RSA SecurID Access SAML Configuration for Box

Last Modified: April 13, 2015

Box offers a secure cloud based business collaboration solution that enables customers to share files, view and comment on any kind of document, and connect with coworkers. Users can create shared folders for projects of any size, and control user access to shared files.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Box.
- Submit the SecurID Access metadata file to Box. Allow 5 days for Box support to upload the file.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

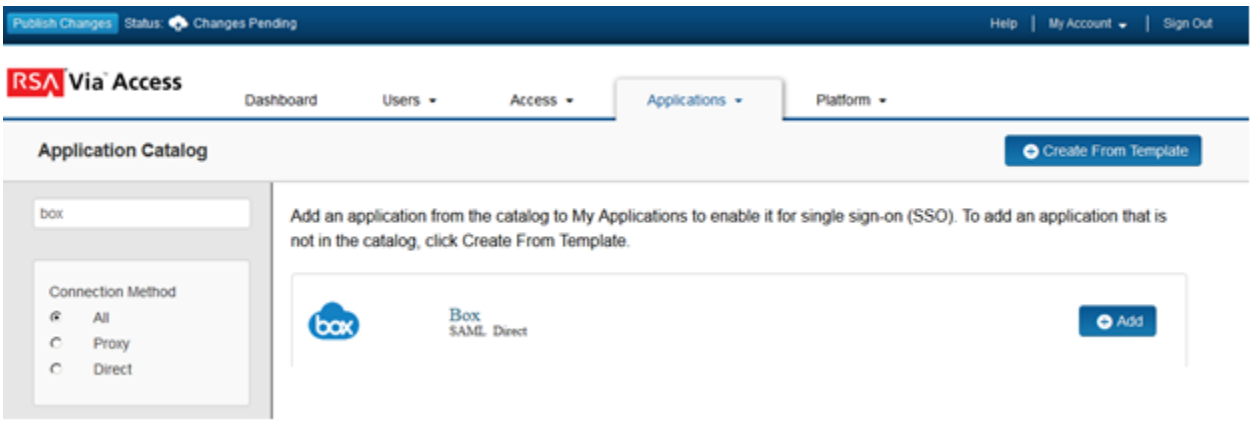
Procedure

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

Add the Application in RSA SecurID Access

Procedure

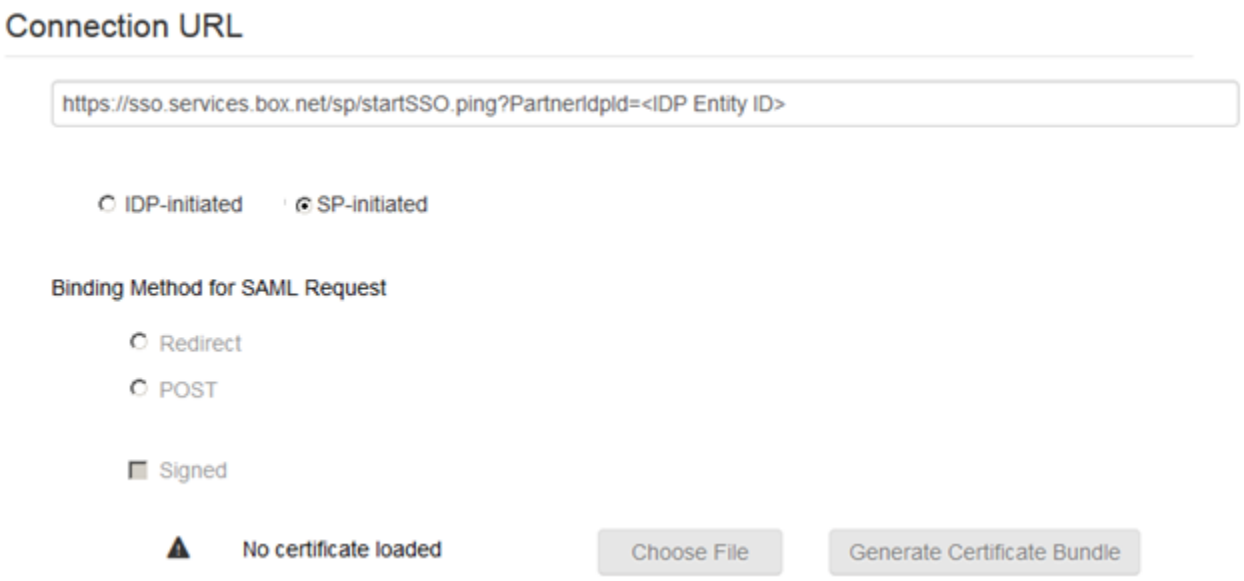
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, select **Box SAML Direct** and click **+Add**.



3. On the Basic Information page, specify the application name and click **Next Step**.

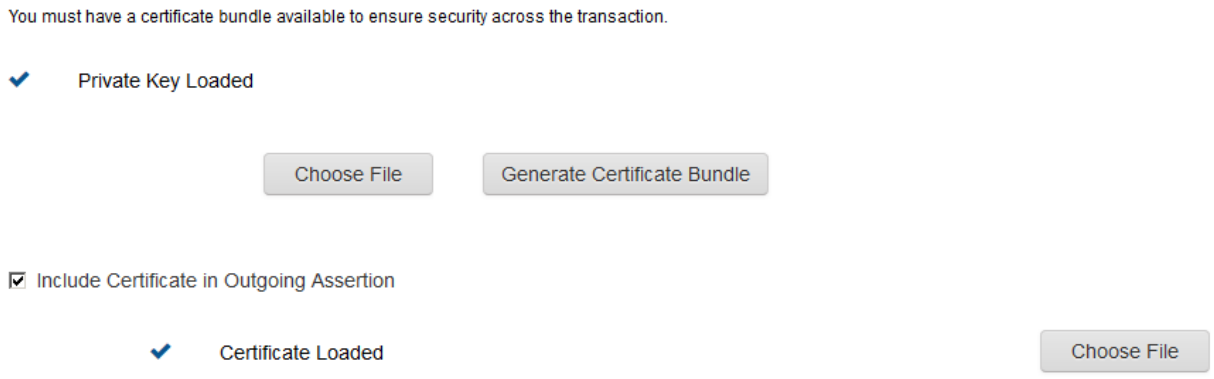
> **Note: The following SP-initiated configuration works for both SP-initiated and IDP- initiated connections.**

4. On the Connection Profile page, choose **SP-initiated**.
5. Replace ***<IDP Entity ID>*** in the Connection URL with the default value from step 6.



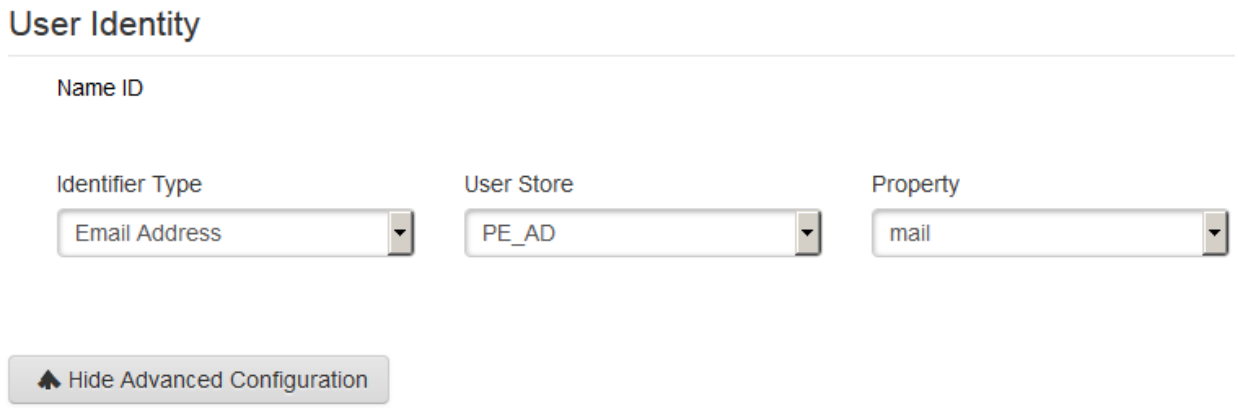
6. Scroll down to the **SAML Identity Provider ("Issuer")** section. Take note of the Issuer Entity ID default value. This is need in step 5 above.

7. Select **Choose File** and upload the private key.
8. Check **Include Certificate in Outgoing Assertion** and select **Choose File** and upload the public certificate.



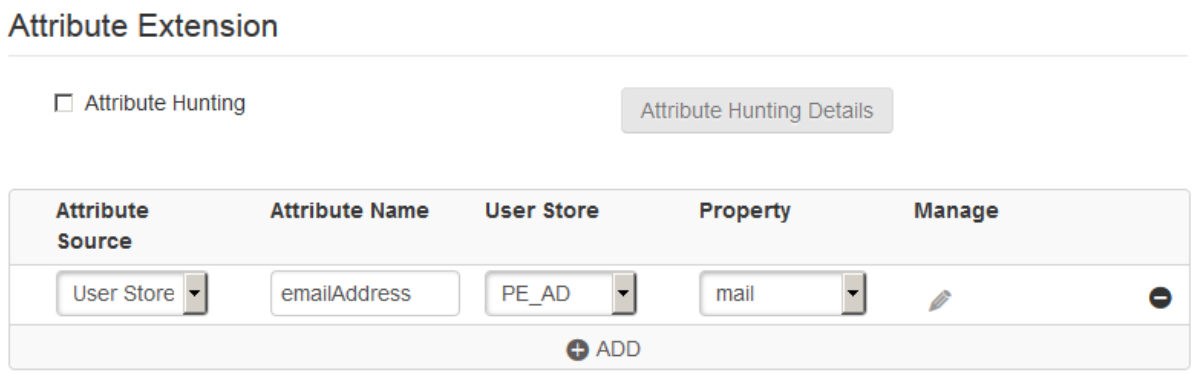
9. Scroll down to the **Service Provider** section.

   a. In the **Service Provider ACS URL** field, enter https://sso.services.box.net/sp/ACS.saml2
   b. In the **Audience (Service Provider Entity ID)** field, enter **box.net**.
10. Scroll down to **User Identity** section. Set the Identifier Type to **Email** and Property to **mail**.

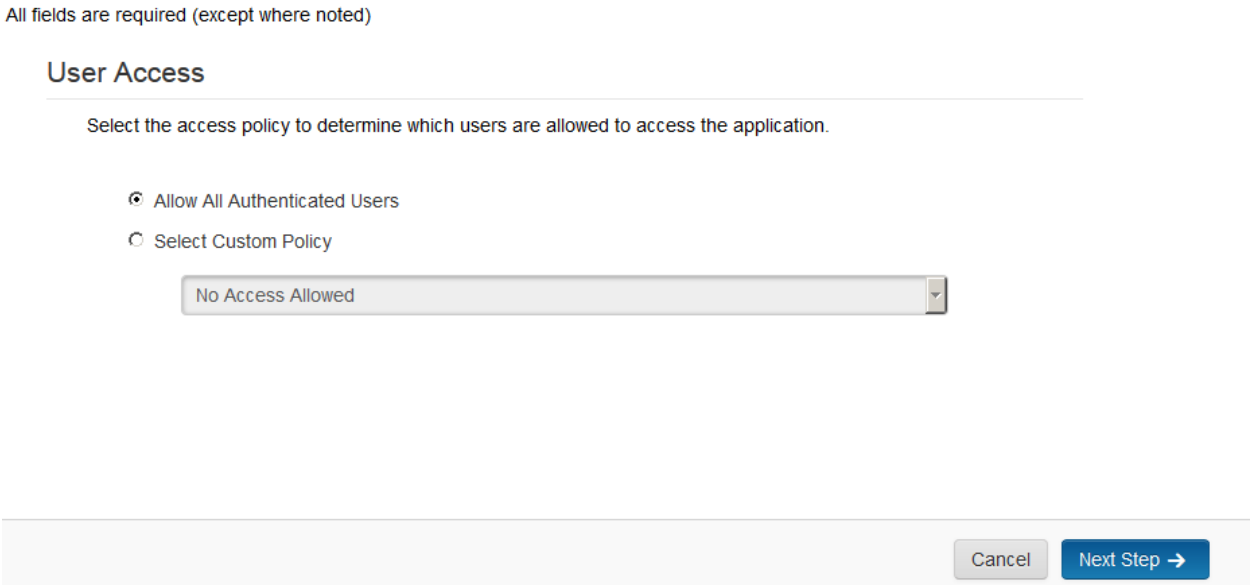


11. Click **Hide Advanced Configuration**.

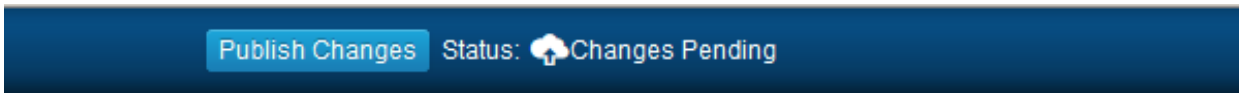
12. Scroll down to **Attribute Extension**. In the **Attribute Name** field enter **emailAddress** and in the **Property** field select **mail**.



13. Click **Next Step**.
14. On the **User Access** page, select the desired user policy from the drop down list.



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



Create the RSA SecurID Access Metadata file

1. Modify the example below with your environment information.
2. When inserting the cert.pem file do not include the -----BEGIN CERTIFICATE---- and ----END CERTIFICATE----lines.

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<EntityDescriptor xmlns:xsi="https://www.w3.org/2001/XMLSchema-instance"
    xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="CHANGEME_TO_CONNECTOR_IDP_ENTITY_ID">
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <!-- public saml cert -->
          <ds:X509Certificate>CHANGEME_TO_PUBLIC_SAML_CERT_CONTENT</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>

    <!-- Supported Name Identifier Formats -->
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</NameIDFormat>

    <!-- POST binding and location=idp url -->
    <SingleSignOnService
      Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="CHANGEME_TO_IDP_URL" />

  </IDPSSODescriptor>
</EntityDescriptor>
```

Next Steps

Configure Box to Use RSA SecurID Access as an Identity Provider

Configure Box to Use RSA SecurID Access as an Identity Provider

Procedure

1. You will need an Enterprise Box.net account.
2. Submit a support ticket with your metadata file to enable SSO.
   Please reserve 3-5 business days for the SSO feature to be added.
3. Login to your Box account and select **Admin console**.
4. Select the User icon.
5. Add your Active Directory user to Box.
6. The user will receive an email to activate their Box account. Once activated that user is ready to login via single sign-on.

GLS