RSA SecurID Access SAML Configuration for Microsoft Office 365 sign-in for Yammer

Last Modified: August 25, 2016

Microsoft Yammer is a team collaboration tool to bring work together in one place.

> Note: Yammer supports Office 365 sign-in. Please refer to RSA SecurID Access SAML Implementation Guide for Microsoft Office 365.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Microsoft Office 365.
- Complete the required steps in the *RSA SecurID Access SAML Implementation Guide for Microsoft Office 365.*

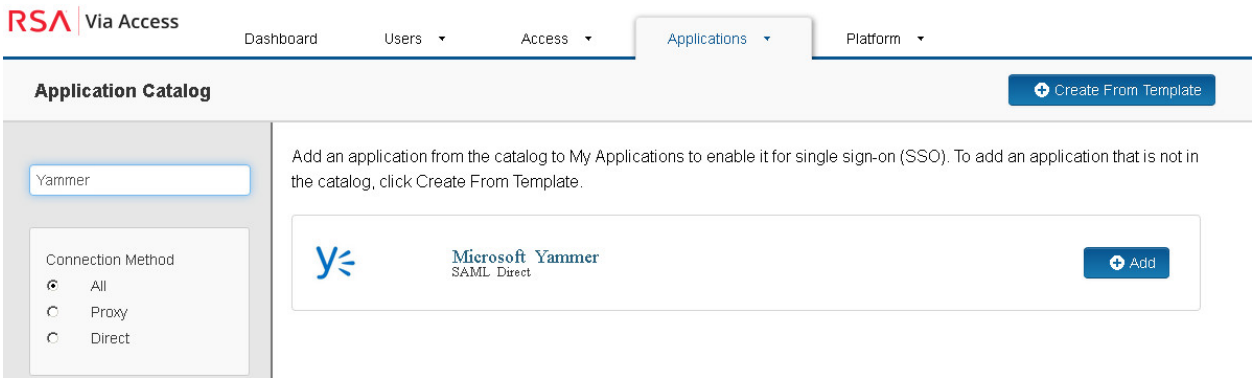
Procedure

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

Add the Application in RSA SecurID Access

Procedure

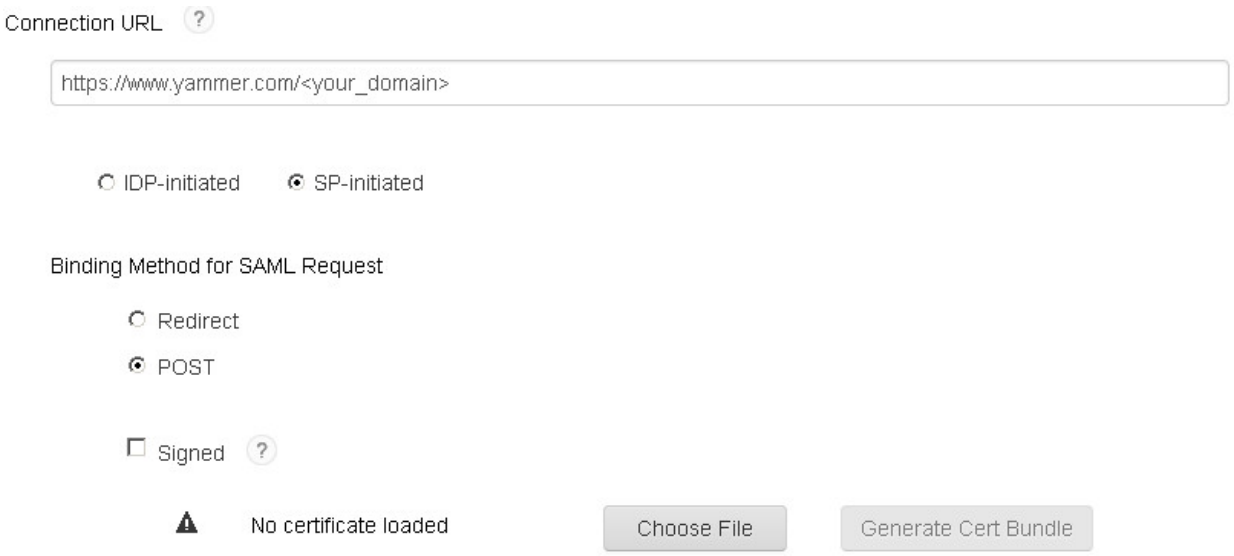
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. Search for Yammer and click **+Add**.



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

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

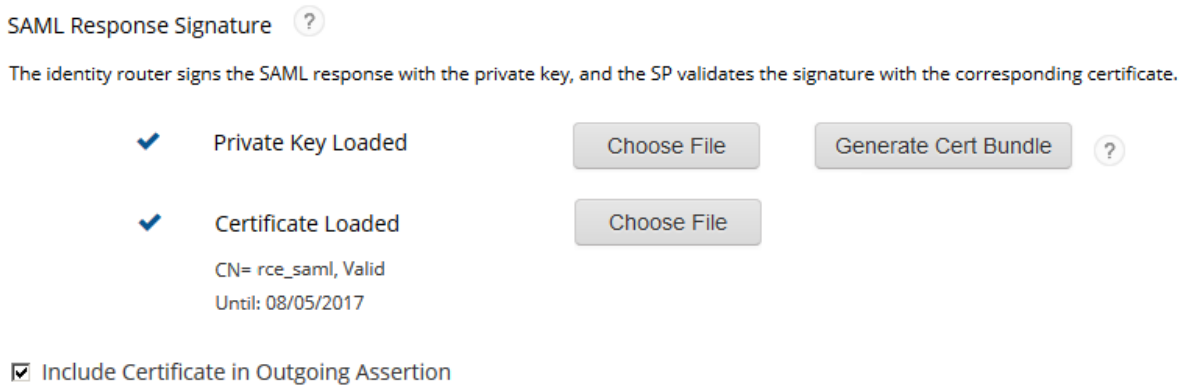
4. Choose **SP -initiated** and replace <your_domain> with your Office 365 domain.



5. Under Issuer Entity ID, select **Override** and enter **urn:uri:<idp_id>** in the field.

Note: The <idp_id> value must match the value defined in your domain federation settings. If you have more than one Microsoft service application configured in RSA SecurID Access use the Office 365 <idp_id> value in the override field.

6. Scroll down to the **SAML Response Signature** section.



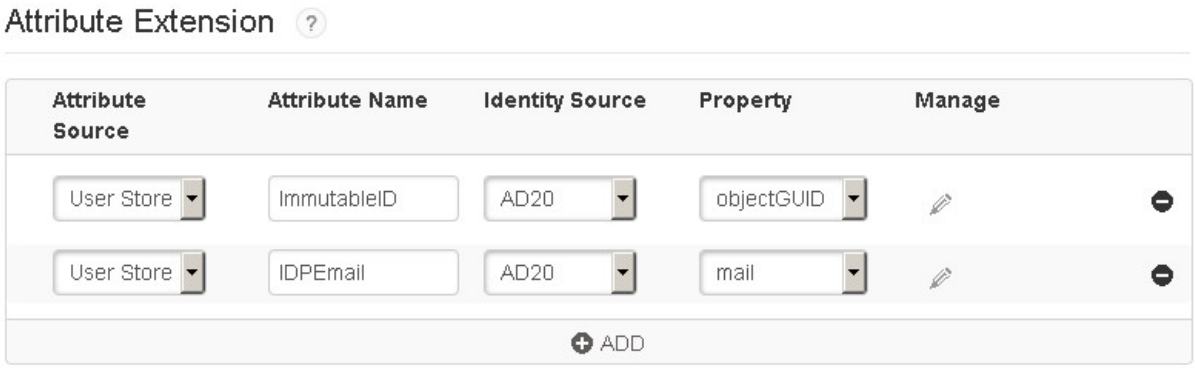
   a. Select **Choose File** and upload the RSA SecurID Access private key.
   b. Select second **Choose File** and upload the RSA SecurID Access public certificate.
   c. Select the check box **Include Certificate in Outgoing Assertion**.
7. Scroll down to the **Service Provider** section.

   a. In the **Assertion Consumer Service (ACS) URL** field enter https://login.microsoftonline.com/login.srf.
   b. In the **Audience (Service Provider Entity ID)** field enter **urn:federation:MicrosoftOnline**.

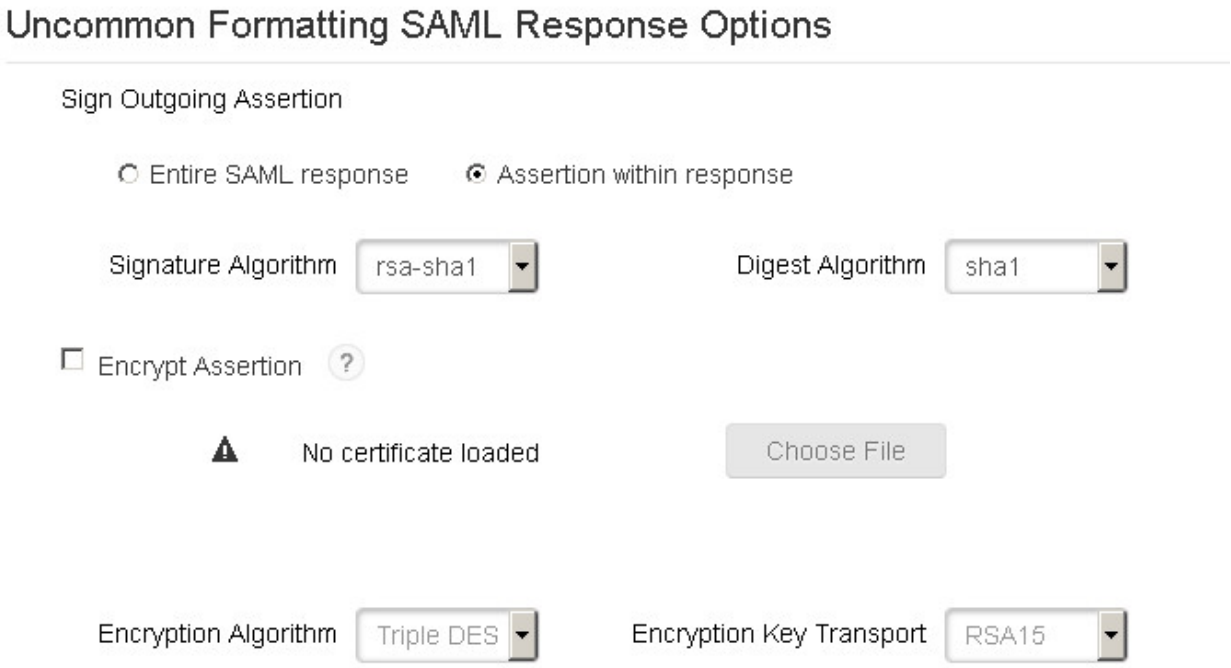
8. Scroll down to **User Identity** section. Set the **Identifier Type** to **persistent** and **Property** to **objectGUID**.

9. Click **Show Advanced Configuration**.

10. Scroll down to **Attribute Extension**.
11. In the **Attribute Name** field, enter **ImmutableID**; and in the **Property** field, enter **objectGUID**.
12. In the **Attribute Name** field, enter **IDPEmail**; and in the **Property** field, enter **mail**.

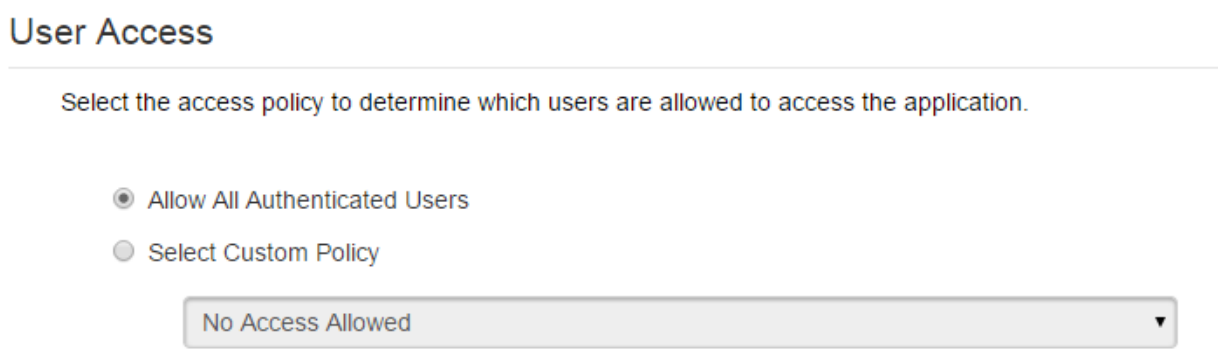


13. Under **Uncommon Formatting SAML Response Options**, select **Assertion within response.**

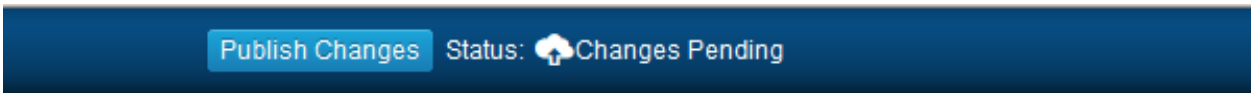


14. Click **Next Step**.

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



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



Next Steps

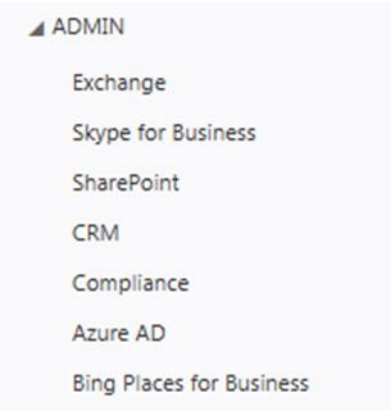
Configure Microsoft Yammer to Use RSA SecurID Access as an Identity Provider

Configure Microsoft Yammer to Use RSA SecurID Access as an Identity Provider

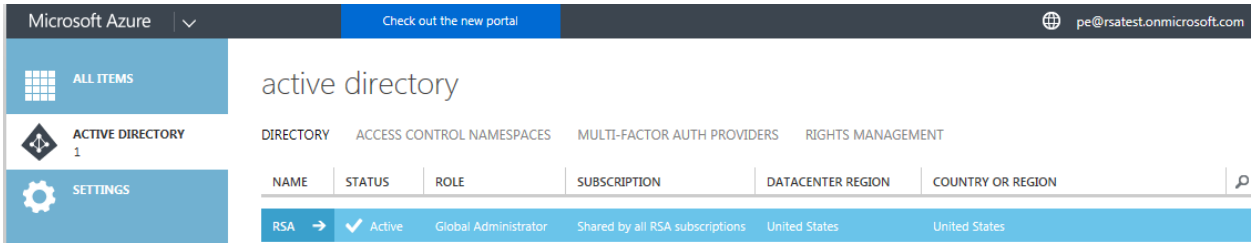
The first time you sign up for a Microsoft cloud service such as Azure, Microsoft Office 365, Microsoft Intune, or Microsoft Yammer you are prompted to provide details about your organization and your organization's Internet domain name registration. This information is then used to create an Azure AD directory instance for your organization. The same Azure AD directory is used to authenticate single sign-on users to multiple Microsoft cloud services.

Verify your federated domain in Microsoft Azure AD

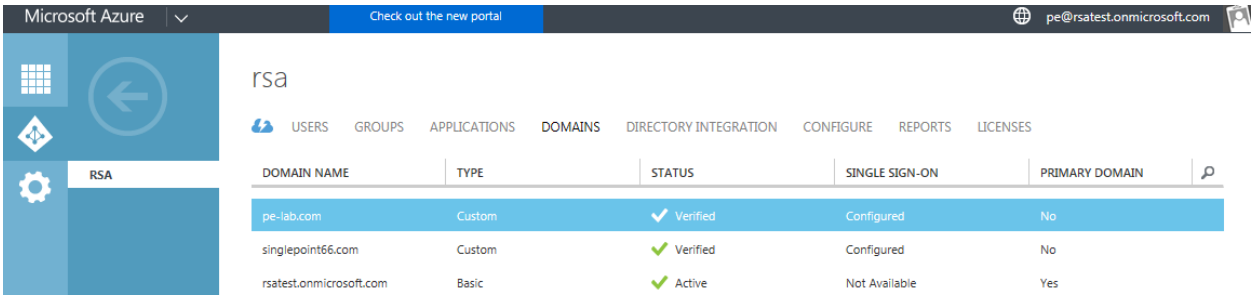
1. Login as an administrator to https://portal.office.com.
2. Under ADMIN in the left menu, select **Azure AD**.



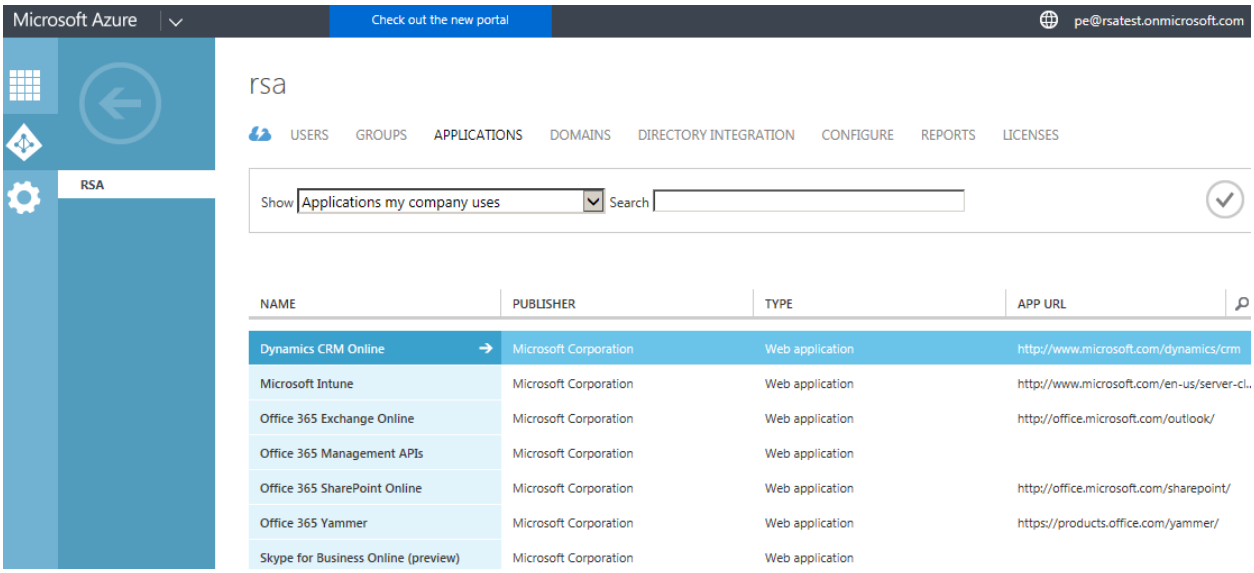
3. Verify your Active Directory status is Active.
4. Click on your directory name.



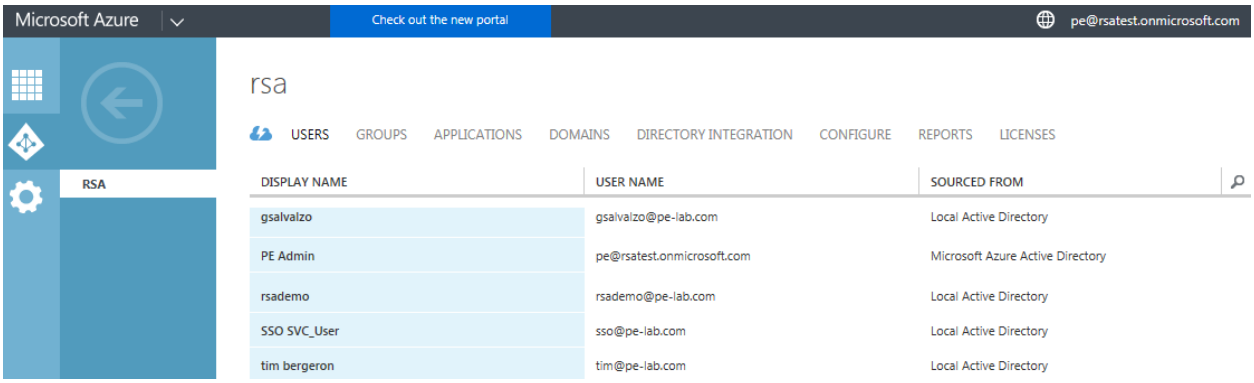
5. Select the **DOMAINS** tab and verify your domain is Active. In this example our single sign-on domain is pe-lab.com.



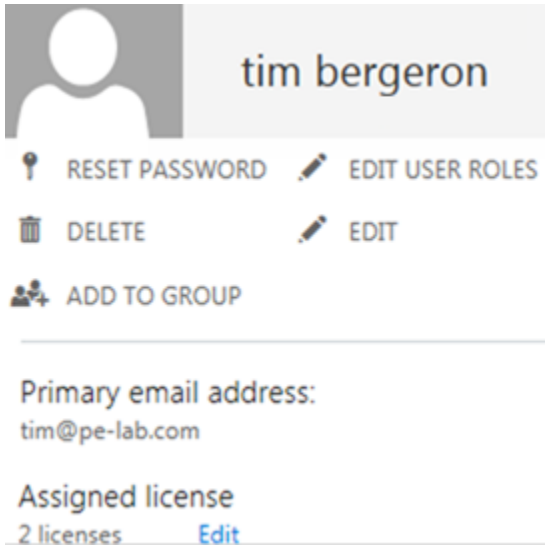
6. Select the **APPLICATIONS** tab and verify that Yammer is present.



7. Select the **USERS** tab and verify that your AD users have been propagated to the cloud service.



8. Return to the Office dashboard and assign a license to the desired users.



GLS