

# 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

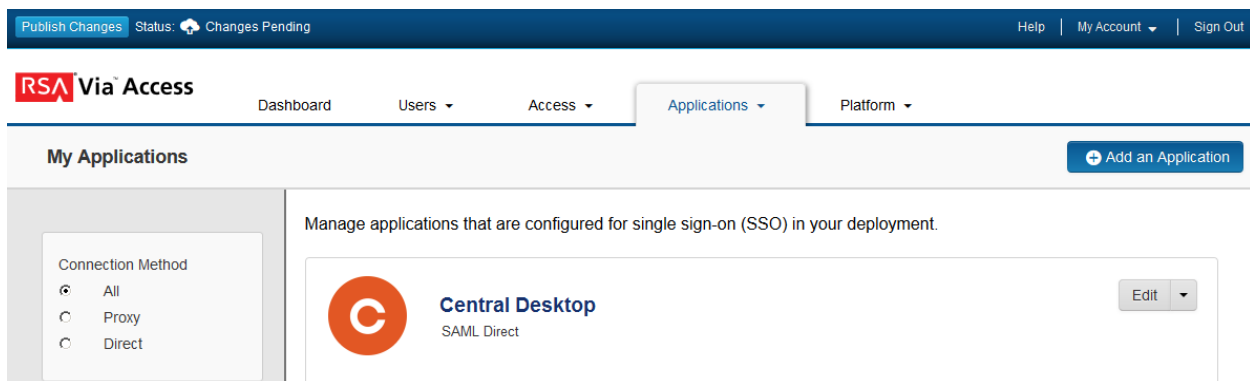
## Procedure

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.

---

## Connection URL


IDP-initiated    SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded     

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

## SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp\_id):centraldesktop

Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

Private Key Loaded     

Include Certificate in Outgoing Assertion

Certificate Loaded  

- 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.

## Service Provider

---

Assertion Consumer Service (ACS) URL

`https://<your_instance>.centraldesktop.com/saml2-assertion.php`

Audience (Service Provider Entity ID)

`https://<your_instance>.centraldesktop.com/saml2-metadata.php`

- 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.

## User Identity

---

Name ID

Identifier Type

Email Address

User Store

PE\_AD

Property

mail

9. Click **Next Step**.

10. 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 →


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.

Publish Changes

Status:  Changes Pending

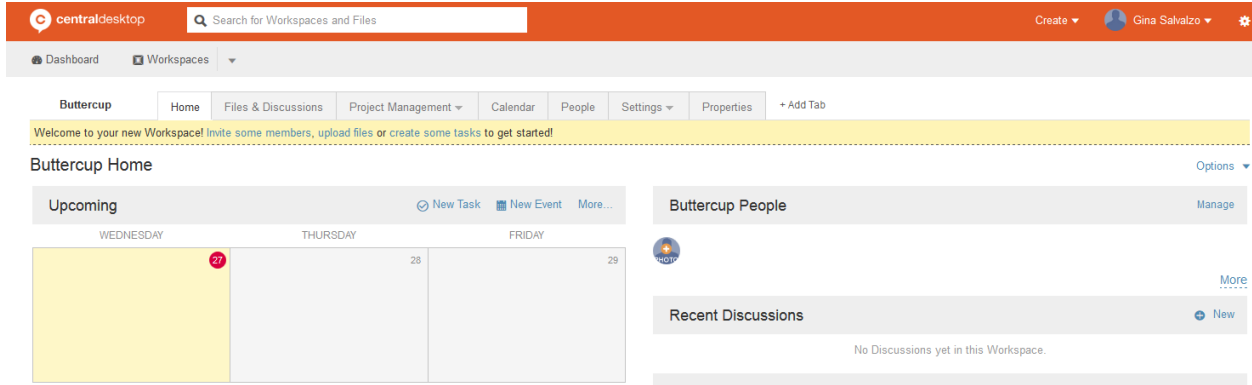
### Next Steps

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

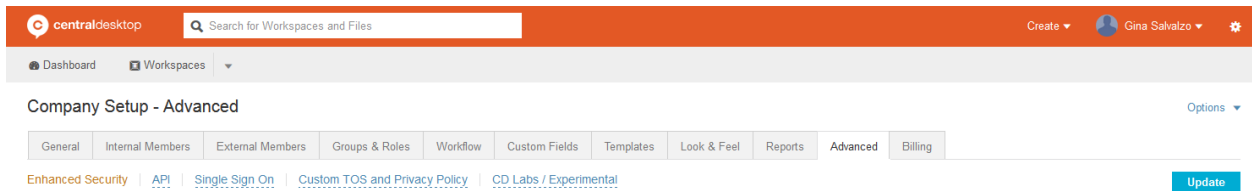
# Configure Central Desktop

## 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**.

Single Sign On  
Settings LDAP /  
Active Directory (via  
SAMLv2)

Single Sign-On allows a user to log into an environment once, without having to login to access different services and resources in that environment. Please read our

SSO Deployment Guide

on how to connect to your LDAP, Active Directory or other Identity Provider Service to Central Desktop.

Enable SAMLv2 Single Sign On

SSO URL (aka SAML Issuer / ID URL / etc)

centraldesktop

This is the link to your SSO Server. (example: <https://sso.mycompany.com/opensso>)

SSO Login URL

[https://pe110.pe-lab.com/idPServlet?idp\\_id=centraldesktop](https://pe110.pe-lab.com/idPServlet?idp_id=centraldesktop)

This is the link to your SSO Login Page. (example: <https://sso.mycompany.com/opensso/SSORedirect/metaAlias/idp>)

SSO Logout URL

<https://pe110.pe-lab.com>

This is the link to your SSO Logout Page. (example: <https://sso.mycompany.com/opensso/SSORedirect/metaAlias/idp>)

Message Signature Verification Method

Certificate FingerPrint  Certificate

SSO Certificate

RSA SHA256

```
-----BEGIN CERTIFICATE-----
MIICrTCCA2UCBgFAT+Rz7TANBgkqhkiG9w0BAQsFADAaMRgwFgYDVQDDA9zYWx1
nT4JjSibLr9SQHPsWEyYCjee/yelAOsQTEgXB1G8SrvzdpD5d+6upvjP5Z1wZXR6
h2dT020AfvdtmPhCSQqs/q/py5rxk1trAXx+cNIPHFzXKG+9RWZYnUQzY74c2V34
fWHkFixZWRiz5L0Fi/ssp1G0jVOUAzfcXuHcTqg0v6msUbf9MYwrcVTw+6X7+a8f
gn1J+e0KDzWbtaSR/To746c=
-----END CERTIFICATE-----
```

Properly formatted PEM public key. This is provided by the SSO Server.

Login page

Display a link to your SAMLv2 login page

If you select this option a "Network Login" link to your identity provider will be displayed on your login page.

If you do not select this option you may access Central Desktop via your identity provider by using <https://pelab.centraldesktop.com/sso>

Most users will want to leave this option checked.

- Check **Enable SAMLv2 Single Sign On**.
- 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.
- In the **SSO Login URL** field, copy the **Identity Provider URL**, from the RSA SecurID Access Identity Provider ("Issuer") section.
- Select **Certificate** for the Message Signature Verification Method.
- In **SSO Certificate**, paste the RSA SecurID Access public certificate.
- Click **Update**.