RSA SECURID® ACCESS
Implementation Guide

Workday

Gina Salvalzo, RSA Partner Engineering
Last Modified: September 10, 2017

Solution Summary

This solution extends the strong authentication and identity assurance of the RSA SecurID Access platform to Workday customers using RSA Cloud Authentication Service as the identity provider.

SAML 2.0 integrations have two specific use cases:

1. When integrated with Identity Router (IdP), RSA provides single sign-on authentication and multi-factor authentication to Workday via SP or IDP initiated login.

2. When integrated with Cloud IdP/ Relying Party, RSA provides both the primary authentication and the multi-factor authentication to protect the Workday login page.

RSA SecurID Access Features	
Workday	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

Configuration Summary

All of the supported use cases of RSA SecurID Access with Workday require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Workday can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

Cloud Authentication Service – Identity Router IdP Configuration
Workday SAML Configuration

SAML via RSA Cloud (IdP)

Cloud Authentication Service – Cloud IdP Configuration

Workday SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Workday in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

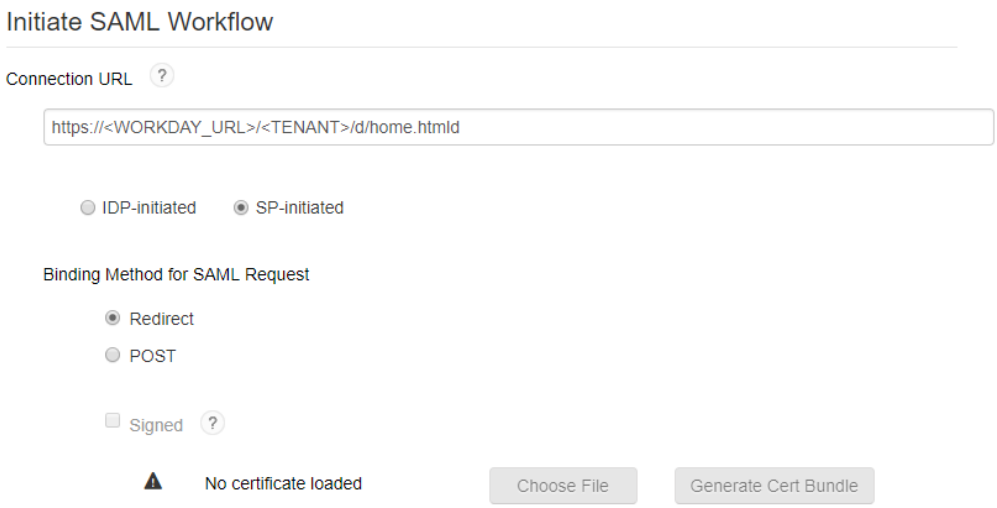
Configure RSA Identity Router SAML IdP

Procedure

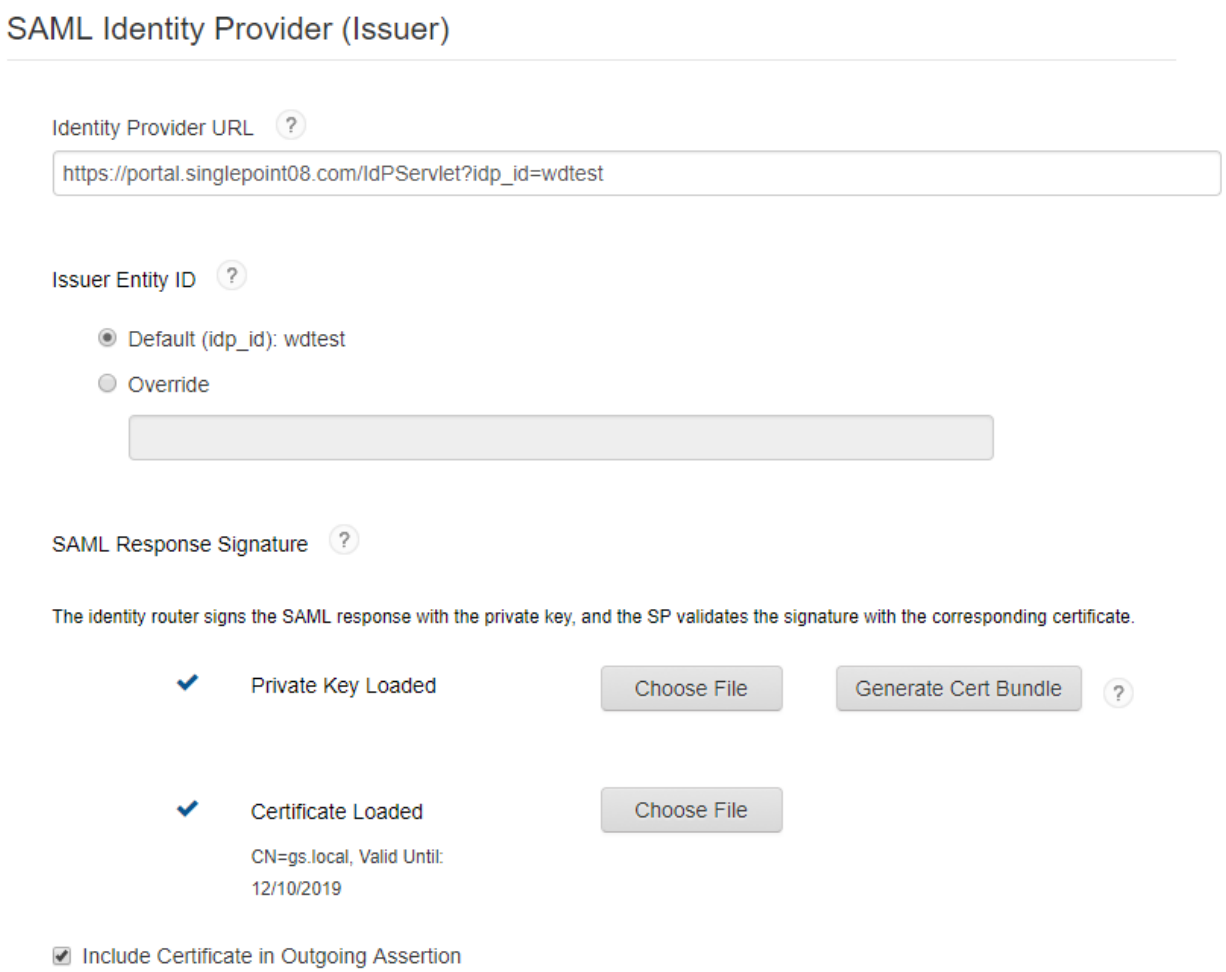
1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for Workday and click **+Add** to add the connector.

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, replace **<WORKDAY_URL>/<TENANT>** with your Workday URL and tenant name.
   Such as: *https://www.myworkday.com/dell3*
   https://impl.workday.com/dell3

   b. Choose the correct workflow for your environment. If the session begins at the Workday login page select **SP-initiated**. If the session begins at the RSA portal select **IDP-initiated**.



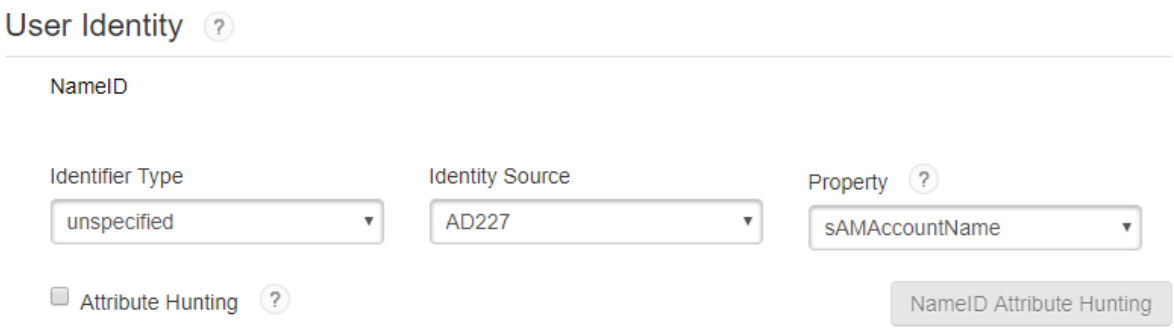
4. Scroll down to SAML Identity Provider (Issuer) section.



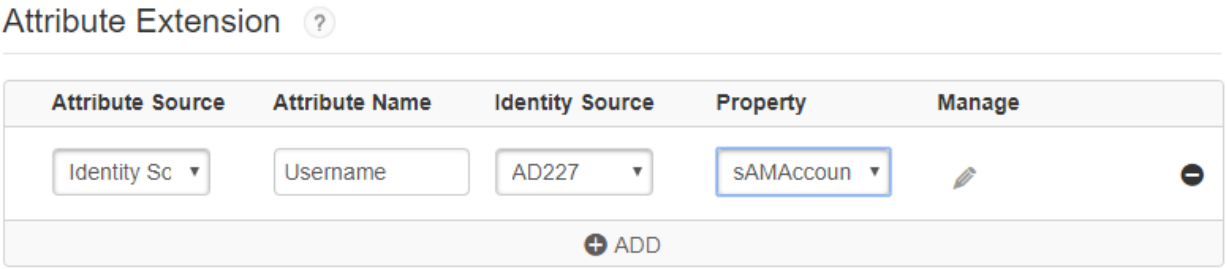
a. Take note of the Identity Provider URL.
b. Take note of the Issuer Entity ID.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for Include Certificate in Outgoing Assertion.

5. Scroll down to the **Service Provider** section.

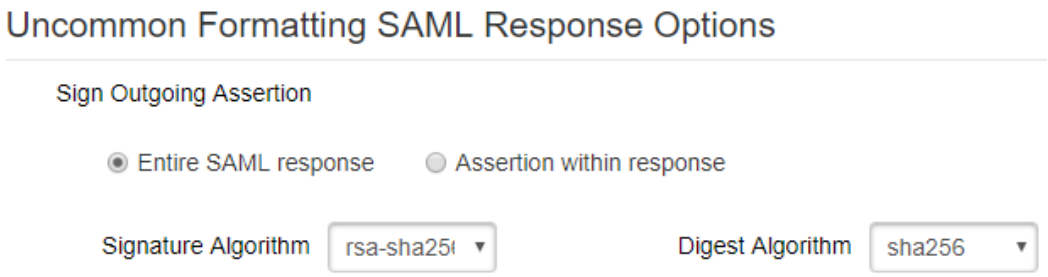
6. In the **Assertion Consumer Service (ACS) URL** field replace <**WORKDAY_URL>/<TENANT>** with your tenant name. Such as: *https://impl.workday.com/dell3/login-saml.htmld*
7. In the **Audience (Service Provider Issuer ID)** field replace <TENANT>. Such as: *http://www.workday.com/dell3*
8. Set the Identifier Type to **unspecified** and Property to **sAMAccountName** when using an identity source types of Active Directory or **uid** when using an identity source types of LDAP.



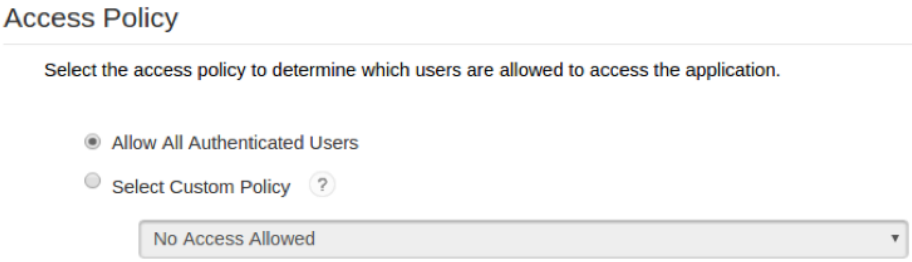
9. Select **Show Advanced Configuration**.
10. In the Attribute Extension section, add attribute **Username** and use the Property pulldown to select **sAMAccountName** when using an identity source types of Active Directory or **uid** when using an identity source types of LDAP.



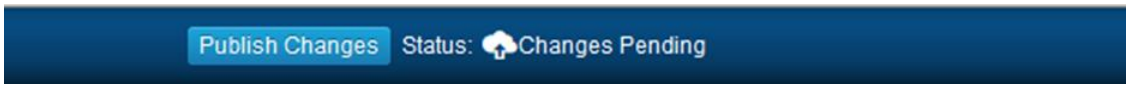
11. Under the section Uncommon Formatting SAML Response Options, use the pulldown to select **rsa-sha256** for Signature Algorithm and **sha256** for Digest Algorithm.



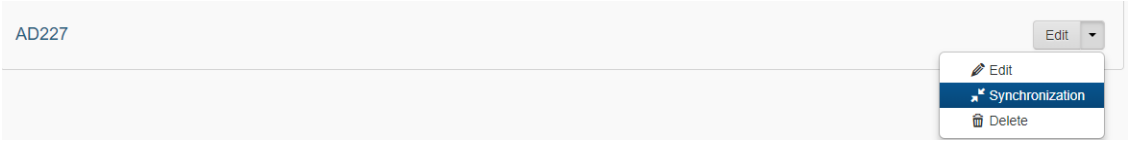
12. Click **Next Step**.
13. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.



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



18. From the **Users > Identity Sources** page, select the **Edit** pulldown for each Identity Source used in the policy and select **Synchronization**.



19. Click **Synchronize Now**.

Next Steps

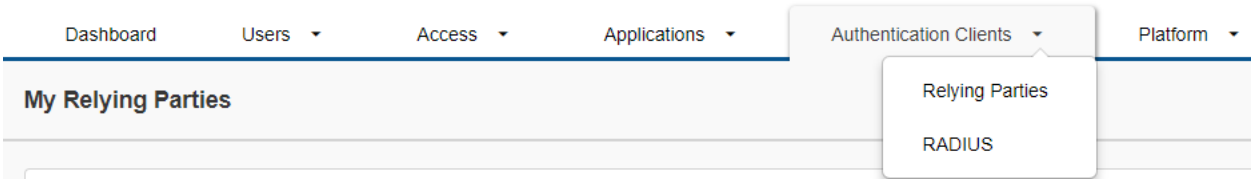
Refer to the **Workday SAML Configuration** section for instructions on how to configure the service provider for SAML SSO.

SAML via RSA Cloud (IdP)

To configure a SAML Service Provider in RSA Cloud IdP, you must add a Service Provider in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

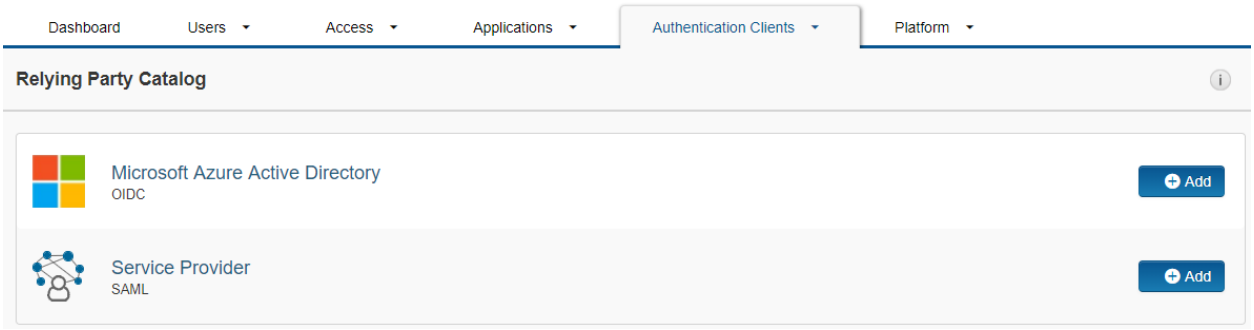
Procedure

1. Log in to the RSA SecurID Access Administration Console.
2. Select the **Authentication Clients > Relying Parties** menu item at the top of the page.



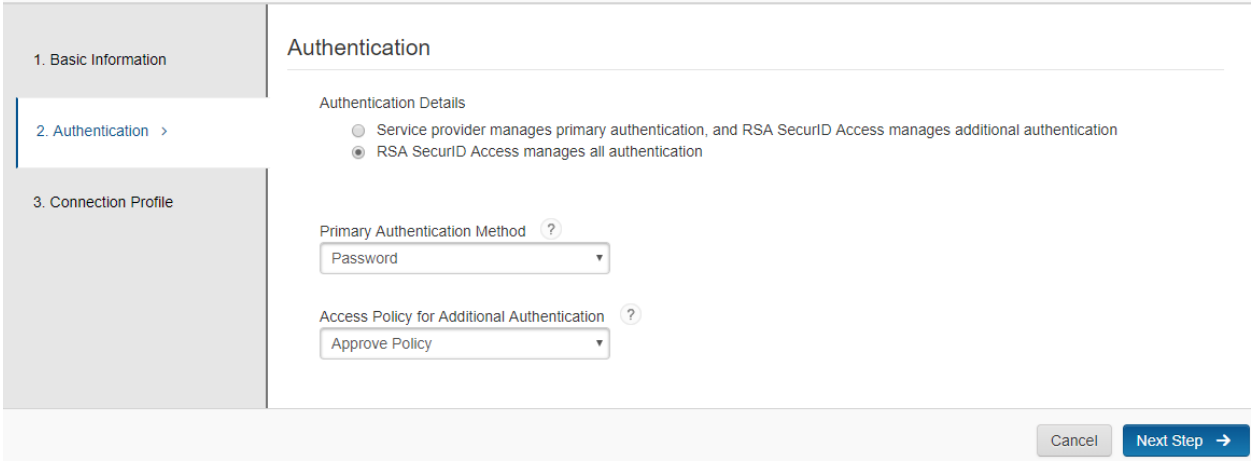
3. Click the **Add a Relying Party** button on the My Relying Parties page.

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

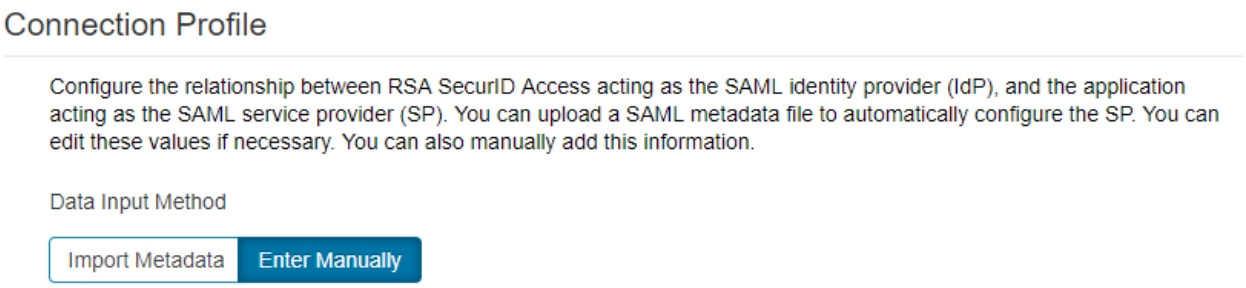


5. Enter a name for the Service Provider in the **Name** field on the Basic Information page.
6. Click the **Next Step** button.

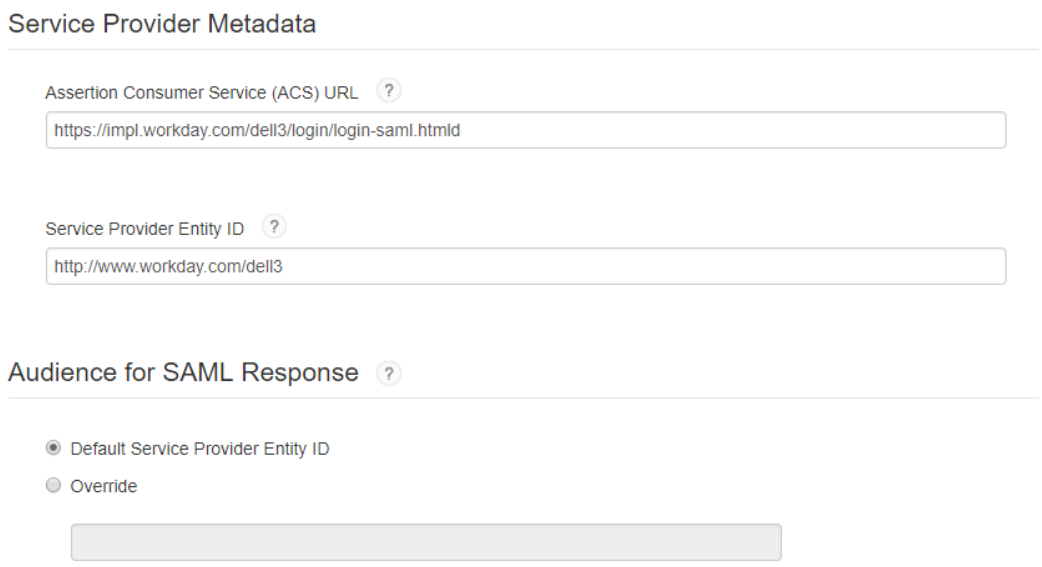
7. On the Authentication page, select **RSA SecurID Access manages all authentication**.
8. From the Primary Authentication Method pulldown, select your desired login method either Password or SecurID.
9. From the Access Policy pulldown select a policy that was previously configured.



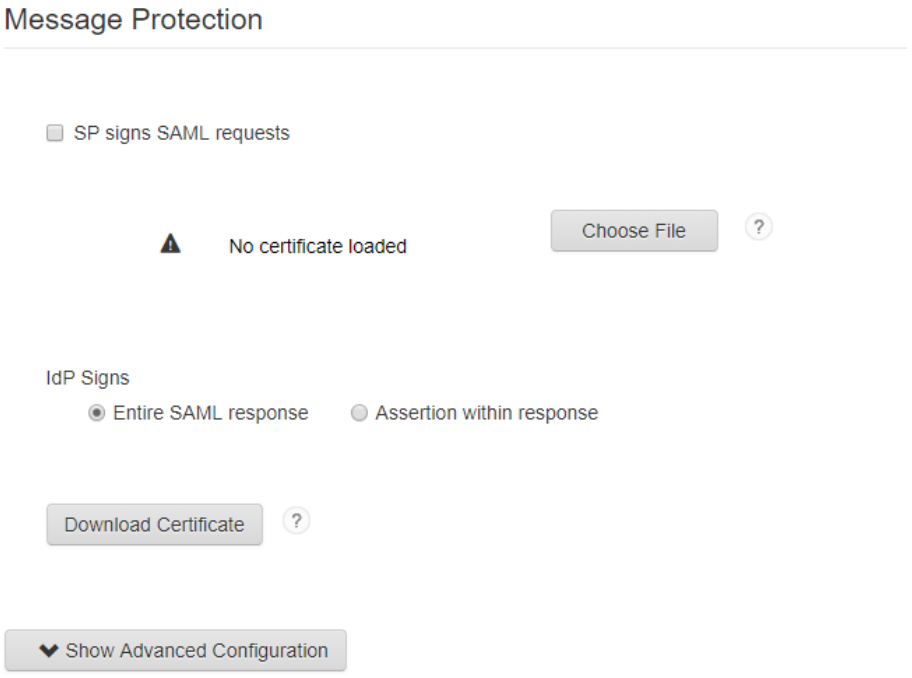
10. Select **Next Step**.
11. Select **Enter Manually**.



12. Enter the **Assertion Consumer Service (ACS) URL** in format:
    https://<WORKDAY_URL>/<TENANT>/login-saml.htmld
    Such as: *htt*ps://impl.workday.com/dell3/login-saml.htmld
13. Enter **Service Provider Entity ID** in format: *http://www.workday.com/<TENANT>*
    Such as: http://www.workday.com/dell3

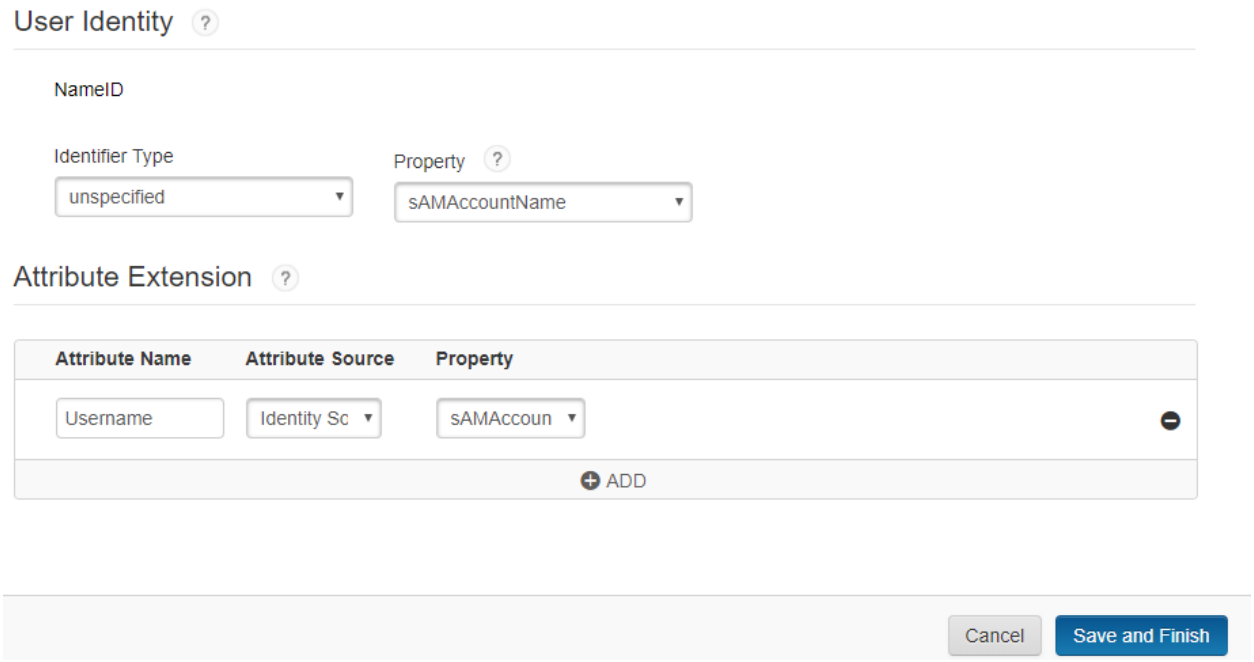


14. In the Message Protection section, for IdP Signs select **Entire SAML response**.
15. Click **Download Certificate**.



16. Next, click **Show Advanced Configuration**.

17. In the NameID field use the Identifier Type pulldown to select **unspecified** and Property to **sAMAccountName** when using an identity source types of Active Directory or **uid** when using an identity source types of LDAP.
18. Under Attribute Extension add **Username** with Property set to **sAMAccountName** when using an identity source types of Active Directory or **uid** when using an identity source types of LDAP.

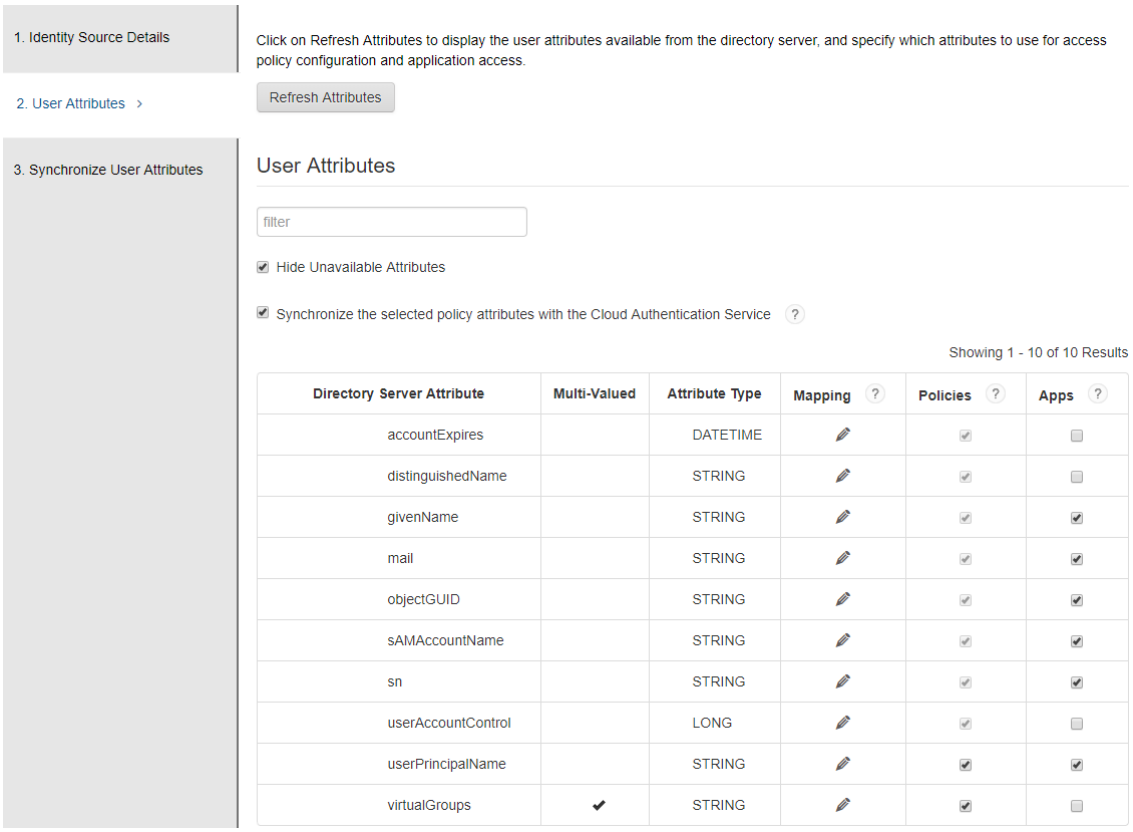


19. Select **Save and Finish**.
20. On the My Relying Parties page, select the **Edit** pulldown and select **View or Download IdP Metadata**.
21. View the metadata file to find the Cloud IdP URL.
    Location=https://<company_id>.auth.securid.com/saml-fe/sso.

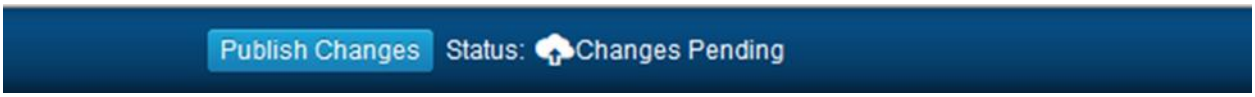
22. Navigate to **Users > Identity Sources**.

> **Note: Perform the following steps to all Identity Sources used in the policy.**

23. Select **Edit** for the Identity Source used in the **Policy**.
24. On the User Attributes page, verify that the **Synchronize the selected policy attributes with the Cloud Authentication Service** is checked.
25. In the Policies column verify that attribute **sAMAccountName** or **uid** is checked.



26. Click **Next Step**.
27. Click **Save and Finish**.
28. On the top menu click **Publish Changes**.



Next Steps

Refer to the **Workday SAML Configuration** section for instructions on how to configure the service provider for SAML SSO.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring Workday with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

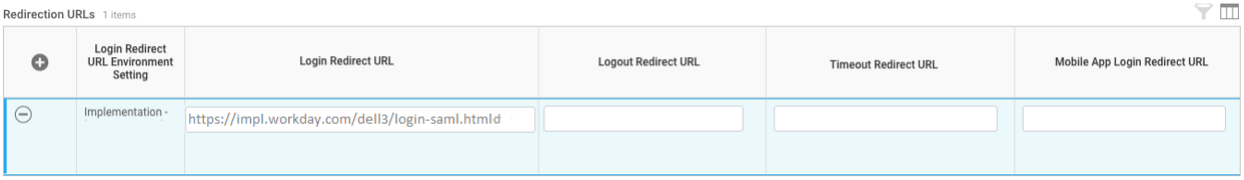
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Workday components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

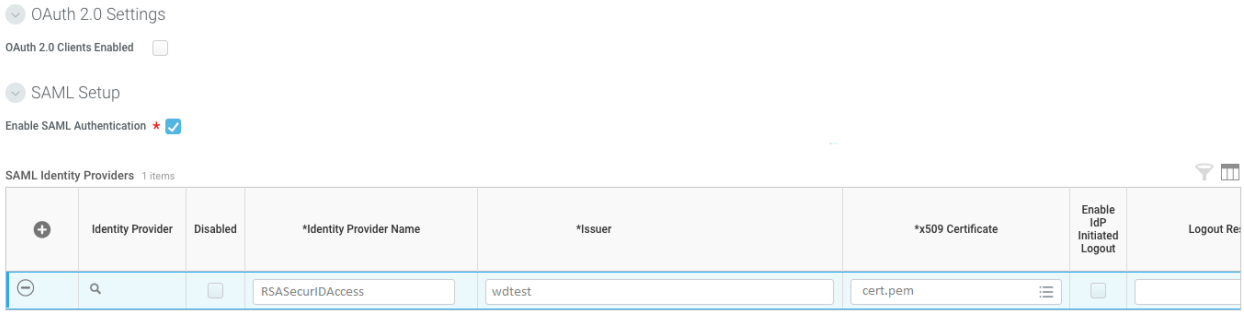
Workday SAML Configuration

Procedure

1. Log into your Workday tenant with an Administrator account.
2. On the Workday admin dashboard, navigate to **Account Administration** > **Edit Tenant Setup – Security**.
3. Click the **+** icon under Redirection URLs to add a row.
4. In the Redirect URLs section, enter the Login Redirect URL for your tenant. This should match the **ACS URL** in the RSA configuration.

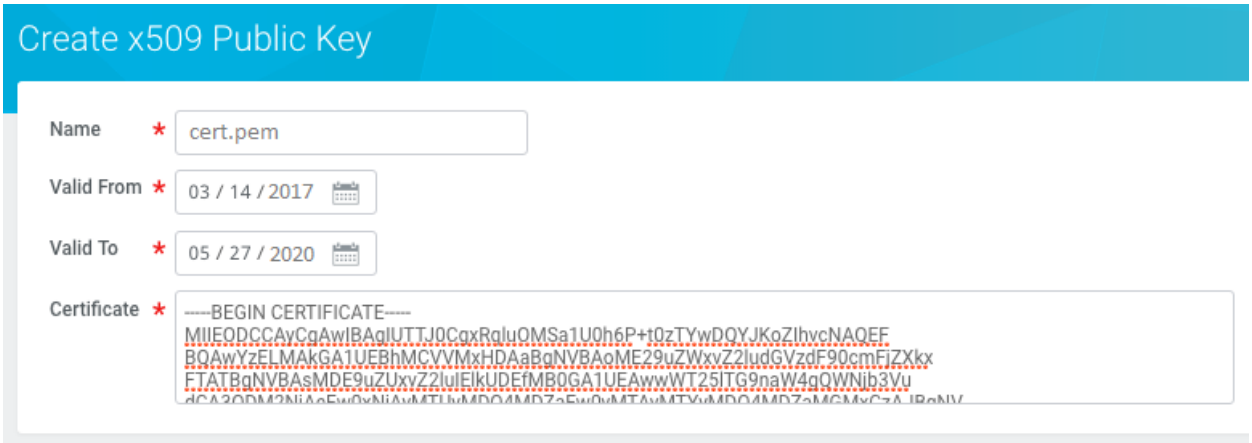


5. Under SAML Setup section, select the check box **Enable SAML Authentication**.
6. Click the **+** icon under SAML Identity Providers.

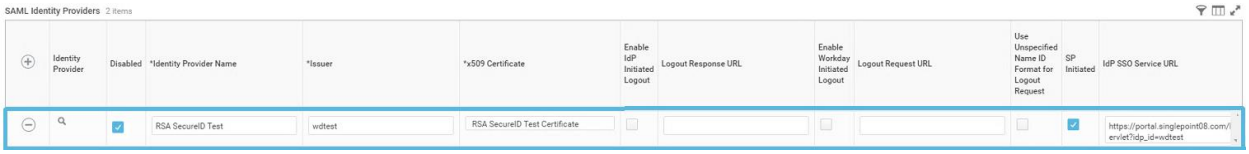


7. In the Identity Provider Name field, enter a descriptive name such as RSASecurIDAccess.
8. In the Issuer field, enter **Issuer Entity ID** when configuring for IDR IdP or enter the **Cloud IdP URL** when configuring for Relying Party.

9. In the X509 Certificate field select the menu icon, and select **Create X509 Public Key** from the pulldown list.
10. Enter a **Name** for the certificate.
11. Enter a **Valid From** and **Valid To** date.
12. Copy and paste the RSA public certificate into the Certificate field. When configuring for IDR IdP use the **public certificate** . When configuring for Cloud IdP/Relying Party use the **Cloud IdP certificate**.

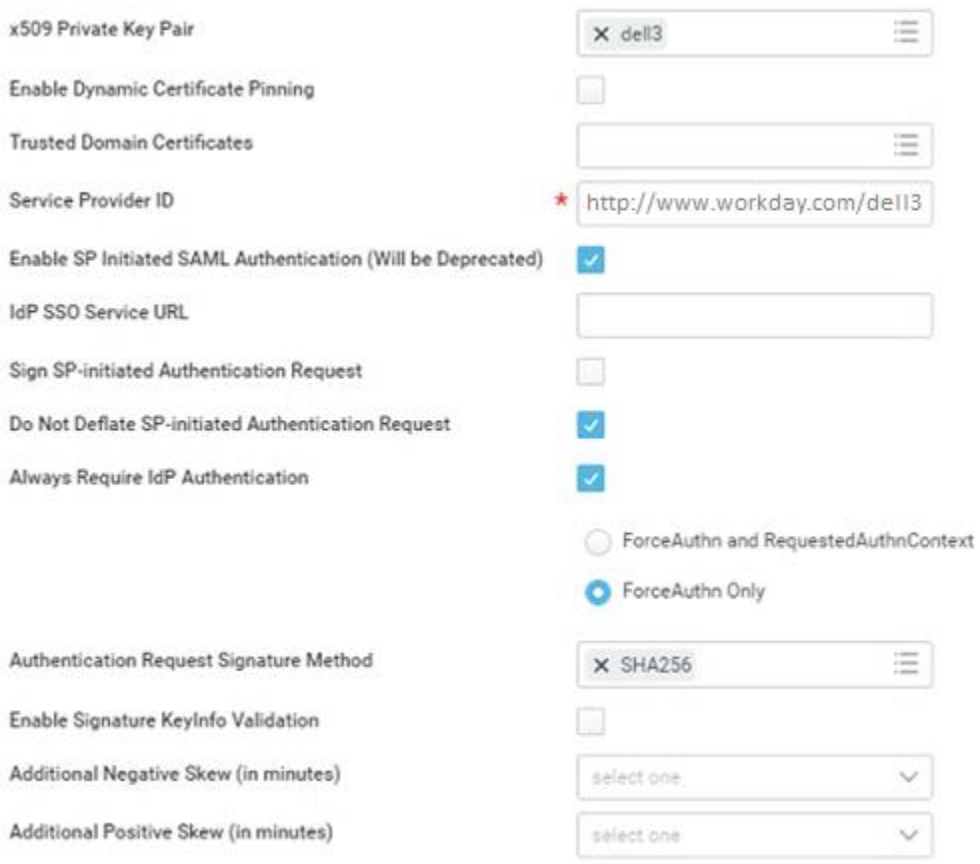


13. Click **OK**.
14. Use the scroll bar to continue filling out the SAML Identity Providers fields.
15. In the **IdP SSO Service URL**, enter the **Identity Provider URL** when configuring for IDR IdP or enter the **Cloud IdP URL** when configuring for Cloud IdP/Relying Party.
16. Click in the **Used for Environments** field and select the environments you would like to use single sign on in.



17. Click **OK**.

18. Next, complete the fields that follow below the SAML Identity Providers table.
19. Enter a unique value for the **Service Provider ID**.
20. Check the **Enable SP Initiated SAML Authentication** box.
21. Check the **Do not Deflate SP-initiated Authentication Request** box.
22. Check the **Always Require IdP Authentication**.
23. Select **ForceAuthn Only**.



24. Click **Save**.