

RSA SecurID Access SAML Configuration for Tableau Online



Last Modified: January 20, 2016

Tableau helps people see and understand data. Tableau offers five main products: Tableau Desktop, Tableau Server, Tableau Online, Tableau Reader and Tableau Public.

The following procedure outlines the steps needed to configure Tableau Online for single sign on.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Tableau.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

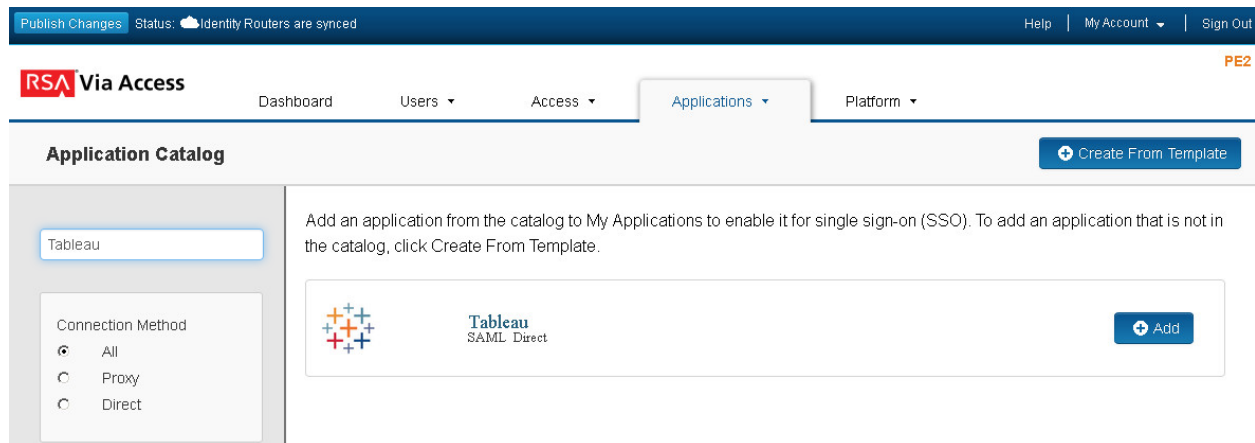
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Tableau to Use RSA SecurID Access as an Identity Provider](#)

Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.



3. On the Basic Information page, specify the application name and click **Next Step**.

 **Note:** The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.

4. Click on **Import Metadata** and select the file you downloaded from Tableau. See step 5 page 8.

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

5. Click **Save** to accept the settings from the metadata file.
6. On the Connection Profile page, choose **IDP –initiated** and leave the URL blank.

Connection URL

http://www.example.com


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

Choose File

Generate Certificate Bundle

7. Scroll down to the **SAML Identity Provider (Issuer)** section.

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): ttestOLD2

Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

Private Key Loaded

Certificate Loaded

CN=salesforce_saml, Valid
Until: 08/05/2017

Include Certificate in Outgoing Assertion

- a. Select **Choose File** and upload the RSA SecurID Access private key.
- b. Select **Choose File** and upload the RSA SecurID Access public certificate.

8. Scroll down to the Service Provider section.

Service Provider

Assertion Consumer Service (ACS) URL

Audience (Service Provider Entity ID)

- a. If you imported the metadata file the **Assertion Consumer Service (ACS) URL** will be autocompleted for you. Example:
<https://sso.online.tableau.com/public/sp/SSO?alias=eca70862-30c0-4f77-bab9-07970dd3c0a2>
- b. If you imported the metadata file the **Audience (Service Provider Entity ID)** will be autocompleted for you. Example:
<https://sso.online.tableau.com/public/sp/SSO?alias=eca70862-30c0-4f77-bab9-07970dd3c0a2>

9. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email** and **Property** to **mail**.

User Identity

Name ID

Identifier Type User Store Property

[Show Advanced Configuration](#)

10. Click **Show Advanced Configuration** and scroll down to **Attribute Extension**.

11. Add Attributes **email**, **FirstName**, and **LastName**.

Attribute Extension

Attribute Source	Attribute Name	User Store	Property	Manage
<input type="text" value="User Store"/>	<input type="text" value="email"/>	<input type="text" value="nga2012"/>	<input type="text" value="mail"/>	
<input type="text" value="User Store"/>	<input type="text" value="FirstName"/>	<input type="text" value="nga2012"/>	<input type="text" value="givenName"/>	
<input type="text" value="User Store"/>	<input type="text" value="LastName"/>	<input type="text" value="nga2012"/>	<input type="text" value="sn"/>	
+ ADD				

12. Scroll down to **Uncommon Formatting SAML Response Options**.
13. Under Sign Outgoing Assertion, select **Assertion within response**.

 **Note:** If you used the Import metadata option the Encrypt Assertion maybe checked. If your account was not configured for this, login will fail. Uncheck this feature and try again.

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response Assertion within response

Signature Algorithm

Digest Algorithm

Encrypt Assertion

 No certificate loaded

Encryption Algorithm

Encryption Key Transport

Relay State URL Encoding

Receive Relay State URL - encoded by SP (in incoming request)

Send Relay State URL - encoded by IDP

Include Issuer NameID Format

NameID Format

14. Click **Next Step**.

15. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

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

Allow All Authenticated Users

Select Custom Policy ?

No Access Allowed

Cancel

Next Step →


16. Click **Next Step**.

17. On the **Portal Display** page, select **Display in Portal**.

18. Click **Save and Finish**.

19. Click **Publish Changes**. Your application is now enabled for SSO.

Publish Changes

Status:  Changes Pending

Next Steps

[Configure Tableau to Use RSA SecurID Access as an Identity Provider](#)

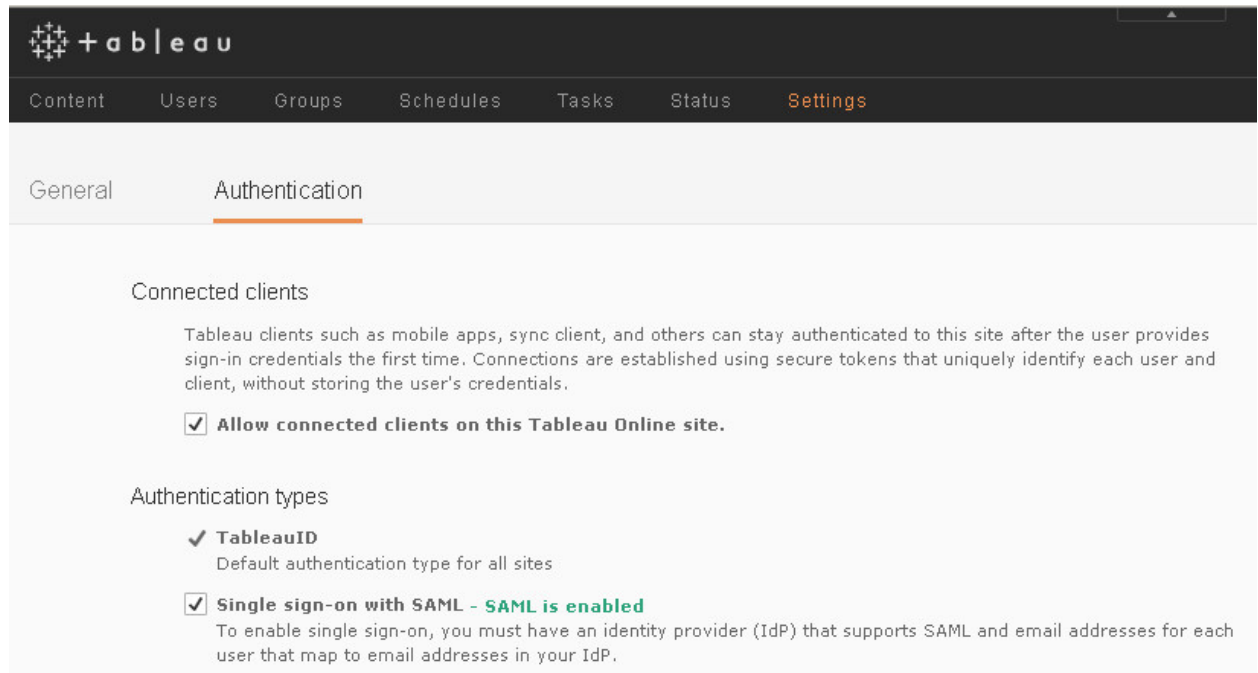
Configure Tableau to Use RSA SecurID Access as an Identity Provider

Procedure

1. Obtain the RSA SecurID Access IDP metadata file which is needed to configure Tableau. The metadata file can be obtained by either exporting the file from the RSA SecurID Access console or manually creating the file (see page 9).
 - a. Login to the RSA SecurID Access console, select **Applications > My Applications**.
 - b. Select the **Edit** pull down for the Tableau application and choose **Export Metadata**.
 - c. Save the file to be used in configuring Tableau. See step 6 on page 8.



2. Sign in to Tableau Online with an administrator account.
3. Select **Settings > Authentication**.



4. Check the **Single sign-on with SAML** box.

5. Click **Export metadata** to download the service provider metadata file, which will be used to configure the RSA SecurID Access in step 4 on page 2.

Follow the steps below to use SAML for single sign-on.

1 Export metadata file from Tableau Online

Select an option for obtaining metadata required by the IdP.

- Save a single XML file that contains all required metadata.

or

- Copy the Tableau Online entity ID and ACS URL individually, and download the X.509 certificate to a CER file.

Tableau Online entity ID

Assertion Consumer Service URL (ACS)

6. Click **Browse** and select the RSA SecurID Access IDP metadata file to import into Tableau Online.
7. Click **Apply** and the IDP Entity ID and SSO Service URL will be automatically filled in.

4 Import metadata file into Tableau Online

Identity provider (IdP) metadata file

IdP Entity ID

SSO Service URL

IdP is configured to support SAML single logout (SLO)

8. Select the **Test Login**. If the connection fails uncheck the Encryption Assertion option in step 13 on page 5 and retry.
9. Select **Add Users** and enter the single sign on user's email address.

6 Select Users

Specify which users can sign in with SAML

[View Users](#) - select users from your Tableau Online user list

[Add Users](#) - type email addresses of new users

Manually Creating the RSA SecurID Access Metadata file

1. Modify the example below with your environment information.
2. When inserting the cert.pem file do not include the -----BEGIN and -----END CERTIFICATE----- lines.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<EntityDescriptor xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="CHANGE_ME_TO_ENTITY_ID">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <!-- public saml cert -->
        <ds:X509Certificate>CHANGE_ME_TO_PUBLIC_SAML_CERT_CONTENT</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>

    <!-- Supported Name Identifier Formats -->
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</NameIDFormat>

    <!-- POST binding and location=idp url -->
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="CHANGE_ME_TO_IDP_URL"/>

    <!-- Extended Attributes -->
    <Attribute
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      account="telephoneNumber">
    </Attribute>

  </IDPSSODescriptor>
</EntityDescriptor>
```