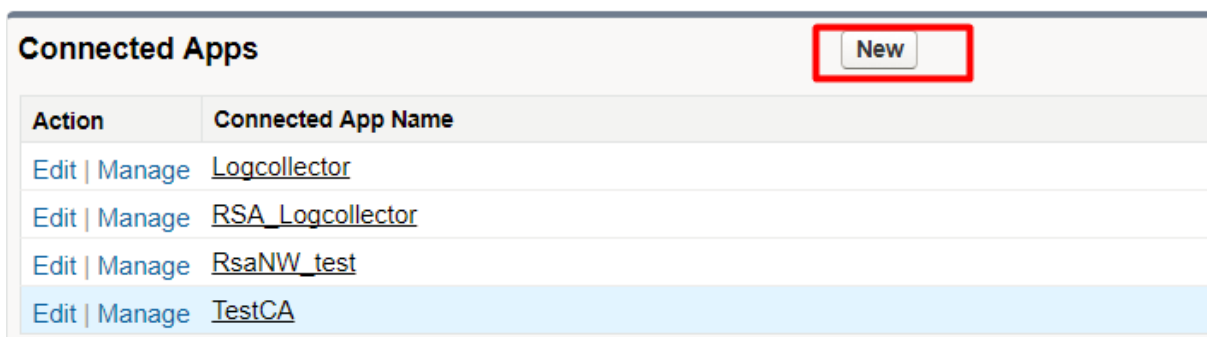
1. Log into to your Salesforce account through Salesforce portal: login.salesforce.com
2. In Salesforce Classic view, click on the Setup tab as shown here:



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	<p>Enter the callback URL (endpoint) that Salesforce calls back to your application during OAuth. This is the OAuth redirect URI.</p> <p>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.</p>
Selected OAuth Scopes	Select Access and manage your data (api) .

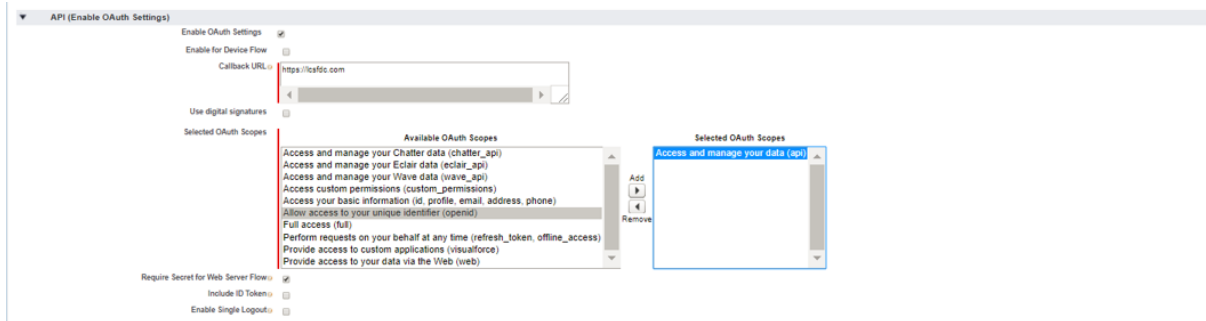
- Click **Save** to complete your Connected App setup.

New Connected App

Save **Cancel**

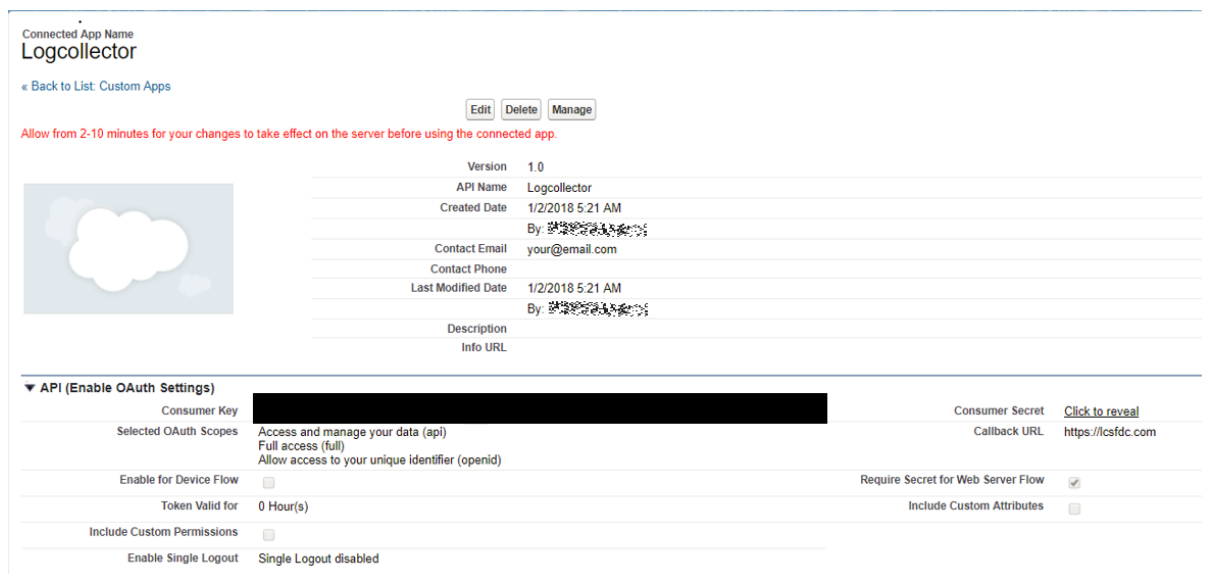
Basic Information

Connected App Name	<input type="text" value="LCTest"/>
API Name	<input type="text" value="LCTest"/>
Contact Email	<input type="text" value="your@email.com"/>
Contact Phone	<input type="text"/>
Logo Image URL 	<input type="text"/>
	Upload logo image or Choose one of our sample logos
Icon URL 	<input type="text"/>
	Choose one of our sample logos
Info URL	<input type="text"/>
Description 	<input type="text"/>



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.

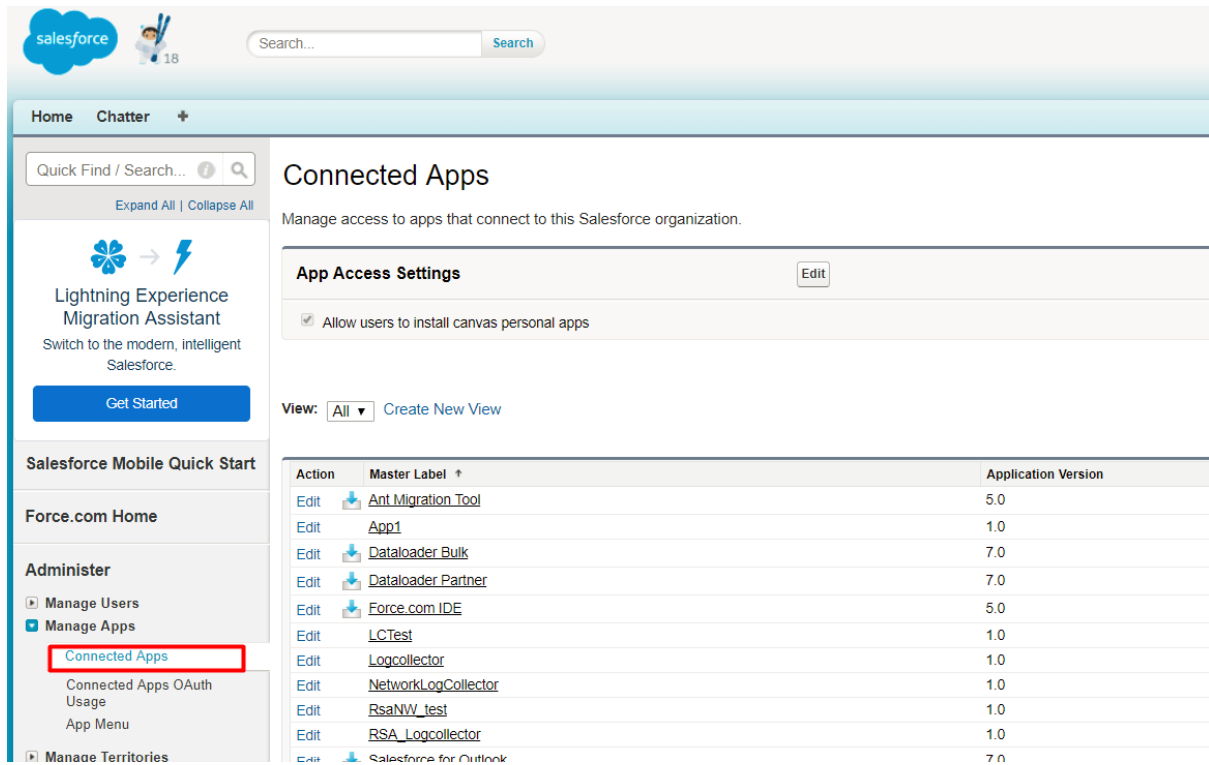
Note: You need the Consumer Key and Consumer Secret values later, while configuring **Client ID** and **Client Secret** values in NetWitness Platform .



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:



The screenshot displays the Salesforce Admin console interface. On the left sidebar, under the 'Administer' section, the 'Manage Apps' option is expanded, and 'Connected Apps' is highlighted with a red rectangular box. The main content area is titled 'Connected Apps' and includes a description: 'Manage access to apps that connect to this Salesforce organization.' Below this, there is an 'App Access Settings' section with an 'Edit' button and a checked checkbox for 'Allow users to install canvas personal apps'. A 'View:' dropdown menu is set to 'All'. A table lists various connected apps with columns for 'Action', 'Master Label', and 'Application Version'.

Action	Master Label	Application Version
Edit	Ant Migration Tool	5.0
Edit	App1	1.0
Edit	Dataloader Bulk	7.0
Edit	Dataloader Partner	7.0
Edit	Force.com IDE	5.0
Edit	LCTest	1.0
Edit	Logcollector	1.0
Edit	NetworkLogCollector	1.0
Edit	RsaNW_test	1.0
Edit	RSA_Logcollector	1.0
Edit	Salesforce for Outlook	7.0

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

Home Chatter +

Quick Find / Search...

Expand All | Collapse All

Lightning Experience Migration Assistant
Switch to the modern, intelligent Salesforce.
[Get Started](#)

Salesforce Mobile Quick Start

Force.com Home

Administer

- Manage Users
- Manage Apps
 - Connected Apps
 - Connected Apps OAuth Usage
 - App Menu
 - Manage Territories
 - Company Profile
 - Security Controls
 - Domain Management
 - Communication Templates
 - Translation Workbench
 - Data Management

App Access Settings [Edit](#)

Allow users to install canvas personal apps

View: All [Create New View](#)

Action	Master Label ↑	Application Version
Edit	Ant Migration Tool	5.0
Edit	App1	1.0
Edit	Dataloader Bulk	7.0
Edit	Dataloader Partner	7.0
Edit	Force.com IDE	5.0
Edit	LCTest	1.0
Edit	Logcollector	1.0
Edit	NetworkLogCollector	1.0
Edit	RsaNW_test	1.0
Edit	RSA_Logcollector	1.0
Edit	Salesforce for Outlook	7.0
Edit	Salesforce Mobile Dashboards	7.0
Edit	Salesforce Touch	8.0
Edit	TestCA	1.0
Edit	Workbench	3.0

Show me fewer [▲](#) records

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

Connected App
LCTest [Help for this Page](#)

Connected App Edit

Version 1
Description

Basic Information ! = Required Information

Start URL [i](#) Mobile Start URL [i](#)

OAuth policies

Permitted Users [All users may self-authorize](#)

Enable Single Logout [i](#)

IP Relaxation [Relax IP restrictions](#)

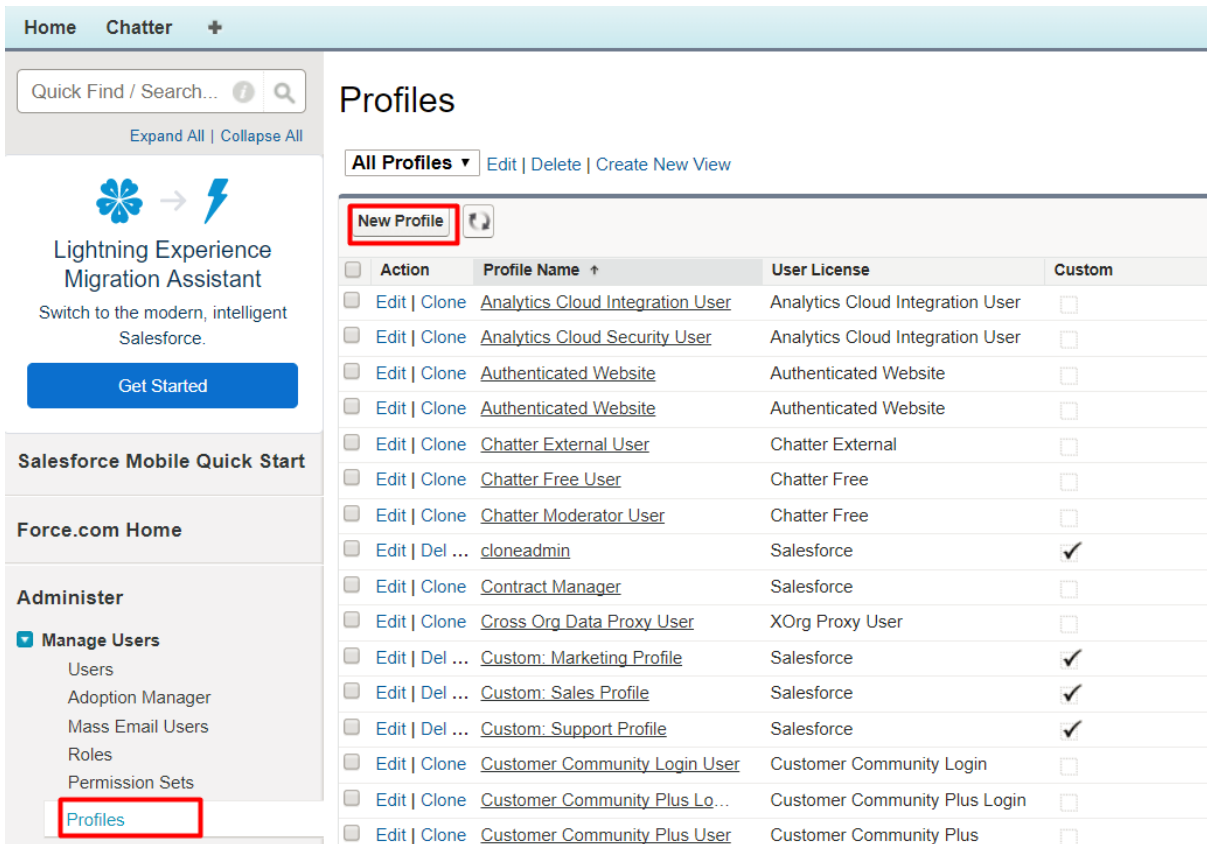
Refresh Token Policy: Immediately expire refresh token

- Save your changes.

Create a custom read-only profile (Classic)

NetWitness Platform 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**.



<input type="checkbox"/>	Action	Profile Name ↑	User License	Custom
<input type="checkbox"/>	Edit Clone	Analytics Cloud Integration User	Analytics Cloud Integration User	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Analytics Cloud Security User	Analytics Cloud Integration User	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Authenticated Website	Authenticated Website	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Authenticated Website	Authenticated Website	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Chatter External User	Chatter External	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Chatter Free User	Chatter Free	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Chatter Moderator User	Chatter Free	<input type="checkbox"/>
<input type="checkbox"/>	Edit Del ...	cloneadmin	Salesforce	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Contract Manager	Salesforce	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Cross Org Data Proxy User	XOrg Proxy User	<input type="checkbox"/>
<input type="checkbox"/>	Edit Del ...	Custom: Marketing Profile	Salesforce	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Edit Del ...	Custom: Sales Profile	Salesforce	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Edit Del ...	Custom: Support Profile	Salesforce	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Customer Community Login User	Customer Community Login	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Customer Community Plus Lo...	Customer Community Plus Login	<input type="checkbox"/>
<input type="checkbox"/>	Edit Clone	Customer Community Plus User	Customer Community Plus	<input type="checkbox"/>

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.

Clone Profile

Enter the name of the new profile.

You must select an existing profile to clone from.

Existing Profile

User License

Profile Name

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.

Profile
TestNWLC
« Back to List: Profiles

Users with this profile have the permissions and page layouts listed below. Administrators can change a user's profile by editing that user's personal information. If your organization uses Record Types, use the Edit links in the Record Type Settings section below to make one or more record types available to users with this profile.

[Login IP Ranges \[0\]](#) |
 [Enabled Apex Class Access \[0\]](#) |
 [Enabled Visualforce Page Access \[0\]](#) |
 [Enabled External Data Source Access \[0\]](#) |
 [Enabled Named Credential Access \[0\]](#) |
 [Enabled Custom Permissions \[0\]](#)

Profile Detail **Edit** Clone Delete View Users

Name	TestNWLC	
User License	Salesforce	Custom Profile <input checked="" type="checkbox"/>
Description		
Created By	Lakshmi prasanna, 1/23/2018 1:52 AM	Modified By Lakshmi prasanna

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.

Profile Edit Save Cancel

Name: NWLLogcollector

User License: Salesforce Custom Profile

Description:

Custom App Settings

	Visible	Default		Visible	Default
App Launcher (standard_AppLauncher)	<input type="checkbox"/>	<input type="radio"/>	Salesforce Chatter (standard_Chatter)	<input type="checkbox"/>	<input type="radio"/>
Community (standard_Community)	<input type="checkbox"/>	<input type="radio"/>	Sample Console (standard_ServiceConsole)	<input type="checkbox"/>	<input type="radio"/>
Content (standard_Content)	<input type="checkbox"/>	<input type="radio"/>	Service (standard_Service)	<input type="checkbox"/>	<input type="radio"/>
Marketing (standard_Marketing)	<input type="checkbox"/>	<input type="radio"/>	Service Console (standard_LightningService)	<input type="checkbox"/>	<input type="radio"/>
Sales (standard_LightningSales)	<input type="checkbox"/>	<input type="radio"/>	Site.com (standard_Sites)	<input type="checkbox"/>	<input type="radio"/>
Sales (standard_Sales)	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	Work.com (standard_Work)	<input type="checkbox"/>	<input type="radio"/>
Sales Console (standard_LightningSalesConsole)	<input type="checkbox"/>	<input type="radio"/>			

- 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.

Connected App Access

Ant Migration Tool	<input type="checkbox"/>	RsaNW_test	<input type="checkbox"/>
Dataloader Bulk	<input type="checkbox"/>	Salesforce for Outlook	<input type="checkbox"/>
Dataloader Partner	<input type="checkbox"/>	Salesforce Mobile Dashboards	<input type="checkbox"/>
Force.com IDE	<input type="checkbox"/>	Salesforce Touch	<input type="checkbox"/>
Logcollector	<input checked="" type="checkbox"/>	Workbench	<input checked="" type="checkbox"/>
RSA_Logcollector	<input type="checkbox"/>		

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

The screenshot shows the 'Administrative Permissions' section. The 'API Enabled' checkbox is checked and highlighted with a red box. Other permissions include 'Access Chatter For SharePoint', 'Access Community Management', 'Access Libraries', 'Add People to Direct Messages', 'Allow Inclusion of Code Snippets from UI', 'Assign Permission Sets', 'Author Apex', 'Bulk API Hard Delete', 'Can Approve Feed Post and Comment', 'Chatter Internal User', 'Configure Custom Recommendations', 'Create and Customize Dashboards', 'Create and Customize List Views', 'Create and Customize Reports', 'Create and Own New Chatter Groups', 'Create and Set Up Communities', 'Create and Update Second-Generation Packages', 'Create Content Deliveries', 'Create Dashboard Folders', 'Create Public Links', 'Manage Knowledge Article Import/Export', 'Manage Letterheads', 'Manage Lightning Sync', 'Manage Login Access Policies', 'Manage Macros Users Can't Undo', 'Manage Mobile Configurations', 'Manage Package Licenses', 'Manage Password Policies', 'Manage Profiles and Permission Sets', 'Manage Promoted Search Terms', 'Manage Public Documents', 'Manage Public List Views', 'Manage Public Templates', 'Manage Reporting Snapshots', 'Manage Reports in Public Folders', 'Manage Roles', 'Manage Salesforce CRM Content', 'Manage Salesforce Knowledge', 'Manage Session Permission Set Activations', 'Manage Sharing', and 'Manage Synonyms'.

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

The screenshot shows the 'General User Permissions' section. The 'View Event Log Files' checkbox is checked and highlighted with a red box. Other permissions include 'Edit Tasks', 'Edit Topics', 'Email-Based Identity Verification Option', 'Enable Work.com Calibration', 'Export Reports', 'Import Leads', 'Import Personal Contacts', 'Import Solutions', 'Insert System Field Values for Chatter Feeds', 'Knowledge One', 'Show Custom Sidebar On All Pages', 'Transfer Cases', 'Transfer Leads', 'Two-Factor Authentication for API Logins', 'Two-Factor Authentication for User Interface Logins', 'Upload AppExchange Packages', 'View Encrypted Data', and 'View My Team's Dashboards'.

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

Standard Object Permissions

The permissions defined here control access at the object level. Access to individual records within that object type is controlled by the sharing model. Set access levels based on the functional requirements for the profile. For example, create different groups of permissions for individual contributors, managers, and administrators. [How do I choose? ?](#)

	Basic Access				Data Administration			Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All		Read	Create	Edit	Delete	View All	Modify All
Accounts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Goal Links	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Assets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Ideas	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Campaigns	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Leads	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cases	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Macros	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Coaching	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Metrics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contacts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Metric Data Links	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contracts	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Opportunities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
D&B Companies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Orders	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Documents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Performance Cycles	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Duplicate Record Sets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Price Books	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Questions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Push Topics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Question Sets	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Scorecards	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Requests	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Scorecard Metrics	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Feedback Templates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Solutions	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Goals	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Streaming Channels	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Desktop Integration Clients

Choose whether users with this profile can use a client, update a client, see client update alerts, or be forced to update to the latest version. To set permissions for Salesforce Configurations permission and define settings in Outlook configurations.

Offline On, updates w/o alerts

Session Settings

Session times out after Session security level required at login

Password Policies

User passwords expire in

Enforce password history

Minimum password length

Password complexity requirement

Password question requirement

Maximum invalid login attempts

Lockout effective period

Obscure secret answer for password resets

Require a minimum 1 day password lifetime

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

Setting	Value
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)

New User

The screenshot shows the 'User Edit' form in Salesforce. The 'General Information' section is highlighted with a red box. It includes fields for First Name, Last Name (John), Alias (john), Email (your@email.com), Username (your@email.com), and Nickname (your). To the right, the 'Role' dropdown is set to '<None Specified>', 'User License' is 'Salesforce', and 'Profile' is 'LogCollector'. Below these are checkboxes for various user types like Marketing User, Offline User, Knowledge User, etc. At the bottom, there are buttons for 'Save', 'Save & New', and 'Cancel'.

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

The screenshot shows the 'Approver Settings' section. It includes fields for 'Delegated Approver' and 'Manager'. The 'Receive Approval Request Emails' dropdown is set to 'Only if I am an approver'. A checkbox labeled 'Generate new password and notify user immediately' is checked and highlighted with a red box. At the bottom, there are buttons for 'Save', 'Save & New', and 'Cancel'.

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.

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

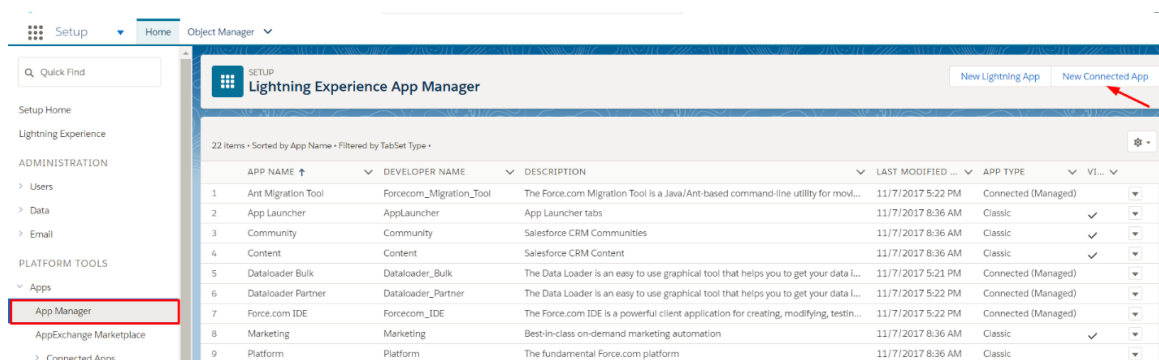
Configure the Salesforce Event Source using Lightning Experience View

To configure Salesforce, you must complete these tasks:

- Create a Salesforce connected app (Lightning)
- Create a custom read-only profile (Lightning)
- Create a user under Salesforce admin account (Lightning)

Create a Salesforce Connected App (Lightning)

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



- 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.

Setting	Value
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) .

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

The screenshot shows the 'New Connected App' configuration page. At the top right, there are 'Save' and 'Cancel' buttons, with 'Save' circled in red. Below this is the 'Basic Information' section with the following fields:

- Connected App Name: Logcollector
- API Name: Logcollector
- Contact Email: your@email.com
- Contact Phone: (empty)
- Logo Image URL: (empty)
- Icon URL: (empty)
- Info URL: (empty)
- Description: (empty)

Below the 'Basic Information' section is the 'API (Enable OAuth Settings)' section, which is expanded. It contains the following settings:

- Enable OAuth Settings:
- Enable for Device Flow:
- Callback URL: https://localhost.com
- Use digital signatures:
- Selected OAuth Scopes: Access and manage your data (api)

The 'Available OAuth Scopes' list includes:

- Access and manage your Chatter data (chatter_api)
- Access and manage your Eclair data (eclair_api)
- Access and manage your Wave data (wave_api)
- Access custom permissions (custom_permissions)
- Access your basic information (id, profile, email, address, phone)
- Allow access to your unique identifier (openid)
- Full access (full)
- Perform requests on your behalf at any time (refresh_token, offline_access)
- Provide access to custom applications (visualforce)
- Provide access to your data via the Web (web)

The 'Selected OAuth Scopes' list is currently empty.

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

The screenshot shows the configuration page for a Connected App named 'Logcollector'. At the top, there are buttons for 'Edit', 'Delete', and 'Manage'. A red warning message states: 'Allow from 2-10 minutes for your changes to take effect on the server before using the connected app.' Below this is a placeholder image of a cloud. To the right, a table lists the app's details:

Version	1.0
API Name	Logcollector
Created Date	1/2/2018 5:21 AM
By	[User Name]
Contact Email	your@email.com
Contact Phone	
Last Modified Date	1/2/2018 5:21 AM
By	[User Name]
Description	
Info URL	

Below the details is the 'API (Enable OAuth Settings)' section:

Consumer Key	[Redacted]	Consumer Secret	Click to reveal
Selected OAuth Scopes	Access and manage your data (api) Full access (full) Allow access to your unique identifier (openid)	Callback URL	https://lcsfdc.com
Enable for Device Flow	<input type="checkbox"/>	Require Secret for Web Server Flow	<input checked="" type="checkbox"/>
Token Valid for	0 Hour(s)	Include Custom Attributes	<input type="checkbox"/>
Include Custom Permissions	<input type="checkbox"/>		
Enable Single Logout	Single Logout disabled		

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:

Setup

Home Object Manager

ADMINISTRATION

- Users
- Data
- Email

PLATFORM TOOLS

- Apps
- App Manager
- AppExchange Marketplace
- Connected Apps
- Connected Apps OAuth Us...
- Manage Connected Apps
- Installed Packages
- Mobile Apps

SETUP

Manage Connected Apps

View: All Create New View

Action	Master Label ↑	Application Version
Edit	Ant Migration Tool	5.0
Edit	App1	1.0
Edit	Dataloader Bulk	7.0
Edit	Dataloader Partner	7.0
Edit	Force.com IDE	5.0
Edit	LCTest	1.0
Edit	Logcollector	1.0
Edit	NetworkLogCollector	1.0
Edit	RsaNW_test	1.0
Edit	RSA_Logcollector	1.0
Edit	Salesforce for Outlook	7.0
Edit	Salesforce Mobile Dashboards	7.0

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

Connected App
LCTest Help for this Page

Connected App Edit

Version 1
Description

Basic Information Required Information

Start URL ? Mobile Start URL ?

OAuth policies

Permitted Users: All users may self-authorize ?

Enable Single Logout ?

IP Relaxation: Relax IP restrictions ?

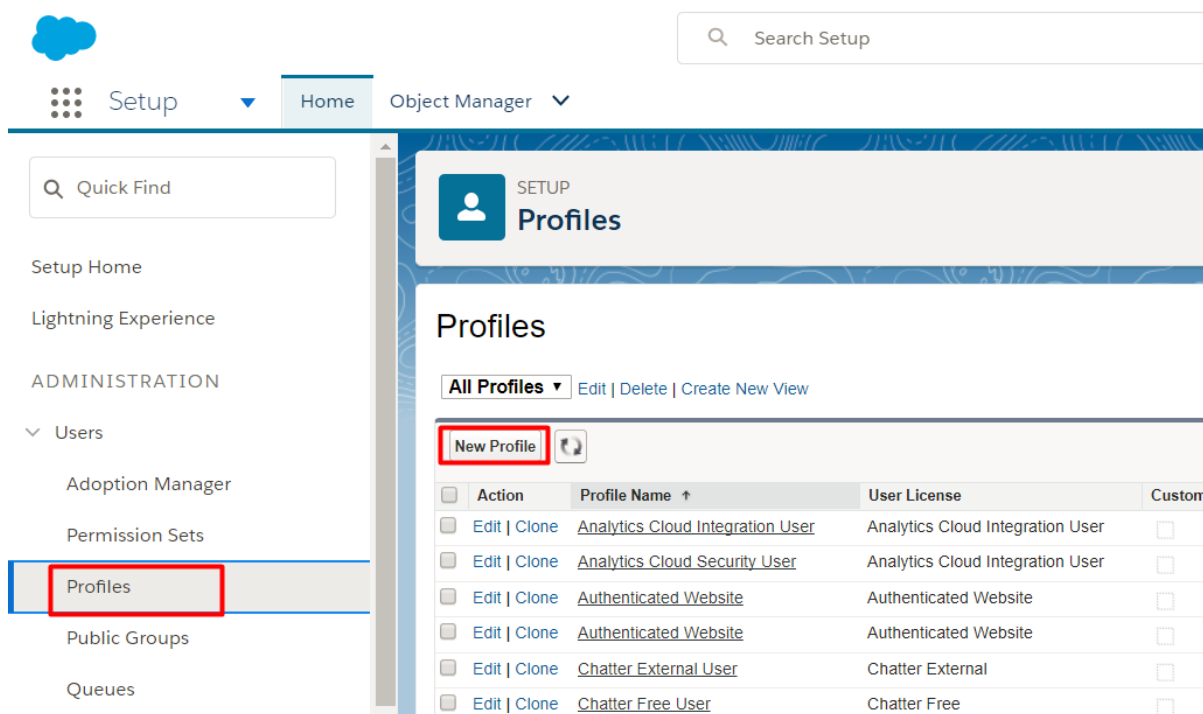
Refresh Token Policy: Immediately expire refresh token

- Save your changes.

Create a Custom Read-Only Profile (Lightning)

NetWitness Platform 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.

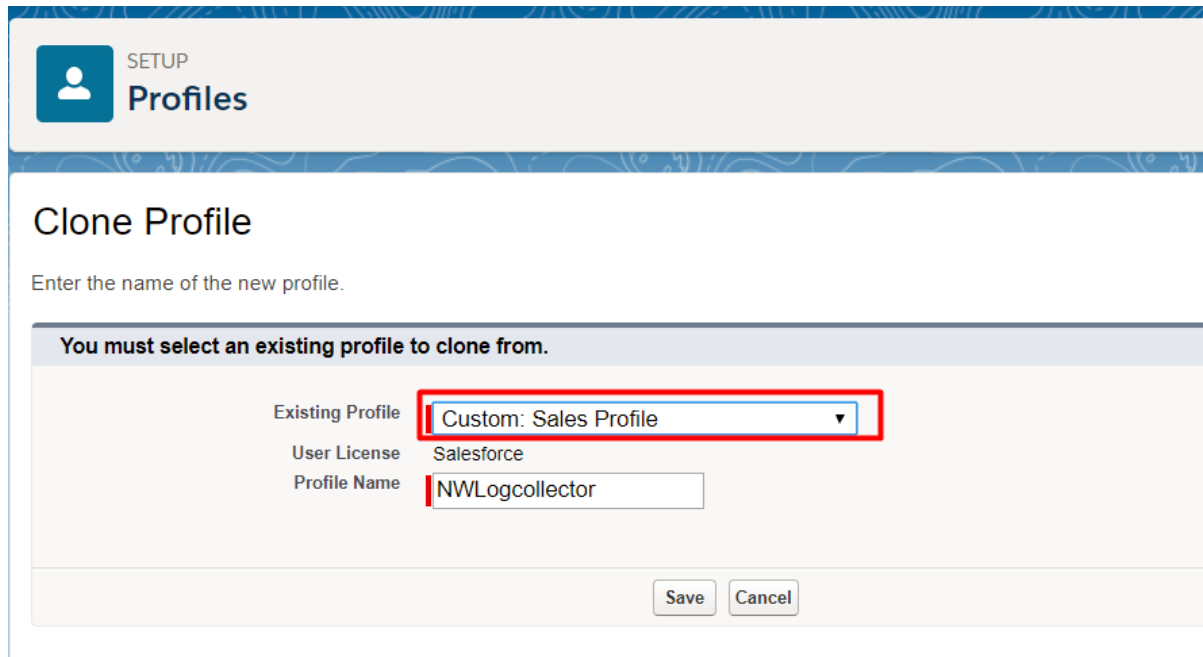
1. In the Salesforce UI, go to **Home > Users > Profiles**, then click **New Profile**.



The screenshot shows the Salesforce Setup interface. The left sidebar contains navigation options, with 'Profiles' highlighted in a red box. The main content area displays the 'Profiles' page, where the 'New Profile' button is also highlighted in a red box. Below the button is a table of existing profiles.

Action	Profile Name ↑	User License	Custom
<input type="checkbox"/> Edit Clone	Analytics Cloud Integration User	Analytics Cloud Integration User	<input type="checkbox"/>
<input type="checkbox"/> Edit Clone	Analytics Cloud Security User	Analytics Cloud Integration User	<input type="checkbox"/>
<input type="checkbox"/> Edit Clone	Authenticated Website	Authenticated Website	<input type="checkbox"/>
<input type="checkbox"/> Edit Clone	Authenticated Website	Authenticated Website	<input type="checkbox"/>
<input type="checkbox"/> Edit Clone	Chatter External User	Chatter External	<input type="checkbox"/>
<input type="checkbox"/> Edit Clone	Chatter Free User	Chatter Free	<input type="checkbox"/>

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.



The screenshot shows the 'Clone Profile' dialog box. The 'Existing Profile' dropdown menu is highlighted with a red box and contains the text 'Custom: Sales Profile'. Below it, the 'User License' is 'Salesforce' and the 'Profile Name' is 'NWLogcollector'. There are 'Save' and 'Cancel' buttons at the bottom right.

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.

The screenshot shows the 'Profile' page for 'NWLogcollector'. At the top, there are links for 'Login IP Ranges [0]', 'Enabled Apex Class Access [0]', 'Enabled Visualforce Page Access [0]', 'Enabled External Data Source Access [0]', and 'Enabled Named Credentials Enabled Custom Permissions [0]'. Below these is the 'Profile Detail' section with buttons for 'Edit', 'Clone', 'Delete', and 'View Users'. The 'Edit' button is highlighted with a red box. A table below shows the profile details:

Name	NWLogcollector
User License	Salesforce
Description	
Created By	[Avatar] 12/28/2017 2:12 AM
Modified By	Laks

On the right side, there is a 'Custom Profile' checkbox which is checked.

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

The screenshot shows the 'Profile Edit' page. The 'Name' field contains 'NWLogcollector' and the 'User License' is 'Salesforce'. The 'Custom Profile' checkbox is checked. Below is the 'Custom App Settings' section with a table of app settings:

	Visible	Default		Visible	Default
App Launcher (standard__AppLauncher)	<input type="checkbox"/>	<input type="radio"/>	Salesforce Chatter (standard__Chatter)	<input type="checkbox"/>	<input type="radio"/>
Community (standard__Community)	<input type="checkbox"/>	<input type="radio"/>	Sample Console (standard__ServiceConsole)	<input type="checkbox"/>	<input type="radio"/>
Content (standard__Content)	<input type="checkbox"/>	<input type="radio"/>	Service (standard__Service)	<input type="checkbox"/>	<input type="radio"/>
Marketing (standard__Marketing)	<input type="checkbox"/>	<input type="radio"/>	Service Console (standard__LightningService)	<input type="checkbox"/>	<input type="radio"/>
Sales (standard__LightningSales)	<input type="checkbox"/>	<input type="radio"/>	Site.com (standard__Sites)	<input type="checkbox"/>	<input type="radio"/>
Sales (standard__Sales)	<input checked="" type="checkbox"/>	<input checked="" type="radio"/>	Work.com (standard__Work)	<input type="checkbox"/>	<input type="radio"/>
Sales Console (standard__LightningSalesConsole)	<input type="checkbox"/>	<input type="radio"/>			

The 'Sales (standard__Sales)' row is highlighted with a red box.

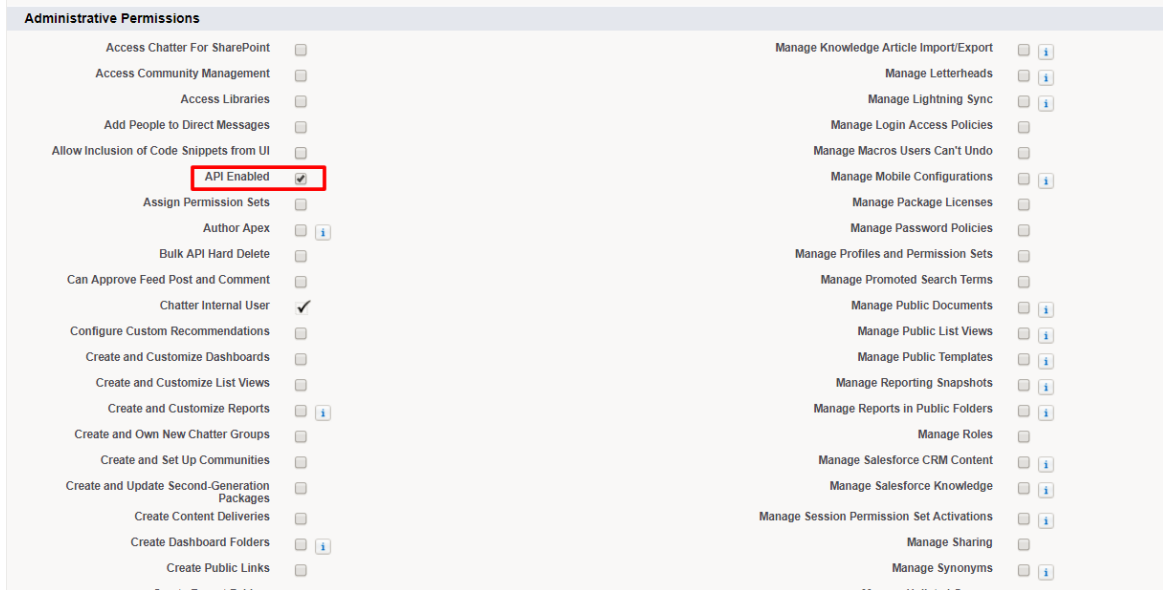
- In the **Connected App Access** section, select the connected app that you created in [Create a Salesforce Connected App \(Lightning\)](#). Optionally, select **Workbench** to use the UI for querying the data using the REST API.

The screenshot shows the 'Connected App Access' section with a list of apps and their access status:

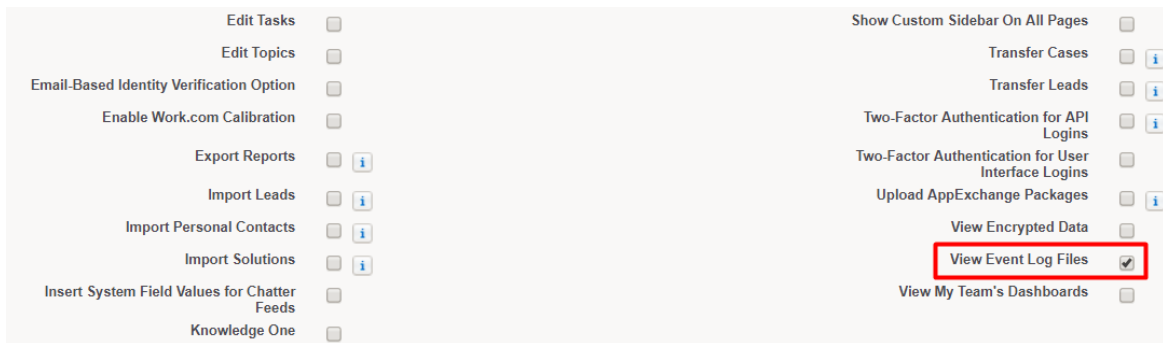
Ant Migration Tool	<input type="checkbox"/>	RsaNW_test	<input type="checkbox"/>
Dataloader Bulk	<input type="checkbox"/>	Salesforce for Outlook	<input type="checkbox"/>
Dataloader Partner	<input type="checkbox"/>	Salesforce Mobile Dashboards	<input type="checkbox"/>
Force.com IDE	<input type="checkbox"/>	Salesforce Touch	<input type="checkbox"/>
Logcollector	<input checked="" type="checkbox"/>	Workbench	<input checked="" type="checkbox"/>
RSA_Logcollector	<input type="checkbox"/>		

The 'Logcollector' row is highlighted with a red box.

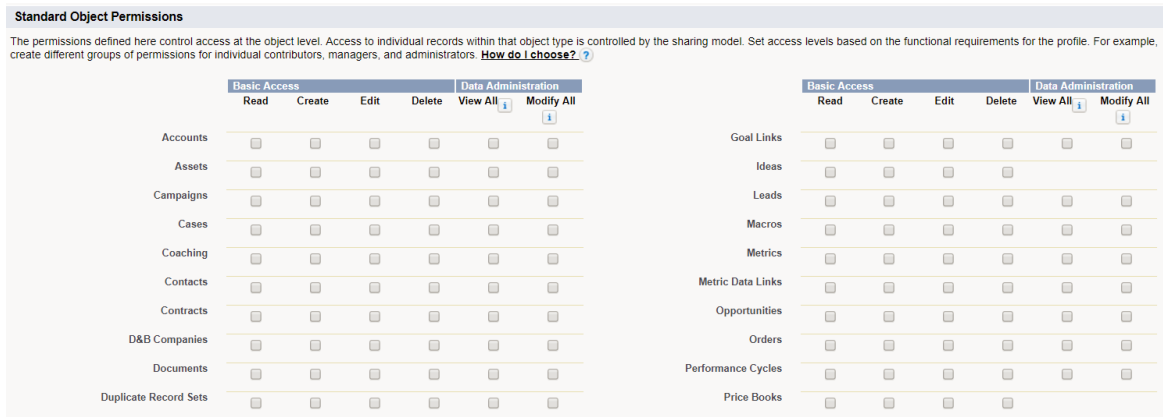
c. In the **Administrative Permissions** section, select the **API Enabled** option as shown below.



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.

Desktop Integration Clients

Choose whether users with this profile can use a client, update a client, see client update alerts, or be forced to update to the latest version. To set permissions for Salesforce Configurations permission and define settings in Outlook configurations.

Offline On, updates w/o alerts ▼

Session Settings

Session times out after Session security level required at login

Password Policies

User passwords expire in

Enforce password history

Minimum password length

Password complexity requirement

Password question requirement

Maximum invalid login attempts

Lockout effective period

Obscure secret answer for password resets

Require a minimum 1 day password lifetime

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)

New User

User Edit Save Save & New Cancel

General Information

First Name

Last Name

Alias

Email

Username

Nickname

Title

Company

Department

Division

Role

User License

Profile

Active

Marketing User

Offline User

Knowledge User

Force.com Flow User

Service Cloud User

Site.com Contributor User

Site.com Publisher User

Work.com User

Data.com User Type

Data.com Monthly Addition Limit

Accessibility Mode (Classic Only)

High-Contrast Palette on Charts

Force.com Quick Access Menu

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

Approver Settings

Delegated Approver

Manager

Receive Approval Request Emails

Generate new password and notify user immediately

Save Save & New Cancel

- Click **Save**.

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

- From the email message, click the verify account hyperlink, then change the password.
- Save the username and password, since you need them later when you are configuring the Salesforce event source in NetWitness Platform.

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

Platform

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.

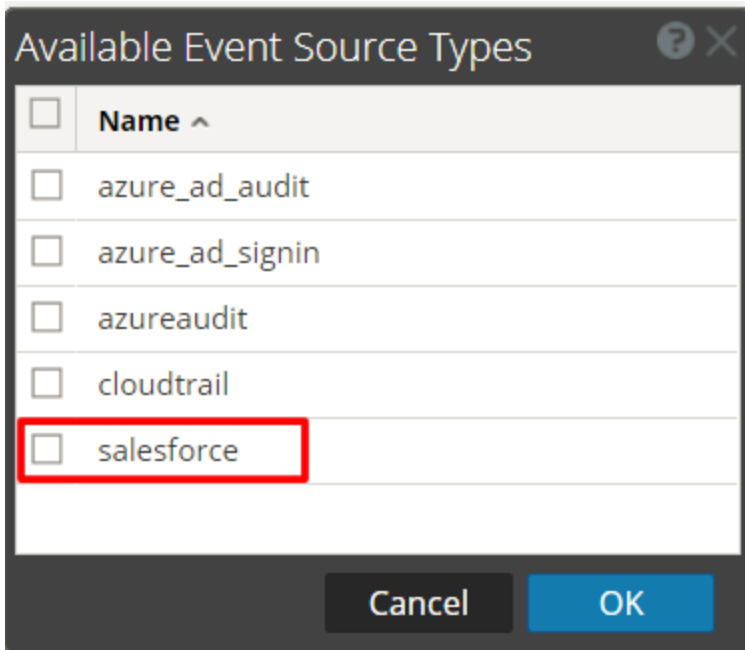
To configure the Salesforce Event Source:

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.

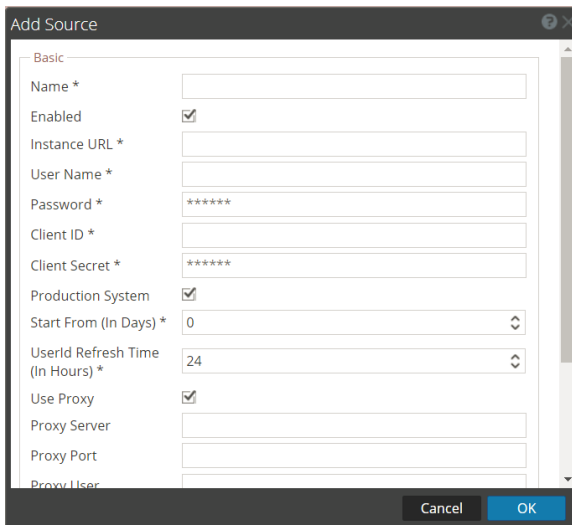


5. Select **salesforce** from the list, and click **OK**.

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 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: <ul style="list-style-type: none"> In Salesforce Lightning Experience UI (LEX): Setup > Company Settings > Company Information In Salesforce Classic UI (Aloha): Setup > Company Profile > Company Information <p>The URL should be https://{instance}.salesforce.com, where <i>{instance}</i> is the name of your organization instance.</p>
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.

Parameter	Description
Production System	<p>By default, the environment type is set to Production. Clear this checkbox to use the sandbox instead.</p> <ul style="list-style-type: none"> 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.
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	<p>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.</p> <p>This value can help you to query or group events collected by a particular instance of the plugin.</p>
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	<p>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.</p> <div data-bbox="386 457 1417 583" style="border: 1px solid green; padding: 5px;"> <p>Note: The Salesforce event source generates events every 24 hours, and max polling interval can be set to 24 hours as well in NetWitness Platform . 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.</p> </div>
Max Duration Poll	<p>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:</p> <ol style="list-style-type: none"> 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	<p>The maximum number of events per polling cycle (how many events collected per polling cycle).</p>
Max Idle Time Poll	<p>Maximum duration, in seconds, of a polling cycle. A zero value indicates no limit.</p>
Command Args	<p>Optional arguments to be added to the script invocation.</p>
Debug	<div data-bbox="386 1201 1417 1297" style="border: 1px solid yellow; padding: 5px;"> <p>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.</p> </div> <div data-bbox="386 1318 1417 1369" style="border: 1px solid yellow; padding: 5px;"> <p>Caution: Enables or disables debug logging for the event source. Valid values are:</p> </div> <ul style="list-style-type: none"> • Off = (default) disabled • On = enabled • Verbose = enabled in verbose mode - adds thread information and source context information to the messages. <p>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.</p>
SSL Enable	<p>The check box is selected by default. Uncheck this box to disable SSL certificate verification.</p>

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See the documentation for Logstash JDBC input plugin here: <https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click Support > Case Portal > View My Cases .
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to feedbacknwdocs@netwitness.com to provide feedback on NetWitness Platform documentation.