How-To Guide:

Configure Okta Single Sign-On (SSO) for Microsoft Dynamics On-Premises

Use Case: Configure Dynamics On-Premises WS-Fed claims-based authentication via Okta

Dynamics (On-Premises) can be configured to use claims-based authentication to authenticate both internal users and to enable access for external users not using VPN.

Claims-based authentication relies on a trust established between a Relying Party—which can be an application like Dynamics On-Premises—and a Trusted Claims Provider or Trusted Issuer like Okta. A user authenticates to an Identity Provider (Okta). The Identity Provider issues a claim containing information about the user. These claims are called "assertions." The Relying Party (Dynamics On-Premises) will allow or deny access based on the information contained within the claim.

A key benefit of using claims-based authentication is the user never needs to provide credentials (user name/password) to the application, but rather, access is based on an established trust between the RP and trusted claims provider and issued claim.

This guide outlines how to configure Microsoft Dynamics On-Premises for SSO via Okta. By following the procedures in this guide, you can replace your Microsoft ADFS infrastructure with Okta for claims-based authentication to Microsoft Dynamics On-Premises.

Note: This guide applies to both Dynamics On-Premises and Dynamics CRM 2016. CRM/Dynamics SDK integration is out of scope for this guide.

Assumptions

- Claims-based authentication and IFD have already been configured with another security token service (i.e. ADFS)
- Users accessing Microsoft Dynamics On-Premises have been created/provisioned within Okta
- User's Okta profile of first name, last name and login match the Microsoft Dynamics On-Premises profile
- Microsoft Dynamics On-Premises users are not provisioned by Okta but are managed by the Microsoft Dynamics admin

Integration Overview

Step 1: Create an Okta Integration Network (OIN) app using the WS-Fed template

Configure Okta with the appropriate Microsoft Dynamics On-Premises application URLs, NameID format and user attributes as well as generate the metadata file and certificate needed by Microsoft Dynamics.

Step 2: Configure Microsoft Dynamics On-Premises for SSO with Okta

Replace ADFS with Okta as the trusted claims provider/ trusted issuer.

Step 3: Configure Microsoft Dynamics On-Premises with Okta as a trusted claims provider/trusted issuer

Add the Okta certificate to the Microsoft Dynamics database.

Step 4: Configure Okta Bookmark app

Create an OIN Bookmark app in Okta that will appear as a chiclet on assigned user's Okta organization homepage.

Step 5: Assign WS-Fed and Okta Bookmark OIN apps

Assign both the WS-Fed and Okta Bookmark OIN apps to allow users access to Microsoft Dynamics On-Premises.

Step 1: Create an Okta Integration Network (OIN) app using the WS-Fed template

In this step of the guide, we will be configuring Okta with the appropriate Microsoft Dynamics On-Premises application URLs, NameID format and user attributes as well as generating the metadata file and certificate needed by Microsoft Dynamics.

1. From the Admin app for your Okta Org, navigate to **Applications>Applications** and click **Add Application** in the top left
2. In the top left search field, type **WS-Fed** and then choose **Template WS-Fed** by clicking **Add**
3. Fill out the following fields, replacing the italicized text with the information specific to your environment:

Field	Value	Notes
Application Label	e.g. Dynamics On-Prem	
Web Application URL	*https://ifd.atkoice.com*	Discovery Web Service Domain URL specified during IFD setup
Realm	https://*ifd.atkoice.com/*	Discovery Web Service Domain URL specified during IFD setup ***Note: Trailing Forward Slash***
ReplyTo URL	https://*ifd.atkoice.com*	Discovery Web Service Domain URL specified during IFD setup
Allow ReplyTo Override	Not selected	
NameID Format	EmailAddress	
Audience Restriction	https://*ifd.atkoice.com*	Discovery Web Service Domain URL specified during IFD setup
Assertion Authentication Context	PasswordProtectedTransport	
Group Attribute Value	WindowsDomainQualifiedName	
Group Attribute Name (Optional)	N/A	Dynamics does not use groups for claims-based access You can accept the default: http://schemas.microsoft.com/ws/2008/06/identity/claims/role
Group Filter	N/A	Dynamics does not use groups for claims-based access
Username Attribute Statements	None	
Custom Attribute Statements	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upnluser.login	***Note: Pipe 'I' between upn and user.login*** Ensure the Okta User Login matches the expected login when the user was added to CRM/Dynamics (i.e. a.user01@acmepartners.com)

Field	Value	Notes
Application Visibility—do not display application icon to users	Checked	
Application Visibility—do not display application icon in the Okta Mobile app	Checked	
Provisioning	Unchecked	
Auto-launch	Unchecked	

Step 2: Configure Microsoft Dynamics On-Premises for SSO with Okta

In this step of the guide, we will be replacing ADFS with Okta as the trusted claims provider/trusted issuer.

Okta WS-Fed OIN app

1. From the properties of your OIN app, click the **Sign On** tab
2. Within the **Settings** section, right-mouse click the **Identity Provider Metadata** hyperlink and choose **Copy Link Address**
3. Next, click the **Setup Instructions** button, which will open another tab in your browser
4. Right-mouse click on the hyperlink labeled **Download Certificate** and save the Okta certificate locally on the Dynamics Server:
    a. example. C:\Tools

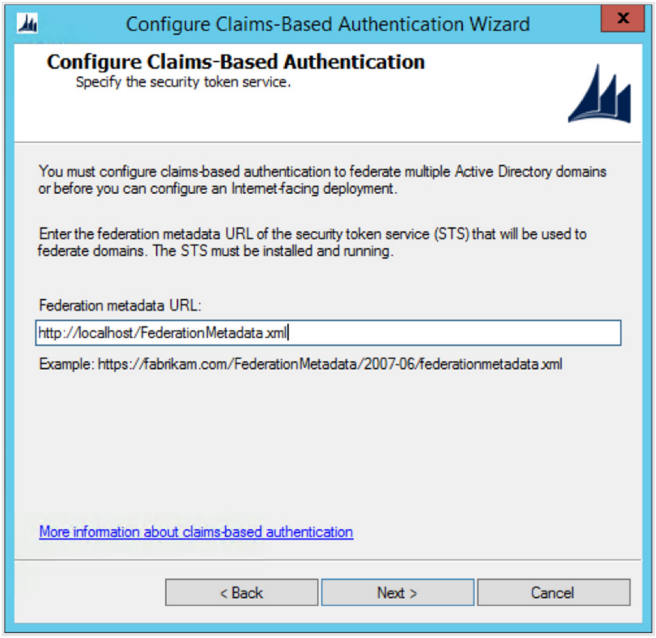
Microsoft Dynamics—Remove existing internet-facing deployment (IFD) and claims-based authentication configurations

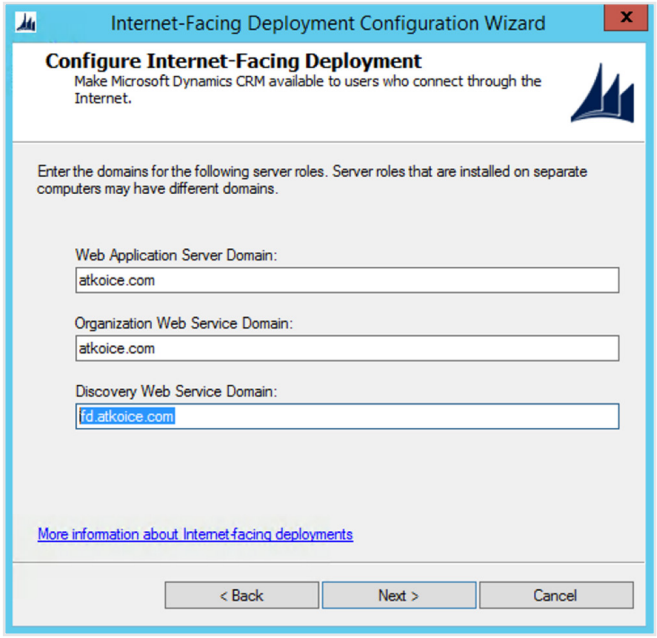
1. On the Microsoft Dynamics server, start the Deployment Manager
2. In the right pane, choose **Disable Internet-Facing Deployment** and from an Administrative Command Prompt type ***iisreset***
3. Return to the Deployment Manager, and in the right pane choose **Disable Claims-Based Authentication** and from an Administrative Command Prompt type ***iisreset***

Note: Resetting IIS after each change should help minimize the chance of any unexpected errors when configuring SSO with Okta

Microsoft Dynamics—Configure claims-based authentication

1. On the Microsoft Dynamics server, start the Deployment Manager
2. In the Deployment Manager console tree, click **Microsoft Dynamics**, and then in the right pane, click **Configure Claims-Based Authentication**
3. Review the contents of the page, and then click **Next >**
4. On the **Specify the security token service** page, enter the Okta federation metadata URL previously copied and click **Next >**
5. On the **Specify the encryption certificate** page, click **Select...** and choose the certificate previously used when configuring claims-based authentication and click **Next >**
6. Review the results on the **System Checks** page, resolve any issues (as-needed); otherwise click “Next >”
    a. Note: Microsoft does not support TLS1.2 out of the box. If you receive an error stating the metadata URL is inaccessible, perform the following steps:
        ii. Download the metadata file by clicking the link on the OIN app setup page
        iii. Copy the file to the CRMWeb Directory (i.e. C:\Program Files\Microsoft Dynamics CRM\CRMWeb)
        iv. Use http://localhost/FederationMetadata.xml or https://localhost/FederationMetadata.xml; based on your available IIS bindings

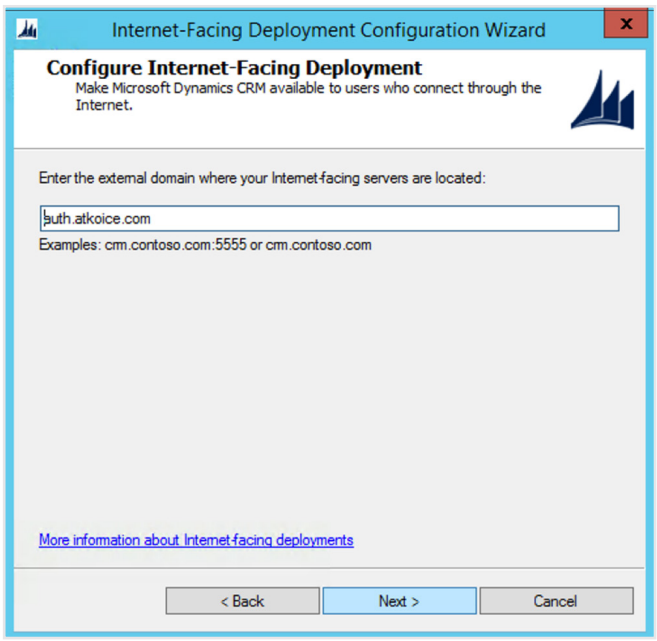




7. On the **Review your selections and then click Apply** tab, click **Apply** and then click **Finish**

Microsoft Dynamics—Configure internet-facing deployment (IFD)

1. On the Microsoft Dynamics server, start the Deployment Manager
2. In the Deployment Manager console tree, click **Microsoft Dynamics**, and then in the right pane, click **Configure Internet-Facing Deployment**
3. Review the contents of the page, and then click **Next >**
4. On the **Make Microsoft Dynamics CRM available to user who connect through the Internet** page, the following three (3) fields should be present and contain the previous configuration's URLs:
    a. Web Application Service Domain
        ii. i.e. *atkoice.com*
    b. Organization Web Service Domain
        i. i.e. *atkoice.com*
    c. Discovery Web Service
        iii. i.e. *ifd.atkoice.com*
            4. For external access, this URL needs to be publicly resolvable and accessible
5. Once verified, click **Next >**
6. On the next **Make Microsoft Dynamics CRM available to user who connect through the Internet** page, the following field should be present and contain the previous configuration's URL:
    a. i.e. *auth.atkoice.com*
        ii. For external access, this URL needs to be publicly resolvable and accessible



3. Once verified, click **Next >**
4. Review the results on the **System Checks** page, resolve any issues (as needed); otherwise click **Next >**
    a. If you receive an error regarding the Discovery Web Service (e.g. "*The Discovery Web Service could not be accessed. The domain is unavailable or does not exist.*"; this can be ignored)
    b. Click **Next >**
9. On the **Review your selections and then click Apply** tab, click **Apply** and then click **Finish**

Note: If you add/remove organizations to your Microsoft Dynamics On-Premises deployment, simply re-run this section of the setup guide.

Step 3: Configure Microsoft Dynamics On-Premises with Okta as a trusted claims provider/trusted issuer

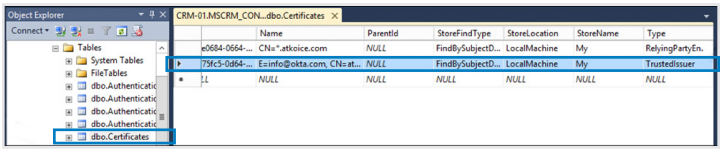
In this step of the guide, we will be adding the Okta certificate to the Microsoft Dynamics database.

PowerShell

1. Launch PowerShell as Administrator
2. Type ***Add-PSSnapin Microsoft.Crm.PowerShell*** and hit **Enter**
3. Type ***Set-CrmCertificate -DataFile C:\Tools\okta.cert -StoreName "My" -CertificateType "AppFabricIssuer" –StoreLocation "LocalMachine"–StoreFindType "FindBySubjectDistinguishedName"*** and hit **Enter**
    a. Update **-DataFile** to match the download path of the Okta certificate
    b. Ensure there is a single **"** at the end of the PowerShell string
        i. i.e. ***FindBySubjectDistinguishedName***

SQL Server Management Studio

1. Launch SQL Server Management Studio (SSMS) connecting to the SQL server hosting your CRM/ Dynamics database
2. Expand ***Databases> MSCRM_CONFIG>Tables***
3. Right-mouse click ***dbo.Certificates*** and click ***Edit Top 200 Rows***
4. Locate the row for the Okta certificate, and change the ***Type*** to ***TrustedIssuer***
    a. Once saved, verify the ***CertificateData*** contains the plain text contained within the Okta certificate
    b. If not, simply copy and paste the relevant text from the Okta certificate downloaded in **Step 2: Okta WS-Fed OIN app** to the ***CertificateData*** field



Step 4: Configure Okta Bookmark app

In this step of the guide, we will be creating an OIN Bookmark app in Okta that will appear as a chiclet on assigned users' Okta organization homepage, allowing users to access the appropriate Microsoft Dynamics organization.

Okta Bookmark OIN app

1. From the Admin app for your Okta Org, navigate to "**Applications>Applications** and click **Add Application** in the top left
2. In the top left search field, type "**Bookmark**" and then choose **Bookmark App** by clicking **Add**
3. Fill out the following fields, replacing the italicized text with the information specific to your environment:

Field	Value	Notes
Application label	*e.g. Acme CRM*	
URL	https://ifd.atkoice.com	https://DiscoveryWebServiceUrl The default behavior with this integration is the user will login using the Discovery Web Service URL and land on the Microsoft Dynamics organization they were created in ***Note: To access any other Microsoft Dynamics Organizations, the user can simply type https://crmOrgname.domainName.com or create/deploy browser bookmarks***
Request Integration	Unchecked	
Application Visibility—do not display application icon to users	Unchecked	
Application Visibility—do not display application icon in the Okta Mobile app	Unchecked	

Step 5: Assign WS-Fed and Okta Bookmark OIN apps

In the final step of this guide, we will be assigning both the WS-Fed and Okta Bookmark OIN apps to allow users access to Microsoft Dynamics On-Premises.

WS-Fed and Okta Bookmark OIN app

1. From the Admin app for your Okta Org, navigate to **Applications>Applications** and click each of the previously created OIN apps
2. From the **Assignments** tab, click **Assign to People** or **Assign to Groups**, as appropriate
3. No username format is needed for the Bookmark OIN app
4. For the WS-Fed OIN app **Assign to People**, verify the username matches the expected CRM/Dynamics username
    a. For **Assign to Groups**, no username format confirmation is needed

Closing summary

You have now successfully replaced your Microsoft ADFS infrastructure for Microsoft Dynamics On-Premises with Okta for claims-based authentication.