

RSA | **Identity Governance and Lifecycle**

Salesforce Application Guide

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

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. 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 SecurCare Online. 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 EMC software described in this publication requires an applicable software license. EMC 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." EMC CORPORATION 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.

Contents

Revision History	3
Preface	4
Audience	4
What’s in this Guide	4
Collectors and Connectors for Salesforce	5
Using Collectors	6
Salesforce Account Data Collector and Federated Salesforce Account Data Collector	6
Prerequisites	6
Data/Attributes collected by the Account Data Collector	9
Adding Additional Attributes for Account Data Collector (ADC)	10
Configuration	11
Salesforce Entitlement Data Collector	16
Prerequisites	16
Adding Additional Attributes for the Entitlement Data Collector (EDC)	16
Configuration	17
Using Connectors	20
Salesforce Connector	20
Prerequisites	20
Configuration	20
SCIM-based Salesforce Connector	56
Prerequisites	56
Configuration	56
Salesforce Application Wizard Configuration	82
Tips & Troubleshooting	84
APPENDIX A	88
Adding Additional Attributes	88

Revision History

Revision Number	Description
Revision 1.0	Salesforce
Revision 1.1	Updated document with minimum version support.
Revision 1.2	Support for Salesforce V40.0 API
Revision 1.3	Support for additional attributes in ADC
Revision 1.4	Support for Salesforce V44.0 API
Revision 1.5	Support for Salesforce V48.0 API

Preface

This guide provides an overview of Collectors and Connectors which use REST or SCIM to communicate with Salesforce for data collection, provisioning and de-provisioning of entities. It describes all the required configurations, parameters and mappings of different attributes between the Collectors, Connectors and Salesforce. This guide includes use cases and troubleshooting tips.

Supported software

- RSA Identity Management and Governance 6.9.1 P15 and later
- RSA Identity Management and Governance 7.0.0 P03 and later
- RSA Identity Governance and Lifecycle 7.0.1 and later

Supported Salesforce Versions

- Salesforce V37.0 and lower (RSA Identity Governance and Lifecycle 7.0.2 and earlier)
- Salesforce V40.0 and lower (RSA Identity Governance and Lifecycle 7.1.0)
- Salesforce V44.0 and lower (RSA Identity Governance and Lifecycle 7.1.1)
- Salesforce V48.0 and lower (RSA Identity Governance and Lifecycle 7.2.1)

Audience

This guide is intended for the users of RSA Identity Governance and Lifecycle, including security administrators. Salesforce can be integrated with RSA Identity Governance and Lifecycle using these Collectors and Connectors. Having basic RESTful and SCIM protocol knowledge is an advantage.

What's in this Guide

- Description of supported Collectors and Connectors for Salesforce
- How to configure Collectors and Connectors for Salesforce
- Salesforce Application Wizard Configuration
- Tips and troubleshooting

Collectors and Connectors for Salesforce

The following table lists the Collectors and Connectors for Salesforce.

Name	Data Source Type/Connector Template	Description
Salesforce Account Data Collector	Salesforce	Collects Account related data from Salesforce.
Salesforce Entitlement Data Collector	Salesforce	Collects Entitlement related data from Salesforce.
Federated Salesforce Account Data Collector	Federated Salesforce	Collects Federation Identifier in addition to other Account related data from Salesforce
Salesforce Connector	Salesforce	Provisions data on Salesforce. This Connector uses REST APIs internally.
SCIM-based Salesforce Connector	Salesforce, SCIM Based	Provisions data on SCIM-enabled Salesforce instance. This Connector uses SCIM APIs internally.

Using Collectors

The following sections describe how to use the Salesforce Collectors.

Salesforce Account Data Collector and Federated Salesforce Account Data Collector

These Collectors communicate with Salesforce and collect the Account data.

Prerequisites

1. Create a Profile for API access

RSA Identity Governance and Lifecycle collects data from Salesforce by using Salesforce APIs. Create an integration user in Salesforce for the purpose of API access. This user must have permission to access the APIs and update all data.

Follow these steps to create a New Profile:

1. Log in to Salesforce.
2. Click Setup next to your account name.
3. In the Administer section, click Manage Users > Profiles.
4. Click New Profile and select the required Profile from the 'Existing Profile' dropdown > Fill in Profile Name > Save.
5. Make sure that the following permissions are set in the Administrative Permissions section of the created Profile.
 - API Enabled
 - Modify All Data (This is not mandatory if only collection is required)

2. Determine the URL for API access

Salesforce uses different URLs for different customer accounts. Log in to Salesforce and find the URL that appears in your address bar, for example:
`https://<your_instance_name>.salesforce.com`

3. Create a User for API access

Using the profile that you have created, create an account for API access by following these steps:

- Log in to Salesforce.
- Click Setup next to your account name.
- In the Administer section, click Manage Users > Users.
- Click New User and select the Profile you created in Step 1.

4. Enable User Skills

Perform the following steps to enable User Skills:

1. Log in to Salesforce.
2. Next to your account name, click Setup > Customize > Work.com > Settings.
3. Under Skills Settings, select Enable for settings available.

4. Click Save.

5. Installing required certificates

Add Salesforce and Certificate Authority (only if required) certificates to the appropriate keystores. Perform the following to add certificates to the keystores of WebSphere, WebLogic and WildFly application servers, respectively.

WebSphere Application Server:

1. Log in to the WebSphere console using your host name: http://<HOST_NAME>:9060/ibm/console/login.do
2. In left panel, expand the Security menu.
3. Click SSL certificate and click key management.
4. Under Configuration Settings, click 'Manage endpoint security configurations.
5. Select Outbound properties for the appropriate node.
6. Click the appropriate node link to get the properties.
7. Under Related Items, click Key stores and certificates and click the NodeDefaultTrustStore keystore.
8. Under Additional Properties, click Signer certificates and click Retrieve from Port.
9. In the Host field, enter: <your_salesforce_host_name>; in the Port field, enter 443 , and in the Alias field, enter salesforce_cert.
10. Click Retrieve Signer Information.
11. Verify that the certificate information is for a certificate that you can trust.
12. Click Apply and click Save.
13. Now, again go to Key stores and certificates and click the Aveksa Keystore.
14. Under Additional Properties, click Signer certificates and click Retrieve from Port.
15. In the Host field, enter <authority url>; in the Port field, enter 443; and in the Alias field, enter authority_cert.
16. Click Retrieve Signer Information.
17. Verify that the certificate information is for the certificate that you trust.
18. Click Apply and click Save.
19. Log into the WebSphere machine using SSH (e.g. putty).
20. At command prompt, run: /home/oracle/AFX/afx stop.
21. At command prompt, run: /opt/IBM/WebSphere/AppServer/bin/stopServer.sh server1.
22. At command prompt, run: /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1.
23. At command prompt, run: /home/oracle/AFX/afx start.

For Connector: If you see PKIX error while using the connector, we need to add certificate in JAVA_HOME/jar/lib/security/cacerts

1. Download/retrieve Salesforce and Certificate Authority (only if required) certificates in PEM format.
2. Add certificates in cacerts by using keytool command:


```
keytool -import -file <authority_certificate> -alias <authority_alias> -keystore
<JAVA_HOME>/jre/lib/security/cacerts -storepass changeit
```

3. Restart the Application Server

WebLogic application Server:

1. Download/retrieve Salesforce and Certificate Authority (only if required) certificates in PEM format and save them at location /home/oracle.
2. Log in to the WebLogic console using your host name:
http://<HOST_NAME>.aveksa.local:7001/console/login/LoginForm.jsp
3. In the Environment section under Domain Configurations, click Servers.
4. Click aveksaServer.
5. Click the SSL tab.
6. Click Advanced.
7. For HostName, select Verification = None.
8. Save the settings.
9. Log into the WebLogic machine using SSH (e.g. putty).
10. Change directory: cd /home/oracle/
11. Add Salesforce and Certificate Authority (only if required) certificates in server.keystore by using the keytool :

```
keytool -import -file <salesforce.pem> -alias salesforce -keystore server.keystore
keytool -import -file <authority_certificate> -alias <alias> -keystore server.keystore
```

- storepass Av3k5a15num83r0n3

12. Restart SSL on WebLogic Server:

Click Servers > controls tab.

Select/check aveksaServer(admin) and then click Restart SSL.

13. Restart the server:

```
/home/oracle/AFX/afx stop
```

```
/home/oracle/wls/12.1.3.0/user_projects/domains/aveksaDomain/bin/stopWebLogic.sh
```

```
/home/oracle/wls/12.1.3.0/user_projects/domains/aveksaDomain/bin/startWebLogic.sh
```

```
/home/oracle/AFX/afx start
```

For Connector: If you see PKIX error while using the connector, we need to add certificate in JAVA_HOME/jar/lib/security/cacerts

1. Download/retrieve Salesforce and Certificate Authority (only if required) certificates in PEM format.
2. Add certificates in cacerts by using keytool command:

```
keytool -import -file <authority_certificate> -alias <authority_alias> -keystore  
<JAVA_HOME>/jre/lib/security/cacerts -storepass changeit
```

3. Restart the Application Server

WildFly Application Server:

1. Download/retrieve Salesforce and Certificate Authority (only if required) certificates in PEM format.
2. Add certificates in cacerts by using keytool command:

```
keytool -import -file <authority_certificate> -alias <authority_alias> -keystore  
<JAVA_HOME>/jre/lib/security/cacerts -storepass changeit
```

3. To restart the server, run these commands:
afx stop
acm stop
acm start
afx start

Data/Attributes collected by the Account Data Collector

User Attributes

- ID
- Username
- FederationIdentifier (Applicable only for Federated Salesforce Collector)
- Email
- LastLoginDate
- UserRoleId
- UserRoleName
- IsDisabled
- EmployeeNumber (7.0.2 P12, 7.1.0 P06 and later)
- FirstName (7.0.2 P12, 7.1.0 P06 and later)
- LastName (7.0.2 P12, 7.1.0 P06 and later)

Group Attributes

- GroupID
- GroupName
- GroupEmail
- GroupOwnerID

- GroupType

Adding Additional Attributes for Account Data Collector (ADC)

Additional attributes are available to the ADC. To add additional attributes for collection and review:

1. Click Admin > Attributes.
2. Click the appropriate tab and add the attribute. The following tables describe the format for each attribute.

Account

In the Account tab, you can add the following attributes:

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
External Id	String	<one of available>	Collected	No	No	No
Email	String	<one of available>	Collected	Yes	Yes	No
Account Disabled	String	<one of available>	Collected	Yes	Yes	No
User Role Id	String	<one of available>	Collected	No	No	No
User Role Name	String	<one of available>	Collected	Yes	Yes	No
Username	String	<one of available>	Collected	Yes	Yes	No

Group

In the Group tab, you can add the following attributes:

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
External Id	String	<one of available>	Collected	No	No	No
Email	String	<one of available>	Collected	Yes	Yes	No
Type	String	<one of available>	Collected	Yes	Yes	No

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
Group Name	String	<one of available>	Collected	Yes	Yes	No
Owner	String	<one of available>	Collected	Yes	Yes	No

Application Role

In the Application Role tab, you can add the following attributes:

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
External Id	String	<one of available>	Collected	No	No	No
Type	String	<one of available>	Collected	Yes	Yes	No
User Type	String	<one of available>	Collected	Yes	Yes	No
User License Id	String	<one of available>	Collected	No	No	No
User License Name	String	<one of available>	Collected	Yes	Yes	No
Name	String	<one of available>	Collected	Yes	Yes	No

Configuration

You configure the Account Data Collector using multiple screens. This section describes the values for each screen.

To access the Account Data Collector wizard:

1. Log in to RSA Identity Governance and Lifecycle.
2. Click Collectors > Account Collectors.
3. Click Create Account Collector.

Collector Description

Configure the parameters on the Collector Description screen. See the table for information on the field names.

Field Name	Value
Collector Name	Salesforce ADC Name
Description	Salesforce Account Data Collector Description
Business Source	Any Created Application or Directory
Data Source Type	Salesforce/Federated Salesforce
Agent	AvekساAgent
Status	Active
Copy from	Select an Existing Salesforce Account Collector if the same collector configuration is to be used.
Scheduled	Default: No

Configuration Information

Configure the parameters on the Configuration Information screen. See the table for information on the field names.

Field Name	Value
Instance URL	Enter the Salesforce instance URL specified in WSDL under the node " soap:address ". This is the Salesforce instance loginURL appended with "services/Soap/u/" OR "services/Soap/c/". The Salesforce Instance login URL is the URL where Salesforce users log in.
Target Namespace	Enter target namespace specified in WSDL under node "definitions" attribute "targetNamespace". Default Target namespace - urn:enterprise.soap.sforce.com
Salesforce API URL	Base URL of the Salesforce API Access. For example, https://ap1.salesforce.com

Username	Username of the user created for integration
Password	Password of the user created for integration
Security Token	<p>Security token for the user created for integration (i.e. Admin user).</p> <p>A security token is an automatically generated key used to log in to Salesforce from an untrusted network. If network is trusted, you do not need this token. To generate this token explicitly, log in to Salesforce using this user go to the Setup page and click My Personal Information > Reset My Security Token option.</p>
Salesforce API Version	Provide Salesforce API version supported by Salesforce instance.
Collect Skills	Enable the checkbox to collect user skills from the instance. Make sure that skills are enabled at the Salesforce instance.
User Filter	<p>Salesforce User Filter for User classification. This is a text box where a query can be provided to filter users.</p> <p>For example:</p> <p>EmployeeNumber!=null</p> <p>LanguageLocaleKey!=null&EmployeeNumber!=null etc.</p>
Proxy Host	Proxy host, if you are using a proxy server to access internet.
Proxy Port	Proxy port, if you are using a proxy server to access internet.
Proxy Username	Proxy username, if you are using a proxy server to access internet.
Proxy Password	Proxy password, if you are using a proxy server to access internet.

Map Collector Attributes to Account Attributes

Configure the parameters on the Map Collector Attributes to Account Attributes screen.

This screen allows mapping additional information provided by the Collector to the custom attributes of the created accounts. You can configure custom account attributes at Admin > Attributes.

See the table for information on the field names.

Field Name	Value
Last Login Date	LastLoginDate
Account Disabled	IsDisabled
External id	ID
User role name	UserRoleName
Email	Email
Username	Username
User role id	UserRoleId

Map Collector Attributes to Account Mapping Attributes

Configure the parameters on the Map Collector Attributes to Account Mapping Attributes screen.

This screen allows mapping additional information provided by the Collector to the custom attributes of the account mappings that the Collector creates. You can configure custom account attributes at Admin > Attributes.

See the table for information on the field names.

Field Name	Value
User Reference	Username

Map Collector Attributes to Group Attributes

Configure the parameters on the Map Collector Attributes to Group Attributes screen.

This screen allows mapping additional information provided by the Collector to custom attributes of the groups that the Collector creates. You can configure custom account attributes at Admin > Attributes.

See the table for information on the field names.

Field Name	Value
External id	GroupId
Owner	GroupOwnerId
Type	GroupType
Email	GroupEmail
Name	GroupName

Edit User Resolution Rules

Configure the parameters on the Edit User Resolution Rules screen. See the table for information on the field names.

Field Name	Value
Target Collector	Associate an IDC; Default value is Users.
User Attribute	By Default: User Id

Edit Member Account Resolution Rules

Configure the parameters on the Edit Member Account Resolution Rules screen. See the table for information on the field names.

Field Name	Value
Target Collector	Associate a Salesforce Account Data Collector.

Account Attribute	Account Name
-------------------	--------------

Edit Sub-Group Resolution Rules

Configure the parameters on the Edit Sub group Resolution Rules screen. See the table for information on the field names.

Field Name	Value
Target Collector	Associate a Salesforce Account Data Collector.
Group Attribute	Name

Salesforce Entitlement Data Collector

This Collector collects entitlement data from Salesforce..

Prerequisites

For this Collector, make sure you have completed the prerequisites section of Salesforce Account Data Collector.

Adding Additional Attributes for the Entitlement Data Collector (EDC)

Additional attributes are available to the EDC. . To add additional attributes for collection and review:

3. ClickAdmin > Attributes.
4. Select the appropriate tab and add the attribute. The following table describes the format to use for each attribute..

Application Role

In the Application Role tab, you can add the following attributes:

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
External Id	String	<one of available>	Collected	No	No	No
Type	String	<one of available>	Collected	Yes	Yes	No

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
User Type	String	<one of available>	Collected	Yes	Yes	No
User License Id	String	<one of available>	Collected	No	No	No
User License Name	String	<one of available>	Collected	Yes	Yes	No
Name	String	<one of available>	Collected	Yes	Yes	No

Configuration

To configure the Entitlement Data Collector, you use multiple screens. This section describes the values for each screen.

To access the Entitlement Data Collector wizard:

1. Log in to RSA Identity Governance and Lifecycle.
2. Click Collectors > Entitlement Collectors.
3. Click Create Entitlement Collector.

Collector Description

Configure the parameters on the Collector Description screen. See the table for information on the field names.

Field Name	Value
Collector Name	Salesforce EDC Name
Description	Salesforce Entitlement Data Collector Description
Business Source	Any Created Application or Directory
Data Source Type	Salesforce
Agent	AveksaAgent
Status	Active

Copy from	Select Existing Salesforce EDC Collector if same collector configuration is to be used.
Scheduled	Default: No

Configuration Information

Configure the parameters on the Configuration Information screen. See the table for information on the field names.

Field Name	Value
Instance URL	Enter the Salesforce instance URL specified in WSDL under the node " soap:address ". This is Salesforce instance login URL appended with "services/Soap/u/" OR "services/Soap/c/". The Salesforce instance login URL is the URL where Salesforce users log in.
Target Namespace	Enter target namespace specified in WSDL under node "definitions" attribute "targetNamespace". Default Target namespace - urn:enterprise.soap.sforce.com
Salesforce API URL	Base URL of the Salesforce API Access. For example, https://ap1.salesforce.com
Username	Username of the user created for integration
Password	Password of the user created for integration
Security Token	Security token for the user created for integration (i.e. Admin user). A security token is an automatically generated key used to log in to Salesforce from an untrusted network. If network is trusted, you do not need this token. To generate this token explicitly, log in to Salesforce using this user and then, go to the Setup page and select My Personal Information > Reset My Security Token option.
Salesforce API Version	Provide the Salesforce API version supported by Salesforce instance.

Proxy Host	Proxy host, if you are using a proxy server to access internet.
Proxy Port	Proxy port, if you are using a proxy server to access internet.
Proxy Username	Proxy username, if you are a using proxy server to access internet.
Proxy Password	Proxy password, if you are using a proxy server to access internet.

Map Collector Attributes to App Role Attributes

Configure the parameters on the Map Collector Attributes to App Role Attribute” screen. This screen allows mapping additional information provided by the Collector to custom attributes of the application roles that the Collector creates. You can configure custom account attributes at Admin > Attributes.

See the table for information on the field names.

Field Name	Value
External id	ID
Type	AppRoleType

Account Evaluation

Select a known account attribute to resolve known references. See the table for information on the field names.

Field Name	Value
Associated Account Collector	Salesforce ADC to be configured
Account value evaluates to	Account Name

Using Connectors

The following sections describe how to use the Salesforce Connectors.

Salesforce Connector

This REST API based Connector can be used to communicate and to provision data to Salesforce.

Prerequisites

Same as mentioned in Pre-Requisites section of Salesforce/Federated Salesforce Account Data Collector along with the following.

Enable OAuth Settings to be able to use REST APIs

To create a New Connected App at Salesforce:

- Log in to Salesforce.
- Click Setup next to your account name.
- In Build section, click Create >Apps
- Under Connected Apps, click New and fill in the details.
- Click Enable OAuth Settings check box and fill in all mandatory fields.
- Note down your Client Id and Client Secret.

Configuration

To configure the Connector, complete the three sections: General, Settings, and Capabilities.

To access the Connector wizard:

1. Log in to RSA Identity Governance and Lifecycle.
2. Click AFX > Connectors.
3. Click Create Connector.
4. Select each tab and enter the appropriate information. The following tables describe each setting.

General – General details about the Connector like the name, type.

The settings for the tab are listed in the following table:

Field Name	Value
Name	Connector instance name
Description	Connector instance description

Server	Select available AFX server
Connector Template	Salesforce
State	Test/Active Note that when Connector testing is successful, change the state to <i>Active</i> . No automated provisioning occurs while in the <i>Test</i> state. Test all enabled commands using the <i>Test</i> Connector Settings and check Connector Capabilities prior to changing to the <i>Active</i> state.
Export As Template	Use this field to define name of this Connector export zip file, it is used while exporting Connector instance

Settings – The connection settings required to connect RSA Identity Governance and Lifecycle and Salesforce.

The settings for the tab are listed in the following table:

Field Name	Value
Connection Details	
Base URL	Base URL for REST call (for example: https://HostName)
API Version	Salesforce API version used (for example: 30.0)
<p>Parameters applicable for OAuth 2.0 authentication</p> <p>All these parameters are mandatory as endpoint supports OAuth2.</p> <p>It is mandatory to generate OAuth2 access token for endpoints supporting OAuth2.0. Hence, after filling up these OAuth2 fields, click Get OAuth 2.0 Access Token to acquire the access token.</p> <p>If OAuth2 Access Token is not generated, Connector won't be created.</p>	
Client Id	Client Id of registered application

Client Secret	Client Secret of registered application
Authorization URL	Authorization URL of the endpoint to get authorization code from
Access Token URL	Token endpoint URL to get the access token from
Login Email	Email id of the user of endpoint instance
Access Token Expiry	Access token expiry time in milliseconds Default- 3600000
Proxy Settings	
Proxy Host	Hostname of the proxy server Note: Proxy settings are available in 6.9.1Patch-02 and above
Proxy Port	Port of the proxy server
Proxy User Name	User name for the proxy server
Proxy Password	Password for the proxy server

Capabilities – This tab has a list of capabilities, or actions, supported by this Connector.

When creating the Connector, by default, all of the capabilities have parameters pre-populated. Each capability has the same configurations.

Note: Skill-related capabilities will run on Salesforce API v30.0 and above

- Create an Account
- Reset an Account Password
- Add Account to Group
- Remove Account from Group
- Enable an Account
- Disable an Account
- Update an Account
- Add Application Role to Account
- Remove Application Role from Account
- Create a Group

- Delete a Group
- Update a Group
- Add a Group to a Group
- Remove a Group from a Group
- Add Users To Profile Skills
- Create Skills
- Delete Skills
- Remove Users From Profile Skills

Command Input Parameters

Create an Account

Field Name	Value
Parameter Name	FirstName
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	First Name
Mapping	\${User.First_Name}
Description	Salesforce Account First Name

Field Name	Value
Parameter Name	LastName

Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Last Name
Mapping	\${User.Last_Name}
Description	Salesforce Account Last Name

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	User Name
Mapping	\${User.Email_Address}

Description	Salesforce Account User Name
-------------	------------------------------

Field Name	Value
Parameter Name	Password
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	Password
Mapping	\${AccountTemplate.Password}
Description	Salesforce Account Password

Field Name	Value
Parameter Name	Email
Type	STRING
Default Value	None
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Email
Mapping	\${User.Email_Address}
Description	Salesforce Account Email Id

Field Name	Value
Parameter Name	Alias
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Alias
Mapping	\${AccountTemplate.Alias}
Description	Salesforce Account Alias

Field Name	Value
Parameter Name	TimeZoneSidKey

Type	STRING
Default Value	America/Los_Angeles
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Time Zone Sid Key
Mapping	timezone ID, for example, America/Los_Angeles
Description	Salesforce TimeZoneSidKey

Field Name	Value
Parameter Name	LanguageLocaleKey
Type	STRING
Default Value	en_US
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Language Locale Key
Mapping	Language locale, for example, en_US

Description	Language Locale Key
-------------	---------------------

Field Name	Value
Parameter Name	LocaleSidKey
Type	STRING
Default Value	en_US
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Locale Sid Key
Mapping	Locale key, for example, en_US
Description	Salesforce LocaleSidKey

Field Name	Value
Parameter Name	EmailEncodingKey
Type	STRING
Default Value	ISO-8859-1
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Email Encoding Key
Mapping	Encoding key, for example, ISO-8859-1
Description	Salesforce EmailEncodingKey

Field Name	Value
Parameter Name	CommunityNickName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Nickname
Mapping	\${AccountTemplate.Nickname}
Description	Salesforce Account nickname

Field Name	Value
Parameter Name	ProfileName

Type	STRING
Default Value	Chatter Free User
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Profile Name
Mapping	\${AccountTemplate.Profile}
Description	Salesforce ProfileName

Field Name	Value
<p>Note : This parameter is applicable only if Federation Id is to be provisioned using Salesforce Connector.</p>	
Parameter Name	FederationIdentifier
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Federation Identifier

Mapping	<code>\${AccountTemplate.FederationId}</code>
Description	Salesforce Federation Identifier

Reset an Account Password

Field Name	Value
Parameter Name	AccountName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	<code>\$(Account.Name)</code>
Description	Salesforce account whose password is to be reset

Field Name	Value
Parameter Name	Password
Type	STRING

Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	New Password
Mapping	\${AccountPassword}
Description	New Salesforce Account Password

Add Account to Group

Field Name	Value
Parameter Name	AccountName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce Account to be added to a group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce GroupName to which an account is to be added

Remove an Account from Group

Field Name	Value
Parameter Name	AccountName
Type	STRING
Default Value	None
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce Account to be removed from a group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce Group Name from which an account is to be removed

Enable an Account

Field Name	Value
-------------------	--------------

Parameter Name	AccountName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce Account to be enabled

Disable an Account

Field Name	Value
Parameter Name	AccountName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name

Mapping	\${Account.Name}
Description	Salesforce Account to be disabled

Update an Account

Field Name	Value
Parameter Name	AccountName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce Account to be updated

Field Name	Value
Parameter Name	FirstName
Type	STRING
Default Value	None

Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	First Name
Mapping	\${User.First_Name}
Description	Salesforce Account First Name

Field Name	Value
Parameter Name	LastName
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Last Name
Mapping	\${User.Last_Name}
Description	Salesforce Account Last Name

Field Name	Value
Parameter Name	NewUserName
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	New Username
Mapping	-
Description	Salesforce Username to be updated

Field Name	Value
Parameter Name	Alias
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No

Display Name	Alias
Mapping	\${User.First_Name}
Description	Salesforce Account Alias

Field Name	Value
Parameter Name	TimeZoneSidKey
Type	STRING
Default Value	America/Los_Angeles
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Time Zone Sid Key
Mapping	timezone ID, for example, America/Los_Angeles
Description	Salesforce TimeZoneSidKey

Field Name	Value
Parameter Name	LanguageLocaleKey
Type	STRING

Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Language Locale Key
Mapping	Language locale, for example, en_US
Description	Language Locale Key

Field Name	Value
Parameter Name	LocaleSidKey
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Locale Sid Key
Mapping	Locale key, for example, en_US
Description	Salesforce LocaleSidKey

Field Name	Value
Parameter Name	EmailEncodingKey
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Email Encoding Key
Mapping	Encoding key, for example, ISO-8859-1
Description	Salesforce EmailEncodingKey

Field Name	Value
Parameter Name	CommunityNickName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No

Display Name	Nickname
Mapping	\${AccountTemplate.Nickname}
Description	Salesforce Community Nickname

Field Name	Value
Parameter Name	ProfileName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Profile Name
Mapping	\${AccountTemplate.Profile}
Description	Salesforce ProfileName

Add Application Role to Account

Field Name	Value
Parameter Name	AccountName

Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce Account Name

Field Name	Value
Parameter Name	PermissionSetName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Permission Set Name
Mapping	\${ApplicationRole.Name}

Description	Salesforce login Permission Set Name
-------------	--------------------------------------

Remove Application Role from Account

Field Name	Value
Parameter Name	AccountName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce Account Name

Field Name	Value
Parameter Name	PermissionSetName
Type	STRING
Default Value	None

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Permission Set Name
Mapping	\${ApplicationRole.Name}
Description	Salesforce login Permission Set Name

Create a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Name of the group to be created, must be unique

Field Name	Value
Parameter Name	GroupLabel
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Label
Mapping	\${Group.Name}
Description	Label of Group, may not necessarily be unique

Delete a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No

Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce Group Name to be deleted

Update a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Name of salesforce group to be updated

Field Name	Value
Parameter Name	NewGroupName

Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	New Group Name
Mapping	\${Group.Name}
Description	New name to be given to Salesforce group

Field Name	Value
Parameter Name	NewGroupLabel
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	New Group Label
Mapping	\${Group.Name}

Description	New label to be given to Salesforce group
-------------	---

Add a Group to a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Parent Group Name
Mapping	\${Group.Name}
Description	Salesforce parent GroupName

Field Name	Value
Parameter Name	SubGroupName
Type	STRING
Default Value	None

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Subgroup Name
Mapping	\${Group.Name}
Description	Salesforce group to be added to another group

Remove a Group from a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Parent Group Name
Mapping	\${Group.Name}
Description	Salesforce parent GroupName

Field Name	Value
Parameter Name	SubGroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Subgroup Name
Mapping	\${Group.Name}
Description	Salesforce group to be removed from another group

Add Users to Profile Skill

Field Name	Value
Parameter Name	ProfileSkillName
Type	STRING
Default Value	None
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Skill Name
Mapping	\${Group.Name}
Description	Name of the Skill to which user has to be added

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Salesforce User Name
Mapping	\${Account.Name}
Description	Name of user who has to be added to ProfileSkill

Create Skills

Field Name	Value
------------	-------

Parameter Name	SkillName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Skill Name
Mapping	\${Group.Name}
Description	Skill Name

Field Name	Value
Parameter Name	SkillDescription
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Skill Description

Mapping	\${Group.Name}
Description	Skill Description

Delete Skills

Field Name	Value
Parameter Name	SkillName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Skill Name
Mapping	\${Group.Name}
Description	Name of the Skill to be deleted

Remove Users from Profile Skill

Field Name	Value
Parameter Name	ProfileSkillName
Type	STRING

Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Skill Name
Mapping	\${Group.Name}
Description	Name of the Skill from which user has to be removed

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Salesforce User Name
Mapping	\${Account.Name}
Description	Name of user who has to be removed from ProfileSkill

SCIM-based Salesforce Connector

This SCIM-based Connector can be used to communicate and to provision data to Salesforce.

Prerequisites

Same as mentioned in Prerequisites section of Salesforce/Federated Salesforce Account Data Collector along with the following.

Configuration for SCIM readiness

Steps for SCIM configuration can be found on the Salesforce Application Wizard Remote App Setup Page.

Configuration

To configure the Connector complete the three sections: General, Settings, and Capabilities.

To access the Connector wizard:

1. Login to RSA Identity Governance and Lifecycle.
2. Click AFX > Connectors.
3. Click Create Connector.
4. Select each tab and enter the appropriate information. The following tables describe each setting.
- 5.

General – General details about the Connector like the name, type.

The settings for the tab are listed in the following table:

Field Name	Value
Name	<Connector instance name>
Description	<Connector instance description>
Server	Select available AFX server
Connector Template	Salesforce-SCIMBased
State	Test/Active Note that on satisfactory Connector testing, change the state to <i>Active</i> . No automated provisioning will occur while in the <i>Test</i> state. It is recommended

	to test all enabled commands using the <i>Test Connector Settings</i> and check Connector Capabilities prior to changing to the <i>Active</i> state.
Export As Template	Use this field to define name of this Connector export zip file, it will get used while exporting Connector instance

Settings – The connection settings required to connect RSA Identity Governance and Lifecycle and Salesforce.

The settings for the tab are listed in the following table.

Field Name	Value
Connection Details	
Username	<Username for the user created for integration>
Password	<Password for the user created for integration>
Security Token	<Security token for the user created for integration. A security token is an automatically generated key in order to log in to Salesforce from an untrusted network. If network is trusted to Salesforce need not to provide this token. To generate this token explicitly, login to Salesforce using this user and then go to "Setup" page and select "My Personal Information" -> "Reset My Security Token" option.>
Salesforce API Version	<Provide Salesforce API version supported by Salesforce instance. This should be upto 31.0 for current Connector.>
Salesforce SCIM API Version	< SCIM API version for Salesforce (e.g: v1)>
Salesforce Session Url	<Salesforce Session Url e.g. https://login.salesforce.com/services/Soap/c/ >
Salesforce Instance Url	<Salesforce Instance Url e.g. https://ap2.salesforce.com/services/scim >

Salesforce targetNamespace	< Target namespace for salesforce e.g. urn:enterprise.soap.sforce.com >
Proxy Settings	
Proxy Host	<Hostname of the proxy server> Note: Proxy settings are available in 6.9.1Patch-02 and above
Proxy Port	<Port of the proxy server>
Proxy User Name	<User name for the proxy server>
Proxy Password	<Password for the proxy server >

Capabilities – This tab has a list of capabilities, or actions, supported by this Connector.

After creating this Connector, by default, all capabilities have parameters pre-populated. Each capability listed above has the same configuration. Refer to the individual tables to configure the settings for the capabilities.

- Create an Account
- Reset an Account Password
- Add Account to Group
- Remove Account from Group
- Enable an Account
- Disable an Account
- Update an Account
- Add Application Role to Account
- Remove Application Role from Account
- Create a Group
- Delete a Group
- Add a Group to a Group
- Remove a Group from a Group

Command Input Parameters

Create an Account

Field Name	Value
------------	-------

Parameter Name	Username
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Username
Mapping	#{User.Email_Address}
Description	Salesforce Login

Field Name	Value
Parameter Name	Password
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	Password

Mapping	\${AccountTemplate.Password}
Description	Salesforce login Password

Field Name	Value
Parameter Name	Email
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Email
Mapping	\${User.Email_Address}
Description	Salesforce Email

Field Name	Value
Parameter Name	GivenName
Type	STRING
Default Value	None

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	First Name
Mapping	\${User.First_Name}
Description	Salesforce Firstname

Field Name	Value
Parameter Name	FamilyName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Last Name
Mapping	\${User.Last_Name}
Description	Salesforce Lastname

Field Name	Value
Parameter Name	NickName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Nickname
Mapping	\${AccountTemplate.Nickname}
Description	Salesforce Nickname

Field Name	Value
Parameter Name	Locale
Type	STRING
Default Value	en_US
Is the parameter required?	No
Is the parameter encrypted?	No

Display Name	Locale Sid Key
Mapping	en_US
Description	Salesforce LocaleSidKey

Field Name	Value
Parameter Name	Timezone
Type	STRING
Default Value	America/Los_Angeles
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Time Zone Sid Key
Mapping	America/Los_Angeles
Description	Salesforce TimeZoneSidKey

Field Name	Value
Parameter Name	EmailEncodingKey
Type	STRING

Default Value	ISO-8859-1
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Email Encoding Key
Mapping	ISO-8859-1
Description	Salesforce EmailEncodingKey

Field Name	Value
Parameter Name	PreferredLanguage
Type	STRING
Default Value	en_US
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Language Locale Key
Mapping	en_US
Description	Salesforce LanguageLocaleKey

Field Name	Value
Parameter Name	Entitlement
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Salesforce User Type
Mapping	\${AccountTemplate.Profile}
Description	Salesforce User Type

Reset an Account Password

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	UserName
Mapping	\${Account.Name}
Description	Salesforce login

Field Name	Value
Parameter Name	Password
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	Yes
Display Name	New Password
Mapping	\${AccountPassword}
Description	Salesforce login Password

Add Account to Group

Field Name	Value
------------	-------

Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce login

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name

Mapping	\${Group.Name}
Description	Salesforce GroupName

Remove Account from Group

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce login

Field Name	Value
Parameter Name	GroupName
Type	STRING

Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce GroupName

Enable an Account

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}

Description	Salesforce login
-------------	------------------

Disable an Account

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce login

Update an Account

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	User Name
Mapping	\${Account.Name}
Description	Salesforce Login

Field Name	Value
Parameter Name	GivenName
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	First Name
Mapping	\${User.First_Name}
Description	Salesforce Firstname

Field Name	Value
Parameter Name	FamilyName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Last Name
Mapping	\${User.Last_Name}
Description	Salesforce Lastname

Field Name	Value
Parameter Name	NickName
Type	STRING
Default Value	None
Is the parameter required?	No
Is the parameter encrypted?	No

Display Name	Alias
Mapping	\${User.First_Name}
Description	Salesforce Alias

Field Name	Value
Parameter Name	Locale
Type	STRING
Default Value	en_US
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Locale Sid Key
Mapping	en_US
Description	Salesforce LocaleSidKey

Field Name	Value
Parameter Name	Timezone
Type	STRING

Default Value	America/Los_Angeles
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Time Zone Sid Key
Mapping	America/Los_Angeles
Description	Salesforce TimeZoneSidKey

Field Name	Value
Parameter Name	EmailEncodingKey
Type	STRING
Default Value	ISO-8859-1
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Email Encoding Key
Mapping	ISO-8859-1
Description	Salesforce EmailEncodingKey

Field Name	Value
Parameter Name	PreferredLanguage
Type	STRING
Default Value	en_US
Is the parameter required?	No
Is the parameter encrypted?	No
Display Name	Language Locale Key
Mapping	en_US
Description	Salesforce LanguageLocaleKey

Add Application Role to Account

Field Name	Value
Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes

Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce login

Field Name	Value
Parameter Name	EntitlementName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Permission Set Name
Mapping	\${ApplicationRole.Name}
Description	Salesforce Permission Set Name

Remove Application Role from Account

Field Name	Value
------------	-------

Parameter Name	UserName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Account Name
Mapping	\${Account.Name}
Description	Salesforce login

Field Name	Value
Parameter Name	EntitlementName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Permission Set Name

Mapping	\${ApplicationRole.Name}
Description	Salesforce Permission Set Name

Create a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce GroupName

Delete a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING

Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce GroupName

Add a Group to a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Subgroup Name
Mapping	\${Group.Name}

Description	Salesforce group name which is to be sub group
-------------	--

Field Name	Value
Parameter Name	ParentGroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce parent GroupName

Remove a Group from a Group

Field Name	Value
Parameter Name	GroupName
Type	STRING
Default Value	None

Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Subgroup Name
Mapping	\${Group.Name}
Description	Salesforce group name which is to be sub group

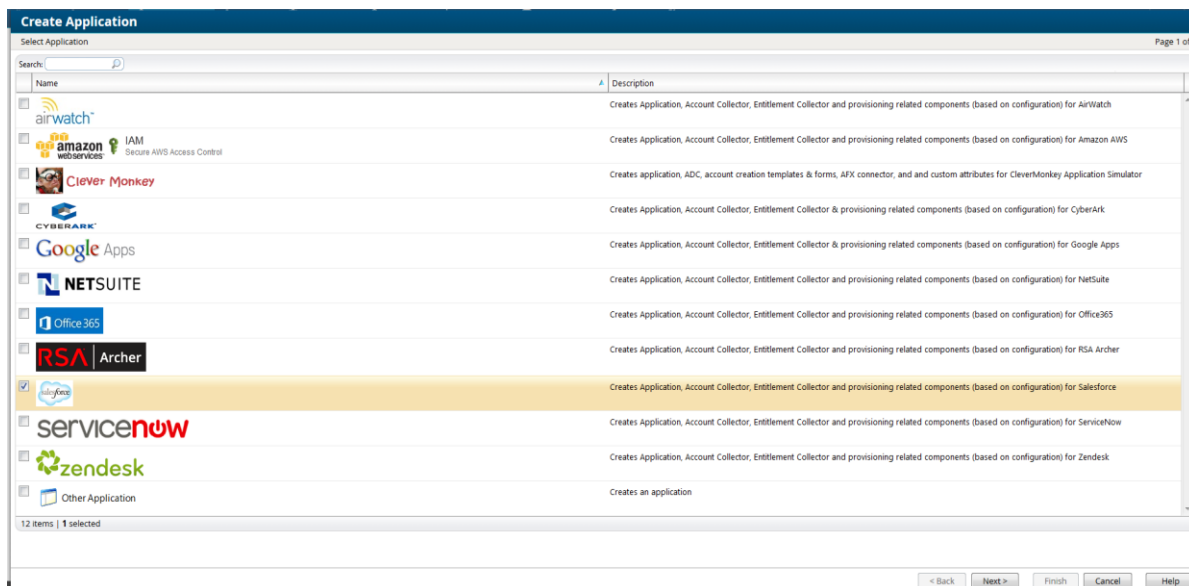
Field Name	Value
Parameter Name	ParentGroupName
Type	STRING
Default Value	None
Is the parameter required?	Yes
Is the parameter encrypted?	No
Display Name	Group Name
Mapping	\${Group.Name}
Description	Salesforce parent GroupName

Salesforce Application Wizard Configuration

You can use the Salesforce application wizard to create the Application, Account Collector, and Entitlement Collector, and provision the related components (based on configuration) for Salesforce.

To create a Salesforce application:

1. Log in to RSA Identity Governance and Lifecycle.
2. Click Resources > Application, and click Create Application.
3. Select Salesforce from the available list of applications and click Next.



4. On the Remote Application Setup page, read the Salesforce endpoint preparation information for configuring Salesforce to communicate with RSA Identity Governance and Lifecycle.
5. The Connect page contains all parameters required to connect to Salesforce. Depending on the Salesforce instance, you may have preconfigured values.

As explained in the section Various Collectors and Connectors for Salesforce, there are different types of Salesforce Collectors and Connectors. The configuration parameters change depending on what type of Connector/Collector you want to create.

- To create a SCIM-based Connector, select the Create SCIM Connector checkbox and configure the parameters.
- To create a Federated Salesforce Account Data Collector, select the Is Federation required checkbox. A Default Salesforce Connector is created, which can provision a Federation Identifier.

- If you do not select a Connector, by default, the parameters are displayed for default Salesforce Connector and Collectors.

Create Application

Connect

User Filter:

Enter API version to use. The Salesforce collector is developed and tested against API Version 25.0.

Salesforce API Version*:

Enable the 'Collect Skills' checkbox to collect skills from Salesforce instance. Make sure that skills are enabled at Salesforce.

Collect Skills:

Is Federation Id support required?

Create SCIM based: salesforce connector

Please provide OAuth2 details

Client Id*:

Client Secret*:

Authorization URL*:

Token URL*:

Token Expiry In: milliseconds*

Enter AFX Server Name:

AFX Server:

Please provide Proxy Settings

Proxy Hostname:

Proxy Port:

Proxy Username:

Proxy Password:

Connection not tested

6. After configuring the connect parameters, click Test Connection. When the test connection is successful, click Next.
7. After confirming all data on the Confirm page, click Finish (if the button exists). All of the application components are created.

Note: The default Salesforce Connector now can provision the Federated Identifier. 'Federation Id' is a non-mandatory parameter to use if required.

Tips & Troubleshooting

Below are possible error responses with error code for the RESTful Web Services. Errors may vary based on the actual API implementation.

Use this table to troubleshoot issues related to endpoint connectivity and responses received. You can view these errors in Server log files when the Connector is in Active mode and from RSA Identity Governance and Lifecycle when the Connector is in Test mode:

For any Connector, you can view this error in the log file – AFX/esb/logs/esb.AFX-CONN-
<ConnectorName>.log.

Expected Condition	HTTP Response Code	Meaning	Example
The business process succeeded or failed in an expected way	200	Success	Request for non-existent entity (user, group, role etc.)
A system process failed (at a deeper level than the business process)	400	bad request	A deserialization exception is thrown or malformed request body
Invalid session	401	Unauthorized	Invalid or incorrect session token in request header
User requests resource to which they do not have permission	403	Forbidden	The admin user requests data of a user but does not have read access to the module
User attempts to POST content using the PUT URI or vice versa	403	Forbidden	The user attempts to save changes to an existing group record using the POST URI on the group controller

No route matching the requested URI is round	404	Not Found	The user requested a URI that has no corresponding route to map it to a controller
--	-----	-----------	--

- Note that the input parameters specified on the configuration page for the Create Account capability are the only ones that can be used.
- **How do I verify which version of TLS is used with Salesforce?**

You can enable SSL logs to verify the TLS version being used. Perform the following steps to enable SSL logs for:

AFX (Access Fulfillment Express)

1. Log in as root.
2. Change directory to: `/home/oracle/AFX/esb/conf`
3. Edit `wrapper.conf` and add the following line:
 - i. `wrapper.java.additional.<n>=-Djavax.net.debug=ssl`
4. Restart AFX.

Wildfly

1. Log on as root.
2. Change directory to: `/home/oracle/wildfly-8.2.0.Final/bin`
3. Edit `standalone.conf` and add an argument :
`-Djavax.net.debug=ssl" in JAVA_OPTS`
4. Save the configuration.
5. Restart the server.

Weblogic

1. Open the admin console for the Weblogic domain and click Lock and Edit .
2. Click on the server for which you want to enable debug.
3. Click the Debug tab
4. Expand the weblogic node.
5. Expand the security node.
6. Select the checkboxes for: `DebugSecuritySSL` and `DebugSecuritySSLEaten`
7. Click Enable.
8. Save the configuration.
9. Restart the server.

Websphere

Depending on your WebSphere version:

1. In the WebSphere Admin Console, click Servers > Application Servers > <YourServer_Name> > Process Management > Java Virtual Machine > Generic JVM arguments.
2. Add the argument: --Djavax.net.debug=ssl
3. Save the configuration.
4. Restart the server.

- ***Why can I log in to Salesforce using my valid credentials, but using the same credentials in the Salesforce Application wizard results in an error: 'Invalid Credentials'?***

An 'Invalid Credentials' error might indicate your Security Token is expired. You need to reset the Security Token and try testing the connection again.

If you are running a VPN, this error could indicate both a VPN and Security Token issue.

- ***How do I troubleshoot a Salesforce Connector?***

1. Go to <AFX_HOME>/esb/apps/<AFX_CONNECTOR> location.
2. Open Connector-flow.xml in any text editor.
3. Locate: <logger level="DEBUG" message="Payload to...>
4. Change logger level to Info; for example <logger level="INFO" message="Payload to...> and save Connector-flow.xml
5. Open mule-config.xml in any text editor. Locate </mule>, and add a new line after it, and then save the file.

This method does a hot deployment of the Connector. Here, you can also use the 'touch' command to facilitate hot deployment.

6. Check that the Connector is in running state. If yes, then run the test capability to verify.

- ***When I configure Salesforce Account Collector using the steps described in Salesforce Collector configuration, why does my collection fail?***

Collection fails when the Collect Skills checkbox is selected when configuring the Collector, but User Skills are not enabled at the Salesforce endpoint.

- ***After I configure User Filter with the Salesforce Account Data Collector, why does my Collector not collect based on the filter?***

Make sure that the User Filter is configured in the correct format (e.g. EmployeeNumber!=null, LanguageLocaleKey!=null&EmployeeNumber!=null). The filter should be referred to as a SOQL query (Salesforce Object Query Language). If your filter has spaces in between words(e.g. email like), then try replacing each space with the plus "+" character (e.g. email+like).

Also for troubleshooting, use a REST Client like Firefox or SOAPUI and invoke the REST URL to see if the filter can retrieve data.

A typical REST URL will look like:

`https://thesalesforceresturl/?q="the SOQL query"`

- ***I exported the Salesforce Connector to a different machine. Why do I get an error (redirect_uri mismatch) while generating an access token on the settings page, but the capability runs successfully?***

This might occur because when the Connector is exported to a different machine, it takes all the settings along with it, except passwords. These settings also include the hidden fields like OAuth Access token and refresh token.

The only field that is required to execute Salesforce capabilities is the OAuth Access token. All capabilities will successfully execute until the OAuth Access token expires. After the access token expires, and you regenerate the access token, you will get a 'redirect_uri mismatch' error. This is probably because you have not updated the callback URI at the endpoint after the machine change.

The callback URL has to be updated as mentioned in the Salesforce Application wizard Remote Application Setup page.

- ***I created all of the Salesforce components using Salesforce App wizard. Why do I get an error saying - Invalid Session while testing connection or executing capabilities?***

This might occur if you do not acquire the access token when creating the application configuration. Without the token, you cannot test the connection or execute capabilities as you do not have a session. You can edit the connector to retrieve the access token.

APPENDIX A

Adding Additional Attributes

If the required attributes do not exist in RSA Identity Governance and Lifecycle, you can add additional attributes.

1. Log on to RSA Identity Governance and Lifecycle.
2. Click Admin > Attributes and create following attributes:

Account

In the Account tab, add the following attributes:

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
External Id	String	<one of available>	Collected	No	No	No
Email	String	<one of available>	Collected	Yes	Yes	No
Account Disabled	String	<one of available>	Collected	Yes	Yes	No
User Role Id	String	<one of available>	Collected	No	No	No
User Role Name	String	<one of available>	Collected	Yes	Yes	No
Username	String	<one of available>	Collected	Yes	Yes	No

Group

In the Group"tab, add the following attributes:

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
External Id	String	<one of available>	Collected	No	No	No
Email	String	<one of available>	Collected	Yes	Yes	No
Type	String	<one of available>	Collected	Yes	Yes	No

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
Group Name	String	<one of available>	Collected	Yes	Yes	No
Owner	String	<one of available>	Collected	Yes	Yes	No

Application Role

In the Application Role tab, add the following attributes:

Attribute Name	Data Type	Database ID	Data Source	In Detail	In Popup	Mandatory
External Id	String	<one of available>	Collected	No	No	No
Type	String	<one of available>	Collected	Yes	Yes	No
User Type	String	<one of available>	Collected	Yes	Yes	No
User License Id	String	<one of available>	Collected	No	No	No
User License Name	String	<one of available>	Collected	Yes	Yes	No
Name	String	<one of available>	Collected	Yes	Yes	No

Copyrights

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

Dell, RSA, the RSA Logo, EMC and other trademarks, are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.