

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>

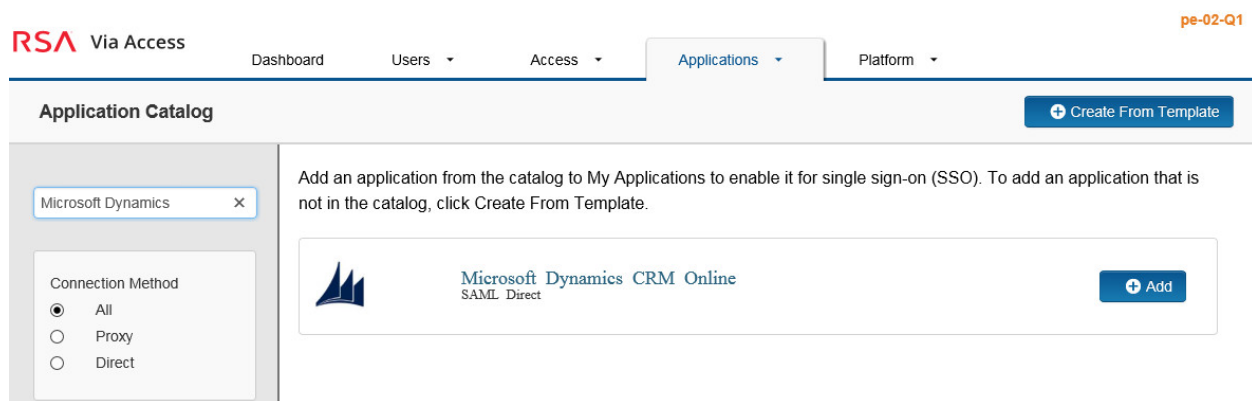
Procedure

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.




The screenshot shows the RSA SecurID Access Administration Console interface. At the top, there is a navigation bar with 'RSA Via Access' and tabs for 'Dashboard', 'Users', 'Access', 'Applications', and 'Platform'. The 'Applications' tab is selected. Below the navigation bar, the 'Application Catalog' section is visible. On the left, there is a search box containing 'Microsoft Dynamics' and a 'Connection Method' section with radio buttons for 'All' (selected), 'Proxy', and 'Direct'. On the right, there is a card for 'Microsoft Dynamics CRM Online SAML Direct' with a blue '+ Add' button. Above the card, there is a text instruction: 'Add an application from the catalog to My Applications to enable it for single sign-on (SSO). To add an application that is not in the catalog, click Create From Template.' A 'Create From Template' button is also visible in the top right of the catalog area.

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.


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 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.

SAML Identity Provider (Issuer)

Identity Provider URL 

Issuer Entity ID 

Default (idp_id): crm

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 **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 Hunting Attribute Hunting Details

Attribute Source	Attribute Name	User Store	Property	Manage
User Store	ImmutableID	PE_AD	objectGUID	
User Store	IDPEmail	PE_AD	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

Relay State URL Encoding

Send encoded URL in outgoing assertion

Include Issuer NameID Format

NameID Format

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 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.

Microsoft Dynamics CRM Online sign-in

Select this sign-in option if you:

- Have Microsoft Office 365 and Microsoft Dynamics CRM Online subscriptions, AND
- Use the Microsoft Online Services portal to administer your subscriptions.

Sign in

Example: youremail@yourorg.onmicrosoft.com

Select this sign-in option if you:

- Have Microsoft Dynamics CRM Online subscriptions, AND
- Don't use the Microsoft Online Services portal for administration.

Sign in

Example: youremail@live.com

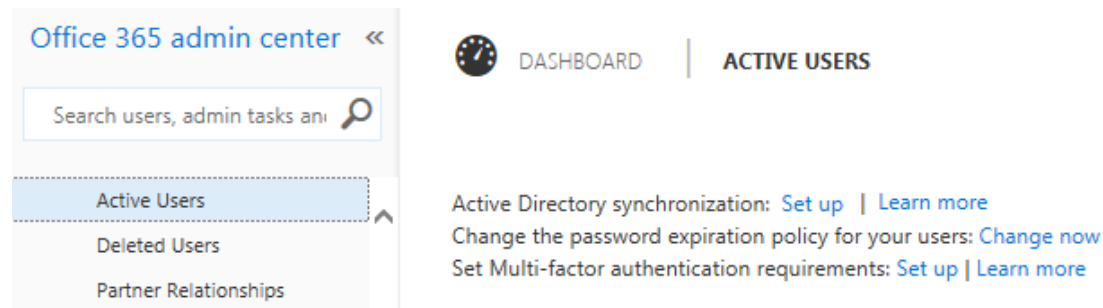
2. Login with an administrator account, from the Office portal select the **Admin** app.
3. From the Office admin center, select **DOMAINS** from the left side menu.
4. Select **+Add domain**.

 **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.

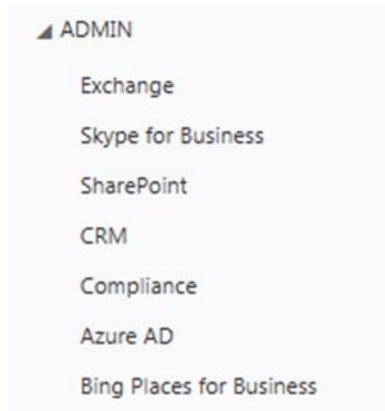
Get-MSolDomain -DomainName \$domain | fl *

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

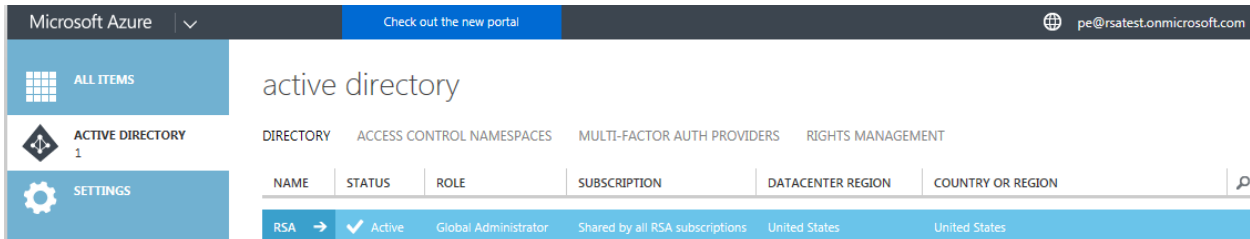
```
ExtensionData           : System.Runtime.Serialization.Extension
                          : DataObject
ActiveLogOnUri          : http://dummysturl.microsoftonline.com
                          : /dummyurl
DefaultInteractiveAuthenticationMethod :
FederationBrandName     : RSA
IssuerUri               : 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      : MII CrTCCA ZUCB gFAT +Rz7TANBgkqhkiG9w0BAQ
                          : sFADAaMRgwFgYDUQDDA9zYWxl c2Zvc mN1X3Nh
                          : bWwHhcNMTMwODA1MTkxMTQ2WhcNMTcwODA1MT
                          : kxMTQ2WjAaMRgwFgYDUQDDA9zYWxl c2Zvc mN1
                          : X3NhbWwggEiMA0GCSqGSI b3DQEBAQUAA4I BDw
                          : AwggEK Ao IBAQC3wyfUcGYvmp pZCip8K75T+m3D
                          : xNMCe9fGCkc pZwQs7P3mPI rOf yo tRRW0U1+Rc k
                          : q/CG53LJy+yythi17Mn Pb5W19Uy+0SXxk1kGGh
                          : MKC/Af BMX5qrXjX PxNTMk JHC1FFX5uQ3gTi9AW
                          : hk4I EnF6kDEOUAc bvbY0aQpRbMz412SD4jrp5T
                          : zJXLjL4Q+TQaydLc hwQ2bE0u C8u9+BLvFH18tB
                          : /qfUIeTu6ezH3+xhEXA5P40gP9cL9SG91DQzsD
                          : 5rvezRm4wc5XT4FG+2TopAB32SZmKAq3A16gP7
                          : Foc7547rbNQJbw/HBOTuI g jvzRt hd4Ht I LNE1C
                          : diCoYS9N0KqTAgMBAAEwDQYJKoZI hvcNAQELBQ
                          : ADggEBABNJ idyUHA FgzzU30kc PymQU DgI70kLj
                          : xaUrwWH8RAqv8XqR/ jNa1zFl rf/xwgUgK0grwP
                          : J+2v6h+zHD5 ibWEe8mt hSKKrvZrDqTU1LBZzgz
                          : s6w7uG0cS61UPwnz6yb9nT4Jjs ibLr9SQHPsWE
                          : yYCjee/ye1A0sQT EgXB1G8SrvzdpD5d+6upv jP
                          : 5ZiwZXR6h2dT020Afv dtmPhCSQqs/q/py5rxk1
                          : trAXx+cNI PHFrXKG+9RWZYnUQzY74c2U34fWHk
                          : FIxZWRIz5L0Pi/s sp1G0jU0UAzfcXuHcTgg0v6
                          : msUbf9MYwrcUTw+6X7+a8f gn lJ+e0KDzWbta8R
                          : /To746o=
SupportsMfa            : False
```

Verify your federated domain in Microsoft Azure AD

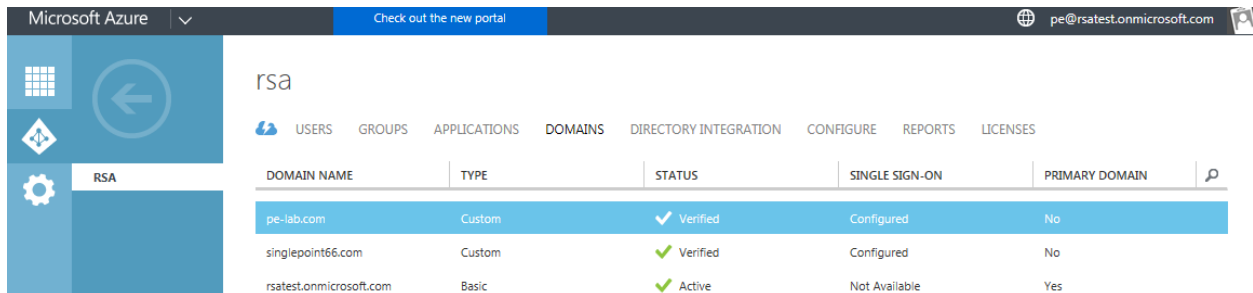
1. Return to the Office portal.
2. Under ADMIN in the left menu, select Azure AD.



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.

The screenshot shows the Microsoft Azure portal interface for a tenant named 'rsa'. The 'APPLICATIONS' tab is selected, displaying a list of installed applications. The 'Dynamics CRM Online' application is highlighted with a blue background and a right-pointing arrow.

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, with the 'USERS' tab selected. A table lists the users that have been propagated to the cloud service.

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 the Microsoft Dynamic CRM Online licenses to the desired users.

The screenshot shows the user profile page for 'tim bergeron'. The user's name is displayed next to a placeholder profile picture. Below the name are several management options: 'RESET PASSWORD', 'EDIT USER ROLES', 'DELETE', 'EDIT', and 'ADD TO GROUP'. At the bottom, the 'Assigned license' section indicates that the user has '2 licenses' assigned, with an 'Edit' link next to it.

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**.

Microsoft Dynamics CRM

CRM Online Administration Center

INSTANCES | UPDATES | SERVICE HEALTH

Manage all CRM Online instances

NAME	STATE	TYPE
RSA	ready	Production instance

RSA
PRODUCTION INSTANCE
Microsoft Dynamics CRM Online 2016

EDIT NOTIFICATIONS OPEN

3. The Administration dashboard will open.

Microsoft Dynamics CRM Settings Administration

Search CRM data

PE Admin RSA

Administration

Which feature would you like to work with?

- Announcements**
Create, edit, and delete announcements that appear in the Workplace area.
- System Settings**
Set the format for various values, such as numbers, the calendar, and currency. Select the email tracking, marketing, and customization options for your organization. Set Microsoft Dynamics CRM for Outlook options. Manage report categories.
- Privacy Preferences**
Set the privacy preferences for the organization.
- System Notifications**
View important system messages such as scheduled outage notifications.
- Yammer Configuration**
Connect Microsoft Dynamics CRM to your enterprise Yammer network.
- Auto-Numbering**
Specify the prefix numbers for contracts, cases, quotes, orders, articles, invoices, and campaigns. Select the suffix length for contracts, cases, quotes, orders, and invoices.
- Languages**
Add or remove support for additional languages.
- Subscription Management**
See payment and billing options, and purchase additional licenses. You must be a member of an appropriate security role to do these tasks.
- Resources In Use**
View details about your organization's use of storage, custom entities, and workflows and dialogs.
- Microsoft Social Engagement Configuration**
Connect Microsoft Dynamics CRM to Microsoft Social Engagement for Social Insights.

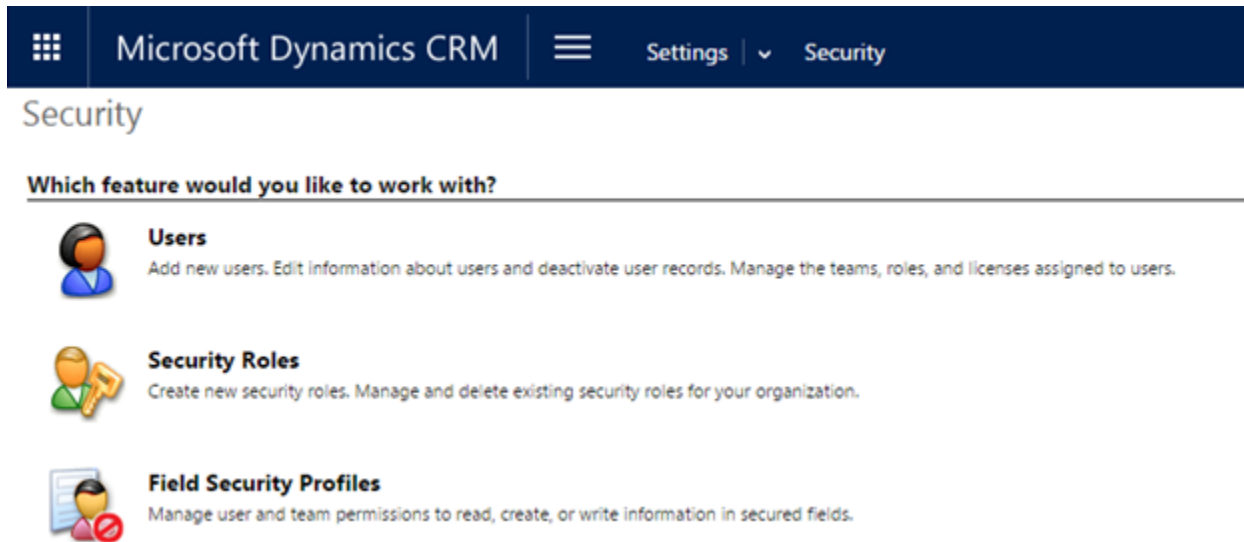
4. Select **Settings > Security**.

Microsoft Dynamics CRM Settings Administration

Business Customization System Process Center

- Business Management
- Templates
- Service Management
- Customizations
- Solutions
- Dynamics Marketplace
- Plug-In Trace Log
- Administration
- Security
- Data Management
- System Jobs
- Document Manage...
- Auditing
- Email Configuration
- CRM App for Outlook
- Processes

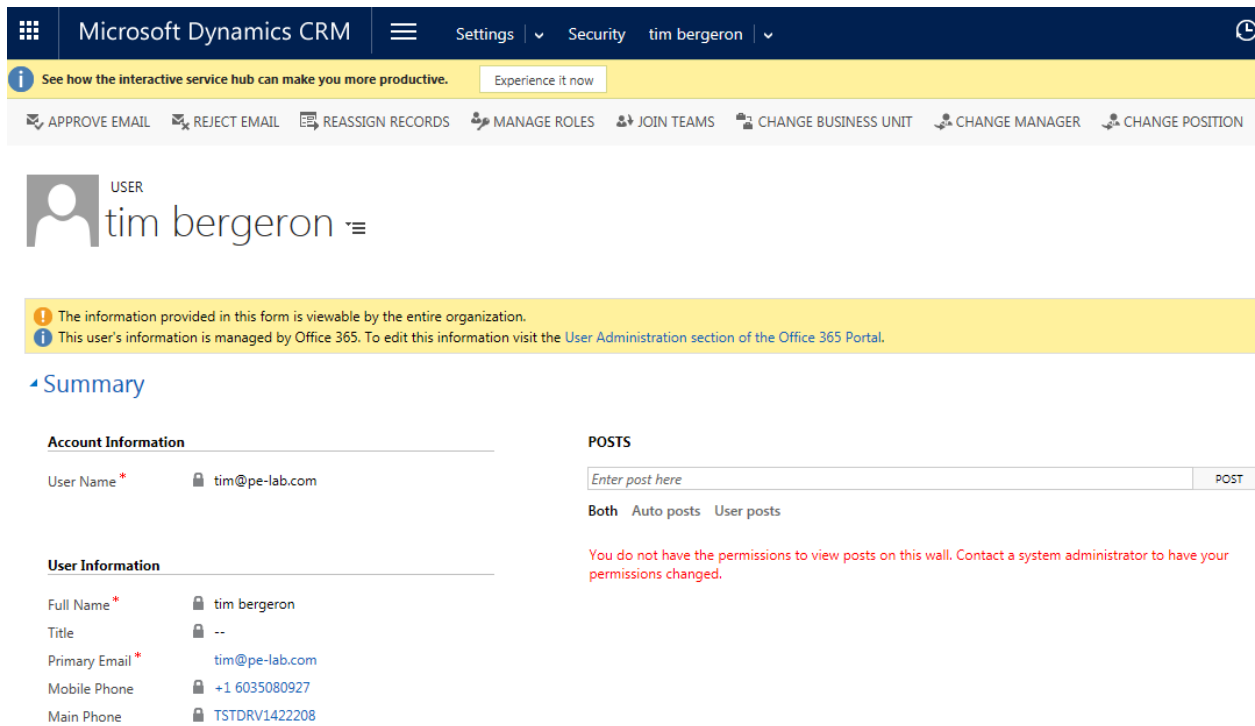
5. Select **Users**.



The screenshot shows the Microsoft Dynamics CRM interface. At the top, there is a dark blue header with the Microsoft Dynamics CRM logo, a hamburger menu icon, and the text "Settings" and "Security". Below the header, the word "Security" is displayed in a large font. Underneath, there is a section titled "Which feature would you like to work with?". This section contains three options, each with an icon and a brief description:

- Users**: Add new users. Edit information about users and deactivate user records. Manage the teams, roles, and licenses assigned to users.
- Security Roles**: Create new security roles. Manage and delete existing security roles for your organization.
- Field Security Profiles**: Manage user and team permissions to read, create, or write information in secured fields.

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



The screenshot shows the Microsoft Dynamics CRM user profile page for "tim bergeron". The page has a dark blue header with the Microsoft Dynamics CRM logo, a hamburger menu icon, and the text "Settings", "Security", and "tim bergeron". Below the header, there is a yellow banner with the text "See how the interactive service hub can make you more productive." and a button "Experience it now". Below the banner, there is a navigation bar with several options: APPROVE EMAIL, REJECT EMAIL, REASSIGN RECORDS, MANAGE ROLES, JOIN TEAMS, CHANGE BUSINESS UNIT, CHANGE MANAGER, and CHANGE POSITION. Below the navigation bar, there is a user profile card for "tim bergeron" with a "USER" label and a hamburger menu icon. Below the user profile card, there is a yellow banner with two warning messages:

- The information provided in this form is viewable by the entire organization.
- This user's information is managed by Office 365. To edit this information visit the [User Administration](#) section of the Office 365 Portal.

Below the banner, there is a section titled "Summary". This section is divided into two columns:

- Account Information**:
 - User Name*: tim@pe-lab.com
- User Information**:
 - Full Name*: tim bergeron
 - Title: --
 - Primary Email*: tim@pe-lab.com
 - Mobile Phone: +1 6035080927
 - Main Phone: TSTDRV1422208
- POSTS**:
 - Enter post here [POST]
 - Both Auto posts User posts
 - You do not have the permissions to view posts on this wall. Contact a system administrator to have your permissions changed.