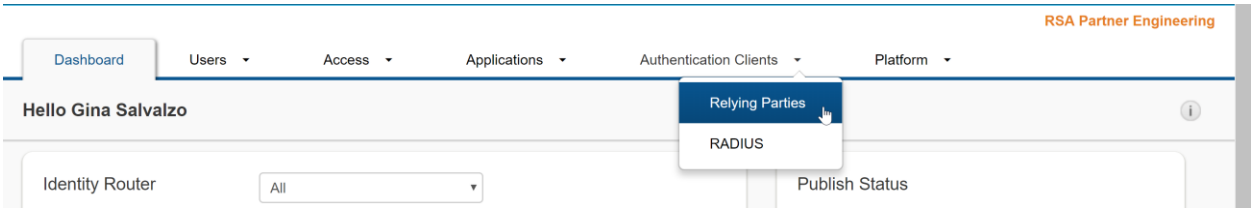
RSA SecurID Access Free Trial Workday Guide

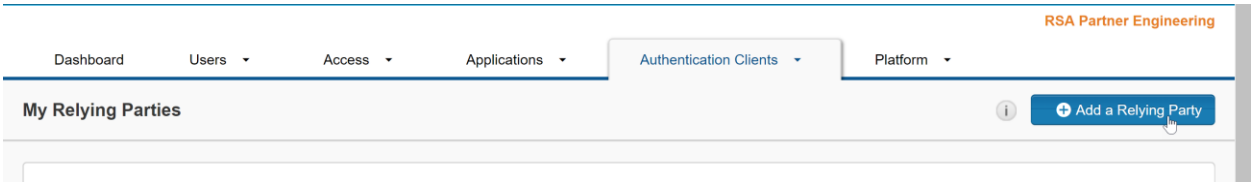
This guide describes how to set up Workday as part of the RSA SecurID Access Free Trial program. Use this guide in conjunction with the RSA SecurID Access Free Trial Quick Setup Guide.

Complete RSA SecurID Access Configuration

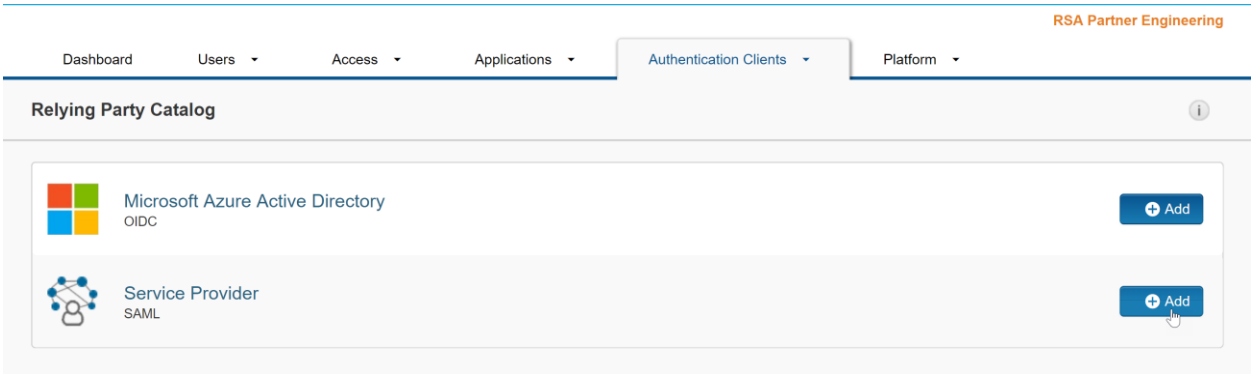
1. Log in to the RSA SecurID Access Administration Console and click **Authentication Clients** > **Relying Parties** menu item at the top of the page.



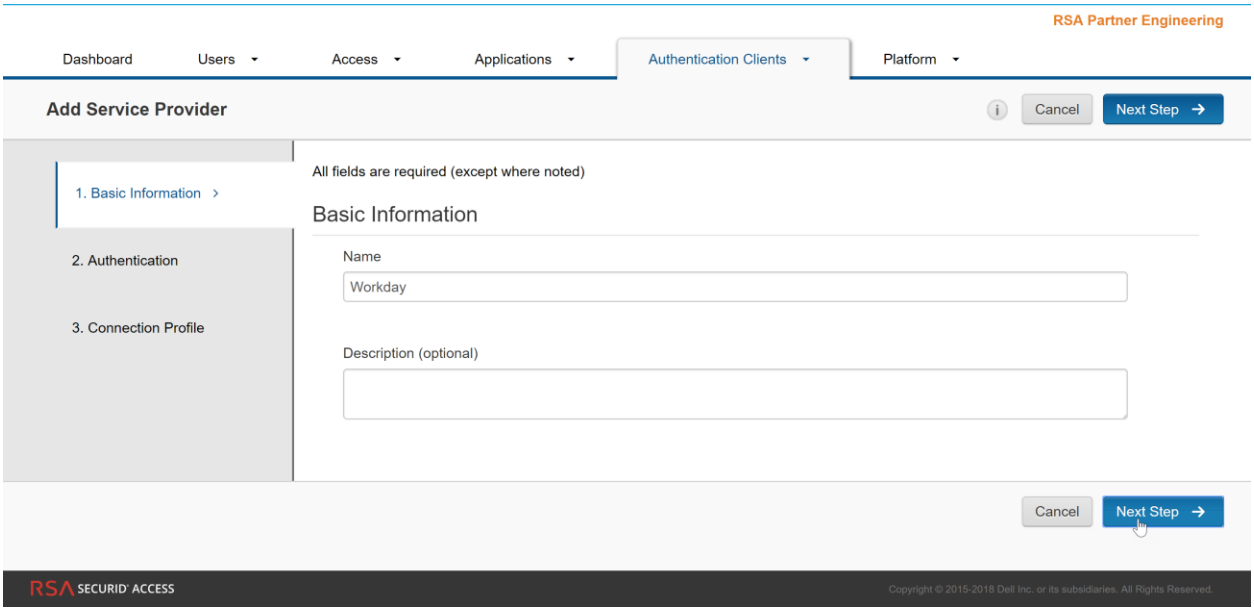
2. Click the **Add a Relying Party** button on the My Relying Parties page.



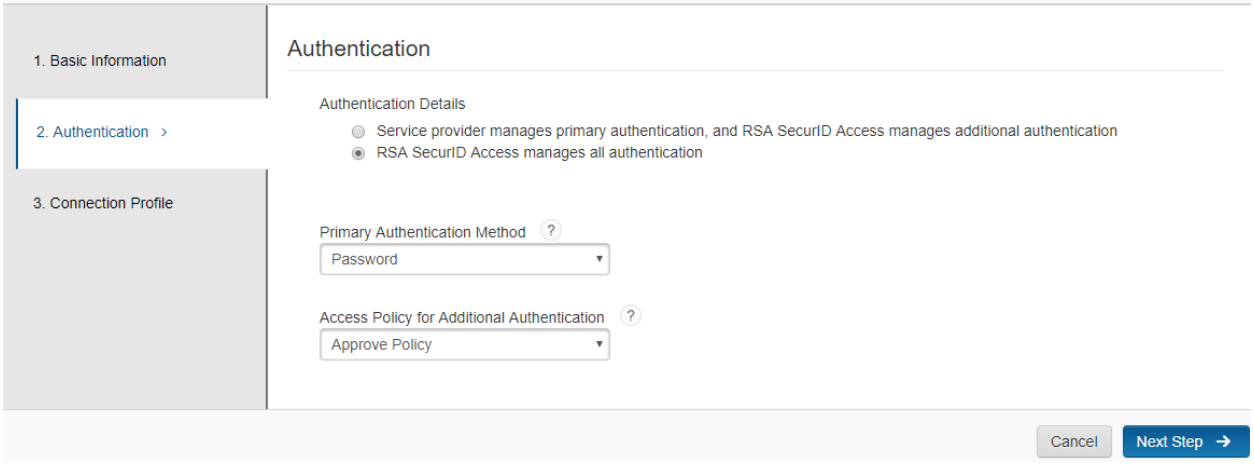
3. From the Relying Party Catalog select the **+Add** button for Service Provider SAML.



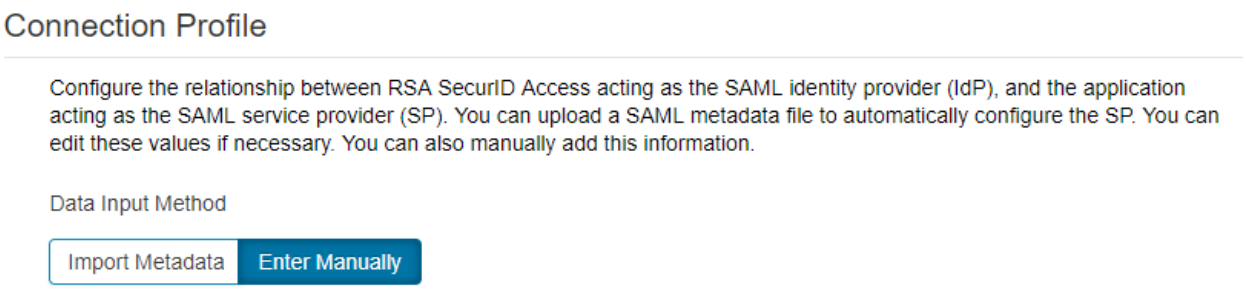
4. Enter a **Name** for the Service Provider and click **Next Step**.



5. Choose **RSA SecurID Access manages all authentication**, **Password**, your Access Policy and click **Next Step**.



6. Choose **Enter Manually** Data Input Method.

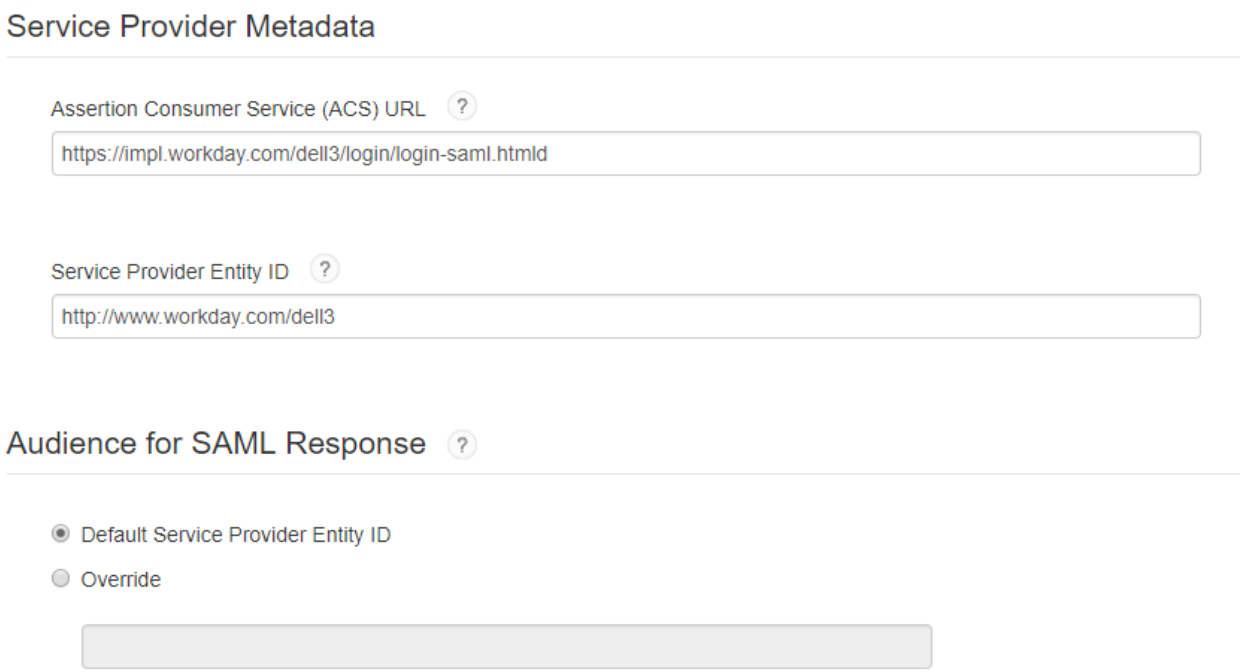


7. Enter the Assertion Consumer Service (ACS) URL in format: https://<workday domain>/<tenant>/login-saml.htmld

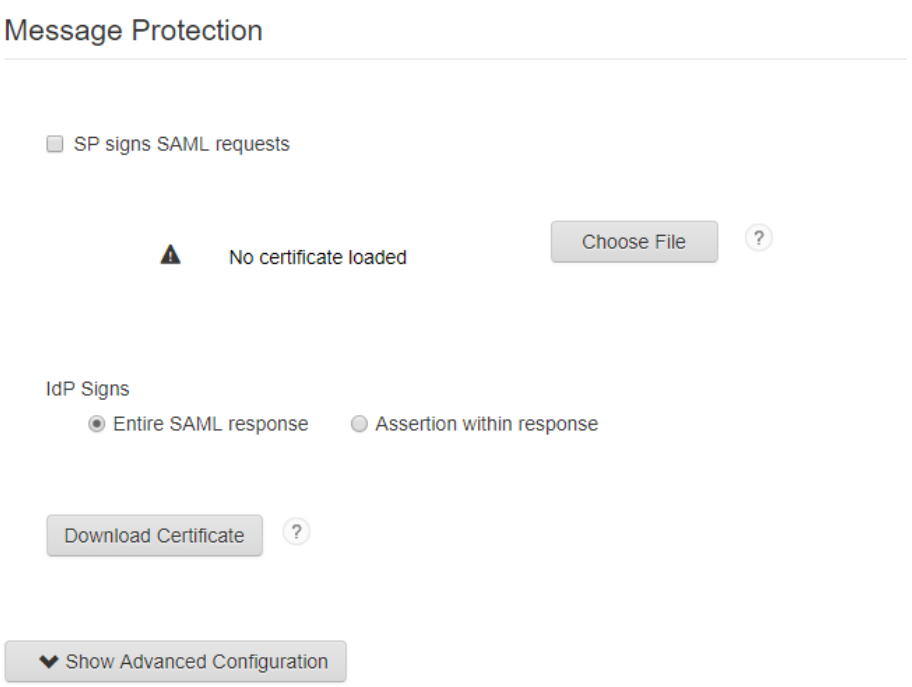
Example: https://impl.workday.com/dell3/login-saml.htmld

8. Enter Service Provider Entity ID in format: http://www.workday.com/<tenant>

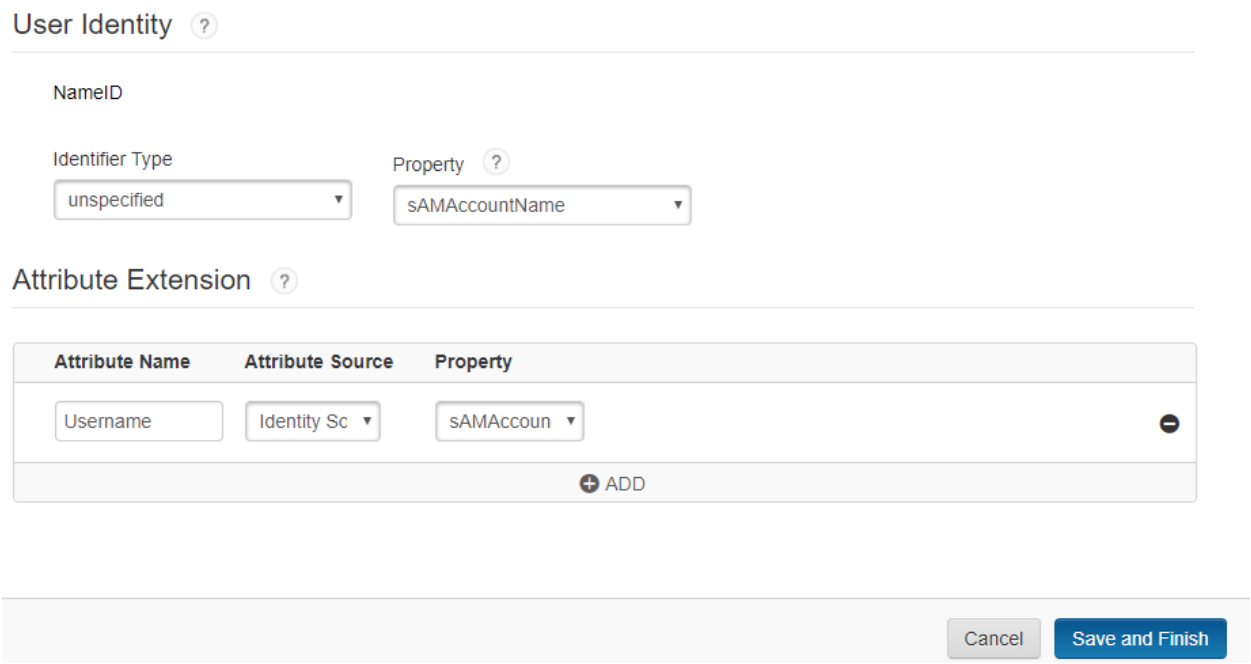
Example: http://www.workday.com/dell3



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

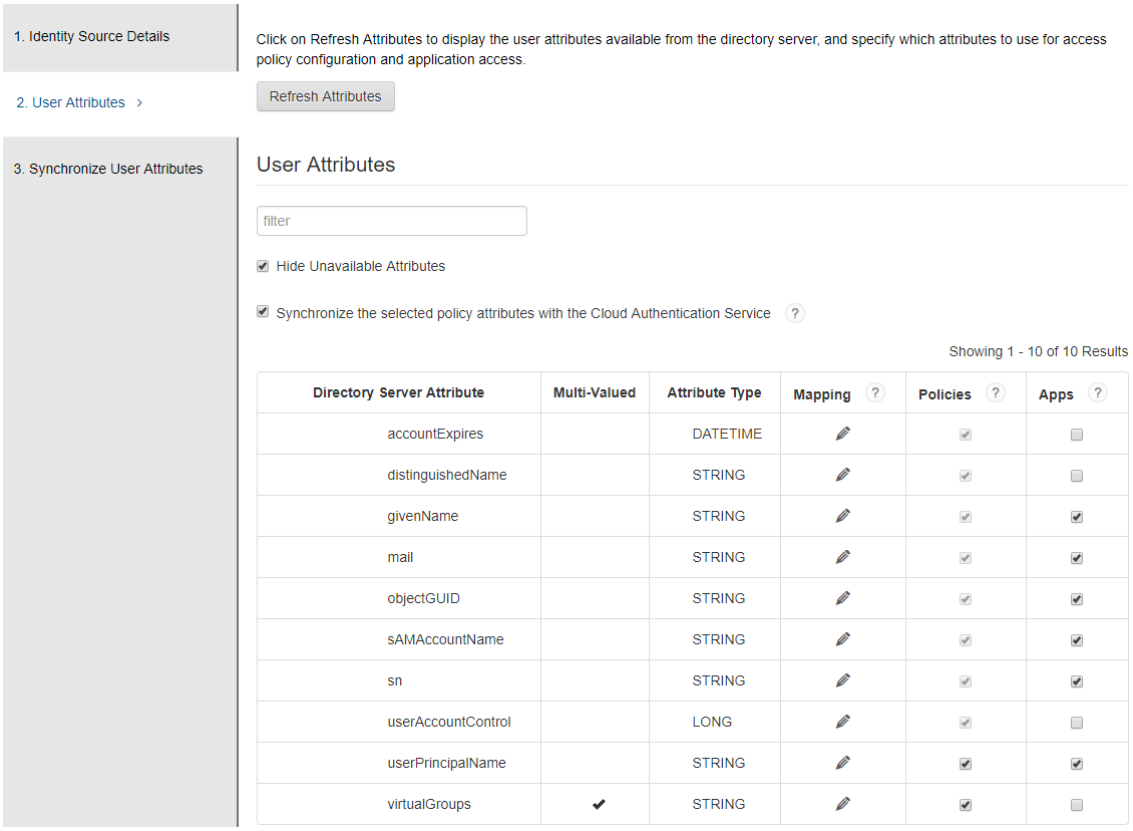


11. Next, click **Show Advanced Configuration**.
12. In the NameID field use the Identifier Type pulldown to select **unspecified** and Property to **sAMAccountName** when using an identity source types of Active Directory or **uid** when using an identity source types of LDAP.
13. Under Attribute Extension 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.



14. Select **Save and Finish**.
15. On the My Relying Parties page, select the **Edit** pulldown and select **View or Download IdP Metadata**.
16. View the metadata file to find the Cloud IdP URL. Location=https://<company_id>.auth.securid.com/saml-fe/sso.
17. Navigate to **Users > Identity Sources**.
18. Select **Edit** for the Identity Source used in the Access Policy.

19. On the User Attributes page, verify that the **Synchronize the selected policy attributes with the Cloud Authentication Service** is checked.
20. In the Policies column verify that attribute **sAMAccountName** or **uid** is checked.



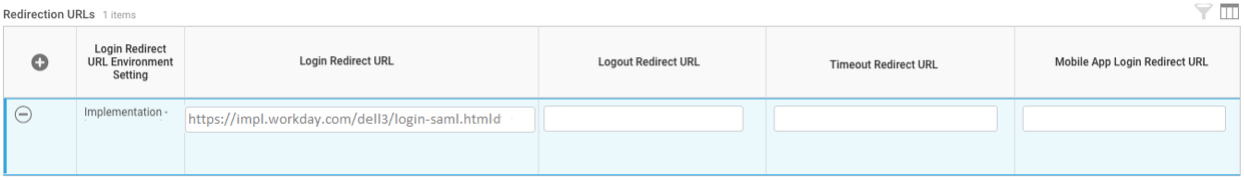
21. Click **Next Step**.
22. Click **Save and Finish**.

Note: Repeat these steps for all of the Identity Sources referenced in the Access Policy.

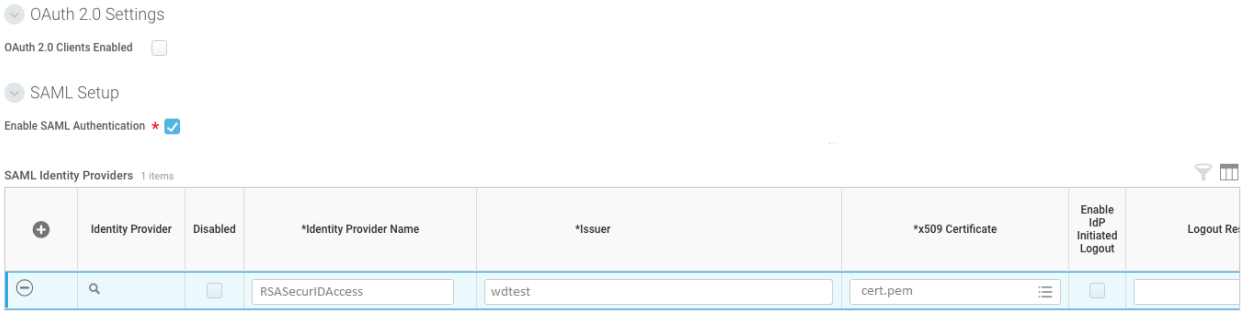
23. On the top menu click **Publish Changes**.

Complete Workday Configuration

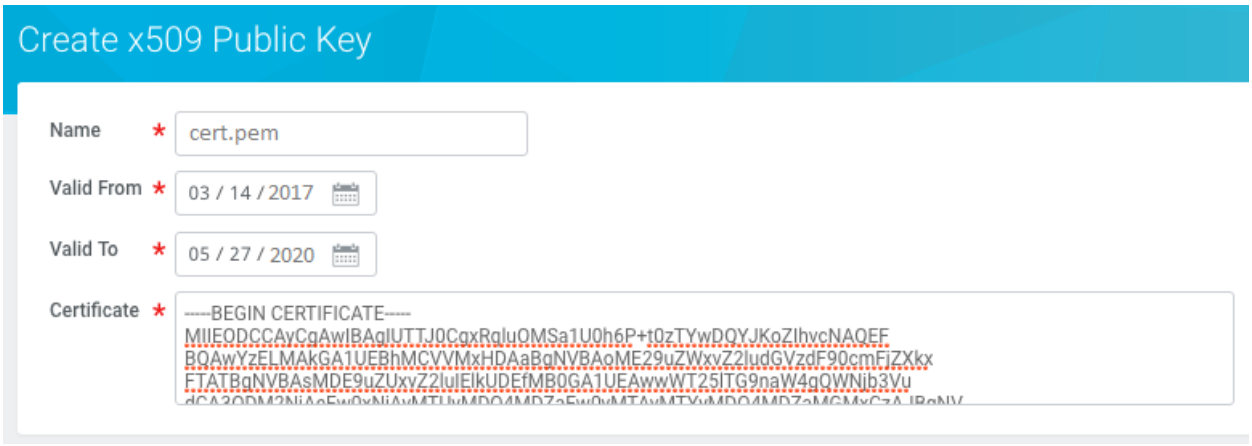
1. Log into your Workday tenant with an Administrator account and navigate to **Account Administration** > **Edit Tenant Setup – Security**.
2. Click the **+** icon under Redirection URLs to add a row. In the Redirect URLs section, enter the Login Redirect URL for your tenant. This should match the **ACS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



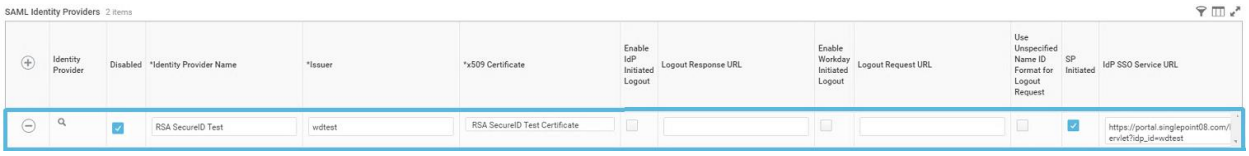
3. Under **SAML Setup** section, select the check box **Enable SAML Authentication** and then click the **+** icon under SAML Identity Providers.
4. Configure the SAML Identity Provider settings and then click **OK**.



- In the Identity Provider Name field, enter a descriptive name such as RSASecurIDAccess.
- In the Issuer field, enter the **Cloud IdP URL**.
- In the X509 Certificate field select the menu icon, and select **Create X509 Public Key** from the pulldown list.
- Enter a **Name** for the certificate.
- Enter a Valid From and Valid To date.
- Copy and paste the RSA public certificate into the Certificate field.

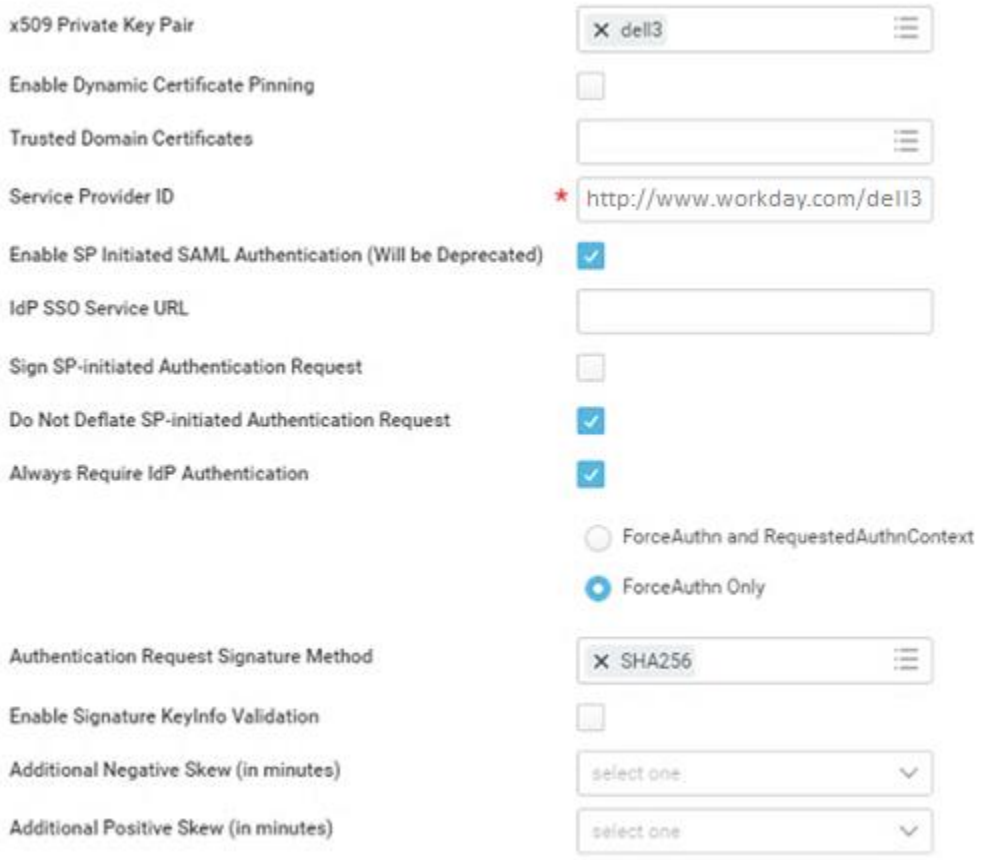


5. Use the scroll bar to continue filling out the SAML Identity Providers fields.



- In the IdP SSO Service URL, enter the Cloud IdP URL.
- Click in the Used for Environments field and select the environments you would like to use single sign on in and click OK.

6. Configure the fields in the SAML Identity Providers table and click **Save**.



- Enter a unique value for the Service Provider ID.
- Check the Enable SP Initiated SAML Authentication box.
- Check the Do not Deflate SP-initiated Authentication Request box.
- Check the Always Require IdP Authentication.
- Select ForceAuthn Only.