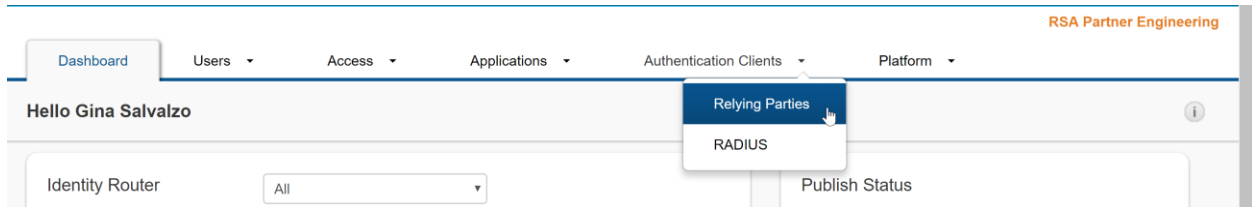


RSA SecurID Access Free Trial Workday Guide

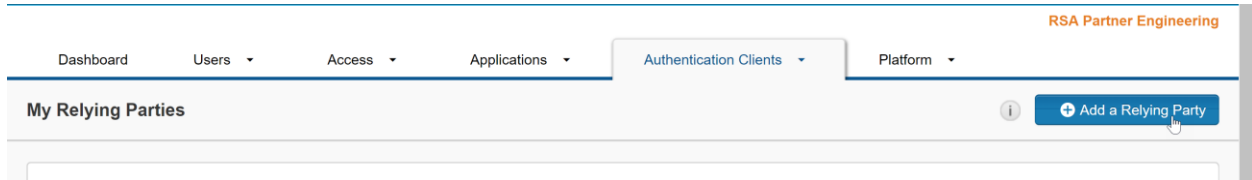
This guide describes how to set up Workday as part of the RSA SecurID Access Free Trial program. Use this guide in conjunction with the RSA SecurID Access Free Trial Quick Setup Guide.

Complete RSA SecurID Access Configuration

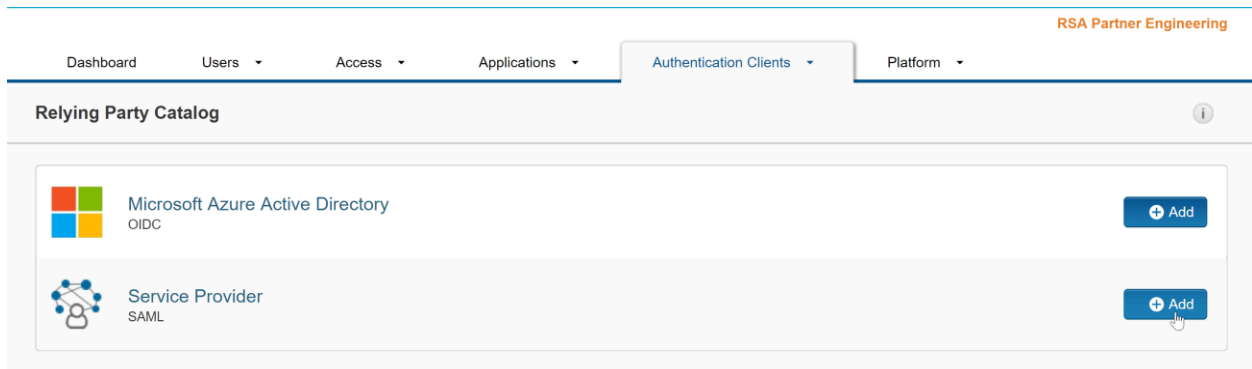
1. Log in to the RSA SecurID Access Administration Console and click **Authentication Clients** > **Relying Parties** menu item at the top of the page.



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**.

Dashboard Users Access Applications Authentication Clients Platform

RSA Partner Engineering

Add Service Provider

All fields are required (except where noted)

Basic Information

Name
Workday

Description (optional)

Cancel Next Step →

Cancel Next Step →

RSA SECURID ACCESS Copyright © 2015-2018 Dell Inc. or its subsidiaries. All Rights Reserved.

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

1. Basic Information

2. Authentication

3. Connection Profile

Authentication

Authentication Details

Service provider manages primary authentication, and RSA SecurID Access manages additional authentication

RSA SecurID Access manages all authentication

Primary Authentication Method ?
Password

Access Policy for Additional Authentication ?
Approve Policy

Cancel Next Step →

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

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

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

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

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

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

Service Provider Metadata

Assertion Consumer Service (ACS) URL ?

Service Provider Entity ID ?

Audience for SAML Response ?


Default Service Provider Entity ID

Override

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

Message Protection

SP signs SAML requests

 No certificate loaded

Choose File ?

IdP Signs

Entire SAML response

Assertion within response

Download Certificate ?

▼ Show Advanced Configuration

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.

User Identity ?

NameID

Identifier Type

unspecified

Property ?

sAMAccountName

Attribute Extension ?

Attribute Name	Attribute Source	Property	
Username	Identity Sc	sAMAccoun	⊖
⊕ ADD			

Cancel

Save and Finish

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.

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

1. Identity Source Details

2. User Attributes >

3. Synchronize User Attributes

Click on Refresh Attributes to display the user attributes available from the directory server, and specify which attributes to use for access policy configuration and application access.

[Refresh Attributes](#)

User Attributes

filter

Hide Unavailable Attributes

Synchronize the selected policy attributes with the Cloud Authentication Service ?

Showing 1 - 10 of 10 Results

Directory Server Attribute	Multi-Valued	Attribute Type	Mapping ?	Policies ?	Apps ?
accountExpires		DATETIME		<input checked="" type="checkbox"/>	<input type="checkbox"/>
distinguishedName		STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>
givenName		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
mail		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
objectGUID		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
sAMAccountName		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
sn		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
userAccountControl		LONG		<input checked="" type="checkbox"/>	<input type="checkbox"/>
userPrincipalName		STRING		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
virtualGroups	<input checked="" type="checkbox"/>	STRING		<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Click **Next Step**.
- Click **Save and Finish**.

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

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

Publish Changes
Status: Changes Pending

Complete Workday Configuration

- Log into your Workday tenant with an Administrator account and navigate to **Account Administration > Edit Tenant Setup – Security**.
- 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.

Redirection URLs 1 items 🔍 📄

	Login Redirect URL Environment Setting	Login Redirect URL	Logout Redirect URL	Timeout Redirect URL	Mobile App Login Redirect URL
+	Implementation -	<input type="text" value="https://impl.workday.com/dell3/login-saml.html"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

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

OAuth 2.0 Settings

OAuth 2.0 Clients Enabled

SAML Setup

Enable SAML Authentication

SAML Identity Providers 1 Items

+	Identity Provider	Disabled	*Identity Provider Name	*Issuer	*x509 Certificate	Enable IdP Initiated Logout	Logout Re
-	q	<input type="checkbox"/>	RSASecurIDAccess	wdtest	cert.pem	<input type="checkbox"/>	

- 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.

Create x509 Public Key

Name * cert.pem

Valid From * 03 / 14 / 2017

Valid To * 05 / 27 / 2020

Certificate *
 -----BEGIN CERTIFICATE-----
 MIIEQDCCAyCgAwIBAgIU7TJ0CgxRqluQMSa1U0h6P+t0zTYwDOYJKoZlhcNAQEF
 BOAwYzELMAkGA1UEBhMCVVMxHDAaBgNVBAoME29uZWxvZ2ludGVzdF90cmFjZXkx
 FTATBqNVBAsMDE9uZUxvZ2lueikUEFMB0GA1UEAwwWT25lTG9naW4gQWNib3Vv
 dCA2ODM2NiA6Fw0yNiAyMTUyMDQAMDZzFw0yMTYyMTYyMDQAMDZzMCMyCzAIBgNV

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

SAML Identity Providers 2 Items

+	Identity Provider	Disabled	*Identity Provider Name	*Issuer	*x509 Certificate	Enable IdP Initiated Logout	Logout Response URL	Enable Workday Initiated Logout	Logout Request URL	Use Unspecified Name ID Format for Logout Request	SP Initiated	IdP SSO Service URL
-	q	<input checked="" type="checkbox"/>	RSA SecureID Test	wdtest	RSA SecureID Test Certificate	<input type="checkbox"/>		<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	https://portal.singlepoint08.com/evlet/idp_id=wdtest

- 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**.

x509 Private Key Pair	<input type="text" value="X dell3"/>
Enable Dynamic Certificate Pinning	<input type="checkbox"/>
Trusted Domain Certificates	<input type="text"/>
Service Provider ID	* <input type="text" value="http://www.workday.com/de113"/>
Enable SP Initiated SAML Authentication (Will be Deprecated)	<input checked="" type="checkbox"/>
IdP SSO Service URL	<input type="text"/>
Sign SP-initiated Authentication Request	<input type="checkbox"/>
Do Not Deflate SP-initiated Authentication Request	<input checked="" type="checkbox"/>
Always Require IdP Authentication	<input checked="" type="checkbox"/>
	<input type="radio"/> ForceAuthn and RequestedAuthnContext
	<input checked="" type="radio"/> ForceAuthn Only
Authentication Request Signature Method	<input type="text" value="X SHA256"/>
Enable Signature KeyInfo Validation	<input type="checkbox"/>
Additional Negative Skew (in minutes)	<input type="text" value="select one"/>
Additional Positive Skew (in minutes)	<input type="text" value="select one"/>

- 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.