


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*.

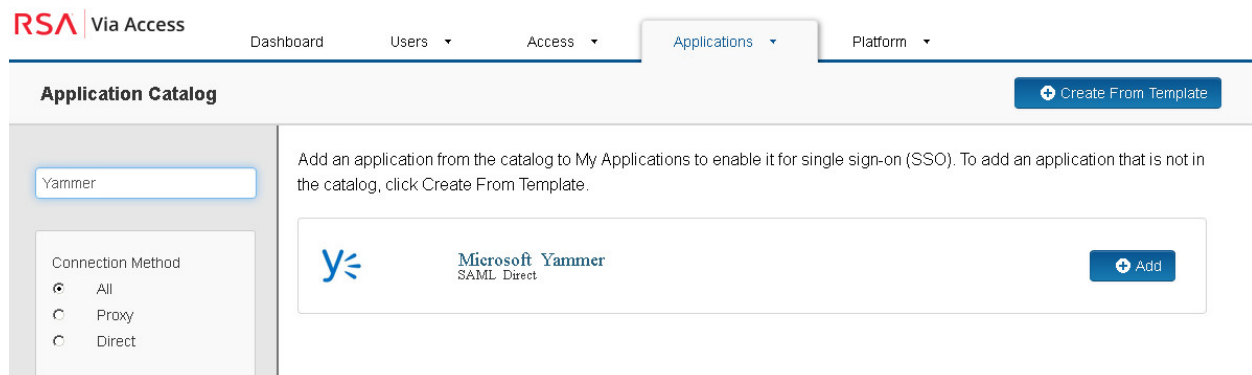
Procedure

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.


Connection URL 

IDP-initiated SP-initiated

Binding Method for SAML Request


Redirect

POST

Signed 

 No certificate loaded

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.

SAML Identity Provider (Issuer)

Identity Provider URL 

Issuer Entity ID 

Default (idp_id): vramptchy9f6

Override

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

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

✓ Private Key Loaded Choose File Generate Cert Bundle ?

✓ Certificate Loaded Choose File

CN= rce_saml, Valid
Until: 08/05/2017

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL

<https://login.microsoftonline.com/login.srf>

Audience (Service Provider Entity ID)

urn:federation:MicrosoftOnline

- 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**.

User Identity

Name ID

Identifier Type

persistent

User Store

PE_AD

Property

objectGUID

⌵ Show Advanced Configuration

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**.

Attribute Extension ?

| Attribute Source | Attribute Name | Identity Source | Property | Manage |
|------------------|----------------|-----------------|------------|--------|
| User Store | ImmutableID | AD20 | objectGUID | |
| User Store | IDPEmail | AD20 | mail | |
| ADD | | | | |

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

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response
 Assertion within response

Signature Algorithm

Digest Algorithm

Encrypt Assertion ?

No certificate loaded

Encryption Algorithm

Encryption Key Transport

14. Click **Next Step**.

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

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 ▼


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.

Publish Changes

Status:  Changes Pending

Next Steps

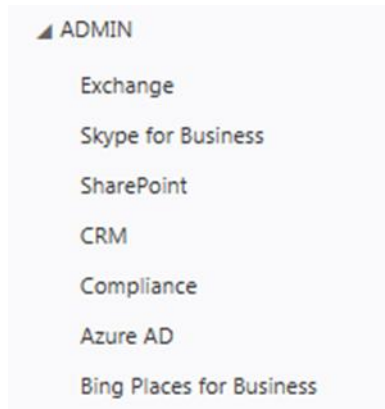
[Configure Microsoft Yammer to Use RSA SecurID Access as an Identity Provider](#)

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

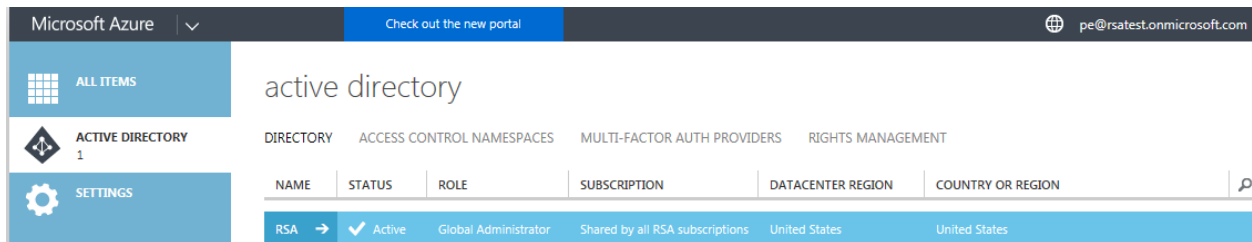
The first time you sign up for a Microsoft cloud service such as Azure, Microsoft Office 365, Microsoft Intune, or Microsoft Yammer you are prompted to provide details about your organization and your organization's Internet domain name registration. This information is then used to create an Azure AD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

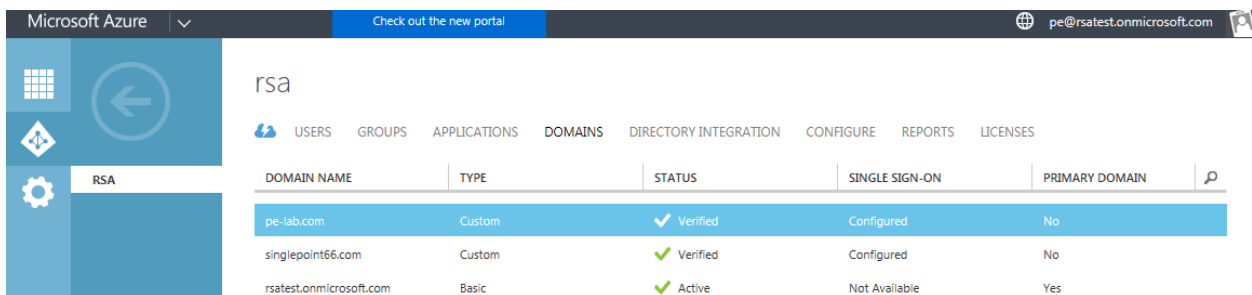
1. Login as an administrator to <https://portal.office.com>.
2. Under ADMIN in the left menu, select **Azure AD**.



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.

The screenshot shows the Microsoft Azure portal interface for the 'rsa' tenant. The 'APPLICATIONS' tab is selected. A search filter is set to 'Applications my company uses'. The following table lists the installed applications:

| NAME | PUBLISHER | TYPE | APP URL |
|-------------------------------------|-----------------------|-----------------|---|
| Dynamics CRM Online | Microsoft Corporation | Web application | http://www.microsoft.com/dynamics/crm |
| Microsoft Intune | Microsoft Corporation | Web application | http://www.microsoft.com/en-us/server-cl. |
| Office 365 Exchange Online | Microsoft Corporation | Web application | http://office.microsoft.com/outlook/ |
| Office 365 Management APIs | Microsoft Corporation | Web application | |
| Office 365 SharePoint Online | Microsoft Corporation | Web application | http://office.microsoft.com/sharepoint/ |
| Office 365 Yammer | Microsoft Corporation | Web application | https://products.office.com/yammer/ |
| Skype for Business Online (preview) | Microsoft Corporation | Web application | |

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

The screenshot shows the Microsoft Azure portal interface for the 'rsa' tenant. The 'USERS' tab is selected. The following table lists the propagated users:

| DISPLAY NAME | USER NAME | SOURCED FROM |
|--------------|----------------------------|----------------------------------|
| gsalvalzo | gsalvalzo@pe-lab.com | Local Active Directory |
| PE Admin | pe@rsatest.onmicrosoft.com | Microsoft Azure Active Directory |
| rsademo | rsademo@pe-lab.com | Local Active Directory |
| SSO SVC_User | sso@pe-lab.com | Local Active Directory |
| tim bergeron | tim@pe-lab.com | Local Active Directory |

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

The screenshot shows the user profile for 'tim bergeron'. The profile includes the following information and actions:

- Actions:** RESET PASSWORD, EDIT USER ROLES, DELETE, EDIT, ADD TO GROUP
- Primary email address:** tim@pe-lab.com
- Assigned license:** 2 licenses (with an Edit link)