RSA SecurID Access SAML Configuration for Microsoft Dynamics CRM Online

Last Modified: March 28, 2016

Microsoft Dynamics CRM Online is a cloud solution for the customer relationship management (CRM) business solution that drives sales productivity and marketing effectiveness through social insights, business intelligence and campaign.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Microsoft Dynamics CRM Online.
- DNS information to register a domain with your DNS provider.
- Install Windows Azure Active Directory Module for Windows Powershell which requires Online Service Sign-In Assistant.
- Install Microsoft Directory Sync tool.

Note: Refer to Microsoft's guidelines for firewall requirements

http://technet.microsoft.com/en-us/library/hh373144.aspx

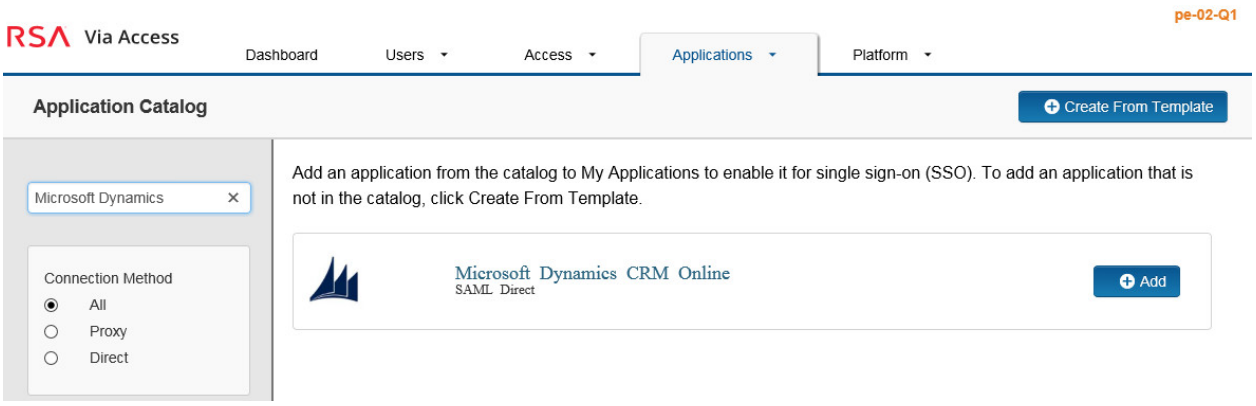
Procedure

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

Add the Application in RSA SecurID Access

Procedure

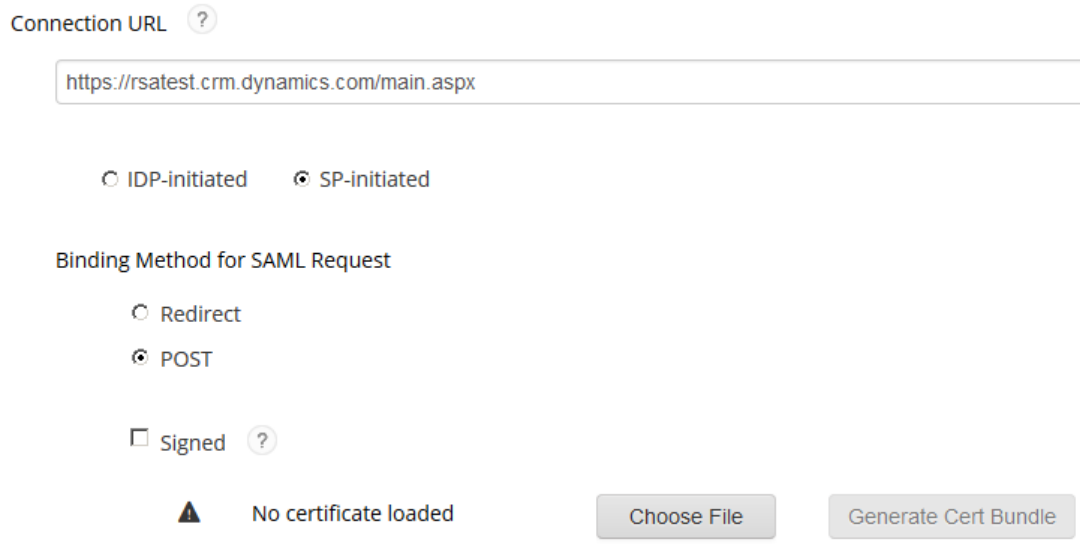
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the application that you wish to add.



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.**

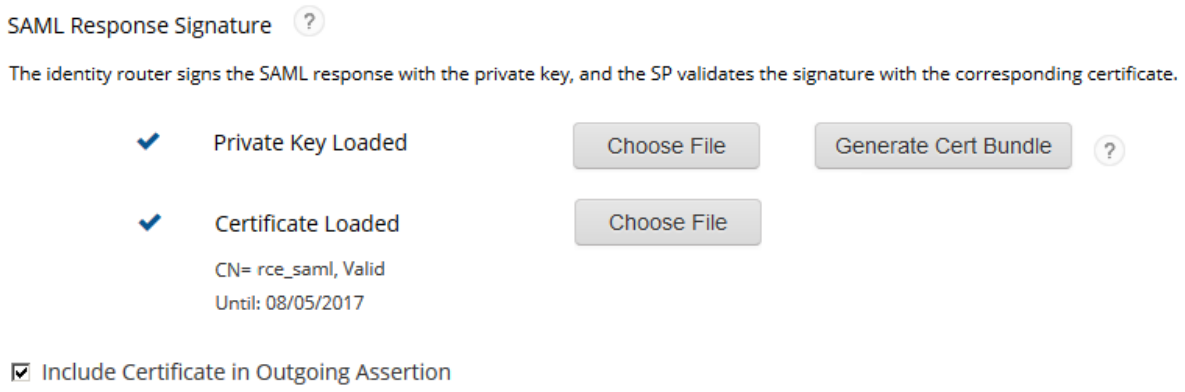
4. Choose **SP -initiated** and replace <org_name> with your Microsoft Services organization name. In this example <org_name> is rsatest.



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 on page 8 step 17 of the 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 **Choose File** and upload the RSA SecurID Access public certificate.
   c. Select the check box **Include Certificate in Outgoing Assertion**.

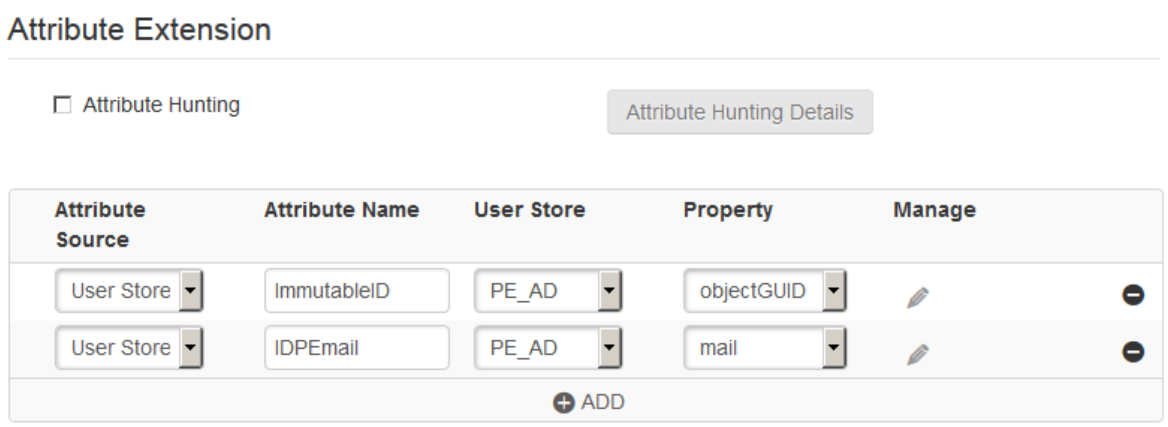
7. Scroll down to the **Service Provider** section.

   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**.

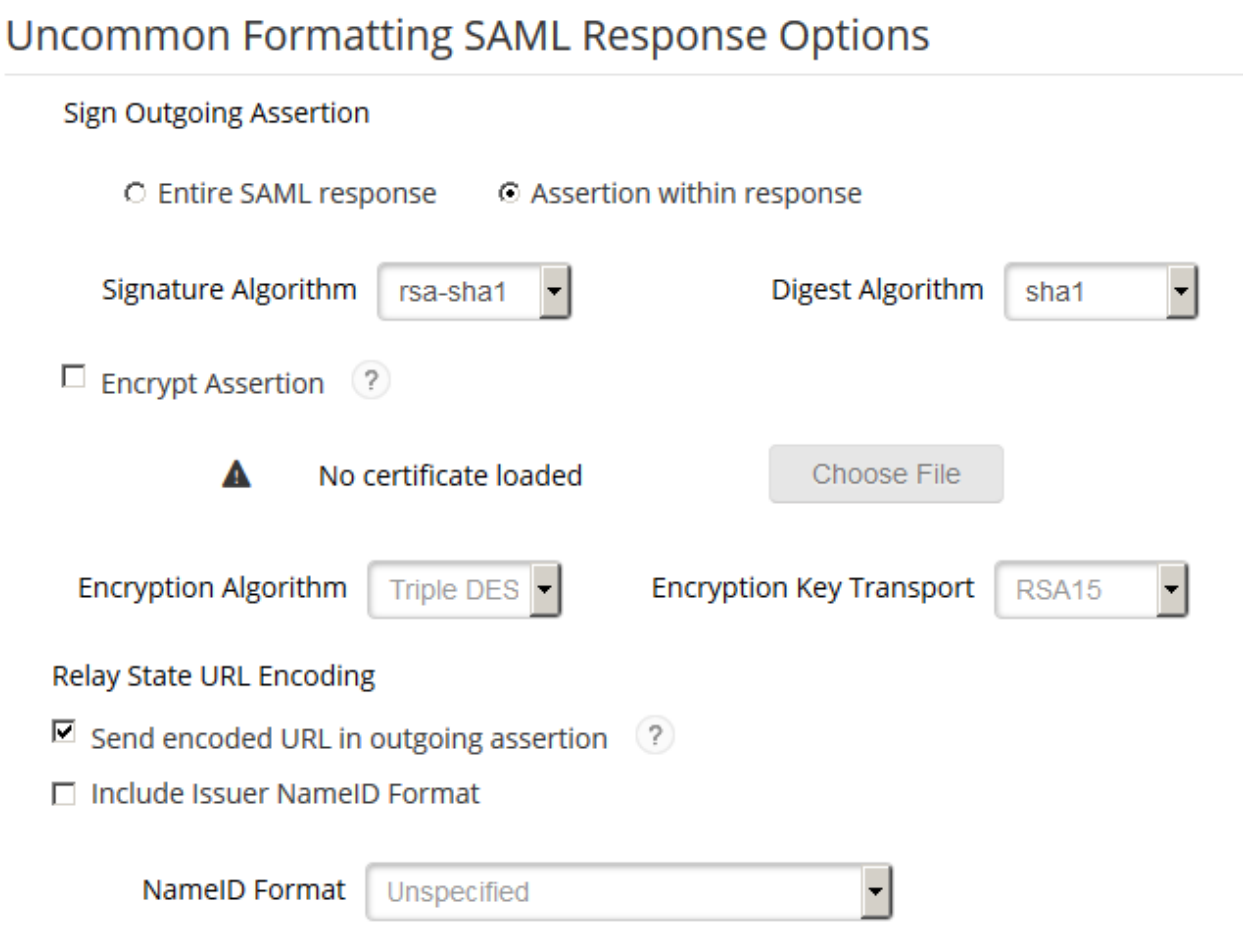
8. Scroll down to **User Identity** section. Set the **Identifier Type** to **persistent** and **Property** to **objectGUID**.

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**.

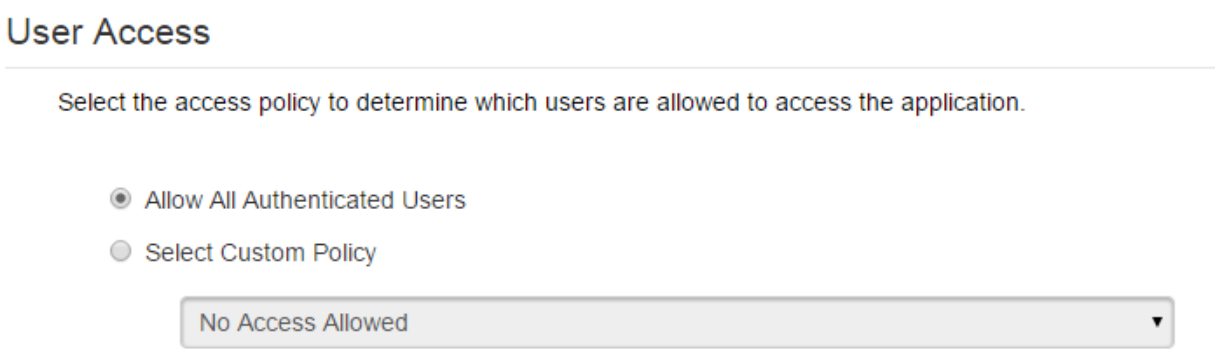


13. Under **Uncommon Formatting SAML Response Options**, select **Assertion within response.**

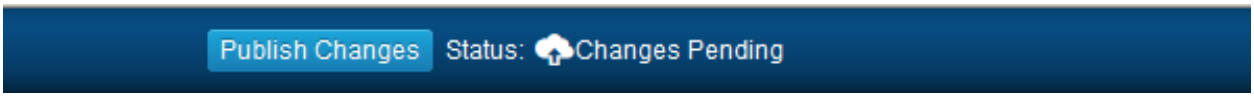


14. Click **Next Step**.

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 Dynamics CRM to Use RSA SecurID Access as an Identity Provider]

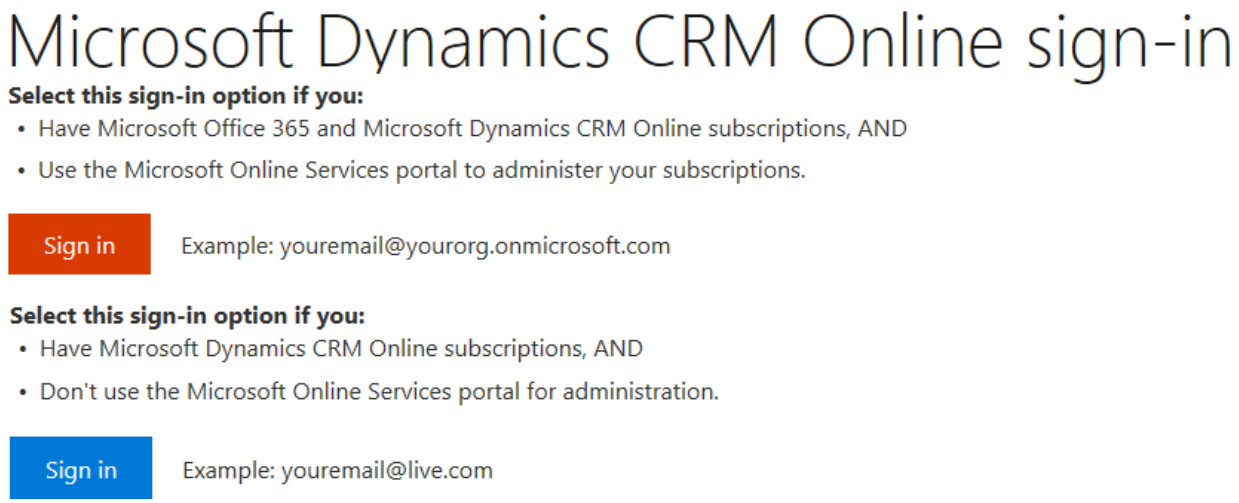
Configure Microsoft Dynamics CRM Online to Use RSA SecurID Access as an Identity Provider

The first time you sign up for a Microsoft cloud service such as Azure, Microsoft Office 365, Microsoft Intune, or Microsoft Dynamics CRM Online 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. Because Microsoft uses the same Azure AD for multiple Microsoft services you may have already completed the steps needed to federate your local AD to your cloud Azure AD instance.

Procedure

1. Sign in to your CRM account. https://www.microsoft.com/en-us/dynamics/crm-login.aspx

> **Note: If you already have Azure AD directory proceed to step 19 on page 9.**



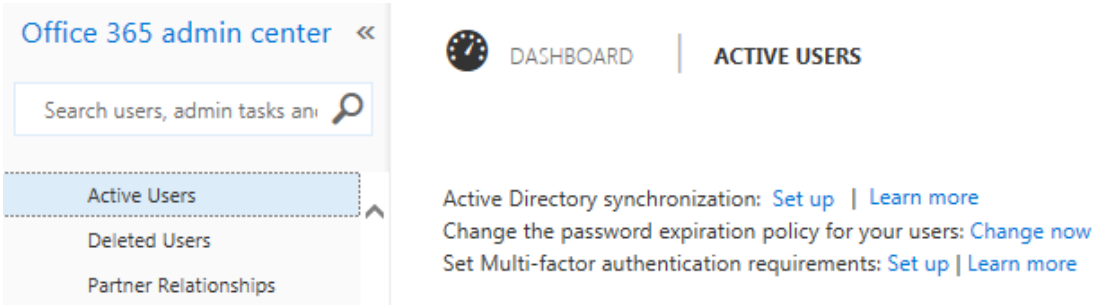
2. Login with an administrator account, from the Office portal select the **Admin** app.
3. From the Office admin center, select **DOMAINS** from the left side menu.
4. Select +**Add domain**.

> **Note: Access to domain registrar is required to set the TXT flag in the host file to allow Microsoft to validate the domain.**

5. Complete the prerequisite steps to enable your domain in Office.

> **Note: Refer to Microsoft TechNet library page "Prepare for single sign-on" for full details.**
> **http://technet.microsoft.com/en-us/library/jj151786**

6. Go to the **USERS > Active Users** and select **Active Directory synchronization: Set up**.



7. Complete the configuration steps and click **Activate**. Synchronization may take up to 24 hours.
8. In the Active Directory synchronization: **Set up**, step 3 has a link to download and install the Directory Sync tool. The Installation process may take up to 20 minutes.
9. From your local Windows server run **Directory Sync**, you will be prompted for your Office admin credentials and your local AD admin credentials. Do not check the hybrid deployment or password sync checkboxes.
10. Click **Next** and **Finish**.
11. Install **Windows Azure Active Directory Module for Windows Powershell**. The install requires Microsoft Online Services Sign-In Assistant for IT Professionals RTW. You will need to restart your server after installing Microsoft Online Services Sign-In Assistant and before installing the Azure AD Module for Windows Powershell.

> **Note: If you are installing the Directory Sync on the same server you must use the version of Microsoft Online Services Sign-In Assistant required by Directory Sync. To avoid a version conflict, install Directory Sync first.**

12. Launch the **Powershell** window and run the cmdlet commands to enable federation.
13. Type **$cred=Get-Credential**.
14. You will be prompted for the Office administrator credentials. The username must be in the format <username>@<org_name>.onmicrosoft.com. The credentials will now be stored in variable **$cred**.

> **Note: Do not login to the Azure Active Module for Windows PowerShell with the domain administrator account for the domain you are enabling federation for. This will lock you out of your Office account if you do not have an administrator account with an @onmicrosoft.com email address.**

15. Type **Connect-MsolService –Credential $cred**.

16. Create the following variables.

$domain = "<your_domain>"
$idpURL = "<IDP_URL_From_RSASecurIDAccess>" see page 2 step 5
$idpID = "<IDP_EntityID_From_RSASecurIDAccess>" Entity ID must be in **urn:uri** format
$logoutURL = "<Your_Portal_logout_URL>" **IE:** *https://portal.yourdomain.com/LogoutServlet*

$cert = "<Full_base64_encoded_value_of_Cert>" or **$certData**

Note: To create **$cert** copy and paste the **cert.pem** file from the certificate bundle downloaded from the RSA SecurID Access administration console. To create **$certData**, follow the 2 step procedure below to create the **$certData**.

First run the command:
$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\temp\saml.crt**")**
where, c:\temp\saml.crt is the path to the RSA SecurID Access certificate.
Next, type:
$certData = [system.convert]::tobase64string($cert.rawdata)

In this example:
$domain = "pe-lab.com"
$idpURL = "https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=o365"
$idpID = "urn:uri:o365"
$logoutURL = "https://pe108.prod0.pe-lab.com"

17. Run the **Set-MsolDomainAuthentication** command.

    Set-MsolDomainAuthentication –DomainName $domain **–FederationBrandName** $domain **-Authentication Federated –PassiveLogonUri** $idpURL **–SigningCertificate** $certData **–IssuerUri** $idpID **-LogOffUri** $logouturl **–PreferredAuthenticationProtocol SAMLP**

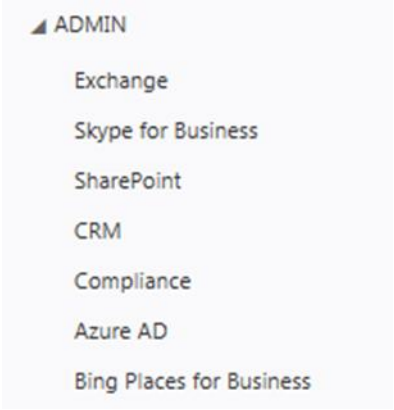
18. Verify your federated settings.

Get-MsolDomain –DomainName $domain | fl *

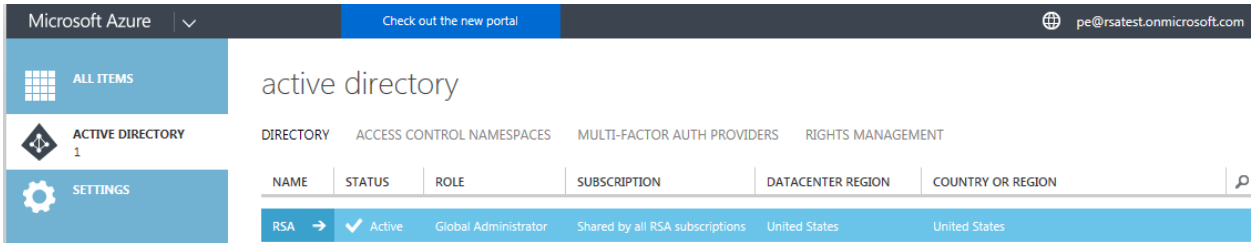
```
PS C:\Users\PARTNER\Desktop> get-MsolDomainFederationSettings -DomainName pe-lab.com : fl *


ExtensionData                             : System.Runtime.Serialization.Extension
                                            DataObject
ActiveLogOnUri                            : http://dummystsurl.microsoftonline.com
                                            /dummyurl
DefaultInteractiveAuthenticationMethod    :
FederationBrandName                       : RSA
IssuerUri                                 : urn:uri:o365
LogOffUri                                 : https://pe108.prod0.pe-lab.com
MetadataExchangeUri                       :
NextSigningCertificate                    :
OpenIdConnectDiscoveryEndpoint            :
PassiveLogOnUri                           : https://pe108.prod0.pe-lab.com/IdPServ
                                            let?idp_id=o365
PreferredAuthenticationProtocol           : Samlp
SigningCertificate                        : MIICrTCCAZUCBgFAT+Rz7TANBgkqhkiG9w0BAQ
                                            sFADAaMRgwFgYDVQQDDA9zYWxlc2ZvcmNlX3Nh
                                            bWwwHhcNMTMwODA1MTkxMTQ2WhcNMTcwODA1MT
                                            kxMTQ2WjAaMRgwFgYDVQQDDA9zYWxlc2ZvcmNl
                                            X3NhbWwwggEiMA0GCSqGSIb3DQEBAQUAA4IBDw
                                            AwggEKAoIBAQC3wyfUcGYvmppZCip8K75T+m3D
                                            xNMCe9fGCkcpZwQS7P3mPIrOfyotRRW0U1+Rck
                                            q/CG53LJy+yythI17MnPb5W19Vy+0SXxk1kGGh
                                            MKC/AfBMX5qrXjXPxNTMkJHC1FfX5uQ3gTi9AW
                                            hk4IEnF6kDEOUAcbvbY0aQpRbMz412SD4jrp5T
                                            zJXLjL4Q+TQaydLchwQ2bE0uC8u9+BLvFH18tB
                                            /qfUIeTu6ezH3+xhEXA5P40gF9cL9SG91DQzsD
                                            5rvezRm4wc5XT4FG+2TopAB32SZmKAg3A16qP7
                                            Foc7547rbNQJbw/HBOTuIgjvzRtbd4HtI1NE1C
                                            diCoYS9N0KqTAgMBAAEwDQYJKoZIhvcNAQELBQ
                                            ADggEBABNJidyVHAFgzzU30kcPymQUDgI70kLj
                                            xaUrwWH8RAqv8XqR/jNa1zFIrf/xwgVqKOgrwP
                                            J+2v6h+zHD5ibWEe8mthSKKnvZrDqTU1lBZzqz
                                            s6w7uG0cS61VPwnz6yb9nT4JjSibLr9SQHPsWE
                                            yYCjee/yelAOsQTEgXB1G8SrvzdpD5d+6upvjP
                                            5ZiwZXR6h2dT020AfvdtmPhCSQqs/q/py5rxkl
                                            trAXx+cNIPHFrXKG+9RWZYnUQzY74c2U34fWHk
                                            FIxZWRIz5L0Pi/ssplG0jVOUAzfcXuHcTqg0v6
                                            msUbf9MYwrcVTw+6X7+a8fgnlJ+e0KDzWbta8R
                                            /To746o=
SupportsMfa                               : False
```

Verify your federated domain in Microsoft Azure AD

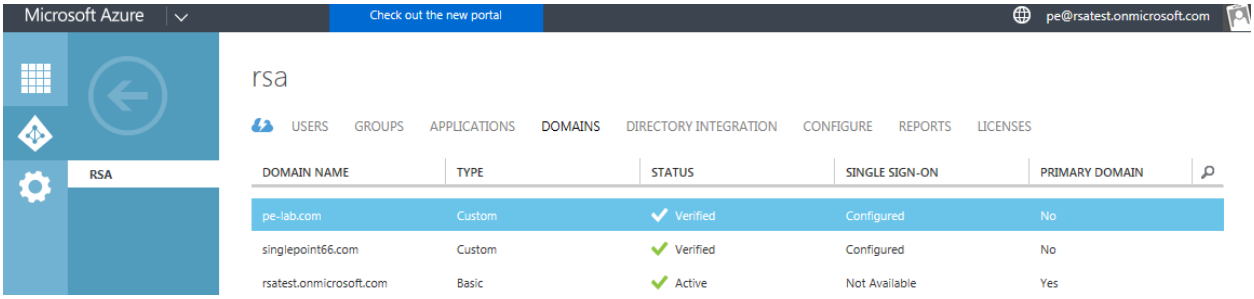
1. Return to the Office portal.
2. Under ADMIN in the left menu, select Azure AD.



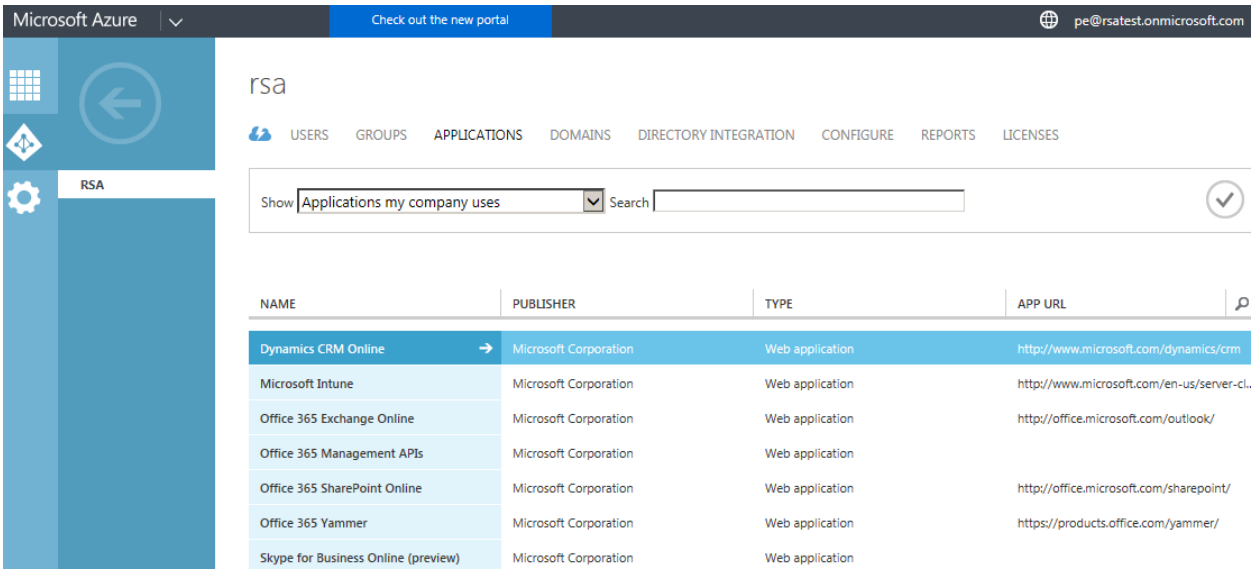
3. Verify your Active Directory status is Active.
4. Click on your directory name.



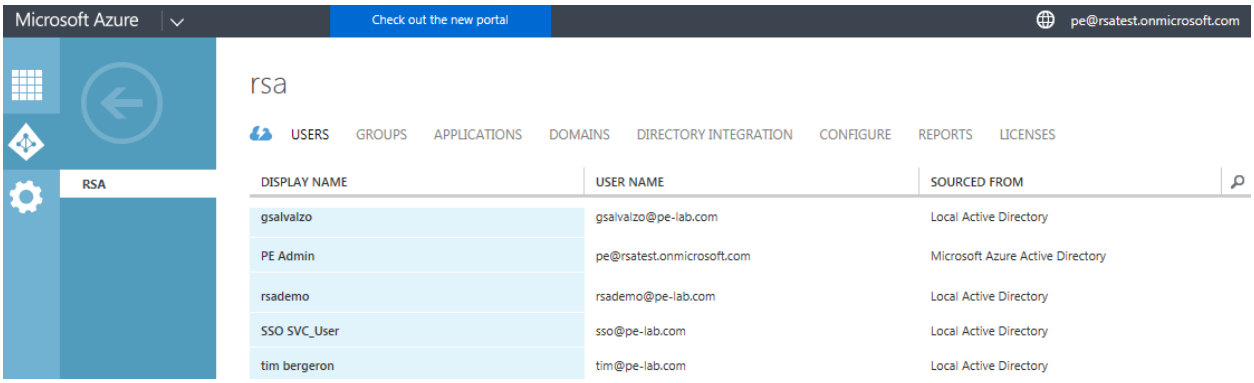
5. Select the **DOMAINS** tab and verify your domain is Active. In this example our single sign-on domain is pe-lab.com.



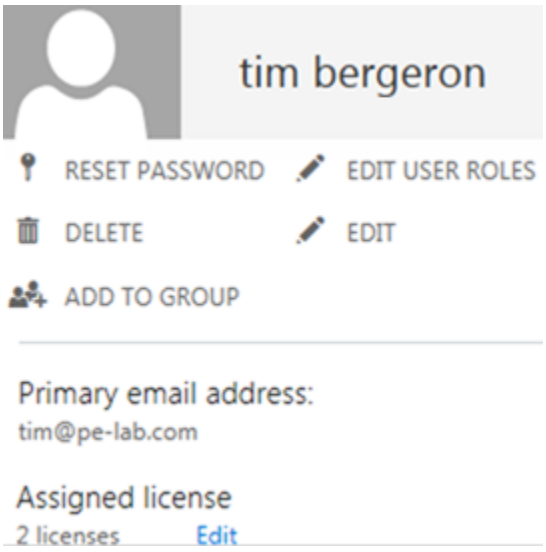
6. Select the **APPLICATIONS** tab and verify that Dynamics CRM Online is present.



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

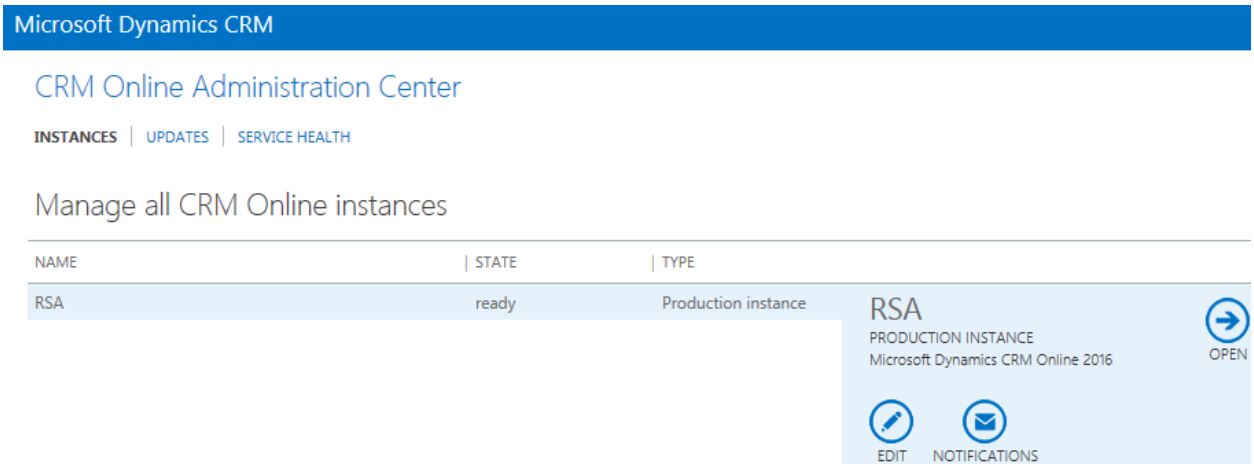


8. Return to the Office dashboard and assign the Microsoft Dynamic CRM Online licenses to the desired users.

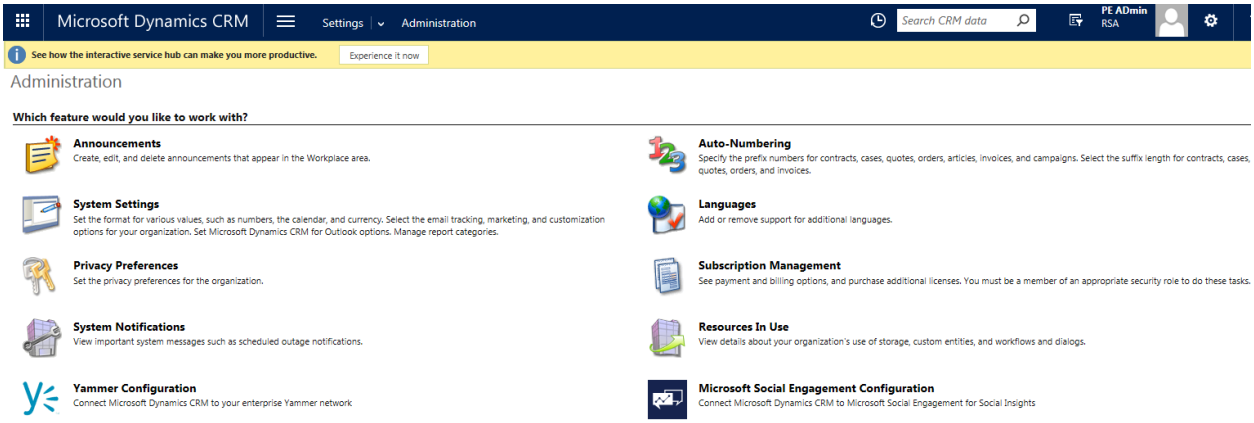


Manage Microsoft Dynamics CRM Online user's roles

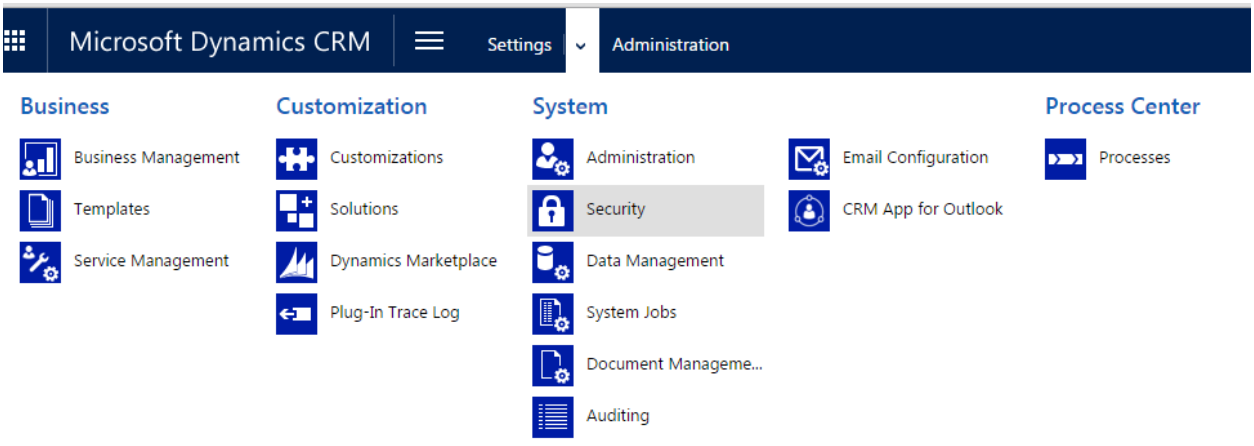
1. From the Office dashboard, select **ADMIN** > **CRM**.
2. On the CRM dashboard, under **Manage all CRM Online instances** select **OPEN**.



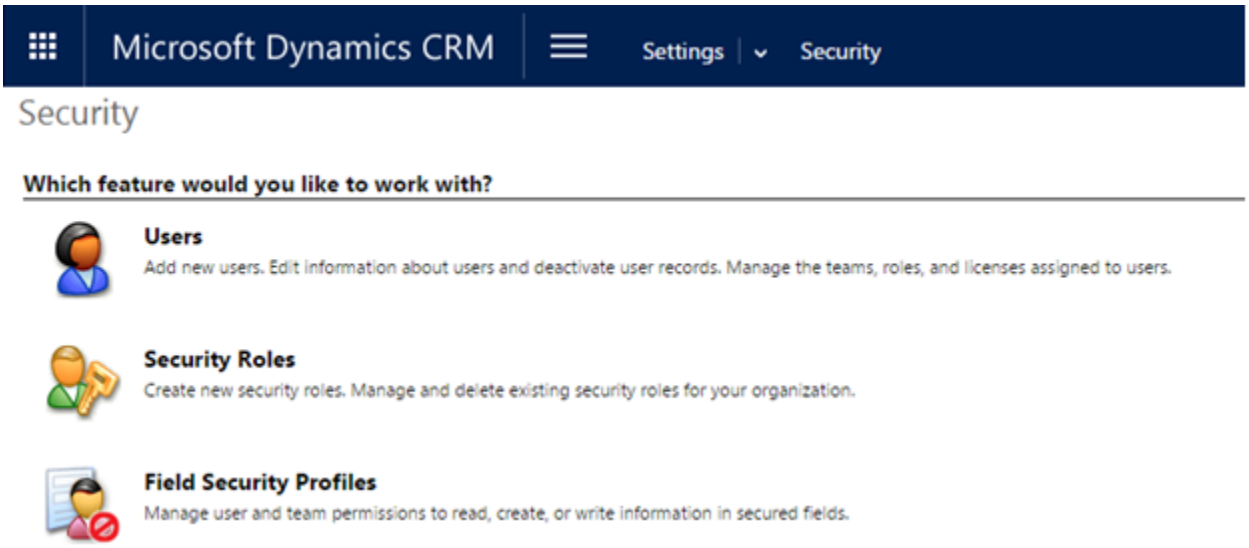
3. The Administration dashboard will open.



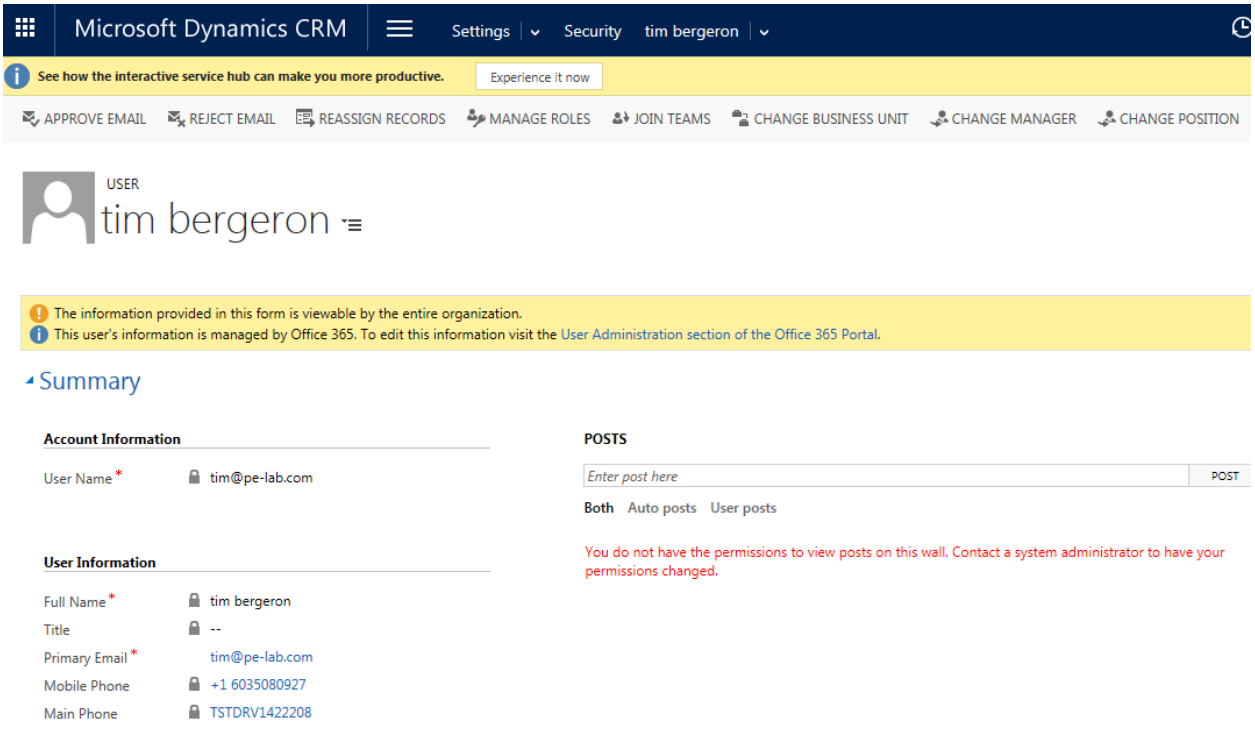
4. Select **Settings > Security**.



5. Select **Users**.



6. If you wish to modify the user's roles, select the user's name from the Enabled Users list.



GLS