



RSA SecurID Access Implementation Guide

Salesforce

Table of Contents

Solution Summary	3
Use Case	3
Integration Types	3
Supported Features	4
Salesforce Integration with RSA Cloud Authentication Service	4
Salesforce Integration with RSA Authentication Manager	4
Configuration Summary	5
Known Issues	5
Integration Configuration	6
Relying Party	6
Configure RSA Cloud Authentication Service	6
Configure Salesforce	9
SSO Agent - SAML	13
Configure RSA Cloud Authentication Service	13
Configure Salesforce	16

Solution Summary

Use Case

When integrated Salesforce end users must authenticate with RSA SecurID Access to sign in. Salesforce can integrate using **SAML SSO Agent** or **Relying Party**. Salesforce does support JIT (just in time) user provisioning.

Integration Types

SSO Agent integrations use SAML 2.0 or HFED technologies to direct users' web browsers to RSA SecurID Access for authentication. SSO Agents also provide Single Sign-On to other applications using the RSA Application Portal.

Relying Party integrations use SAML 2.0 to direct users' web browsers to RSA SecurID Access for authentication.

Supported Features

This section shows all of the supported features by integration type and by RSA SecurID Access component. Use this information to determine which integration type and which RSA SecurID Access component your deployment will use. The next section in this guide contains the instruction steps for how to integrate RSA SecurID Access with Salesforce using each integration type.

Salesforce Integration with RSA Cloud Authentication Service

Authentication Methods	Authentication API	RADIUS	Relying Party	SSO Agent
RSA SecurID	-	-	✓	✓
LDAP Password	-	-	✓	✓
Authenticate Approve	-	-	✓	✓
Authenticate Tokencode	-	-	✓	✓
Device Biometrics	-	-	✓	✓
SMS Tokencode	-	-	✓	✓
Voice Tokencode	-	-	✓	✓
FIDO Token	n/a	n/a	✓	✓

Salesforce Integration with RSA Authentication Manager

Authentication Methods	Authentiacion API	RADIUS	Authentication Agent
RSA SecurID	-	-	-
On Demand Authentication	-	-	-
Risk-Based Authentication	n/a	-	-

- ✓ Supported
- Not supported
- n/t Not yet tested or documented, but may be possible.
- n/a Not applicable

Configuration Summary

This section contains links to the sections that contain instruction steps that show how to integrate Salesforce with RSA SecurID Access using all of the integration types.

This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components. All RSA SecurID Access and Salesforce components must be installed and working prior to the integration.

Links

[Relying Party](#)

[SSO Agent](#)

Known Issues

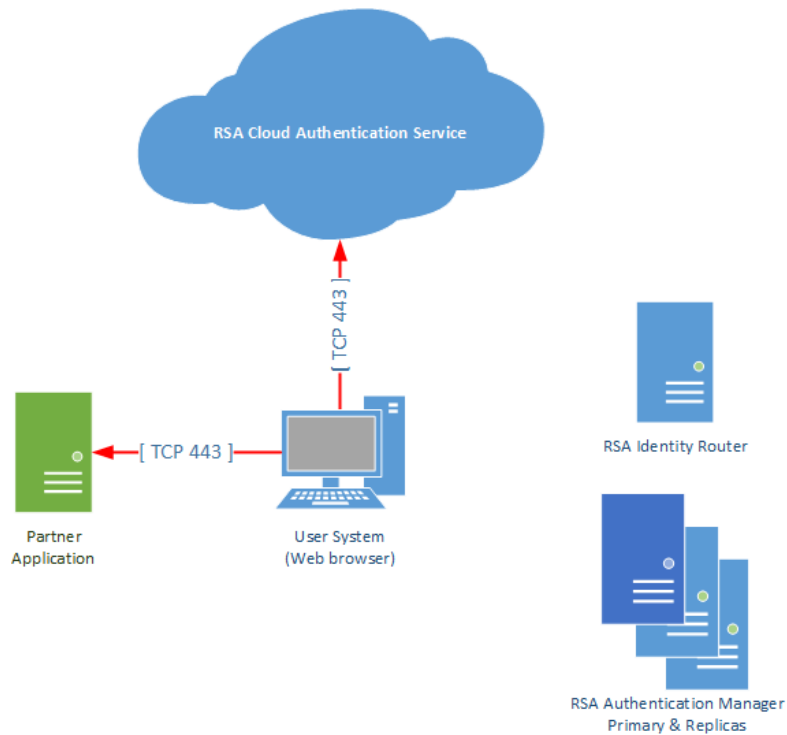
No known issues

Integration Configuration

Relying Party

This section describes on how to integrate RSA SecurID Access with Salesforce using Relying Party. Relying party uses SAML 2.0 to integrate RSA SecurID Access as a SAML Identity Provider (IdP) to Salesforce SAML Service Provider (SP).

Architecture Diagram

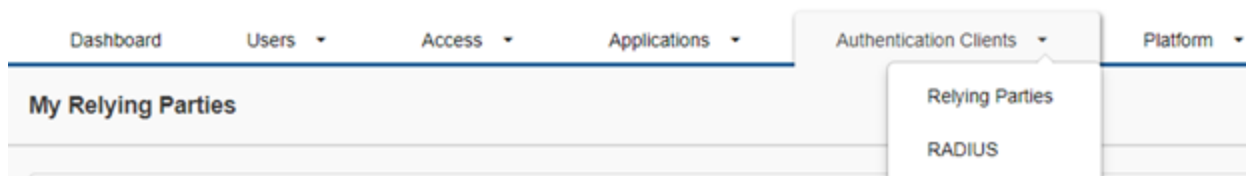


Configure RSA Cloud Authentication Service

Perform these steps to configure RSA Cloud Authentication Service as a Relying Party SAML IdP to Salesforce .

Procedure

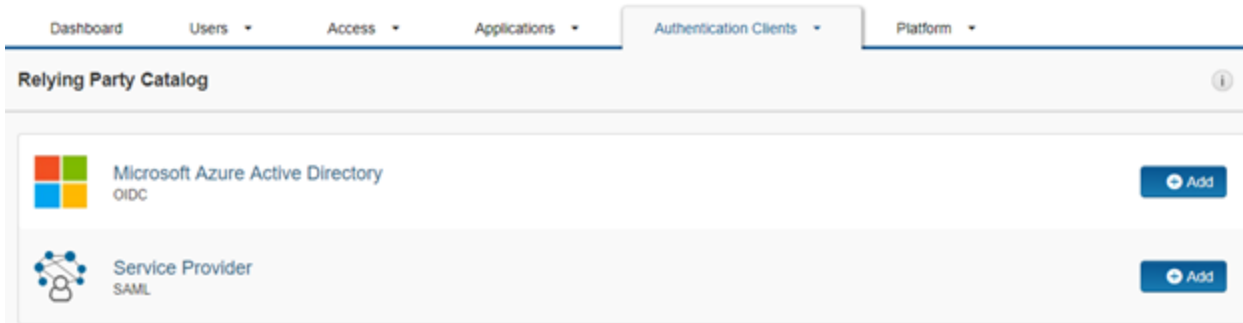
1. Sign into RSA Cloud Administration Console.
2. Select the **Authentication Clients > Relying Parties** menu item at the top of the page.



3. Click the **Add a Relying Party** button on the My Relying Parties page.



4. From the Relying Party Catalog select the **+Add** button for Service Provider SAML.



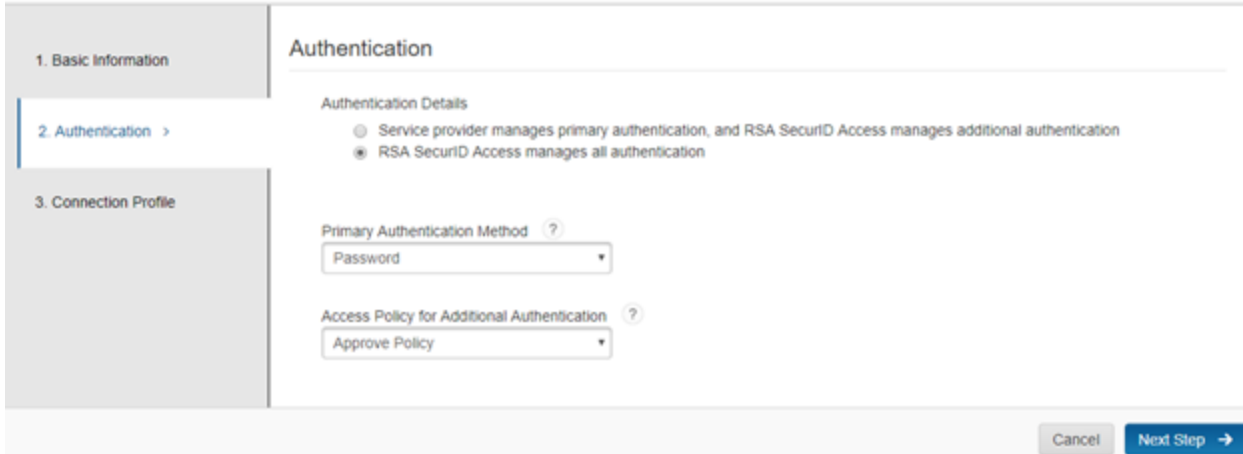
5. Enter a **name** for the Service Provider in the Name field on the Basic Information page.

6. Click the **Next Step** button.

7. On the Authentication page, select **RSA SecurID Access manages all authentication**.

8. From the Primary Authentication Method pulldown, select your desired login method either Password or SecurID.

9. From the Access Policy pulldown select a policy that was previously configured.



10. Select **Next Step**.


11. Select **Import Metadata**.

Connection Profile

Configure the relationship between RSA SecurID Access acting as the SAML identity provider (IdP), and the application acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP. You can edit these values if necessary. You can also manually add this information.

Data Input Method


Import Metadata Enter Manually

 No metadata loaded


Choose File

12. Select **Choose File** and select the file Salesforce metadata file you download from Salesforce.

Service Provider Metadata

Assertion Consumer Service (ACS) URL 

https://rsa-pe-dev-ed.my.salesforce.com?so=00DI0000000kq7D


Service Provider Entity ID (Audience) 

https://rsa-pe-dev-ed.my.salesforce.com


Metadata valid until: Tue Nov 02 2027 14:41:59 GMT-0400 (Eastern Daylight Time)

Message Protection


SP signs SAML requests.

 cert.pem

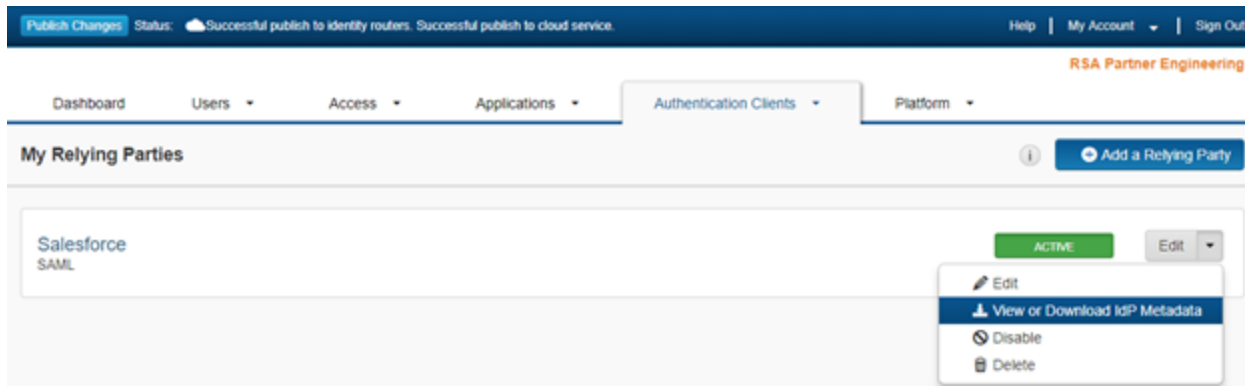
Certificate valid until: Wed Jul 25 2018 00:00:00 GMT-0400 (Eastern Daylight Time)

Choose File 

IdP signs SAML assertions.

Download Certificate 

13. Select **Save and Finish**.
14. On the My Relying Parties page, select the **Edit** pulldown and select **View or Download IdP Metadata**.
15. On the top menu click **Publish Changes**.

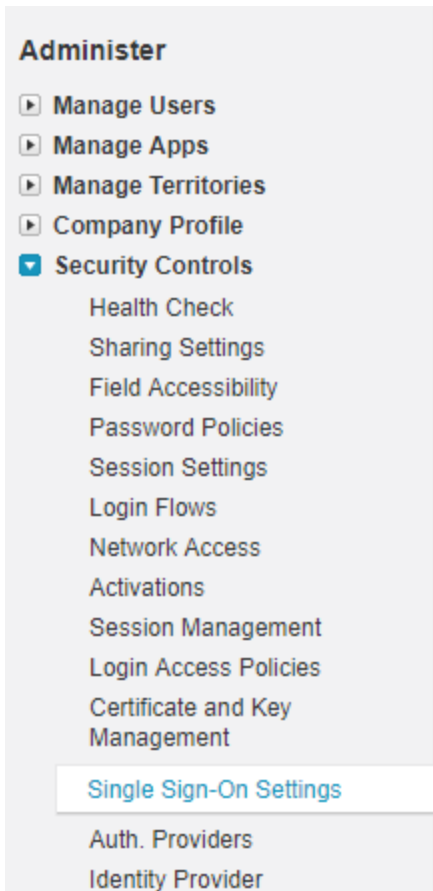


Configure Salesforce

Perform these steps to configure Salesforce as a Relying Party SAML SP to RSA Cloud Authentication Service.

Procedure

1. Login to Salesforce administration console. <https://login.salesforce.com>
2. From the Setup menu, select **Security Controls > Single Sign-On Settings**.



3. Under the **Federated authentication** bullet, click **Edit**.

4. Mark the **SAML Enabled** checkbox, and click **Save**.

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

[Edit](#) [SAML Assertion Validator](#)

Delegated Authentication

Delegated Gateway URL https://portal.example.com/DelegatedAuthenticationServlet?idp_id=1ucytg5ekdh72

Force Delegated Authentication Callout

Federated Single Sign-On Using SAML

SAML Enabled

SAML Single Sign-On Settings

[New](#) [New from Metadata File](#) [New from Metadata URL](#)

Action	Name	SAML Version	Issuer	Entity ID
--------	------	--------------	--------	-----------

5. In the SAML Single Sign-On Settings section, choose **New**, to configure the setting manually or New from Metadata file if you wish to configure from metadata file.

Note: Choose the IDR_metadata file when configuring for IDR integration or choose Cloud_metadata when configuring for a Cloud IdP integration.

6. If you selected to configure manually, click New and complete form.

SAML Single Sign-On Settings

The screenshot shows the 'SAML Single Sign-On Settings' configuration form. Key fields and values include:

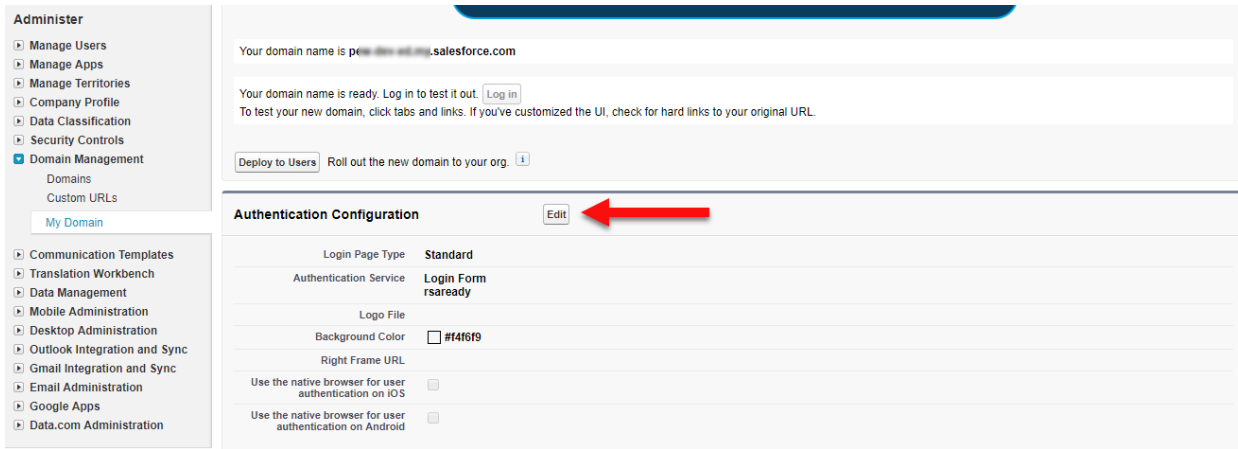
- Name: IDR_SS05
- SAML Version: 2.0
- Issuer: 16w5f6c1x35h
- Identity Provider Certificate: Choose File (No file chosen)
- Request Signing Certificate: SelfSignedCert_25Ju2017_173027
- Request Signature Method: RSA-SHA1
- Assertion Decryption Certificate: Assertion not encrypted
- SAML Identity Type: Assertion contains the User's Salesforce username (selected)
- SAML Identity Location: Identity is in the NameIdentifier element of the Subject statement (selected)
- Service Provider Initiated Request Binding: HTTP Redirect (selected)
- Identity Provider Login URL: https://portal.sso5.pe-lab.com/idpService?idp_id=16w5f6c1x35h
- Custom Logout URL: https://portal.sso5.pe-lab.com
- Custom Error URL: (empty)
- Single Logout Enabled: (checkbox checked)
- Just in time User Provisioning: User Provisioning Enabled (checkbox checked)

- In the Name field, enter a Name for this Authentication Service profile.
- Click in the API Name field, and Salesforce automatically enters the name from the Name field.
- In the Issuer field, enter the Identity Provider Entity ID for an IDR integration or `https://<rsa_tenant>.auth.securid.com/saml-fe/sso` for a Cloud IdP integration.
- In the Entity ID field, enter an ID that starts with `https://`, for example, `https://<instance>.my.salesforce.com`. This must match the Audience (Service Provider Entity ID) field on the RSA SecurID Access.
- In Identity Provider Certificate, click Browse and select RSA SecurID Access public certificate.
- In SAML Identity Type, select Assertion contains User's Salesforce.com username.
- In SAML Identity Location, select Identity is in the NameIdentifier element of the Subject statement.
- In Service Provider Initiated Request Binding, select HTTP Redirect for an IDR integration and HTTP POST for a Cloud IdP integration.
- Click **Save**.

Endpoints	
View SAML endpoints for your organization, communities, or custom domains.	
Your Organization	
Login URL	https://rsa-pe-dev-ed.my.salesforce.com/?p=00000000000000000000000000000000
Logout URL	https://rsa-pe-dev-ed.my.salesforce.com/services/auth/tp/saml2/logout
OAuth 2.0 Token Endpoint	https://rsa-pe-dev-ed.my.salesforce.com/services/oauth2/token?p=00000000000000000000000000000000
▶ For Communities	
<div style="text-align: right;"> Edit Delete Clone Download Metadata SAML Assertion Validator </div>	

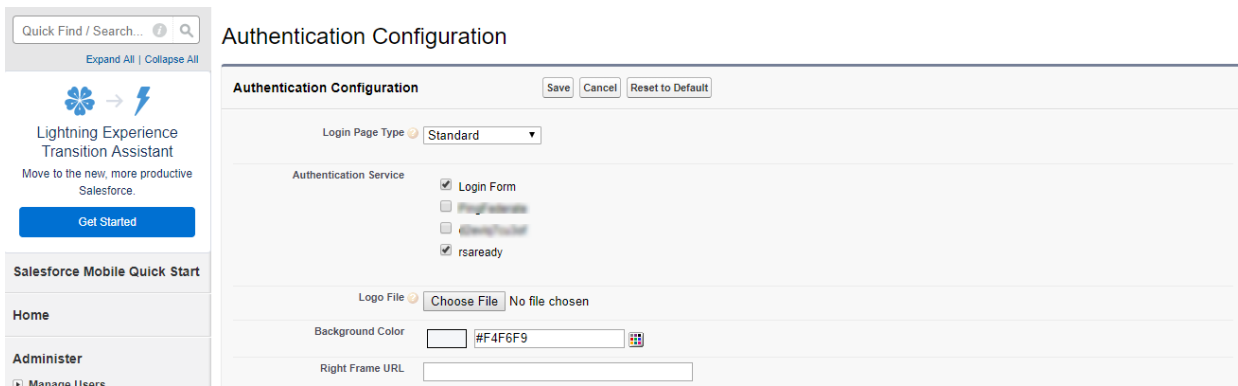
Note: If your environment requires SP signing select the Download Metadata button and return to the RSA console and edit the connector to import the metadata file which will import the certificate.

7. Browse to **Administer > Domain Management > My Domain** and click **Edit**.



8. Mark the check box next to the **Authentication Service** which corresponds to your RSA SecurID Access configuration and click **Save**.

Note: Unmark the checkboxes for Logon Form and other services to prevent side door access.



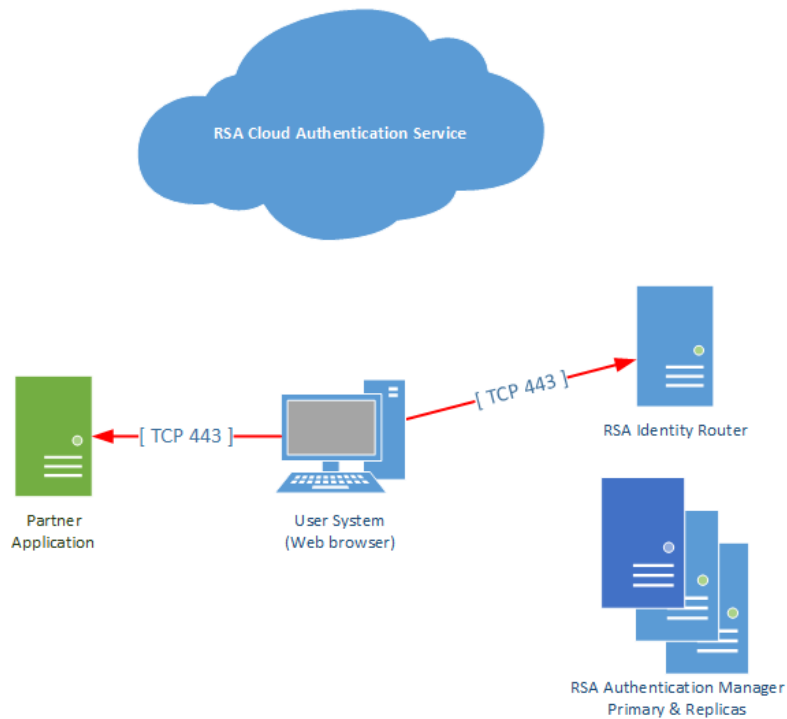
Configuration is complete.

Return to the [main page](#) for more certification related information.

SSO Agent - SAML

This section describes how to integrate RSA SecurID Access with Salesforce using a SAML SSO Agent.

Architecture Diagram

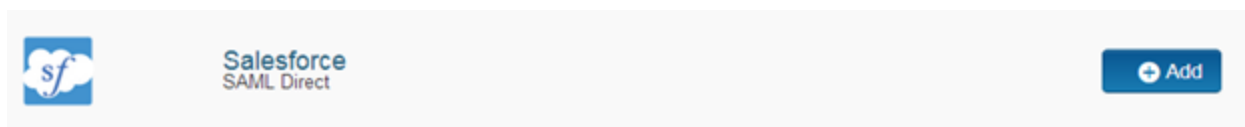


Configure RSA Cloud Authentication Service

Perform these steps to configure RSA Cloud Authentication Service as an SSO Agent SAML IdP to Salesforce .

Procedure

1. Sign into RSA Cloud Administration Console and browse to **Applications > Application Catalog**, search for **Salesforce** and click **+Add** to add the connector.



2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to **Initiate SAML Workflow** section.
 - a. In the Connection URL field, verify the default setting.
 - b. Choose **IDP-initiated**.

Note: The following IDP-initiated configuration works for SP-initiated Salesforce connections as well.

Connection Profile

Configure the relationship between the identity router, acting as the SAML identity provider (IdP), and the application, acting as the SAML service provider (SP). You can upload a SAML metadata file to automatically configure the SP options. You can edit these values if necessary.

No metadata loaded

Import Metadata



Initiate SAML Workflow

Connection URL

home%2Fhome.jsp

IDP-initiated

SP-initiated

4. Scroll down to SAML Identity Provider (Issuer) section.

SAML Identity Provider (Issuer)

Identity Provider URL

https://portal.sso5.pe-lab.com/IdPServlet?idp_id=16wt8gc1x39h

Issuer Entity ID

Default (idp_id): 16wt8gc1x39h

Override

SAML Response Signature

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

private.key

Choose File

Generate Cert Bundle



cert.pem

Choose File

Certificate valid until: Mon
Aug 16 06:45:13 UTC 2021

Include Certificate in Outgoing Assertion

a. Take note of the **Identity Provider URL**.

- b. Take note of the **Issuer Entity ID**.
 - c. Select Choose File and upload the private key.
 - d. Select Choose File to import the public signing certificate.
 - e. Select the checkbox for **Include Certificate in Outgoing Assertion**.
5. Scroll down to the **Service Provider** section.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<DOMAIN>.my.salesforce.com?so=<organizationID>

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.my.salesforce.com

6. In the Assertion Consumer Service (ACS) URL field replace <DOMAIN> with your account domain or if in a developer environment replace with <DOMAIN>-dev-ed.

Note: The string following so= is the Salesforce Organization ID; which can be found on your Salesforce Administrator > Company Profile > Company Information page.

7. In the Audience (Service Provider Issuer ID) field replace <DOMAIN> with your account domain or if in a developer environment replace with <DOMAIN>-dev-ed.

8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.

User Identity ?

NameID

Identifier Type: Email Address

Identity Source: AD20

Property ?: mail

Attribute Hunting ? NameID Attribute Hunting

- 9. Click **Next Step**.
- 10. On the User Access page, select Allow All Authenticated Users user policy from the available options.

Access Policy

Select the access policy to determine which users are allowed to access the application.

- Allow All Authenticated Users
- Select Custom Policy ?

No Access Allowed ▼

11. Click **Next Step**.
12. On the Portal Display page, select **Display in Portal**.
13. Click **Save and Finish**.
14. Click **Publish Changes**. Your application is now enabled for SSO.



15. Navigate to **Applications > My Applications**.
16. Locate Salesforce in the list and from the **Edit** option, select **Export Metadata**.

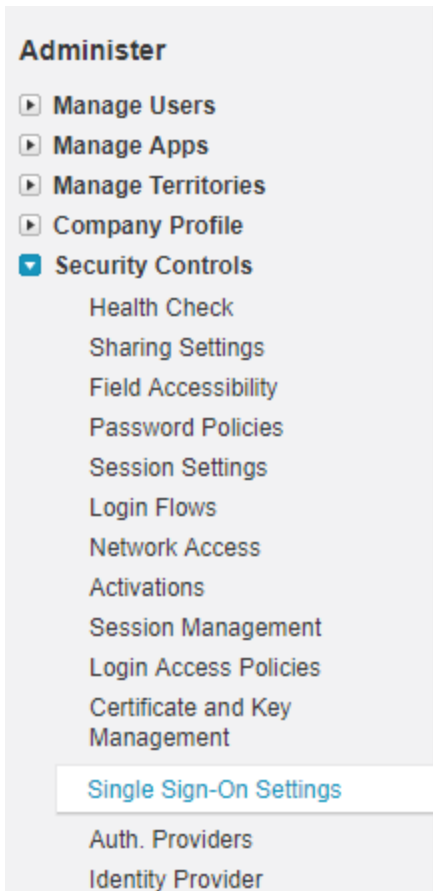


Configure Salesforce

Perform these steps to configure Salesforce as an SSO Agent SAML SP to RSA Cloud Authentication Service.

Procedure

1. Login to Salesforce administration console. <https://login.salesforce.com>
2. From the Setup menu, select **Security Controls > Single Sign-On Settings**.



3. Under the **Federated authentication** bullet, click **Edit**.

4. Mark the **SAML Enabled** checkbox, and click **Save**.

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.

[Edit](#) [SAML Assertion Validator](#)

Delegated Authentication

Delegated Gateway URL https://portal.example.com/DelegatedAuthenticationServlet?idp_id=1ucytg5ekdh72

Force Delegated Authentication Callout

Federated Single Sign-On Using SAML

SAML Enabled

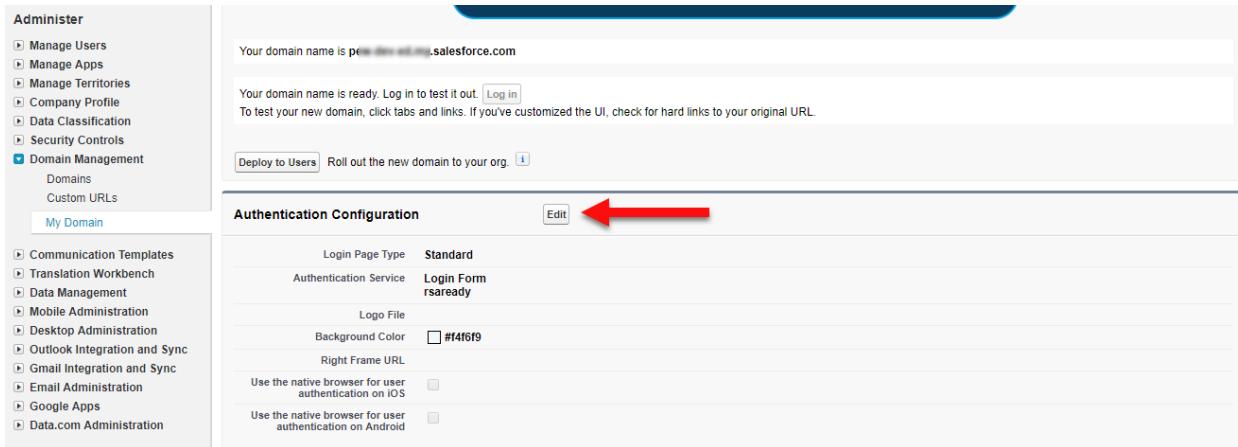
SAML Single Sign-On Settings

[New](#) [New from Metadata File](#) [New from Metadata URL](#)

Action	Name	SAML Version	Issuer	Entity ID
--------	------	--------------	--------	-----------

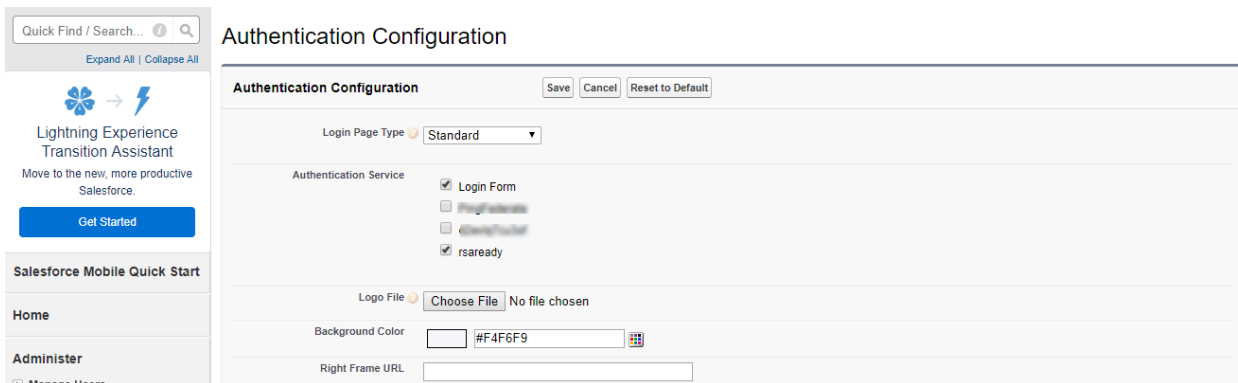
Note: If your environment requires SP signing select the Download Metadata button and return to the RSA console and edit the connector to import the metadata file which will import the certificate.

7. Browse to **Administer > Domain Management > My Domain** and click **Edit**.



8. Mark the check box next to the **Authentication Service** which corresponds to your RSA SecurID Access configuration and click **Save**.

Note: Unmark the checkboxes for Logon Form and other services to prevent side door access.



Configuration is complete.

Return to the [main page](#) for more certification related information.