RSA SecurID Access SAML Configuration for Central Desktop

Last Modified: May 27, 2015

Central Desktop is a Sharepoint alternative for business social collaboration.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Central Desktop.
- Contact Central Desktop support with your email domain

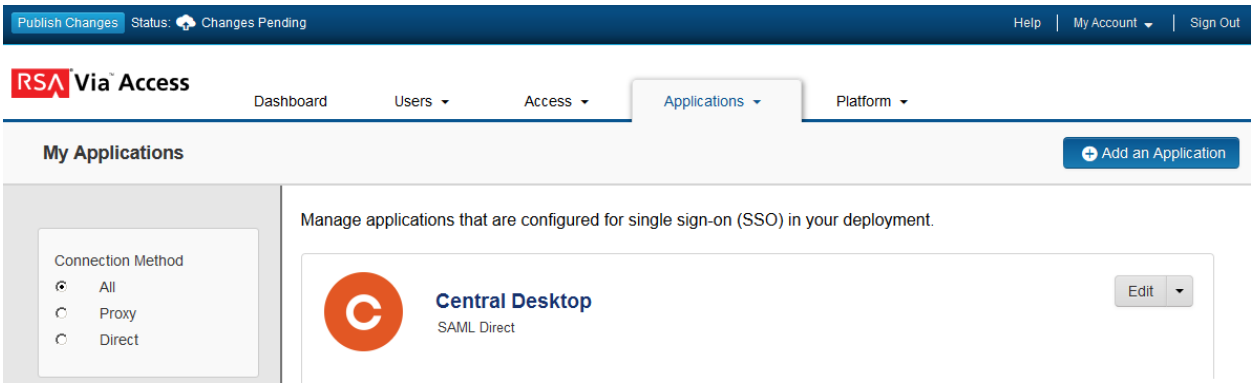
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Central Desktop to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

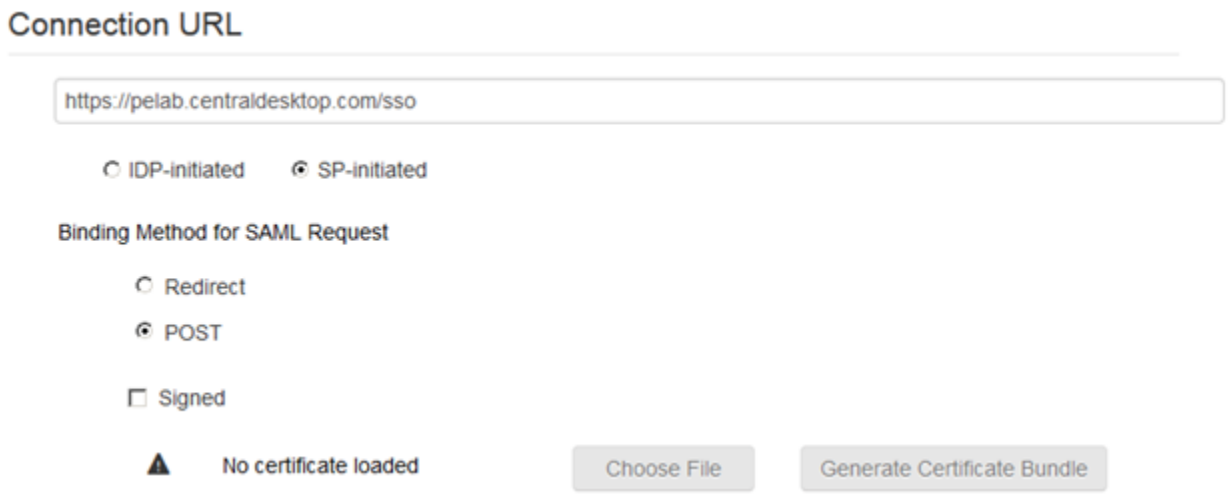
Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, search for **Central Desktop.** Click **+Add**.

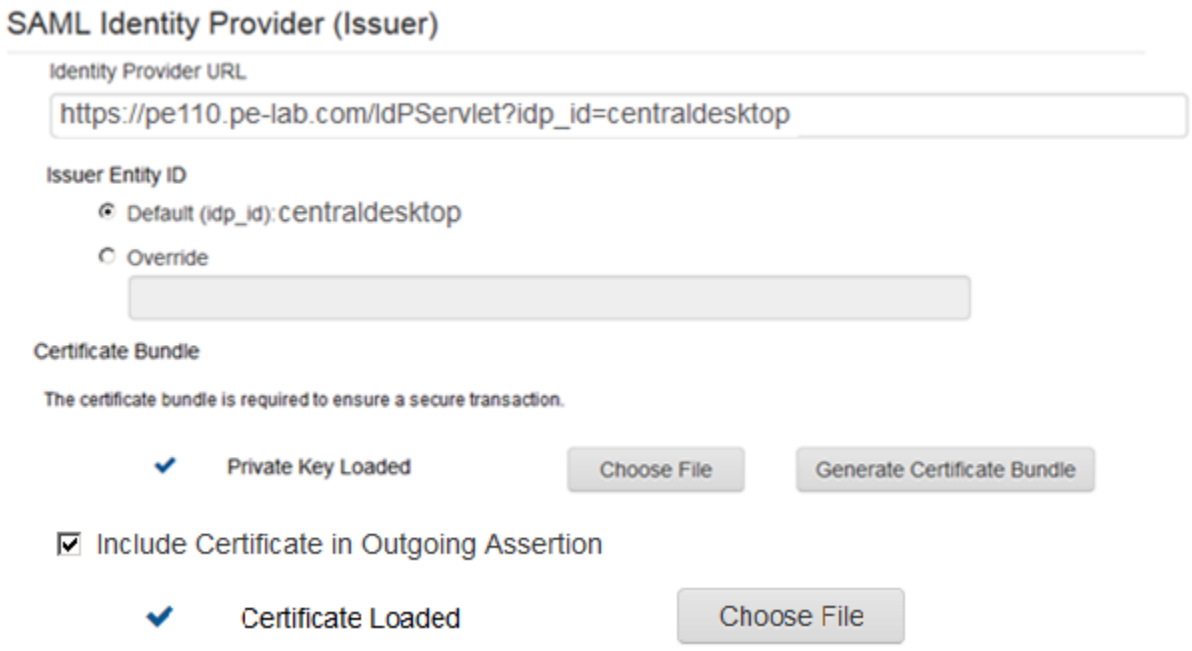


3. On the Basic Information page, specify the application name and click **Next Step**.
4. On the Connection Profile page, choose **SP –initiated** and binding method **POST**.
5. In the Connection URL field enter your domain single sign-on login URL.

> **Note: The following SP -initiated configuration works for both SP -initiated and IDP -initiated connections. If you wish for a IDP initiated only application chose IDP-initiated and leave the Connection URL blank.**



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

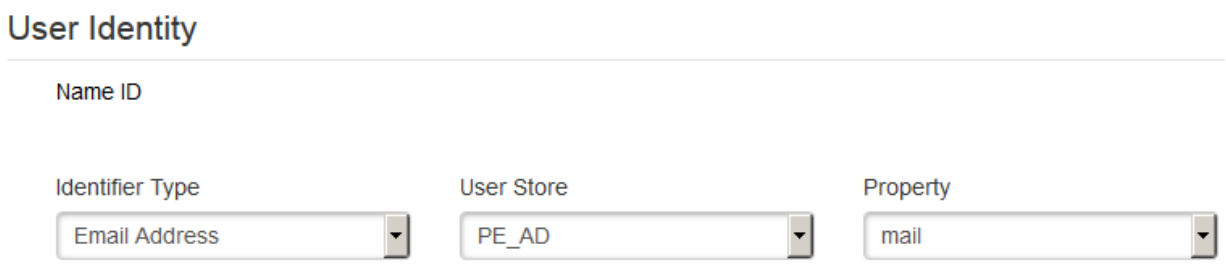


   a. Take note of the **Identity Provider URL** and the Issuer Entity ID **Default** field, which will be needed later to configure the Service Provider configuration.
   b. Select **Choose File** and upload the private key.
   c. Check **Include Certificate in Outgoing Assertion** and select **Choose File** and upload the public certificate.

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

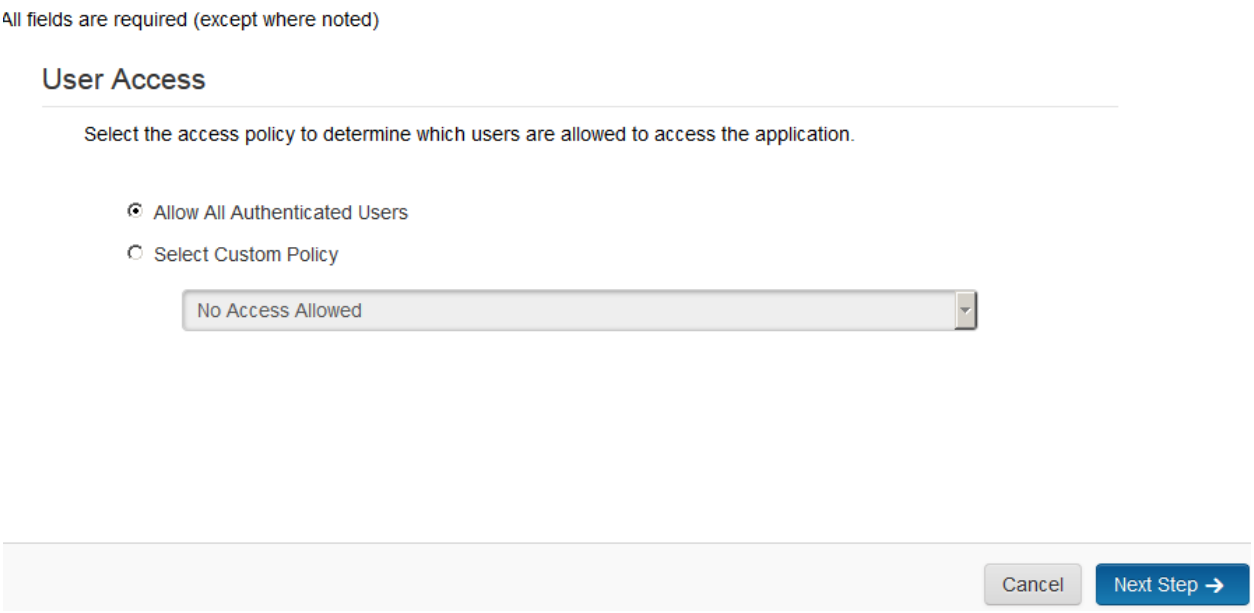
   a. Modify the **Assertion Consumer Service (ACS) URL,** with your specific instance.
   b. Modify the **Audience (Service Provider Entity ID)** field, with your specific instance.

8. Scroll down to **User Identity** section. Select **Email** from the Identifier Type pull down and **mail** from the Property pull down.

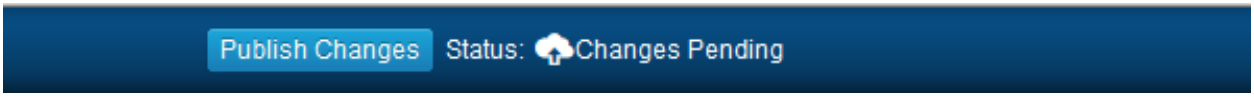


9. Click **Next Step**.

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



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.



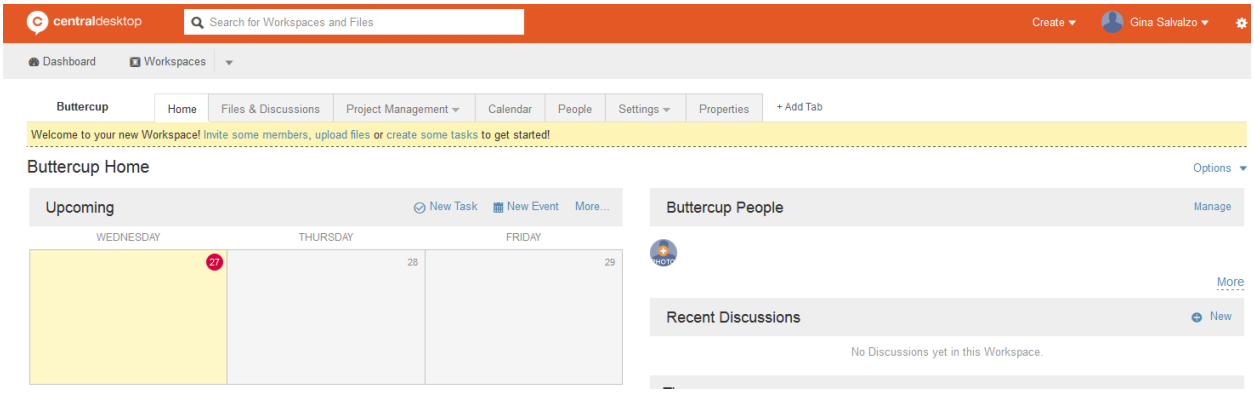
Next Steps

[Configure Central Desktop to Use RSA SecurID Access as an Identity Provider]

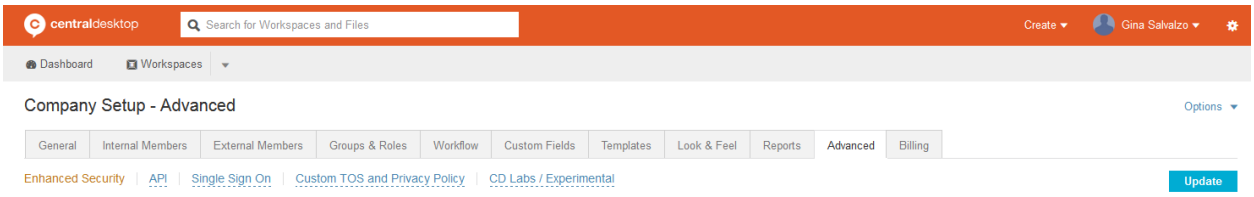
Configure Central Desktop

Procedure

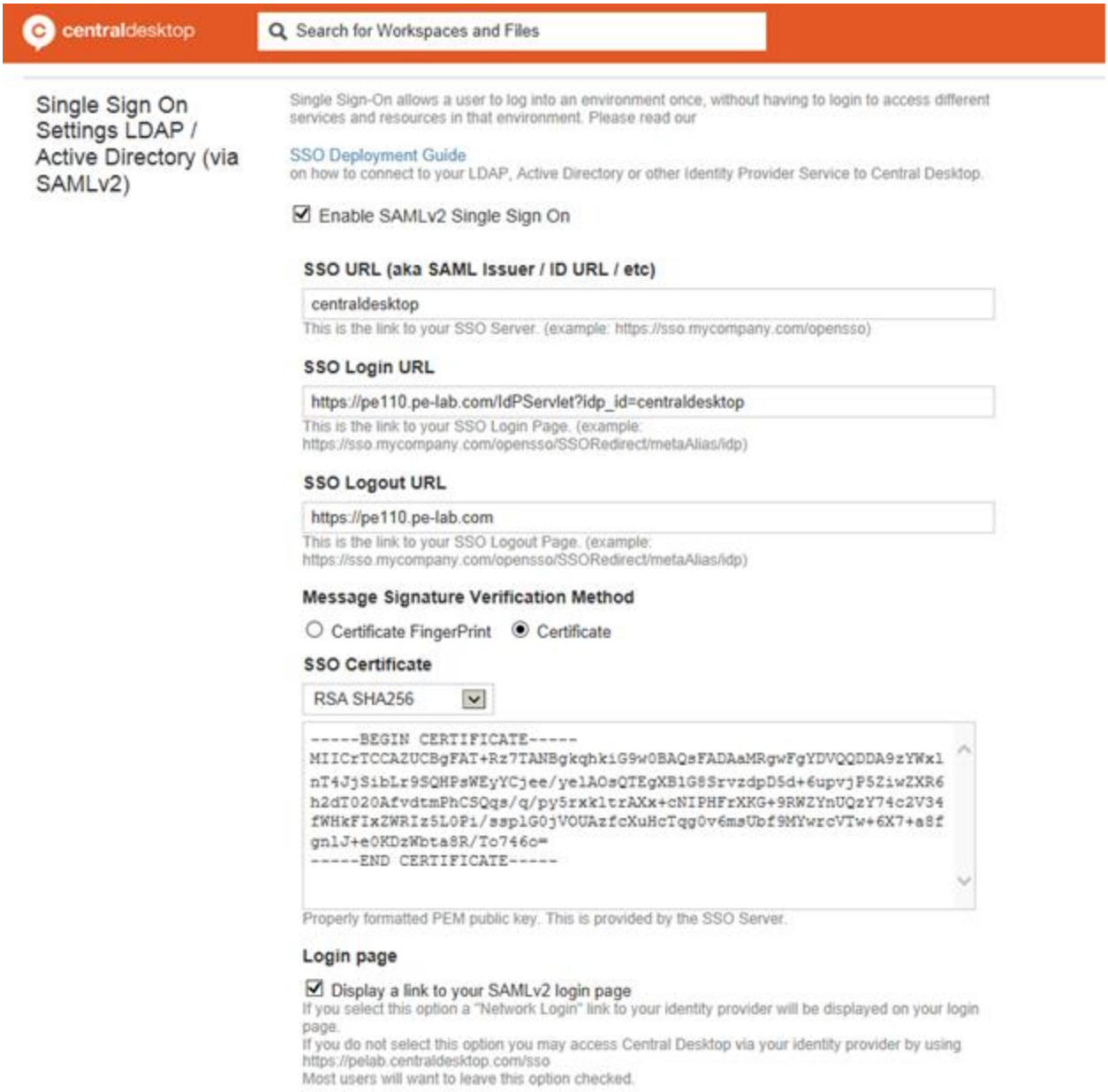
1. Login to the Central Desktop administration. http://app.centraldesktop.com/login



2. Click the gear icon in the upper right corner.
3. Navigate to **Company Setup > Advanced**.



4. Select **Single Sign On**.



a. Check **Enable SAMLv2 Single Sign On**.
b. In the **SSO URL (aka SAML Issuer /ID URL / etc)** field, copy the **Default (idp_id)** from the RSA SecurID Access Identity Provider ("Issuer") section.
c. In the **SSO Login URL** field, copy the **Identity Provider URL**, from the RSA SecurID Access Identity Provider ("Issuer") section.
d. Select **Certificate** for the Message Signature Verification Method.
e. In **SSO Certificate**, paste the RSA SecurID Access public certificate.
f. Click **Update**.

GLS