Microsoft Dynamics AX

Configure Microsoft Dynamics AX Connector for Mobile Applications

This document explains how to configure an environment that runs Microsoft Dynamics AX 2012 so that users can connect the Microsoft Dynamics AX mobile application.

White paper

June 2019

Send feedback.

Learn more about Microsoft Dynamics.

Contents

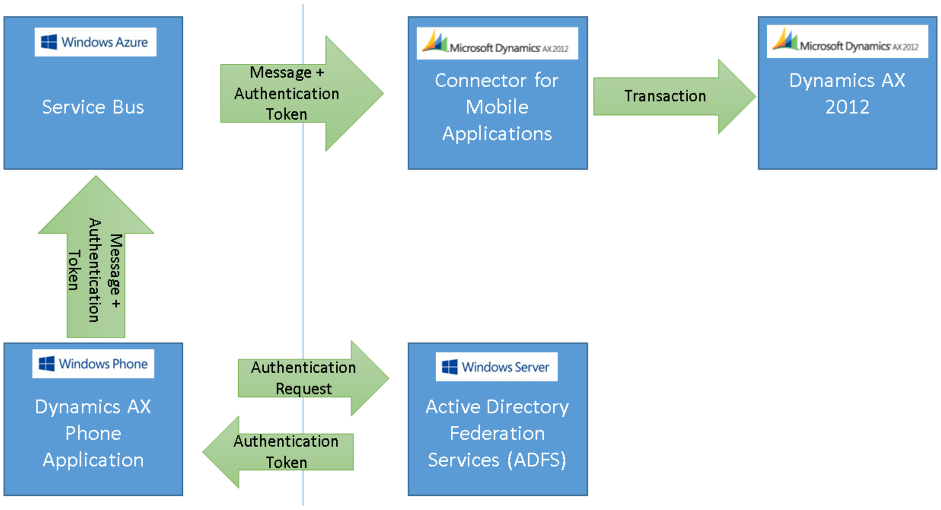
Configure Microsoft Dynamics AX Connector for Mobile Applications

This document explains how to configure an environment that runs Microsoft Dynamics AX 2012 so that users can connect the Microsoft Dynamics AX mobile application.

For the mobile application to interact with AX 2012, the following components must be configured:

- **Active Directory Federation Services (AD FS)** – AD FS works with an organization's instance of Active Directory Domain Services (AD DS) to authenticate users of the mobile application. Users are authenticated based on credentials that the mobile application sends. Upon successful authentication, AD FS returns a token to the mobile application.
  - OR- Azure Active Directory (AAD) instead of AD FS. AAD is alternate form of authentication that can be used.
- **Mobile application** – The mobile application lets a user capture a transaction. It then authenticates the user and sends the message.
- **Microsoft Dynamics AX Connector for Mobile Applications** – Microsoft Dynamics AX Connector for Mobile Applications (the connector) listens for messages that are sent via the Microsoft Azure Service Bus, authenticates the sender of the message, and then sends the message to the AX 2012 instance.
- **Microsoft Dynamics AX 2012** – The AX 2012 instance receives messages that were originally sent from the mobile application. It stores the messages as transactions that are available to the user. For example, in the Microsoft Dynamics AX system, users see expense transactions that they captured on their mobile device.

The following illustration shows these components and the flows among them.


Windows Azure
Service Bus
Message + Authentication Token
Microsoft Dynamics AX 2012
Connector for Mobile Applications
Transaction
Microsoft Dynamics AX 2012
Dynamics AX 2012
Message + Authentication Token
Windows Phone
Dynamics AX Phone Application
Authentication Request
Authentication Token
Windows Server
Active Directory Federation Services (ADFS)

Prerequisites

Before you can configure the connector, you must complete the following prerequisites:

- Set up and configure the Active Directory server:
  - The Active Directory server and domain controller should have been set up during the installation and configuration of AX 2012.
  - Install Active Directory Federation Services 3.0 or Azure Active Directory.
- Configure AX 2012:
  - Configure users for AX 2012.
  - Configure Expense management.
  - Configure Time management.
  - Configure Human resources.
- Configure an Azure account. For more information, go to https://portal.azure.com.

Create a new Service Bus namespace and shared access policies

Create a Shared Access Signature (SAS) Service Bus namespace

1. Start Azure PowerShell.
2. At the command prompt, run the following command to connect Azure PowerShell to your Azure subscription.

```
Login-AzureRmAccount
```

3. Run the following commands to learn the subscriptions that are available and then select one of them.

```
Get-AzureRmSubscription
Select-AzureRmSubscription -SubscriptionId <"subscriptionId">
```

4. Run the following command to create a new Service Bus namespace, such as **contosomobile**, in your appropriate region.

```
New-AzureRmServiceBusNamespace -ResourceGroupName <-resourseGroupName-> -NamespaceName <-
serviceBusName-> -Location <-WestUS->
```

Create shared access policies

1. Sign in to the Azure portal.
2. On the **Service Bus** menu, select the Service Bus that matches the name that you created earlier.
3. Under **Settings**, select **Shared access policies**, and then click **Add**.

4 On the **Add SAS policy** blade, enter a new policy name, such as **SendListen**, select the **Send** and **Listen** check boxes, and then click **Create**.

The SAS policy name that you entered should then be used as the **Azure service identity name** value in the connector parameters.

5 Select the new shared access policy (**SendListen**), and copy the primary key that should be used as the **Azure service identity password** value in the connector parameters.

Configure an Active Directory Federation Service for authentication

AD FS management

After the Active Directory federation server and AD FS 3.0 are installed, as specified in the Prerequisites section, use the AD FS 3.0 Management tool to configure the Federation Service.

For guidance about federation servers, how to configure certificates, and how to install the AD FS 3.0 software by using the setup wizard and server management, see the Windows Server 2016 and 2012 R2 AD FS Deployment Guide.

Next, run the AD FS 3.0 Federation Server Configuration Wizard to configure a new federation server and a new Federation Service. For guidance, see Configure a New Federation Server.

The configuration that is described here is for a Federation Service role for a stand-alone federation server.

1 Enable the endpoint for Microsoft Windows authentication.
2 Establish a trust relationship between the Federation Service and the relying party.

Configure Microsoft Dynamics AX Connector for Mobile Applications 7

1 Create rules to pass claims through the Federation Service.
2 Obtain the thumbprint of the X.509 token signing certificate that is required when you configure the Microsoft Dynamics AX Connector for Mobile Applications service.

Enable the endpoint

1 Click **Start** > **Administrative Tools** > **AD FS 3.0 Management** to open the AD FS 3.0 Management tool.
2 In the left navigation pane, expand the **Service** node, and then select **Endpoints**. In the list of endpoints in the **Token Issuance** section, select the endpoint that has the URL **/adfs/services/trust/13/usernamemixed**. Right-click, and enable the endpoint.

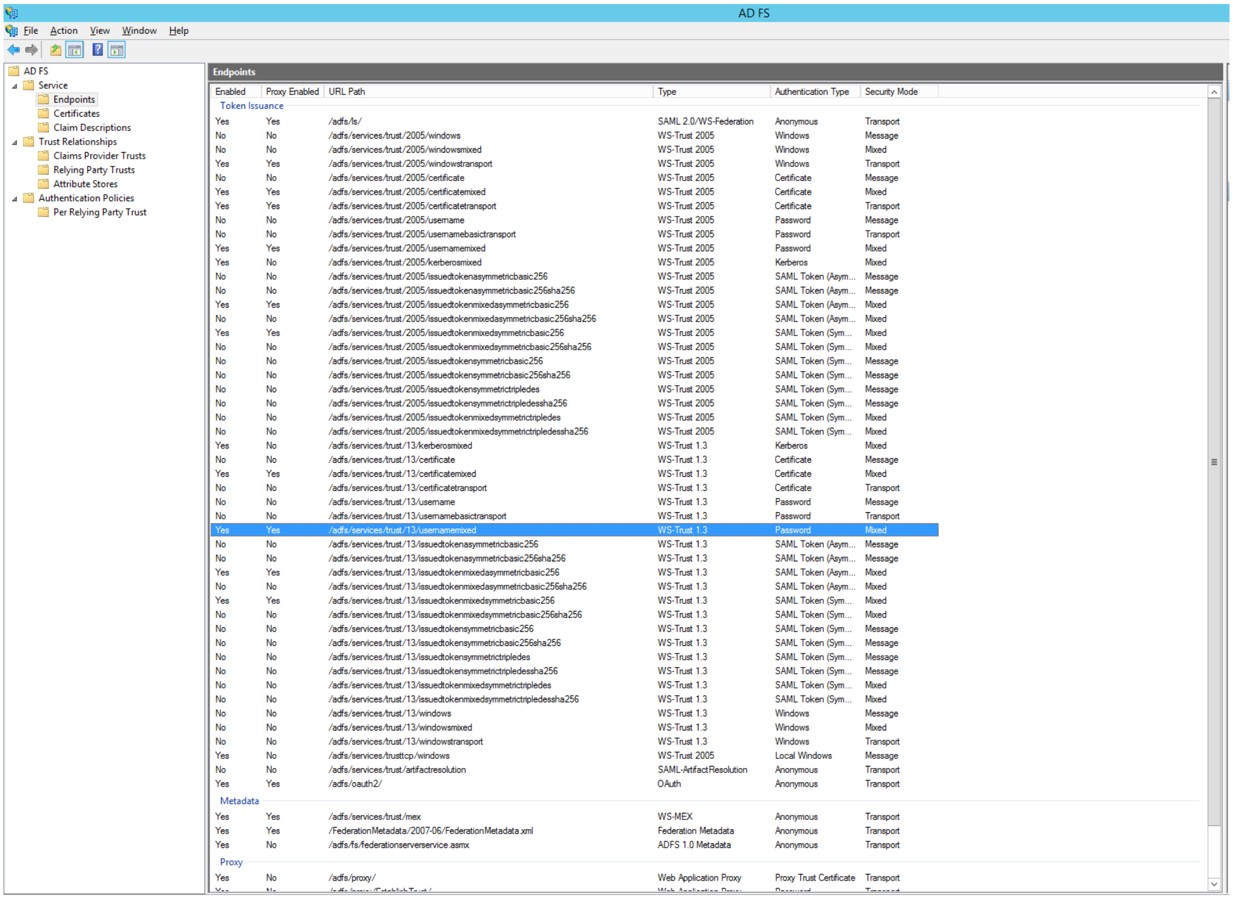
After you enable the service endpoint, the authentication server URL of this Federation Service will be in the form https://<FederationServiceName>/adfs/services/trust/13/usernamemixed.

In this example, the URL is **https://contosoadfs.com/adfs/services/trust/13/usernamemixed**.

Also select the endpoint that has the URL **/FederationMetadata/2007-06/FederationMetadata.xml**. Right-click, and enable the endpoint.

3 Click **Start** > **Administrative Tools** > **Service** to open the Windows Services list. Restart the AD FS 3.0 Windows service.

4 In the **Endpoints** list, make sure that the three endpoints in the **Metadata** section are enabled, as shown in the following illustration.



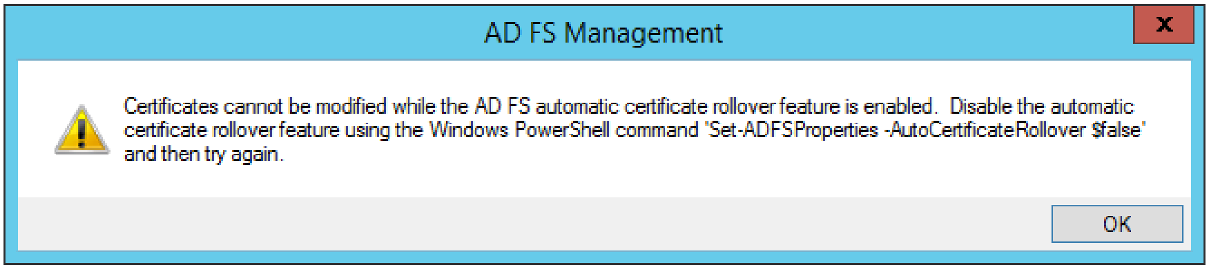
Enabled	Proxy Enabled	URL Path	Type	Authentication Type	Security Mode
Token Issuance					
Yes	Yes	/adfs/ls/	SAML 2.0/WS-Federation	Anonymous	Transport
No	No	/adfs/services/trust/2005/windows	WS-Trust 2005	Windows	Message
No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005	Windows	Mixed
Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005	Windows	Transport
No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005	Certificate	Message
Yes	Yes	/adfs/services/trust/2005/certificatemixed	WS-Trust 2005	Certificate	Mixed
Yes	Yes	/adfs/services/trust/2005/certificatetransport	WS-Trust 2005	Certificate	Transport
No	No	/adfs/services/trust/2005/usemame	WS-Trust 2005	Password	Message
No	No	/adfs/services/trust/2005/usemamebasictransport	WS-Trust 2005	Password	Transport
Yes	Yes	/adfs/services/trust/2005/usemamemixed	WS-Trust 2005	Password	Mixed
Yes	No	/adfs/services/trust/2005/kerberosmixed	WS-Trust 2005	Kerberos	Mixed
No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic256	WS-Trust 2005	SAML Token (Asym...	Message
No	No	/adfs/services/trust/2005/issuedtokenasymmetricbasic256sha256	WS-Trust 2005	SAML Token (Asym...	Message
Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256	WS-Trust 2005	SAML Token (Asym...	Mixed
No	No	/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256sha256	WS-Trust 2005	SAML Token (Asym...	Mixed
Yes	Yes	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256	WS-Trust 2005	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256sha256	WS-Trust 2005	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokensymmetricbasic256sha256	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledes	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokensymmetrictripledessha256	WS-Trust 2005	SAML Token (Sym...	Message
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripledes	WS-Trust 2005	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripledessha256	WS-Trust 2005	SAML Token (Sym...	Mixed
Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	Kerberos	Mixed
No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	Certificate	Message
Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	Certificate	Mixed
No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	Certificate	Transport
No	No	/adfs/services/trust/13/usemame	WS-Trust 1.3	Password	Message
No	No	/adfs/services/trust/13/usemamebasictransport	WS-Trust 1.3	Password	Transport
Yes	Yes	/adfs/services/trust/13/usemamemixed	WS-Trust 1.3	Password	Mixed
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...	Message
No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sha256	WS-Trust 1.3	SAML Token (Asym...	Message
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256	WS-Trust 1.3	SAML Token (Asym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256sha256	WS-Trust 1.3	SAML Token (Asym...	Mixed
Yes	Yes	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256sha256	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetricbasic256sha256	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledes	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokensymmetrictripledessha256	WS-Trust 1.3	SAML Token (Sym...	Message
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledes	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/issuedtokenmixedsymmetrictripledessha256	WS-Trust 1.3	SAML Token (Sym...	Mixed
No	No	/adfs/services/trust/13/windows	WS-Trust 1.3	Windows	Message
No	No	/adfs/services/trust/13/windowsmixed	WS-Trust 1.3	Windows	Mixed
No	No	/adfs/services/trust/13/windowstransport	WS-Trust 1.3	Windows	Transport
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005	Local Windows	Message
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution	Anonymous	Transport
Yes	Yes	/adfs/oauth2/	OAuth	Anonymous	Transport
Metadata					
Yes	Yes	/adfs/services/trust/mex	WS-MEX	Anonymous	Transport
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata	Anonymous	Transport
Yes	No	/adfs/fs/federationserverservice.asmx	ADFS 1.0 Metadata	Anonymous	Transport
Proxy					
Yes	No	/adfs/proxy/	Web Application Proxy	Proxy Trust Certificate	Transport
Yes	No	/adfs/proxy/EstablishTrust/	Web Application Proxy	Password	Transport

Add and configure the token signing certificate

The Microsoft Dynamics AX Connector for Mobile Applications service requires the thumbprint of the X.509 token signing certificate that is used by the Federation Service.

Both the service communications and token signing certificates are configured when you run the AD FS 3.0 setup wizard. For more about certificate requirements for federation servers, see Certificate Requirements for Federation Servers.

- For Windows desktop version of the app, an internally signed certificate should work with the desktop version of the apps if the certificate is installed on every device. If the certificate is necessary to authenticate, it should be installed with the Certificate Manager and should be located within Trusted Root Certification Authorities.
- For Android and iOS, an SSL certificate signed by an external certificate authority (CA), such as Verisign is required. An self-signed certificate is not sufficient. This certificate should have an https:// endpoint available and be recognized outside the corporate network.
- You can view the certificates by clicking **Certificates** under the **Services** node in the left navigation pane. You can also add new token certificates from this management tool by right-clicking the **Certificates** node.
- Before you can add any new certificates, you might have to disable the automatic certificate rollover feature by using Microsoft Windows PowerShell commands.



Certificates cannot be modified while the AD FS automatic certificate rollover feature is enabled. Disable the automatic certificate rollover feature using the Windows PowerShell command 'Set-ADFSProperties -AutoCertificateRollover $false' and then try again.

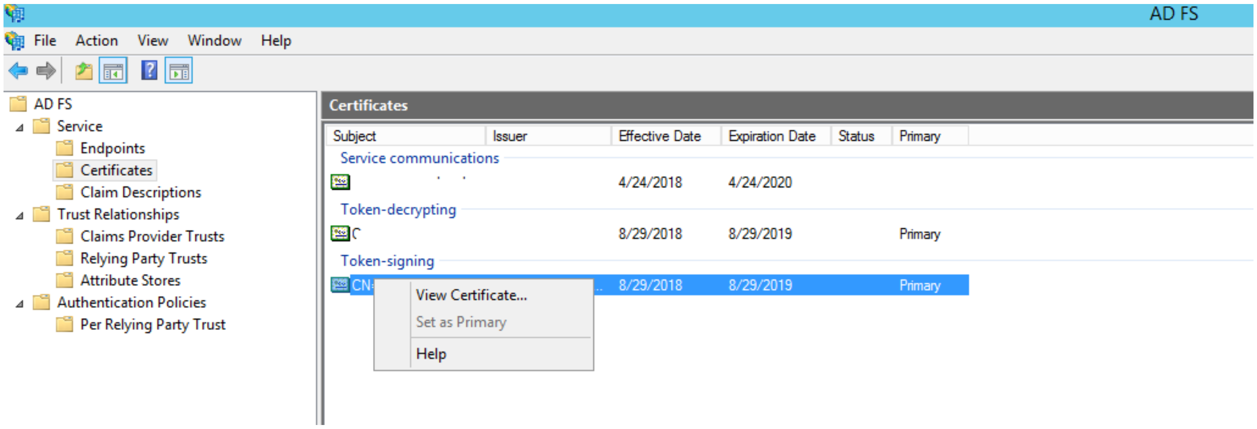
Make sure that the token signing certificate is linked to a trusted root in the Federation Service and issued by an enterprise certification authority

For more information about token signing certificates, see Add a Token-Signing Certificate.

- Set the new token signing certificate as the primary certificate.

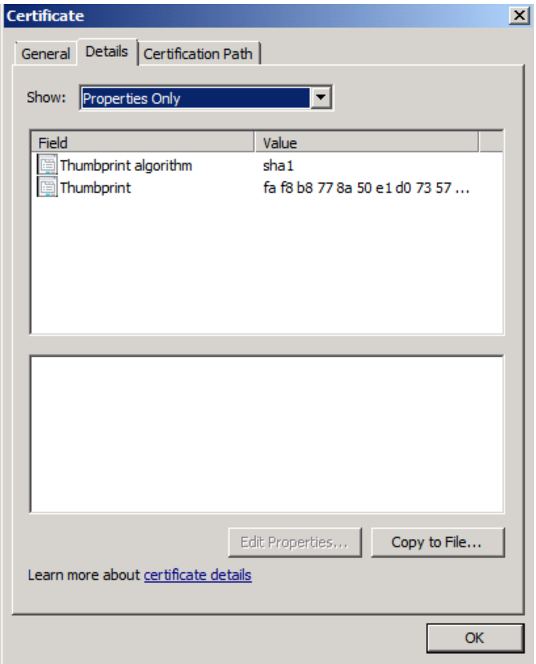
Obtain the thumbprint of the X.509 token signing certificate (digital signature)

1 In the **Certificates** list, select the token signing certificate, right-click, and then select **View Certificate**.



Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
		4/24/2018	4/24/2020		
Token-decrypting					
C		8/29/2018	8/29/2019		Primary
Token-signing					
CN-		8/29/2018	8/29/2019		Primary

2 In the **Certificate** dialog box, on the **Details** tab, copy the **Thumbprint** value, delete the spaces between pairs of characters, and then save the value. This thumbprint value is used when you configure the connector parameters in the Microsoft Dynamics AX Connector for Mobile Applications service.



Show: Properties Only

Field	Value
Thumbprint algorithm	sha1
Thumbprint	fa f8 b8 77 8a 50 e1 d0 73 57 ...

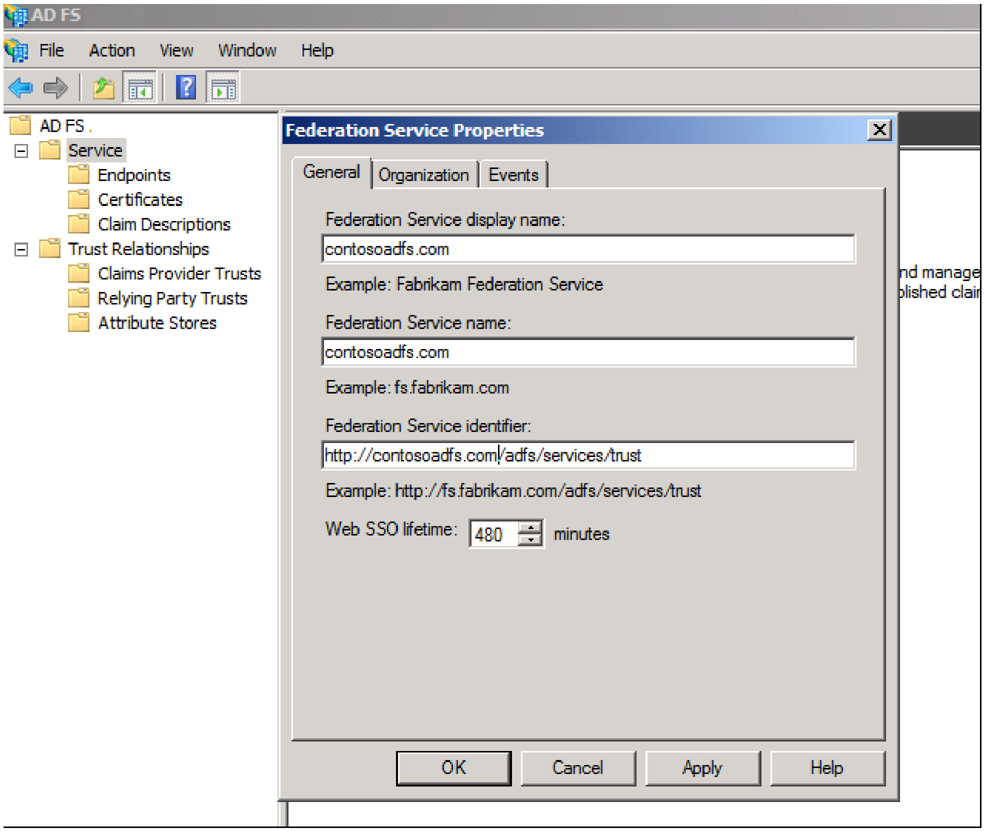
3 Export this token signing certificate, and save it to a location.

This certificate must be installed in the Trusted Root Certification Authorities and Trusted people stores on the server computer that hosts the Microsoft Dynamics AX Connector for Mobile Applications service.

Here are a few more points to keep in mind about these certificates:

- Make sure that the **Subject Name (CN)** or **Issued to** property of the service communications certificate (SSL certificate) matches the name of the Federation Service.
- To view or edit the name of the Federation Service, right-click **Service** in the left navigation pane, and then select **Edit Federation Service Properties**.
- In this example, the service communications certificate has its **Subject Name(CN)** property set to **contosoadfs.com**. This setting helps define the URL of the Federation Server endpoint, such as **https://contosoadfs.com/adfs/ls/**.

To validate that your service is set up correctly, open the following URL in a browser: **https://contosoadfs.com/adfs/fs/federationserverservice.asmx**. Be sure to replace the first part of the URL with your configured environment.



Federation Service Properties

Federation Service display name: contosoadfs.com

Example: Fabrikam Federation Service

Federation Service name: contosoadfs.com

Example: fs.fabrikam.com

Federation Service identifier: http://contosoadfs.com/adfs/services/trust

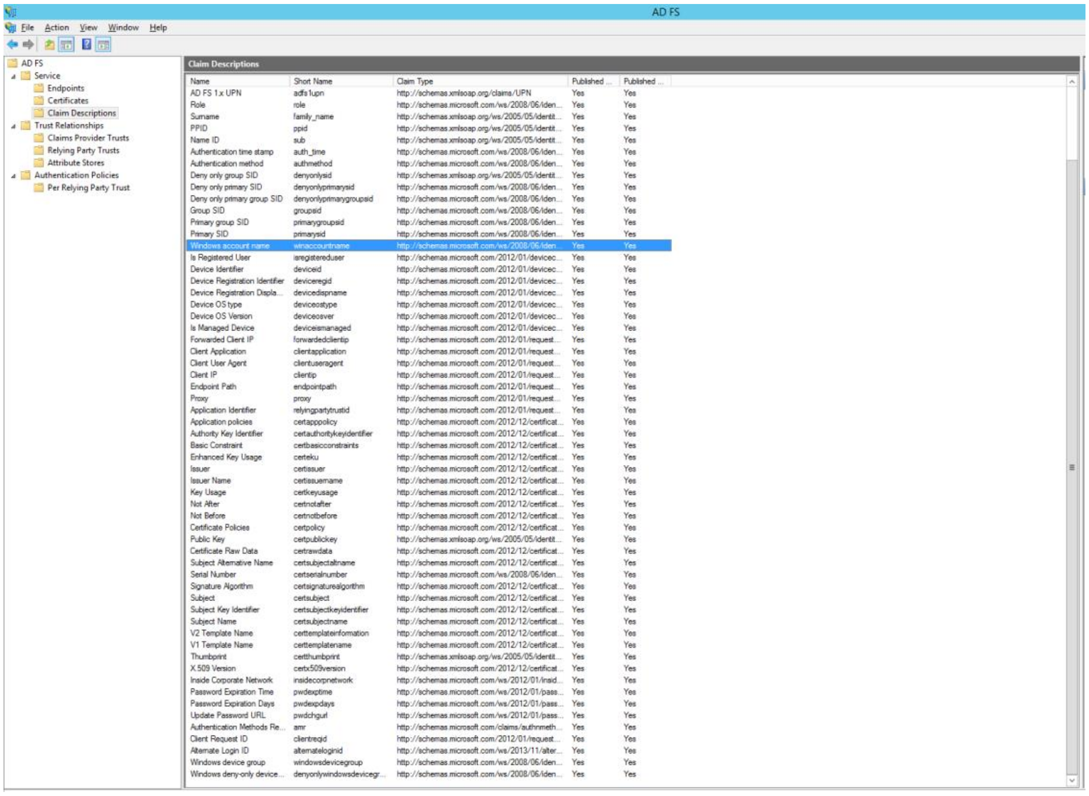
Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime: 480 minutes

For additional debugging and troubleshooting, click the **Events** tab in the **Federation Services Properties** dialog box, and turn on logging for error and other events. You can then debug issues by looking at the logged events in Windows Event Viewer.

Verify claim descriptions

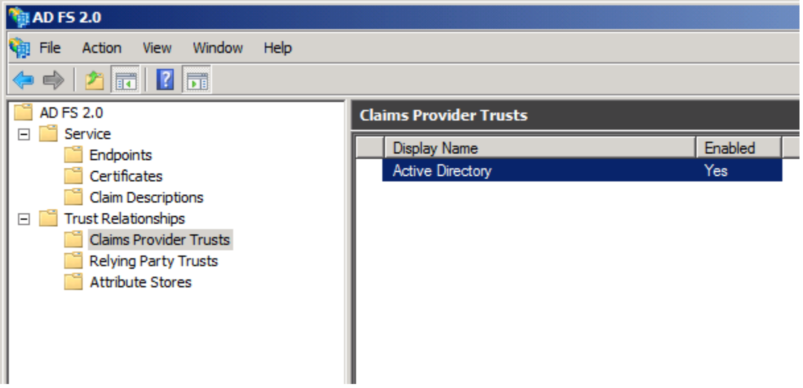
- Make sure that the claim that is named **Windows account name** exists, and that the **Published** property is set to **Yes**. This setting should be configured by default when AD FS 3.0 is installed.



Name	Short Name	Claim Type	Published ...	Published ...
AD FS 1.x UPN	adfs1upn	http://schemas.xmlsoap.org/claims/UPN	Yes	Yes
Role	role	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Surname	family_name	http://schemas.xmlsoap.org/ws/2005/05/identit...	Yes	Yes
PPID	ppid	http://schemas.xmlsoap.org/ws/2005/05/identit...	Yes	Yes
Name ID	sub	http://schemas.xmlsoap.org/ws/2005/05/identit...	Yes	Yes
Authentication time stamp	auth_time	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Authentication method	authmethod	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Deny only group SID	denyonlysid	http://schemas.xmlsoap.org/ws/2005/05/identit...	Yes	Yes
Deny only primary SID	denyonlyprimarysid	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Deny only primary group SID	denyonlyprimarygroupsid	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Group SID	groupsid	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Primary group SID	primarygroupsid	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Primary SID	primarysid	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Windows account name	winaccountname	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Is Registered User	isregistereduser	http://schemas.microsoft.com/2012/01/devicec...	Yes	Yes
Device Identifier	deviceid	http://schemas.microsoft.com/2012/01/devicec...	Yes	Yes
Device Registration Identifier	deviceregid	http://schemas.microsoft.com/2012/01/devicec...	Yes	Yes
Device Registration Displa...	devicedispname	http://schemas.microsoft.com/2012/01/devicec...	Yes	Yes
Device OS type	deviceostype	http://schemas.microsoft.com/2012/01/devicec...	Yes	Yes
Device OS Version	deviceosver	http://schemas.microsoft.com/2012/01/devicec...	Yes	Yes
Is Managed Device	deviceismanaged	http://schemas.microsoft.com/2012/01/devicec...	Yes	Yes
Forwarded Client IP	forwardedclientip	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Client Application	clientapplication	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Client User Agent	clientuseragent	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Client IP	clientip	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Endpoint Path	endpointpath	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Proxy	proxy	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Application Identifier	relyingpartytrustid	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Application policies	certappolicy	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Authority Key Identifier	certauthoritykeyidentifier	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Basic Constraint	certbasicconstraints	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Enhanced Key Usage	certeku	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Issuer	certissuer	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Issuer Name	certissuername	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Key Usage	certkeyusage	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Not After	certnotafter	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Not Before	certnotbefore	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Certificate Policies	certpolicy	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Public Key	certpublickey	http://schemas.xmlsoap.org/ws/2005/05/identit...	Yes	Yes
Certificate Raw Data	certrawdata	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Subject Alternative Name	certsubjectaltname	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Serial Number	certserialnumber	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Signature Algorithm	certsignaturealgorithm	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Subject	certsubject	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Subject Key Identifier	certsubjectkeyidentifier	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Subject Name	certsubjectname	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
V2 Template Name	certtemplateinformation	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
V1 Template Name	certtemplatename	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Thumbprint	certthumbprint	http://schemas.xmlsoap.org/ws/2005/05/identit...	Yes	Yes
X.509 Version	certx509version	http://schemas.microsoft.com/2012/12/certificat...	Yes	Yes
Inside Corporate Network	insidecorpnetwork	http://schemas.microsoft.com/ws/2012/01/insid...	Yes	Yes
Password Expiration Time	pwdexptime	http://schemas.microsoft.com/ws/2012/01/pass...	Yes	Yes
Password Expiration Days	pwdexpdays	http://schemas.microsoft.com/ws/2012/01/pass...	Yes	Yes
Update Password URL	pwdchgurl	http://schemas.microsoft.com/ws/2012/01/pass...	Yes	Yes
Authentication Methods Re...	amr	http://schemas.microsoft.com/claims/authnmeth...	Yes	Yes
Client Request ID	clientreqid	http://schemas.microsoft.com/2012/01/request...	Yes	Yes
Alternate Login ID	alternateloginid	http://schemas.microsoft.com/ws/2013/11/alter...	Yes	Yes
Windows device group	windowsdevicegroup	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes
Windows deny-only device...	denyonlywindowsdevicegr...	http://schemas.microsoft.com/ws/2008/06/iden...	Yes	Yes

Add claims on claims provider trusts

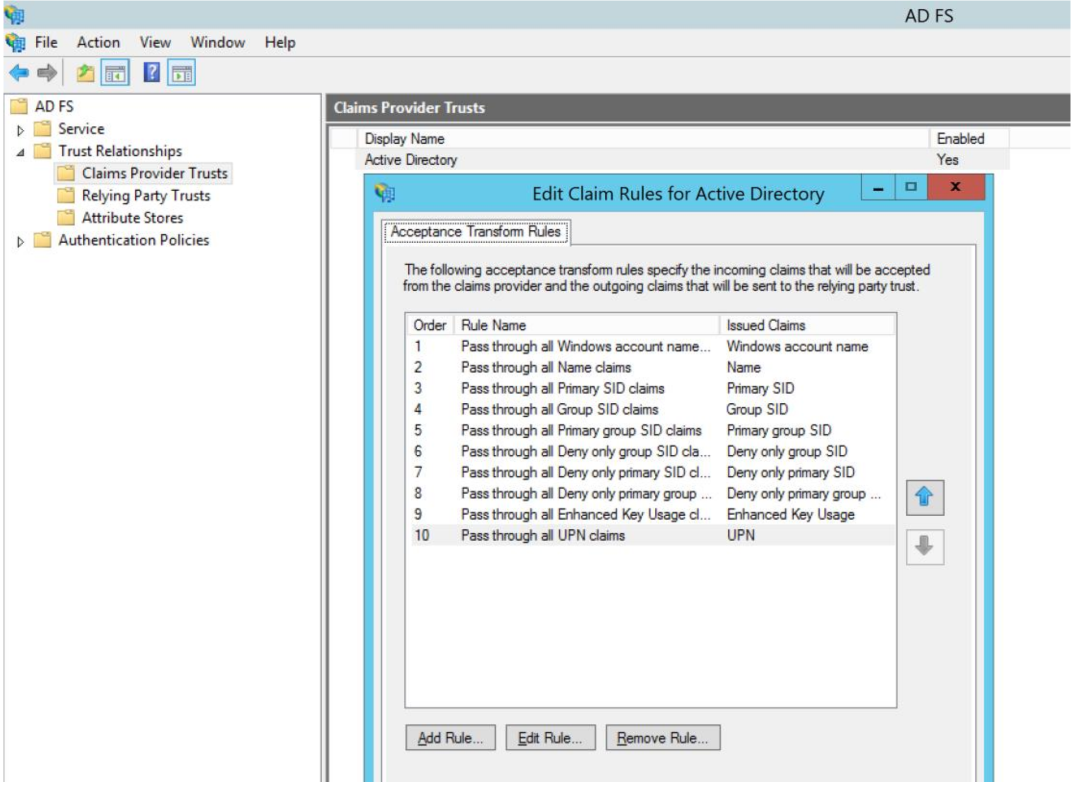
AD DS is the claim provider trust that is used to issue claims about an authenticated user.



Display Name	Enabled
Active Directory	Yes

1 In the left navigation pane, expand the **Trust Relationships** node, right-click **Relying Party Trusts**, and then select **Add Relying Party Trust**.

2 Select the **Active Directory** claims provider trust, right-click, and then select **Edit claim rules**.



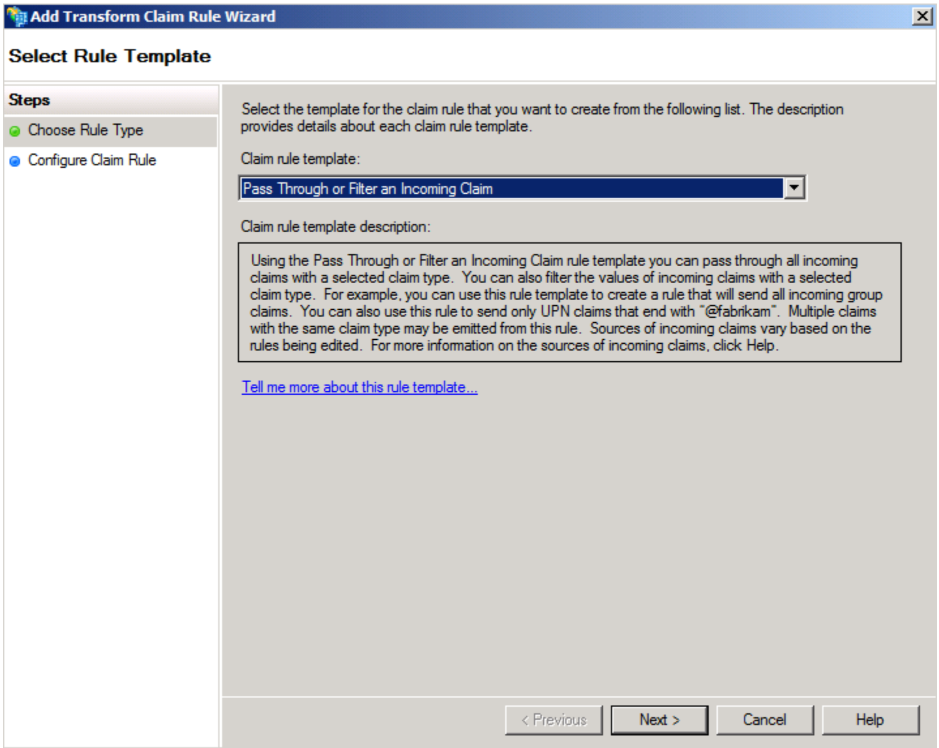
Display Name	Enabled
Active Directory	Yes

The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

Order	Rule Name	Issued Claims
1	Pass through all Windows account name...	Windows account name
2	Pass through all Name claims	Name
3	Pass through all Primary SID claims	Primary SID
4	Pass through all Group SID claims	Group SID
5	Pass through all Primary group SID claims	Primary group SID
6	Pass through all Deny only group SID cla...	Deny only group SID
7	Pass through all Deny only primary SID cl...	Deny only primary SID
8	Pass through all Deny only primary group ...	Deny only primary group ...
9	Pass through all Enhanced Key Usage cl...	Enhanced Key Usage
10	Pass through all UPN claims	UPN

3 Click **Add rule**. The Add Transform Claim Rule Wizard is started.

4 On the **Select Rule Template** page, in the **Claim rule template** field, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.



Select Rule Template

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

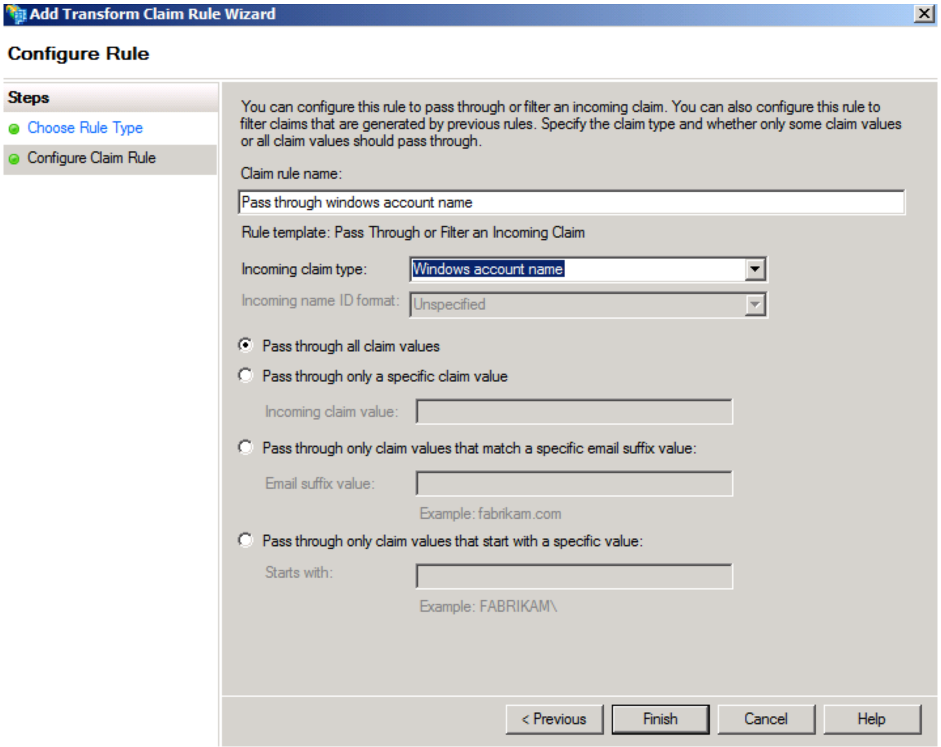
Claim rule template: Pass Through or Filter an Incoming Claim

Claim rule template description:

Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

Tell me more about this rule template...

5 On the **Configure rule** page, enter a name for the claim rule. In the **Incoming claim type** field, select **Windows account name**. Then select the **Pass through all claims value** option, and click **Next**.



Configure Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name: Pass through windows account name

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type: Windows account name

Incoming name ID format: Unspecified

● Pass through all claim values

○ Pass through only a specific claim value

Incoming claim value:

○ Pass through only claim values that match a specific email suffix value:

Email suffix value:

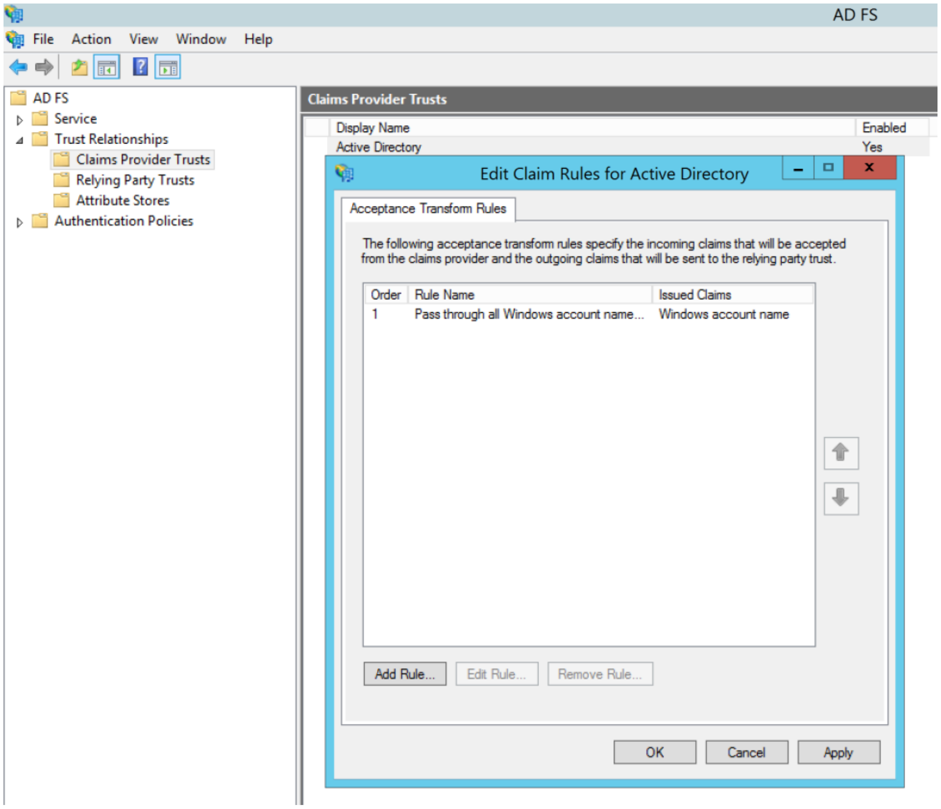
Example: fabrikam.com

○ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

6 The **Edit Claim Rules** dialog box shows the new claim rule. Click **Apply** and then **OK** to save your changes.



Display Name	Enabled
Active Directory	Yes

Edit Claim Rules for Active Directory
Acceptance Transform Rules

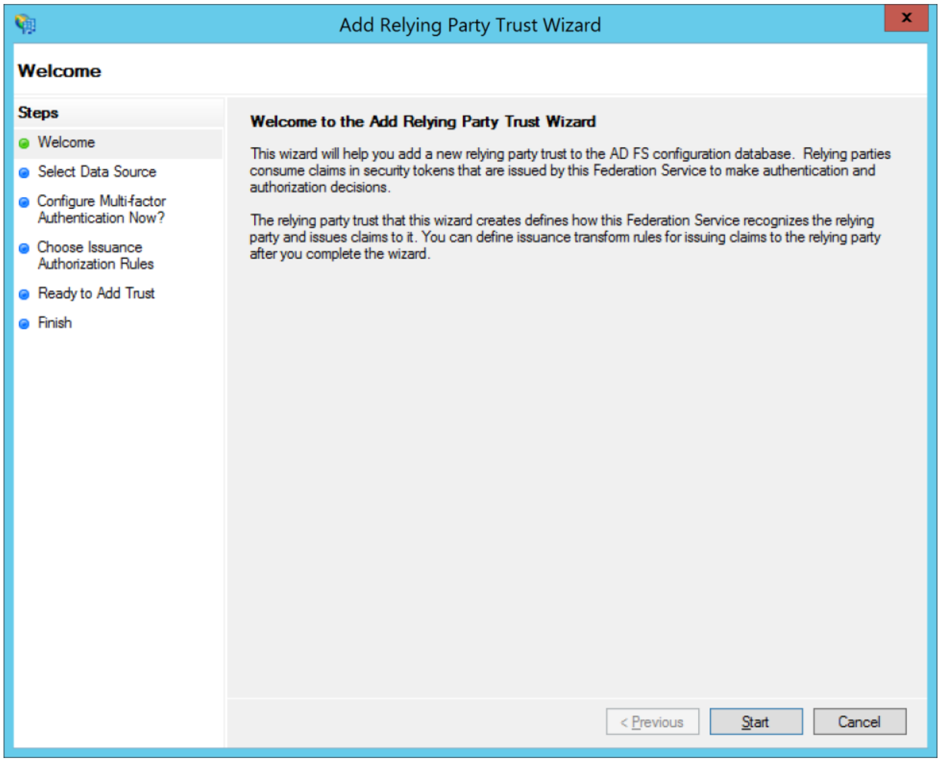
The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

Order	Rule Name	Issued Claims
1	Pass through all Windows account name...	Windows account name

Add a relying party trust

1 Expand the **Trust Relationships** node, select **Relying Party Trusts**, right-click, and then select **Add Relying Party Trust**.

2 Click **Start** on the **Add Relaying Trust Wizard,** and then click Start on the **Welcome** page.



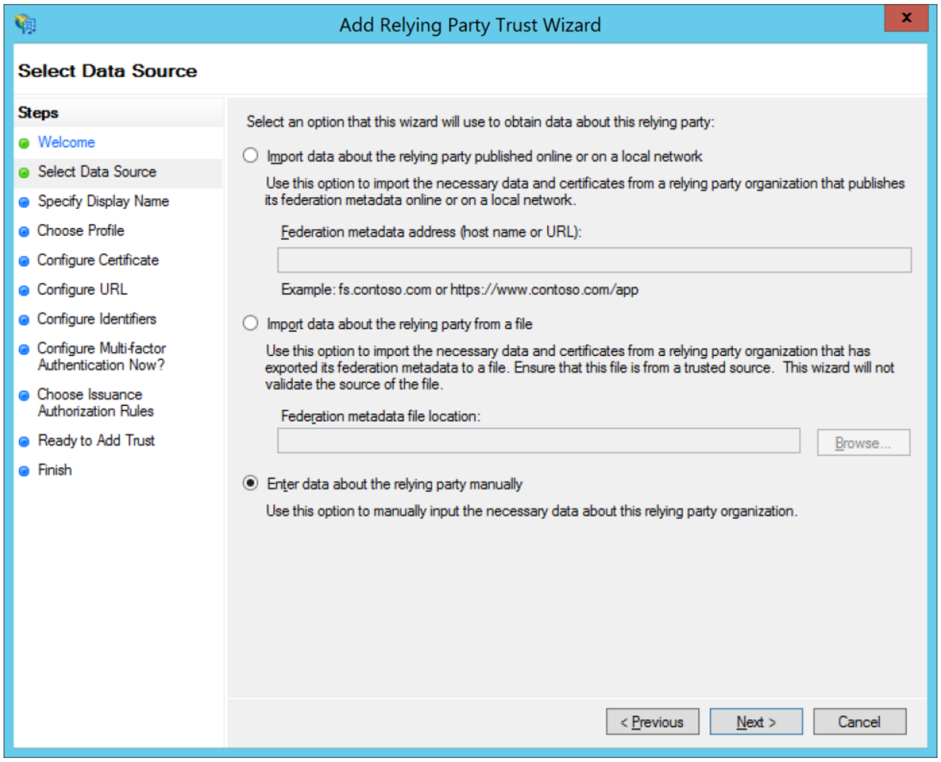
Add Relying Party Trust Wizard
Welcome
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish
< Previous
Start
Cancel

Welcome to the Add Relying Party Trust Wizard

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

3 On the **Select Data Source** page, select the **Enter data about the relying party manually** option, and then click **Next**.



Add Relying Party Trust Wizard

Select Data Source

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

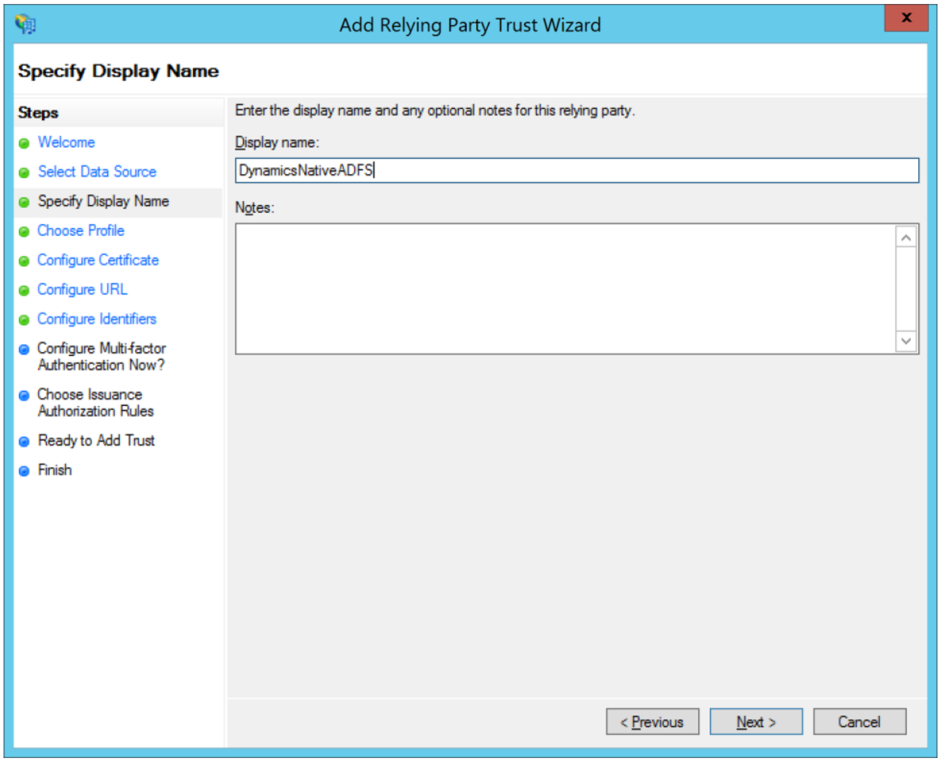
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

4 On the **Specify Display Name** page, enter a display name, such as **DynamicsNativeADFS**, and then click **Next**.



Add Relying Party Trust Wizard

Specify Display Name

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

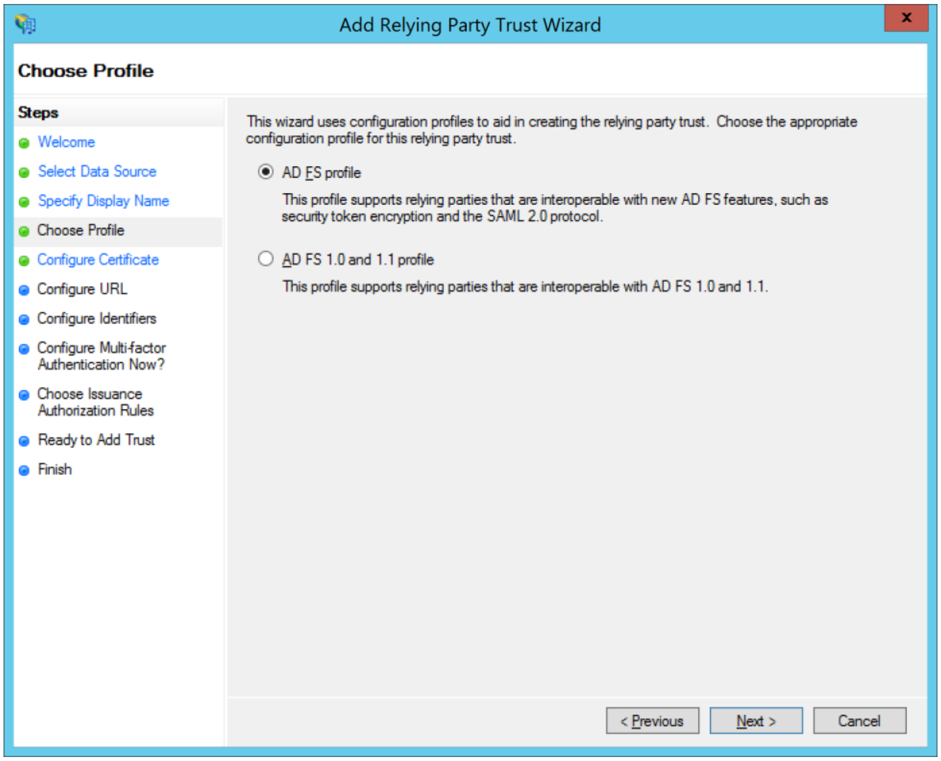
Enter the display name and any optional notes for this relying party.

Display name:

DynamicsNativeADFS

Notes:

5 On the **Choose Profile** page, select the default AD FS profile, and then click **Next**.



This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate configuration profile for this relying party trust.

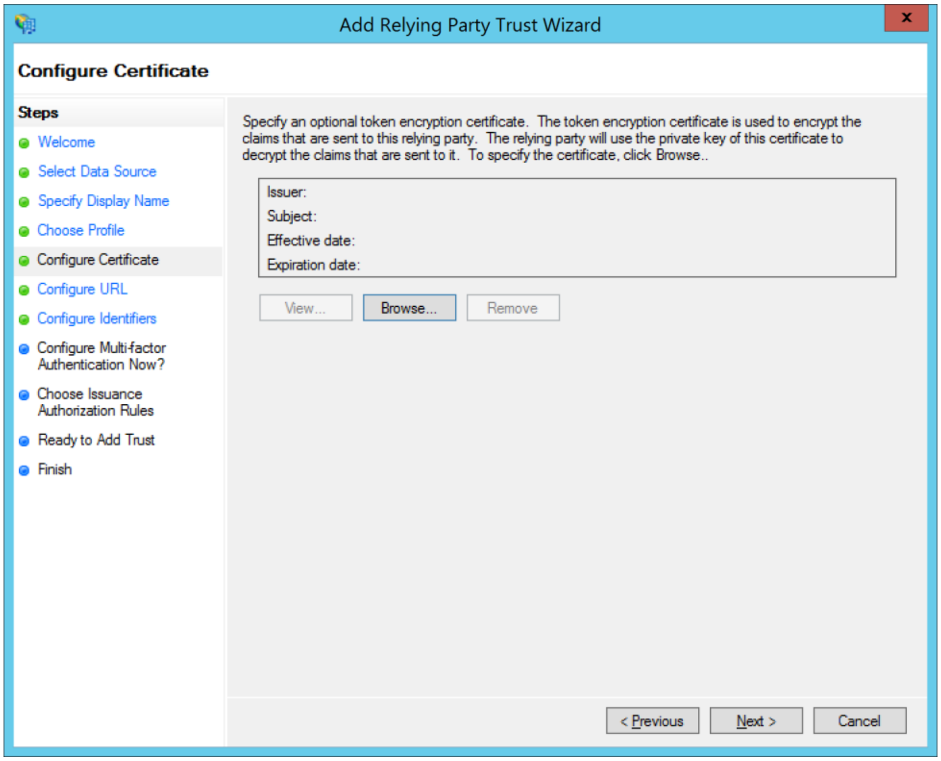
● AD FS profile

This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.

○ AD FS 1.0 and 1.1 profile

This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.

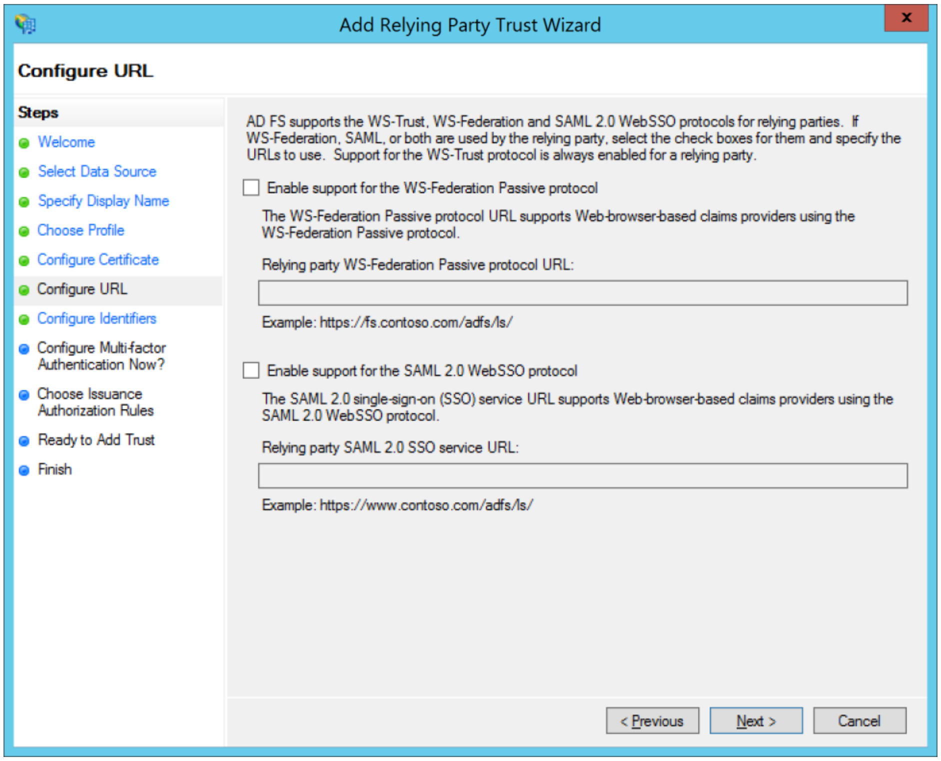
6 On the **Configure Certificate** page, don’t select any certificate. Leave the default values, and click **Next**.



Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

7 On the **Configure URL** page, leave the default values, and click **Next**.



AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

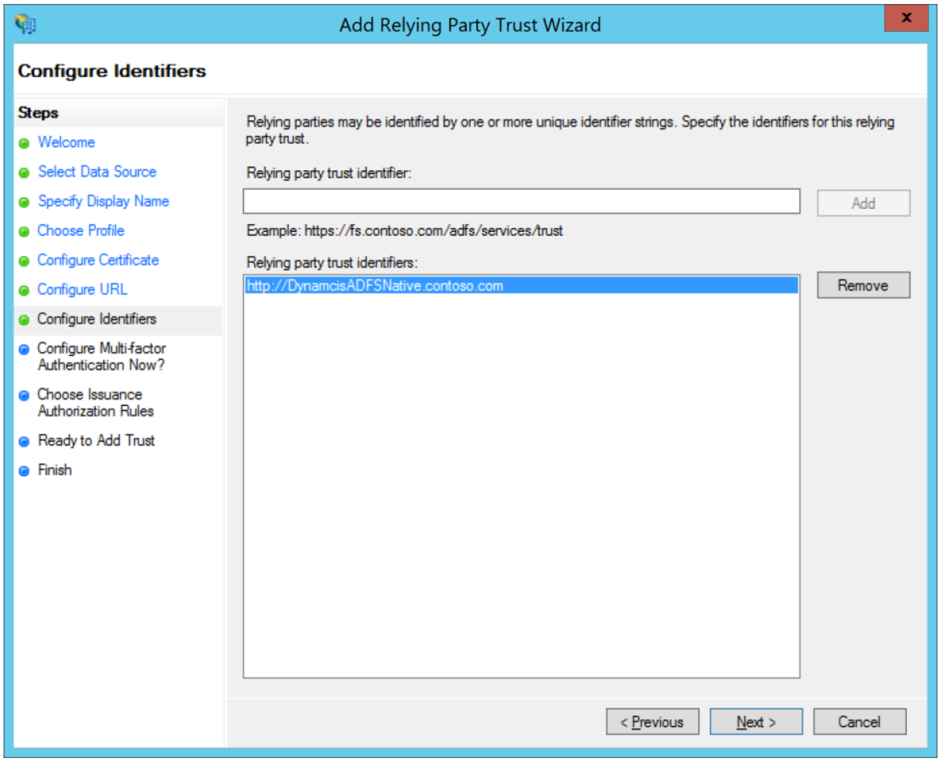
□ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

8 On the **Configure Identifiers** page, enter a URL, such as **http://DynamicsAADFSNative.contoso.com**, and click **Add**. Then click **Next**.



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

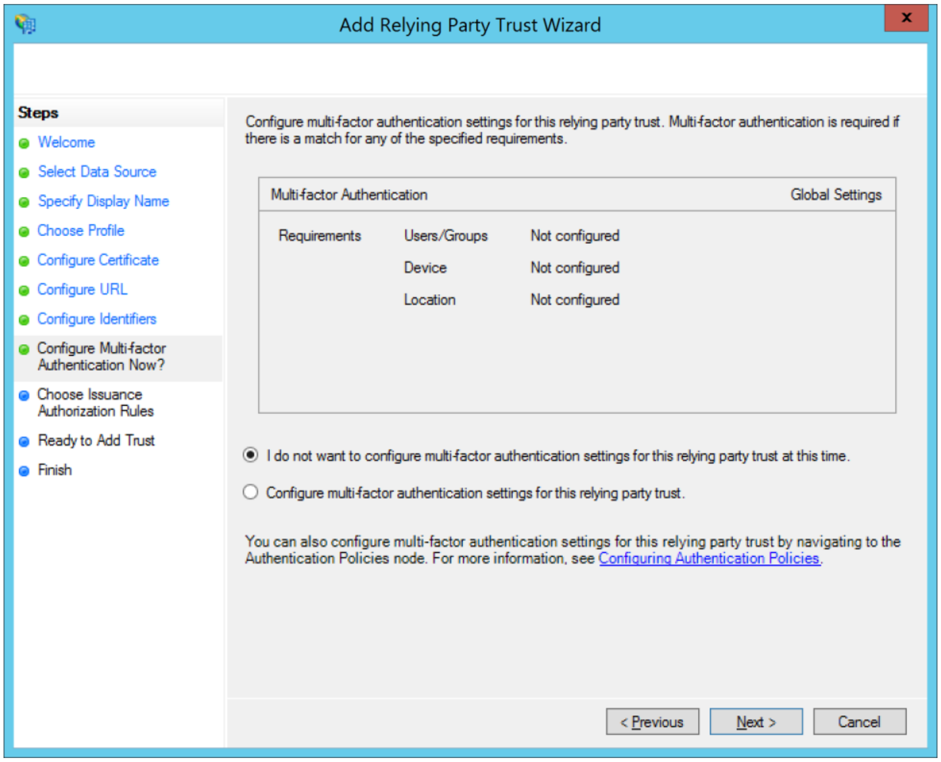
Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

http://DynamcisADFSNative.contoso.com

9 On the next page, you can configure multi-factor authentication according to your preference. In this example, the **I do not want to configure multi-factor authentication settings for this relying party trust at this time** option is selected.



Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

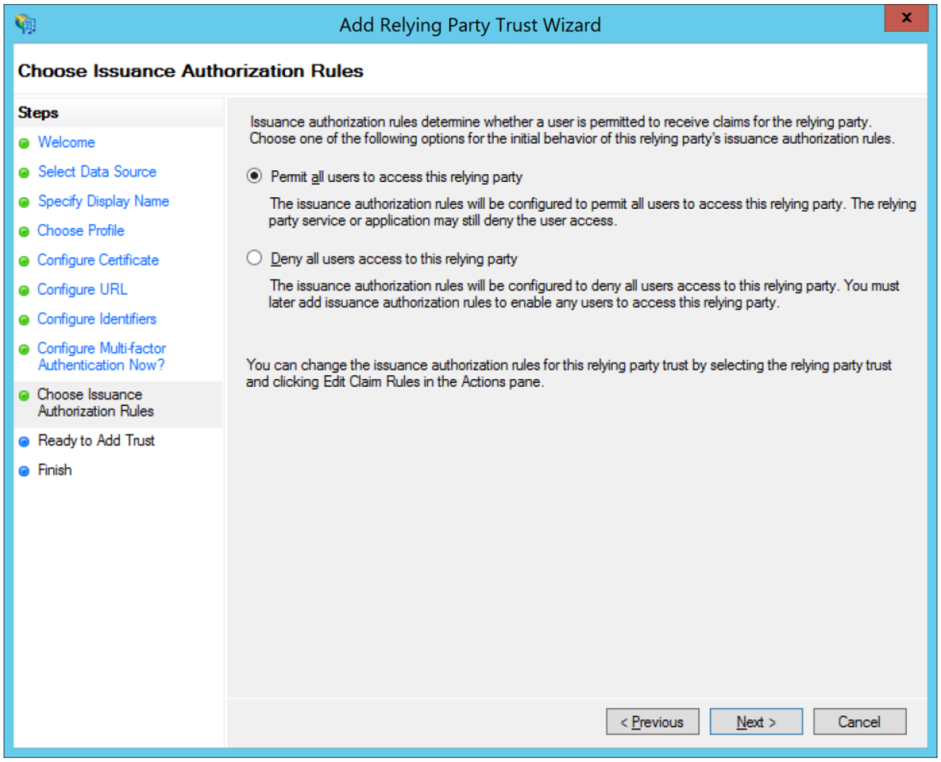
Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

● I do not want to configure multi-factor authentication settings for this relying party trust at this time.

○ Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see Configuring Authentication Policies.

10 In the **Choose Issuance Authorization Rules** page, make sure that the **Permit all users to access this relying party** option is selected, and then click **Next**.



Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

● Permit all users to access this relying party

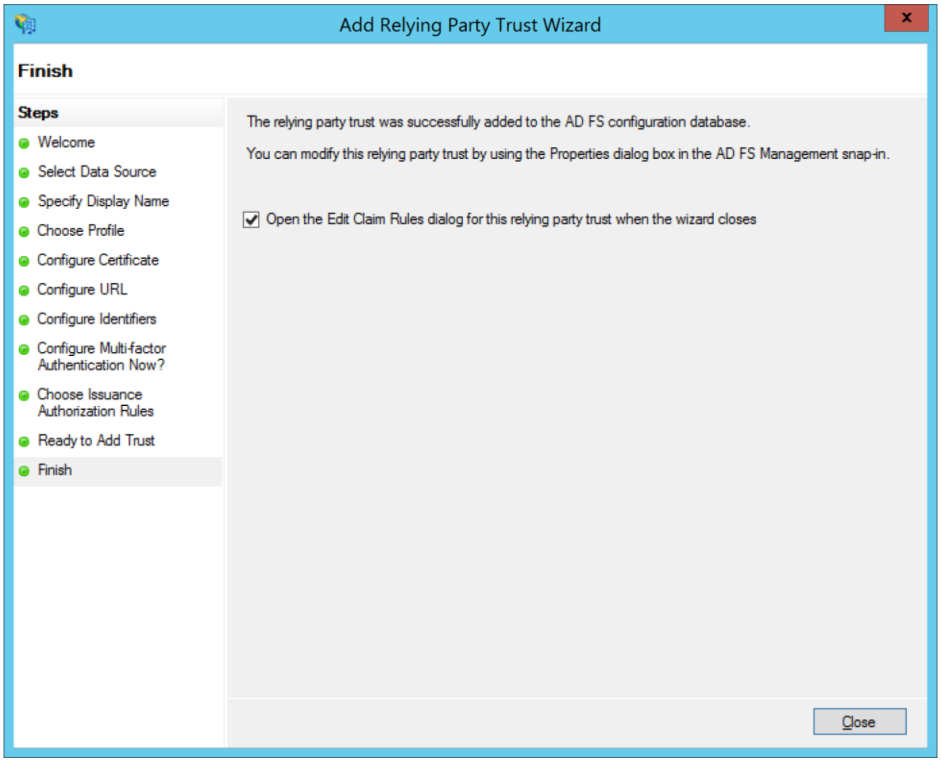
The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

○ Deny all users access to this relying party

The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

11 On the **Ready to Add Trust** page, click **Next**, and then, on the **Finish** page, click **Close** to complete the setup. By default, the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box is selected. Therefore, when the wizard is closed, the **Edit Claim Rules** dialog box appears.



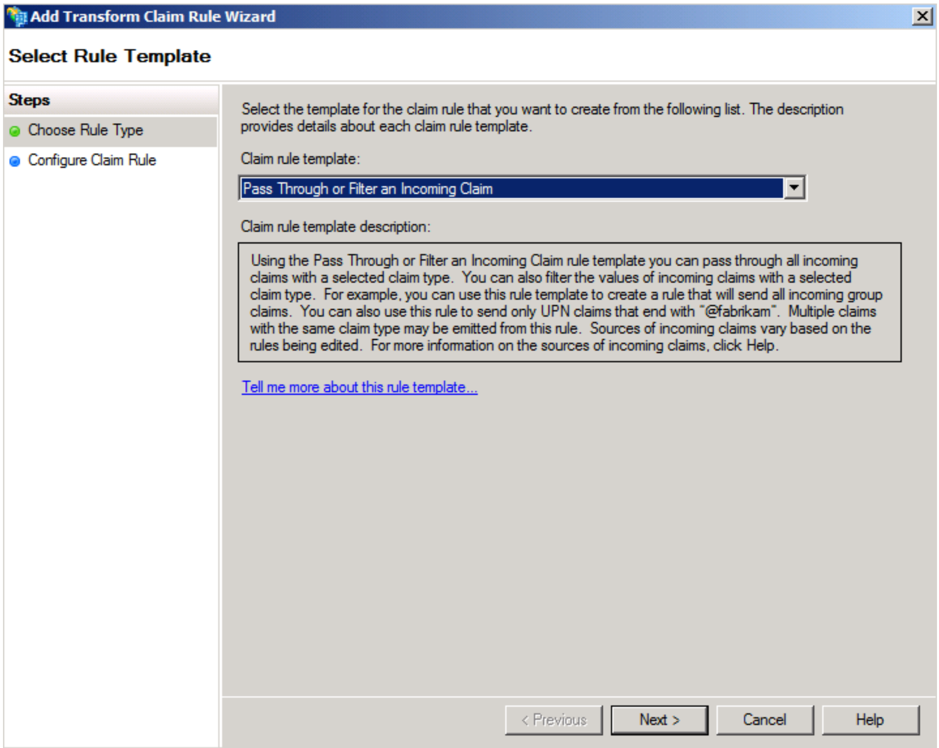
The relying party trust was successfully added to the AD FS configuration database.

You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap-in.

☑ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes

12 Click **Add Rule**. The Add Transform Claim Rule Wizard is started.

13 On the **Select Rule Template** page, in the **Claim rule template** field, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.



Add Transform Claim Rule Wizard

Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

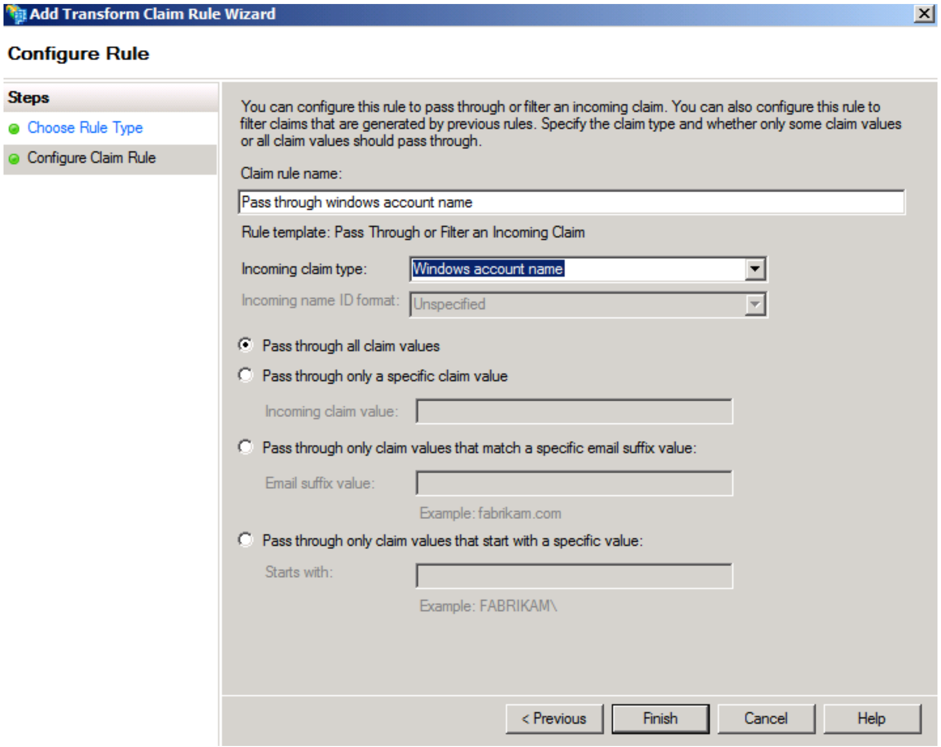
Claim rule template: Pass Through or Filter an Incoming Claim

Claim rule template description:

Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help.

Tell me more about this rule template...

14 On the **Configure Rule** page, enter a name for the claim rule. In the **Incoming claim type** field, select **Windows account name**. Then select the **Pass through all claim values** option, and click **Next**.



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name: Pass through windows account name

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type: Windows account name

Incoming name ID format: Unspecified

● Pass through all claim values

○ Pass through only a specific claim value

Incoming claim value:

○ Pass through only claim values that match a specific email suffix value:

Email suffix value:

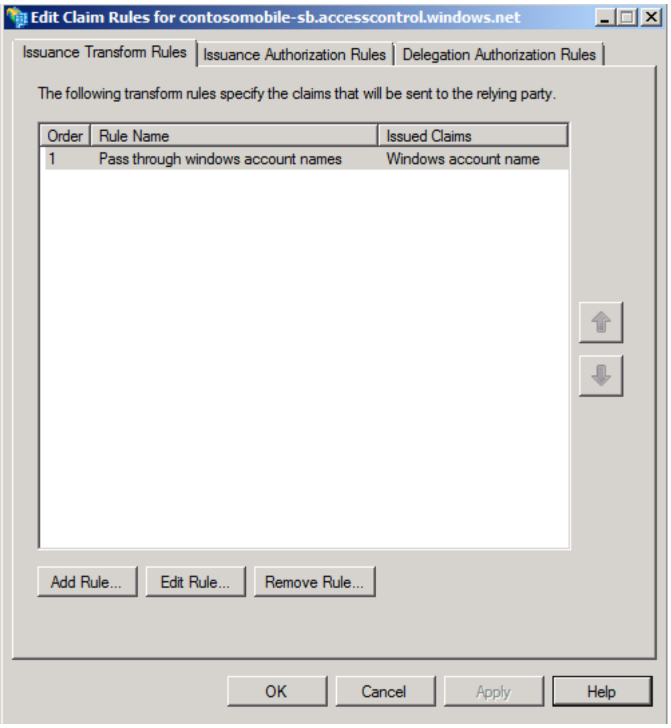
Example: fabrikam.com

○ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

15 The **Edit Claim Rules** dialog box shows the new claim rule. Click **Apply** and then **OK** to save your changes.



Edit Claim Rules for contosomobile-sb.accesscontrol.windows.net
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply
Help

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	Pass through windows account names	Windows account name

You can get back to the **Edit Claim Rules** form by right-clicking the relying party trust that you just added and then selecting **Edit Claim Rules**.

16 Start Azure PowerShell, and enable the JavaScript Object Notation Web Token (JWT) for new relying party trust. The target name is the display name that you specified in the wizard earlier.

```
Set-AdfsRelyingPartyTrust -TargetName "DynamicsNative" -EnableJWT $true
```

Save the AD FS FederationMetadata.xml file

1 On your federation server, open the following address in a browser: **https://<FederationServiceName>/FederationMetadata/2007-06/FederationMetadata.xml**

In this example, the address is **https://contosoadfs.com/FederationMetadata/2007-06/FederationMetadata.xml**.

2 Save the **FederationMetadata.xml** file to a location.

3 If the Federation Service doesn't have an internet-facing Internet Protocol (IP) address, you must upload this federation metadata file.

Create AD FS clients

1. Start Windows PowerShell in administrator mode.
2. Run these commands to enable access by the mobile apps:
   - For the Windows Expenses desktop app

     ```
     Add-ADFSClient ClientId "abcd-123-efgh-4567" RedirectUri "ms-app://S-1-15-2-3928788700-3789986351-
     3052964962-3352193189-1654392005-971744669-2270453158/"
     ```

   - For the Windows Timesheets desktop app

     ```
     Add-ADFSClient ClientId "bcde-123-efgh-4567" RedirectUri "ms-app://s-1-15-2-1686823218-3869368799-
     4003585847-1074717996-2718656644-2639155508-3087402168/"
     ```

   - For the Windows Approvals desktop app

     ```
     Add-ADFSClient ClientId "cdef-123-efgh-4567" RedirectUri "ms-app://s-1-15-2-256616160-1993905071-
     509288680-1590138783-827304346-2645043696-2039586845/"
     ```

   - For the Google Android app

     ```
     Add-ADFSClient ClientId "abcd-123-efgh-9123" RedirectUri
     "msauth://microsoft.dynamicsax/azvBvNWkMH4gNvJYX3ssUoXXqDI="
     ```

   - For the Apple iOS app

     ```
     Add-ADFSClient ClientId "abcd-123-efgh-8709" RedirectUri "x-msauth-
     dynamicsax://com.microsoft.dynamics.ax"
     ```

3. Record the preceding client IDs and enter them in Rapid start connector for these App registration for native client id (windows), Android ADFS Native App Id, IOS ADFS Native App Id in Rapid start connector parameters.

You've now completed the required AD FS configuration. Continue to the "Configure the on-premises server with AX 2012 and the connector" section.

Configure Azure Active Directory (AAD) for authentication

Azure Active Directory with SAS is supported for Dynamics AX 2012 Expenses, Approvals, and Timesheets (Desktop), Dynamics AX 2012 (Android), and Dynamics AX (iOS).

Prerequisites

Before you can configure the connector, you must complete the following prerequisites:

- Configure AX 2012:

    - Configure users for AX 2012
    - Configure Expense management
    - Configure Time management if planned use is for time entry
    - Configure Human resources
- Configure an Azure account and make sure Azure active directory authentication is available for the users in your organization. For more information, go to https://portal.azure.com.
- Logging for the AIF inbound port needs to be set to logging disabled. If you have a setting other than disabled, follow Issue 3979651 in LCS issue search for updated code to prevent a “Some or all identity references could not be translated” error preventing login.

Create SAS authorization-based Service Bus and shared access policies

Create a shared access signature (SAS) Service Bus namespace

1 Open Azure PowerShell.

2 In the PowerShell command prompt, run the following command to connect AzurePowerShell to your Azure subscription.

- *Login-AzureRmAccount*

3 Run these commands to know the subscriptions available and then to select one.

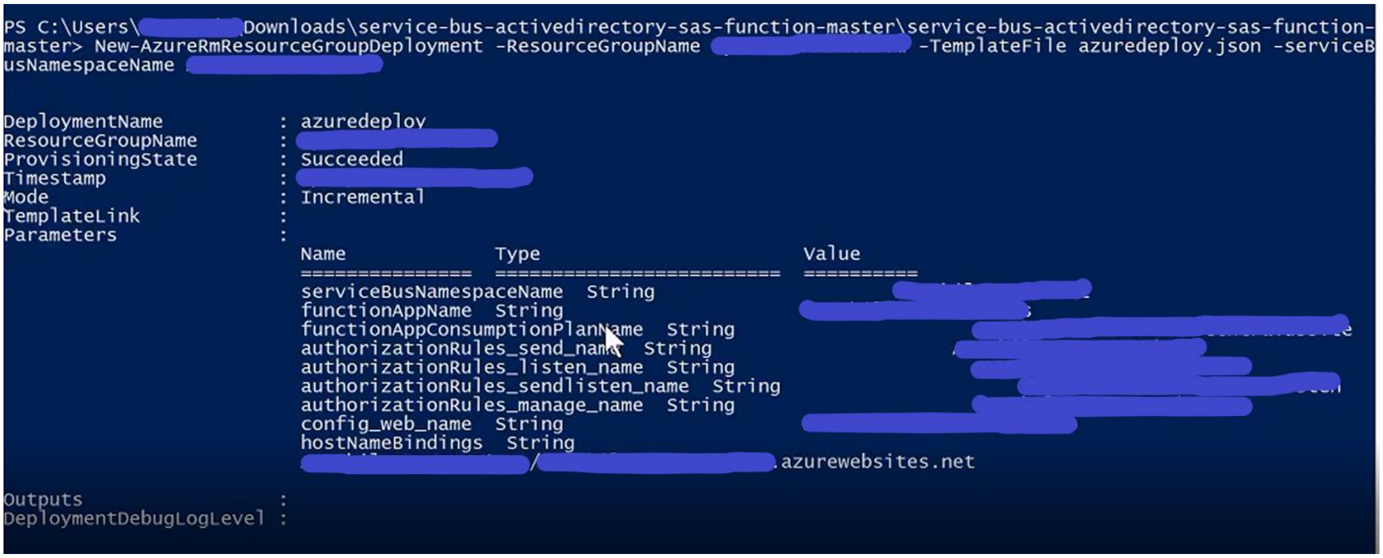
- *Get-AzureRmSubscription*
- *Select-AzureRmSubscription -SubscriptionId <"subscriptionId">*

4 Before you create or update the service bus, download the service bus active directory SAS function project using the following link and extract the folder in your local machine. https://github.com/clemensv/service-bus-activedirectory-sas-function

5 In the PowerShell Command prompt, go to the exact path where azuredeploy.json file located in the extracted project folder.

6 Run the following command to create a new SAS authorized service bus namespace or use the same command to enable the SAS authorization for the existing service bus.

- *New-AzureRmResourceGroupDeployment -ResourceGroupName <-resourceGroupName-> -TemplateFile azuredeploy.json -serviceBusNamespaceName <-serviceBusName->*
- **Note:** Replace your Azure subscriptionId, resourceGroupName and serviceBusName that you want to create in the above commands.



```
PS C:\Users\[redacted]Downloads\service-bus-activedirectory-sas-function-master\service-bus-activedirectory-sas-function-
master> New-AzureRmResourceGroupDeployment -ResourceGroupName [redacted] -TemplateFile azuredeploy.json -serviceB
usNamespaceName [redacted]

DeploymentName          : azuredeploy
ResourceGroupName       : [redacted]
ProvisioningState       : Succeeded
Timestamp               : [redacted]
Mode                    : Incremental
TemplateLink            :
Parameters              :
                          Name             Type                       Value
                          ===============  =========================  ==========
                          serviceBusNamespaceName  String             [redacted]
                          functionAppName  String                     [redacted]
                          functionAppConsumptionPlanName  String      [redacted]
                          authorizationRules_send_name  String        [redacted]
                          authorizationRules_listen_name  String      [redacted]
                          authorizationRules_sendlisten_name  String  [redacted]
                          authorizationRules_manage_name  String      [redacted]
                          config_web_name  String                     [redacted]
                          hostNameBindings  String
                          [redacted]/[redacted].azurewebsites.net

Outputs                 :
DeploymentDebugLogLevel :
```

After running the command, it will create or update the service bus with a function app, shared access policies. If the shared access policies are not created automatically you can create them by following steps below.

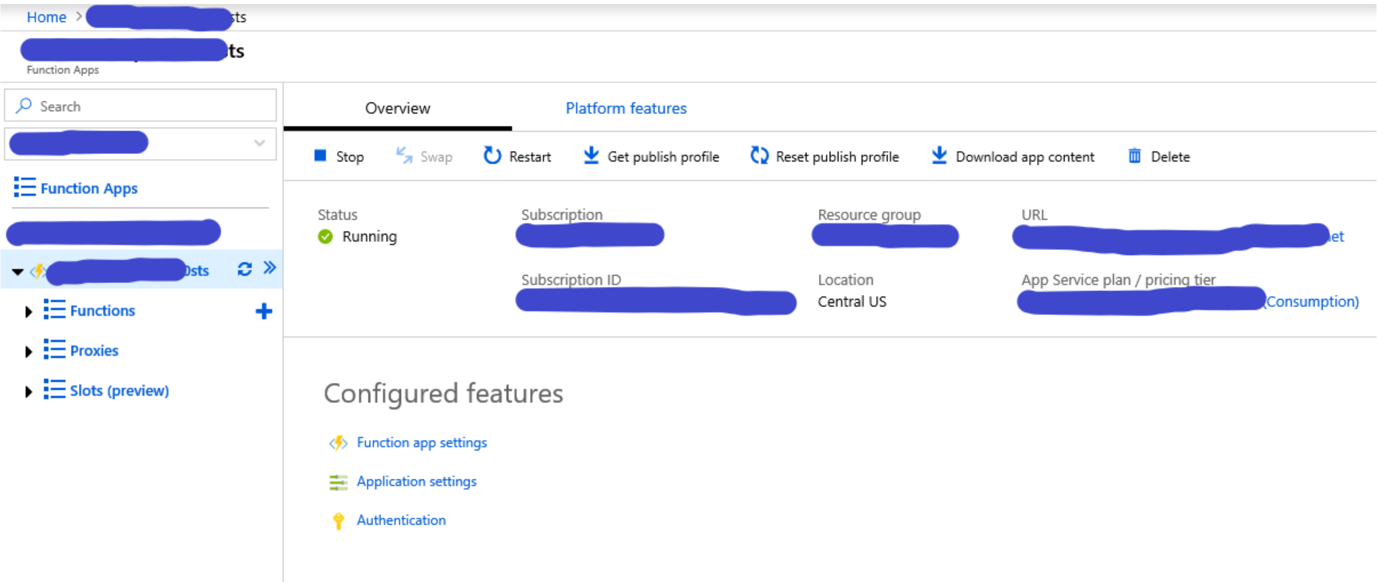
Create shared access policies

1. Sign in to the Azure portal.
2. On the **Service Bu**s menu, select the service bus that matches the name that you created earlier.
3. Under **Settings**, select **Shared access policies**, and then click **Add**.
4. On the **Add SAS policy** blade, enter a new policy name, such as SendListen. Select the **Send** and **Listen** check boxes, and then click **Create**.
5. The SAS policy name that you entered should then be used as the Azure service identity name value in the connector parameters.
6. Select the new shared access policy (SendListen), and copy the primary key that should be used as the Azure service identity password value in the connector parameters.

Configure Azure active directory for authentication

Validate the function app creation

1. Sign in to the Azure portal.
2. Search for Function Apps and open them.
3. On the **Service Bus** menu, select the service bus that matches the name that you created earlier.



Home > [redacted]ts

[redacted]ts

Function Apps

Status: Running

Subscription: [redacted]

Resource group: [redacted]

URL: [redacted]et

Subscription ID: [redacted]

Location: Central US

App Service plan / pricing tier: [redacted](Consumption)

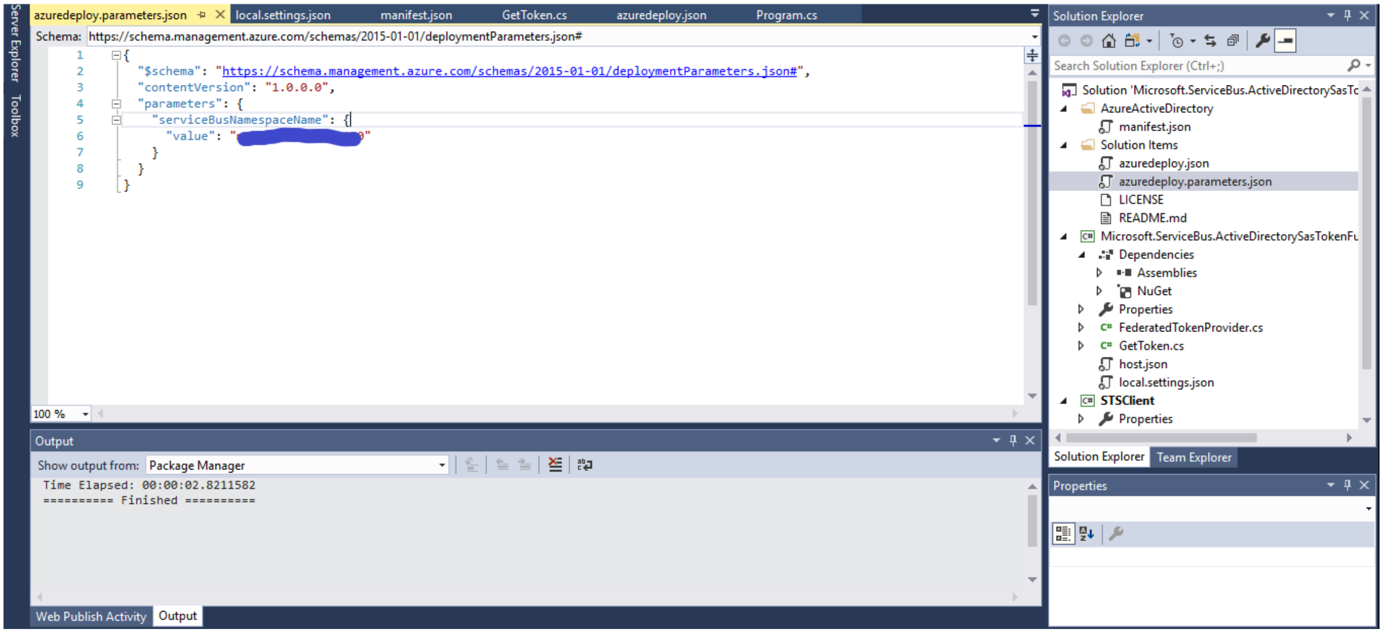
Configured features

Add GetToken function to the function app:

1 Open the ActiveDirectorySASTokenFunction solution in Visual Studio from the extracted folder.

2 Enter the service bus namespace values in the azuredeploy.parameters.json and local.settings.json files as shown in the following screenshots.

3 Open the Azuredeploy.parameters.json file in AzureActiveDirectory project and enter the service bus namespace for the servicebusNamespaceName parameter.



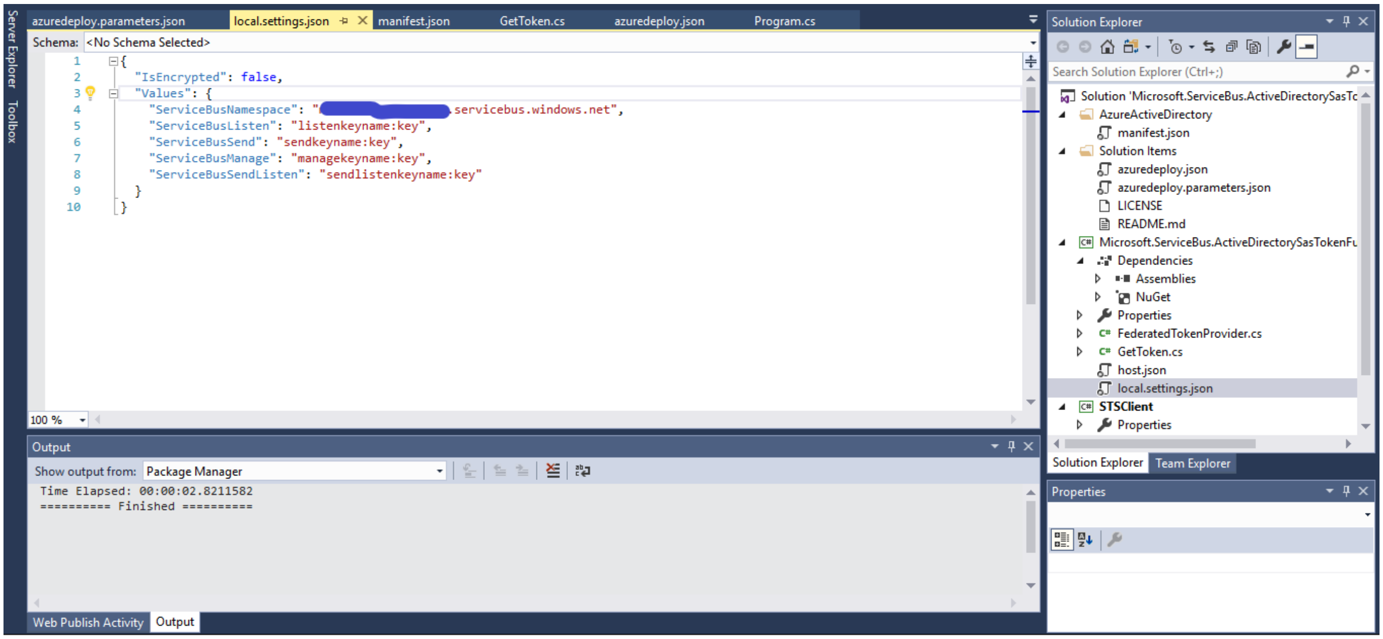
Schema: https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "serviceBusNamespaceName": {
      "value": "[redacted]"
    }
  }
}
```

Show output from: Package Manager

```
Time Elapsed: 00:00:02.8211582
========== Finished ==========
```

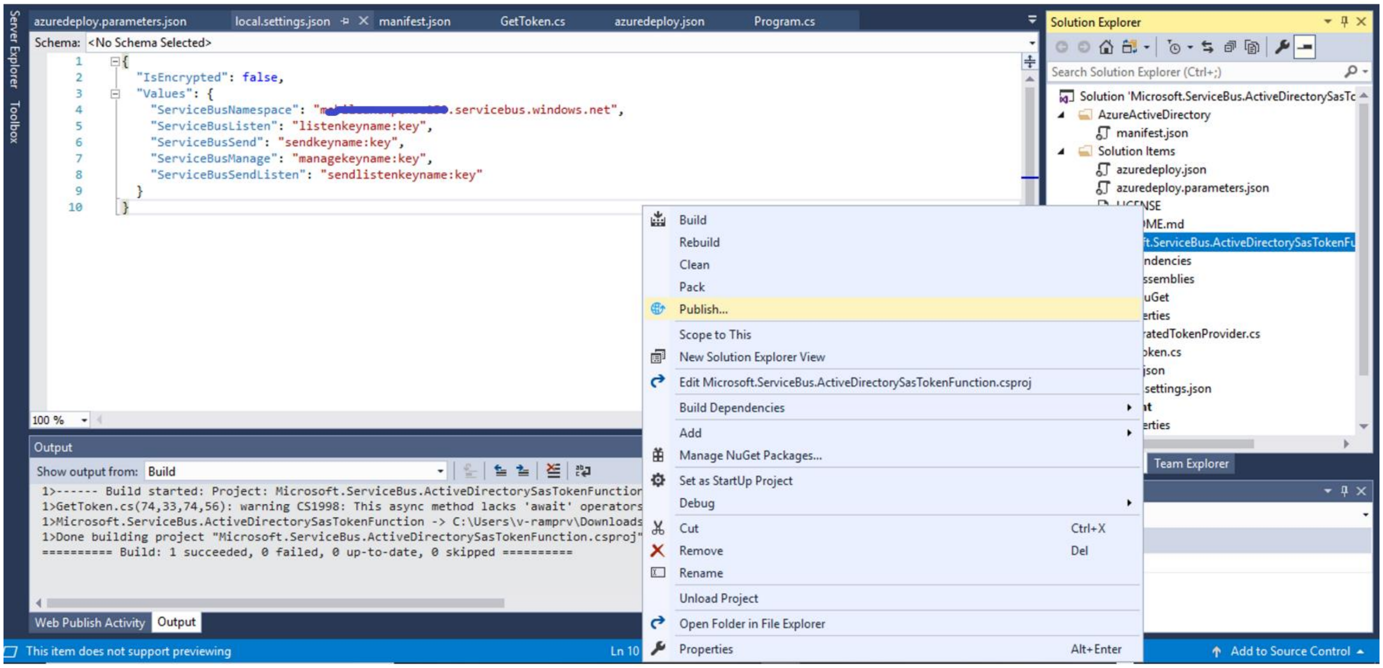
4 Open the local.settings.json file in Microsoft.ServiceBus.ActiveDirectorySasTokenFunction project and enter the service bus name space in ServiceBusNamespaceName parameter.



```
{
  "IsEncrypted": false,
  "Values": {
    "ServiceBusNamespace": "[redacted].servicebus.windows.net",
    "ServiceBusListen": "listenkeyname:key",
    "ServiceBusSend": "sendkeyname:key",
    "ServiceBusManage": "managekeyname:key",
    "ServiceBusSendListen": "sendlistenkeyname:key"
  }
}
```

```
Time Elapsed: 00:00:02.8211582
========== Finished ==========
```

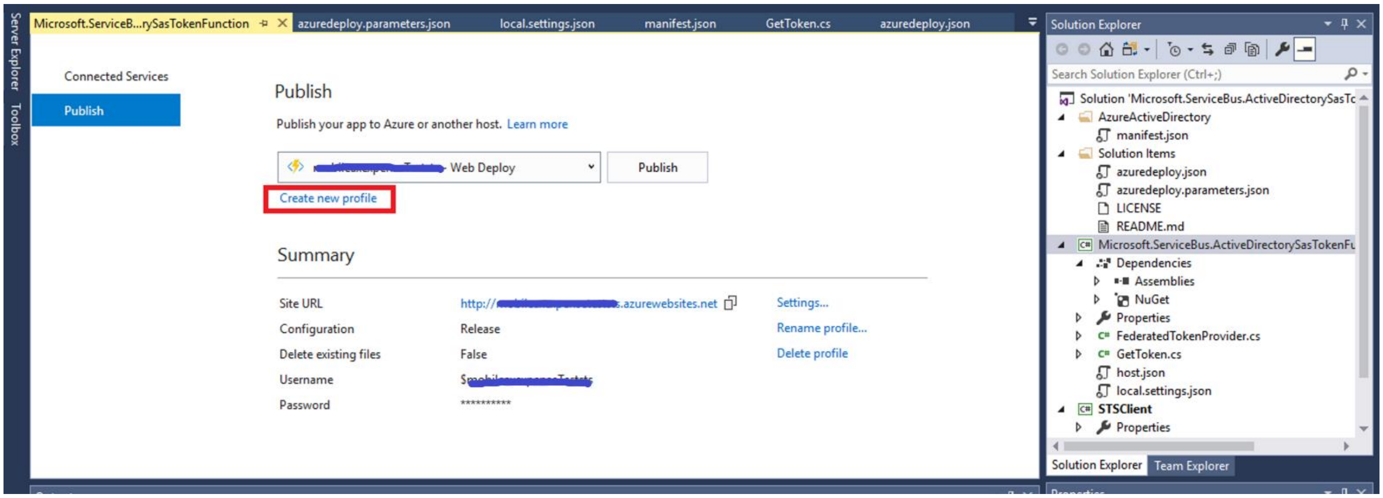
5 Right-click the Microsoft.ServiceBus.ActiveDirectorySasTokenFunction project and click **Publish** to open a publish tab.



```
{
  "IsEncrypted": false,
  "Values": {
    "ServiceBusNamespace": "[redacted].servicebus.windows.net",
    "ServiceBusListen": "listenkeyname:key",
    "ServiceBusSend": "sendkeyname:key",
    "ServiceBusManage": "managekeyname:key",
    "ServiceBusSendListen": "sendlistenkeyname:key"
  }
}
```

```
1>------ Build started: Project: Microsoft.ServiceBus.ActiveDirectorySasTokenFunctior
1>GetToken.cs(74,33,74,56): warning CS1998: This async method lacks 'await' operators
1>Microsoft.ServiceBus.ActiveDirectorySasTokenFunction -> C:\Users\v-ramprv\Downloads
1>Done building project "Microsoft.ServiceBus.ActiveDirectorySasTokenFunction.csproj"
========== Build: 1 succeeded, 0 failed, 0 up-to-date, 0 skipped ==========
```

6 In the **Publish** window, click **Create new profile**.



Publish

Publish your app to Azure or another host. Learn more

[redacted] Web Deploy | Publish

Create new profile

Summary

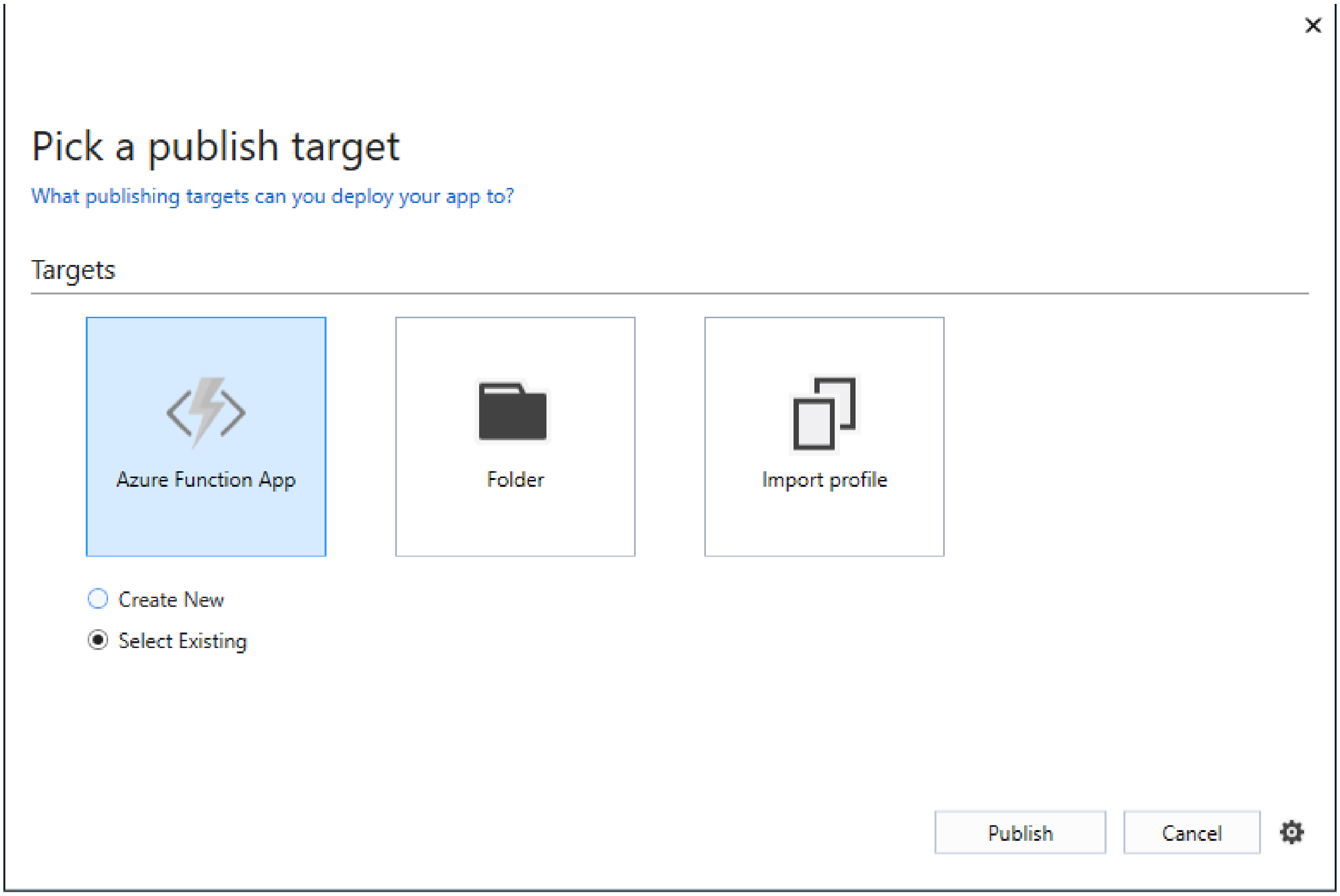
Site URL	http://[redacted].azurewebsites.net	Settings...
Configuration	Release	Rename profile...
Delete existing files	False	Delete profile
Username	[redacted]	
Password	**********	

Solution Explorer

Search Solution Explorer (Ctrl+;)

- Solution 'Microsoft.ServiceBus.ActiveDirectorySasTo
  - AzureActiveDirectory
    - manifest.json
  - Solution Items
    - azuredeploy.json
    - azuredeploy.parameters.json
    - LICENSE
    - README.md
  - Microsoft.ServiceBus.ActiveDirectorySasTokenFu
    - Dependencies
      - Assemblies
      - NuGet
    - Properties
    - FederatedTokenProvider.cs
    - GetToken.cs
    - host.json
    - local.settings.json
  - STSClient
    - Properties

7 In the **Pick a publish target** window, select **Azure function app**. Select **Create new** or **Select existing**.



Pick a publish target

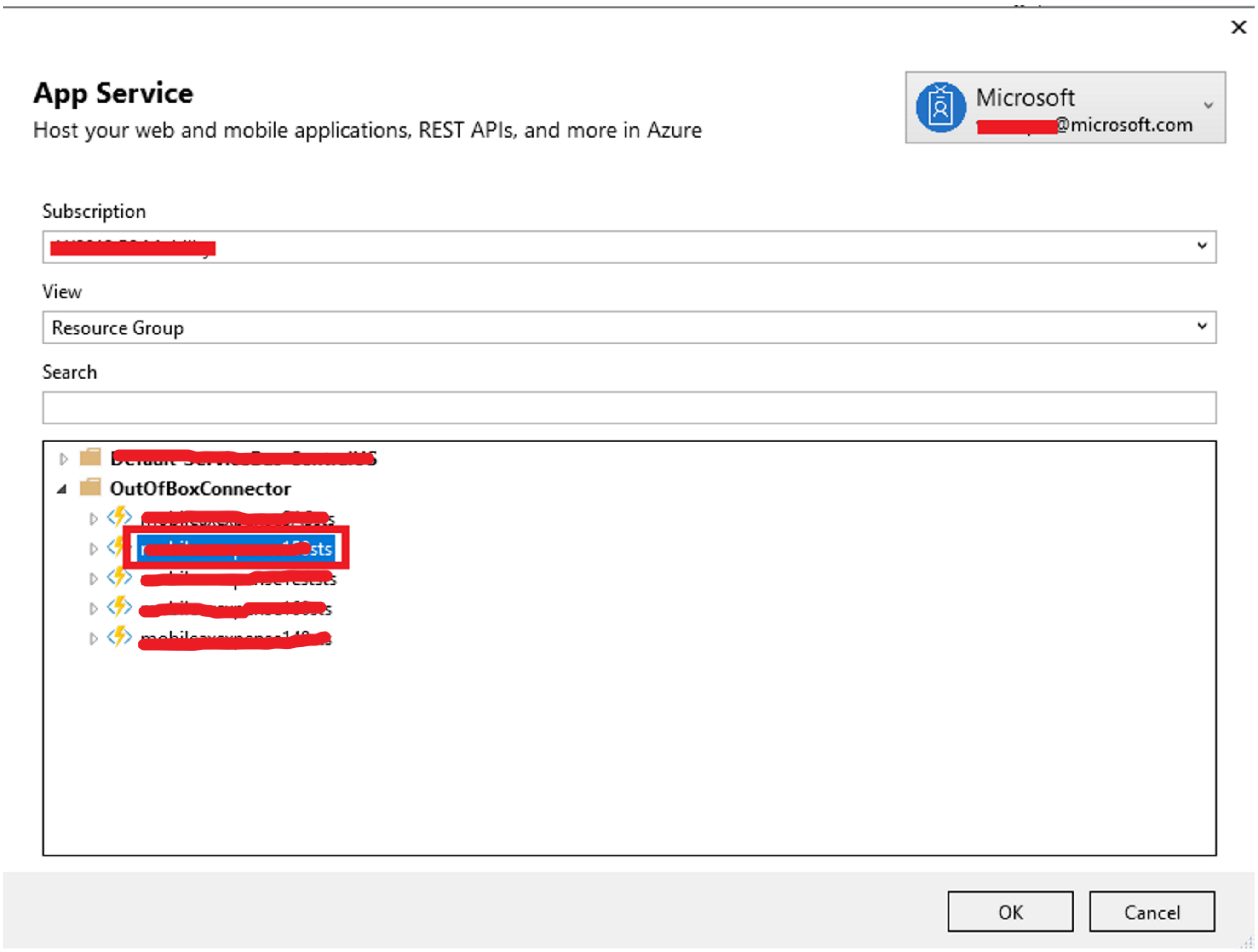
What publishing targets can you deploy your app to?

Targets

○ Create New

● Select Existing

8 This opens up the **Create App Service** window. On the **Hosting** tab, select the newly created function app (typically the name will be "<servicebusName>sts"). Select the **Subscription**, **Resource group**, and **App service plan**.



App Service

Host your web and mobile applications, REST APIs, and more in Azure

Microsoft
[redacted]@microsoft.com

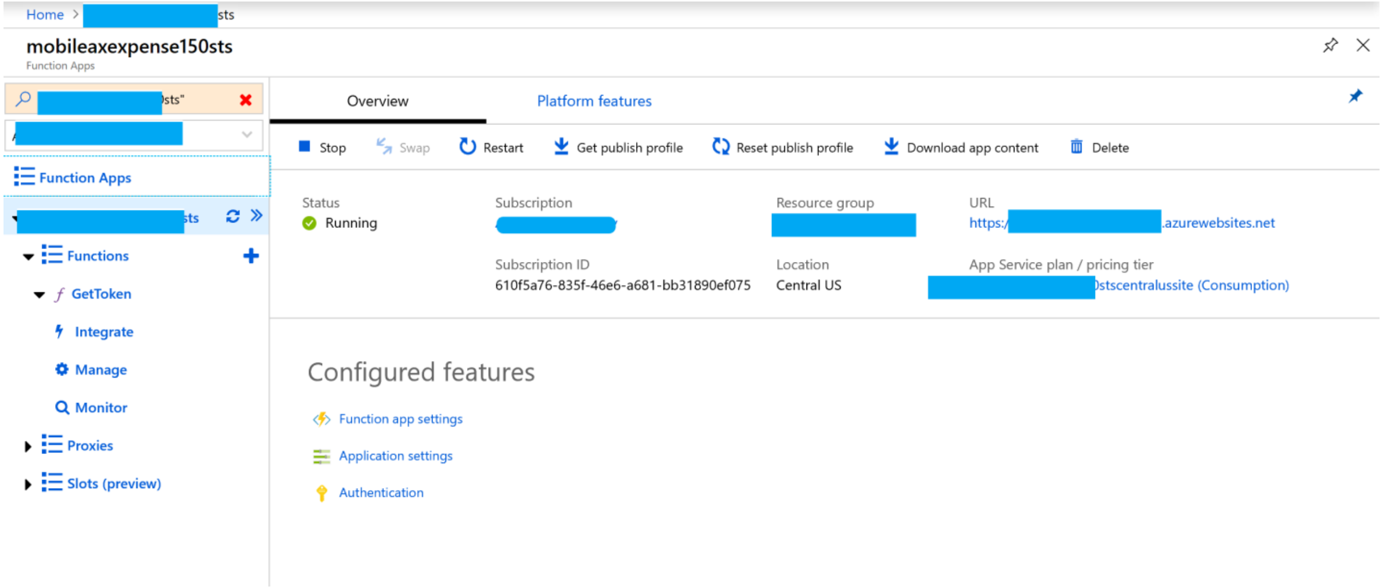
Subscription: [redacted]

View: Resource Group

Search:

[redacted]
OutOfBoxConnector
[redacted]
[redacted]sts
[redacted]
[redacted]
[redacted]

9 Click **OK** to deploy GetToken function, which can be used to retrieve the token.



Home > [redacted]sts

mobileaxexpense150sts
Function Apps

[redacted]sts"
[redacted]

Status: Running

Subscription: [redacted]

Resource group: [redacted]

URL: https:/[redacted].azurewebsites.net

Subscription ID: 610f5a76-835f-46e6-a681-bb31890ef075

Location: Central US

App Service plan / pricing tier: [redacted]0stscentralussite (Consumption)

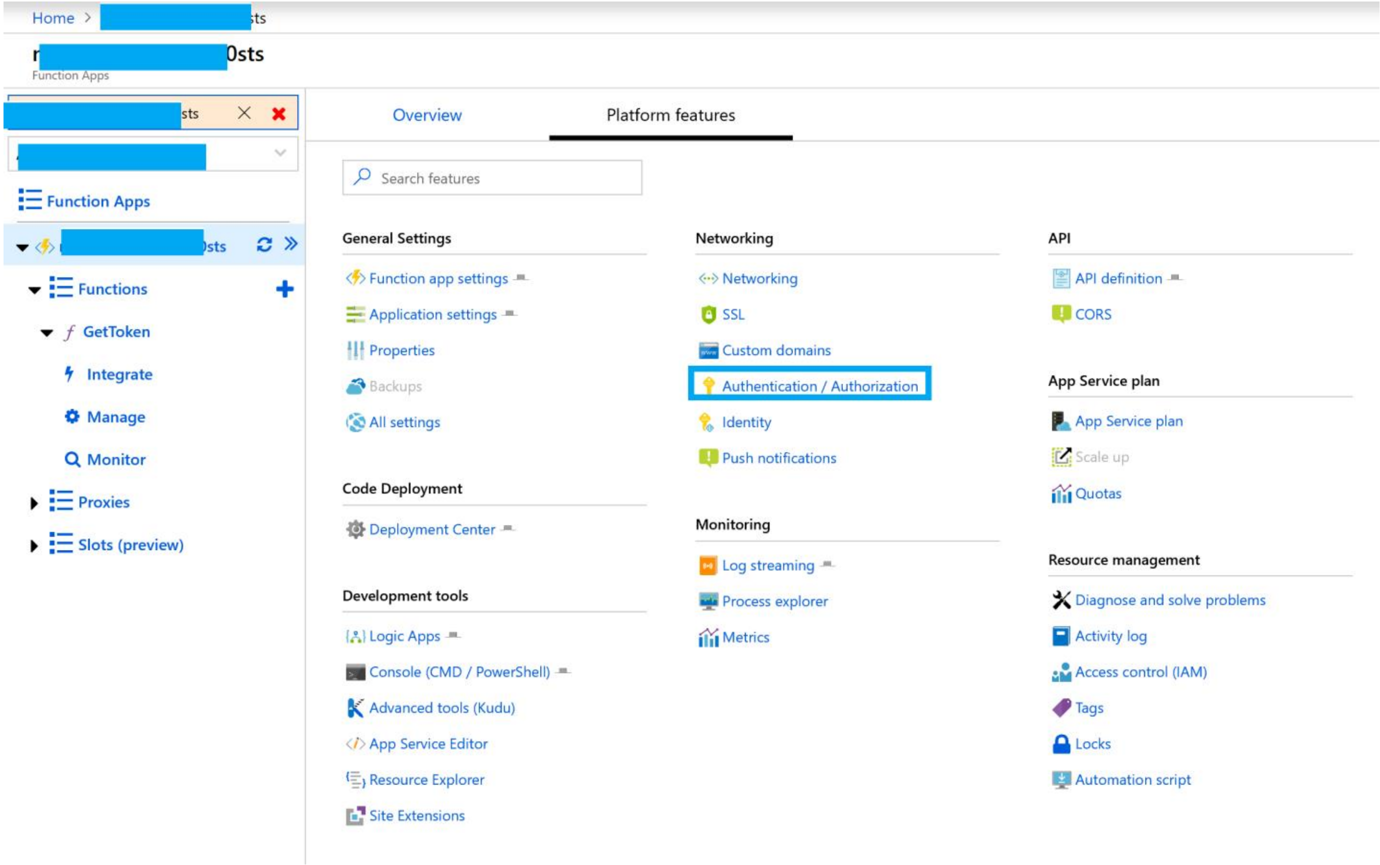
Configured features

Enabling Active Directory for the Function app

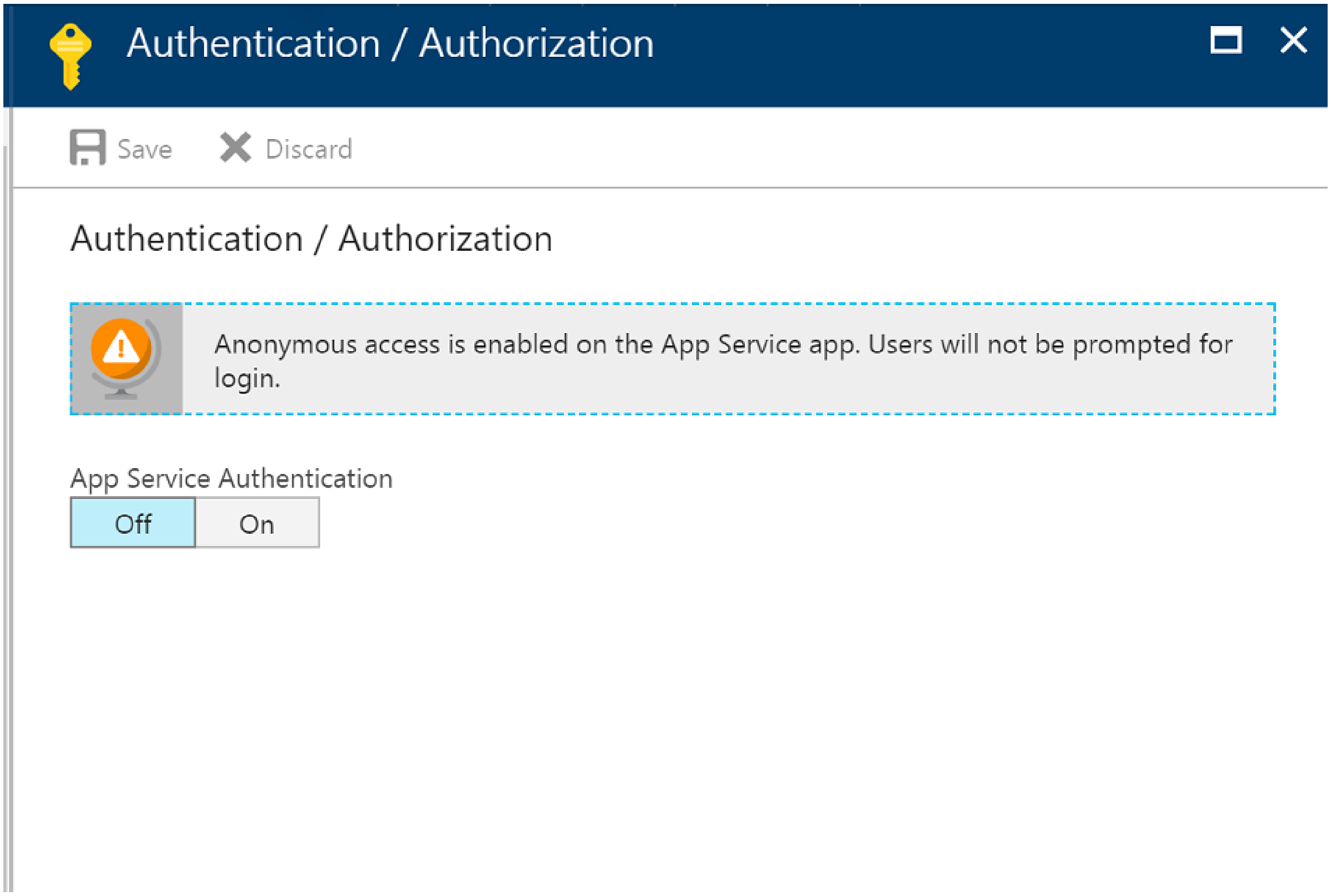
After the Function app is set up and the code is deployed, the Function needs to be enabled for Active Directory. This is best done through the Azure portal.

Setting up authorization

1 First, find your application in the Azure portal and go to the **Platform Features** tab. Find **Authentication/Authorization**.



2 The **Authentication/Authorization** blade will show the feature turned off. Turn it on.

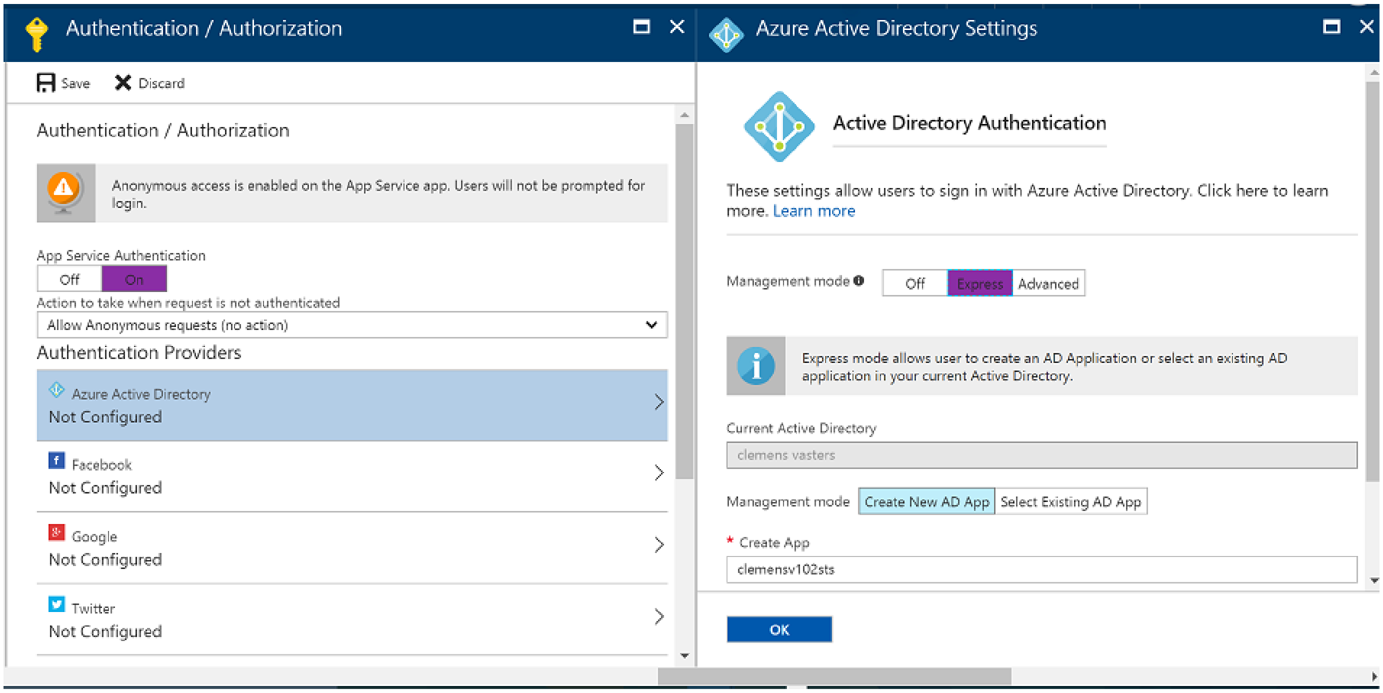


Authentication / Authorization

Anonymous access is enabled on the App Service app. Users will not be prompted for login.

App Service Authentication: Off | On (Off selected)

3 Next, select the Azure Active Directory authentication provider, set the management mode to **Express** and provide a name for the app to create or select the existing app. This should be the same as the STS function app name, something like this <*servicebusnamespace*>*STS*.


Authentication / Authorization
Save
Discard
Azure Active Directory Settings
OK

Authentication / Authorization

Anonymous access is enabled on the App Service app. Users will not be prompted for login.

App Service Authentication: Off | On (On selected)

Action to take when request is not authenticated: Allow Anonymous requests (no action)

Authentication Providers

Azure Active Directory	Not Configured
Facebook	Not Configured
Google	Not Configured
Twitter	Not Configured

Active Directory Authentication

These settings allow users to sign in with Azure Active Directory. Click here to learn more. Learn more

Management mode: Off | Express | Advanced (Express selected)

Express mode allows user to create an AD Application or select an existing AD application in your current Active Directory.

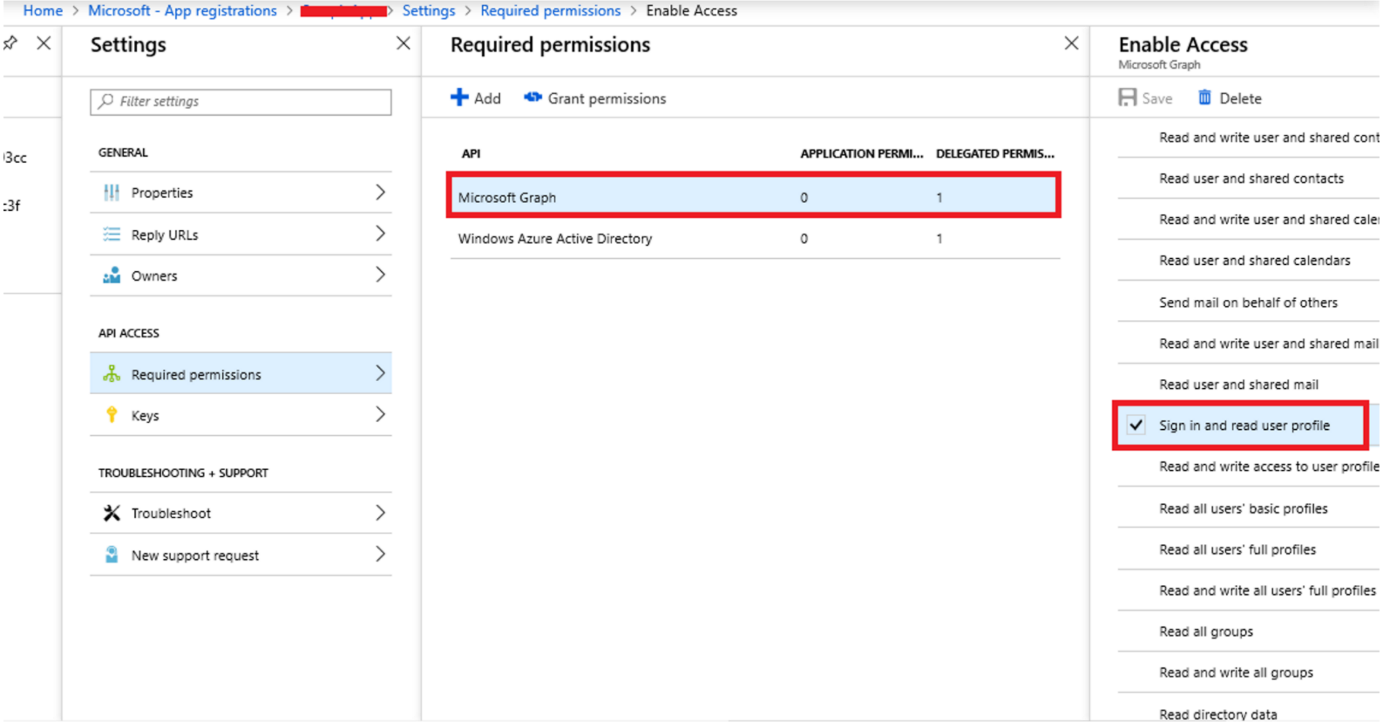
Current Active Directory: clemens vasters

Management mode: Create New AD App | Select Existing AD App (Create New AD App selected)

* Create App: clemensv102sts

4 After you click **OK**, and save the resulting changes to your Function app, Azure will run an automated deployment in the background that creates the Active Directory app entry and wires it to the Functions app.

5 Go to **App Registrations** and search for the newly created Active Directory app in the list. Add and enable the required permissions for the Microsoft Graph API and Windows Azure Active Directory API as shown below.



Home > Microsoft - App registrations > [redacted] > Settings > Required permissions > Enable Access

3cc

:3f

Settings

Filter settings

GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

Required permissions

Add | Grant permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Microsoft Graph	0	1
Windows Azure Active Directory	0	1

Enable Access

Microsoft Graph

Save | Delete

Read and write user and shared cont

Read user and shared contacts

Read and write user and shared cale

Read user and shared calendars

Send mail on behalf of others

Read and write user and shared mail

Read user and shared mail

☑ Sign in and read user profile

Read and write access to user profile

Read all users' basic profiles

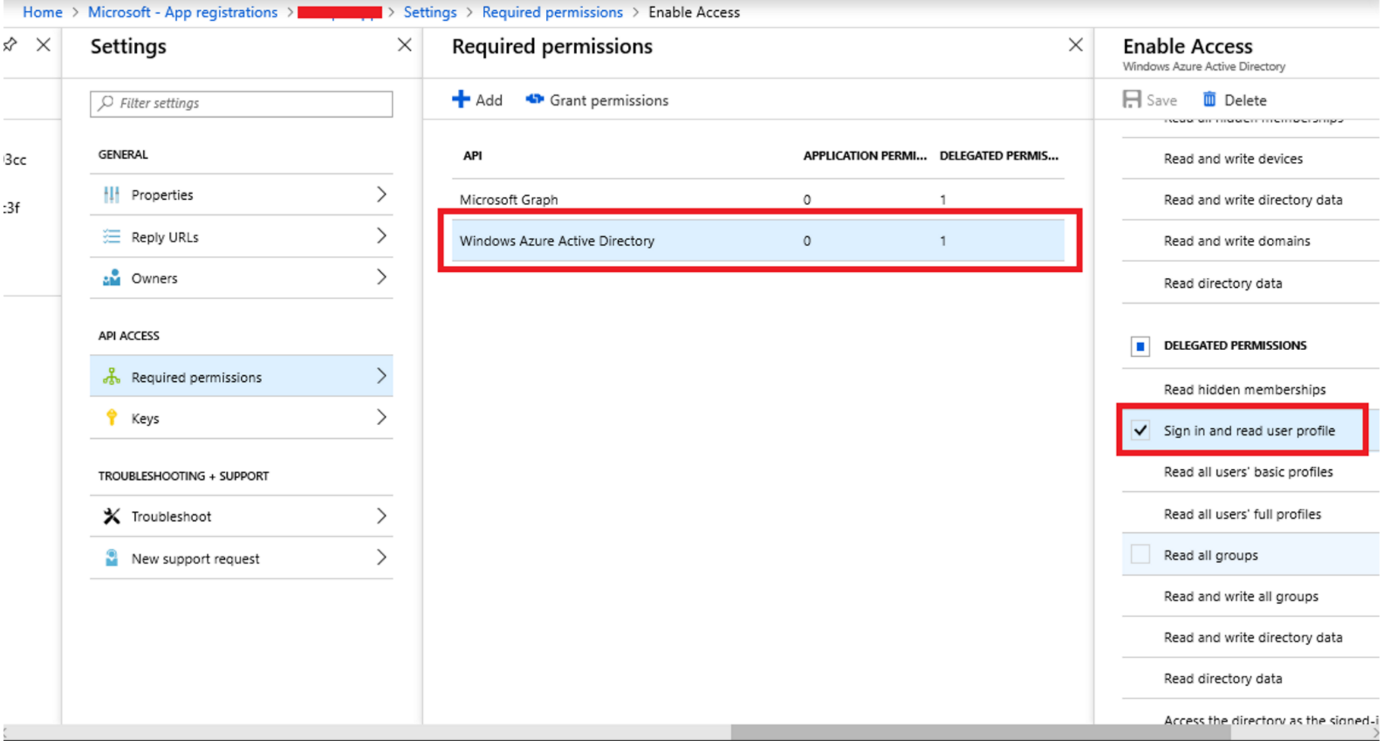
Read all users' full profiles

Read and write all users' full profiles

Read all groups

Read and write all groups

Read directory data



Home > Microsoft - App registrations > [redacted] > Settings > Required permissions > Enable Access

3cc

:3f

Settings

Filter settings

GENERAL

- Properties
- Reply URLs
- Owners

API ACCESS

- Required permissions
- Keys

TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

Required permissions

Add | Grant permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
Microsoft Graph	0	1
Windows Azure Active Directory	0	1

Enable Access

Windows Azure Active Directory

Save | Delete

Read and write devices

Read and write directory data

Read and write domains

Read directory data

■ DELEGATED PERMISSIONS

Read hidden memberships

☑ Sign in and read user profile

Read all users' basic profiles

Read all users' full profiles

☐ Read all groups

Read and write all groups

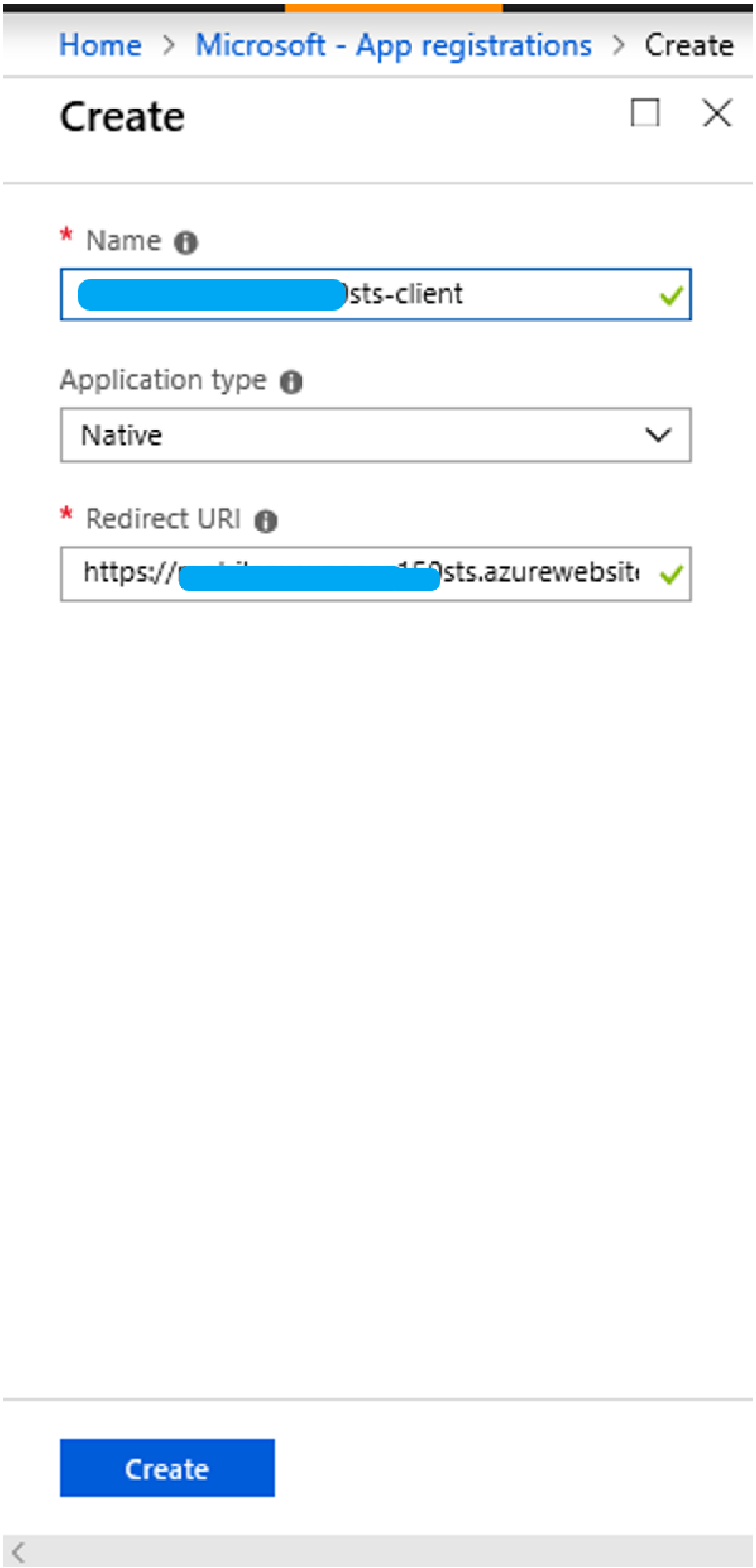
Read and write directory data

Read directory data

Access the directory as the signed-i

6 To be able to log into the STS (the Functions app) with a client and obtain a Service Bus token, you need to create a client application. This client application needs to be permitted to access the STS.

7 Go to **App Registrations**. Click **New application registration** to create an identity for your client application. This is what will be done for each new client. The name needs to be unique inside the tenant. The URL isn't used but will need to be syntactically valid.



Home > Microsoft - App registrations > Create

Create

* Name

[redacted]sts-client ✓

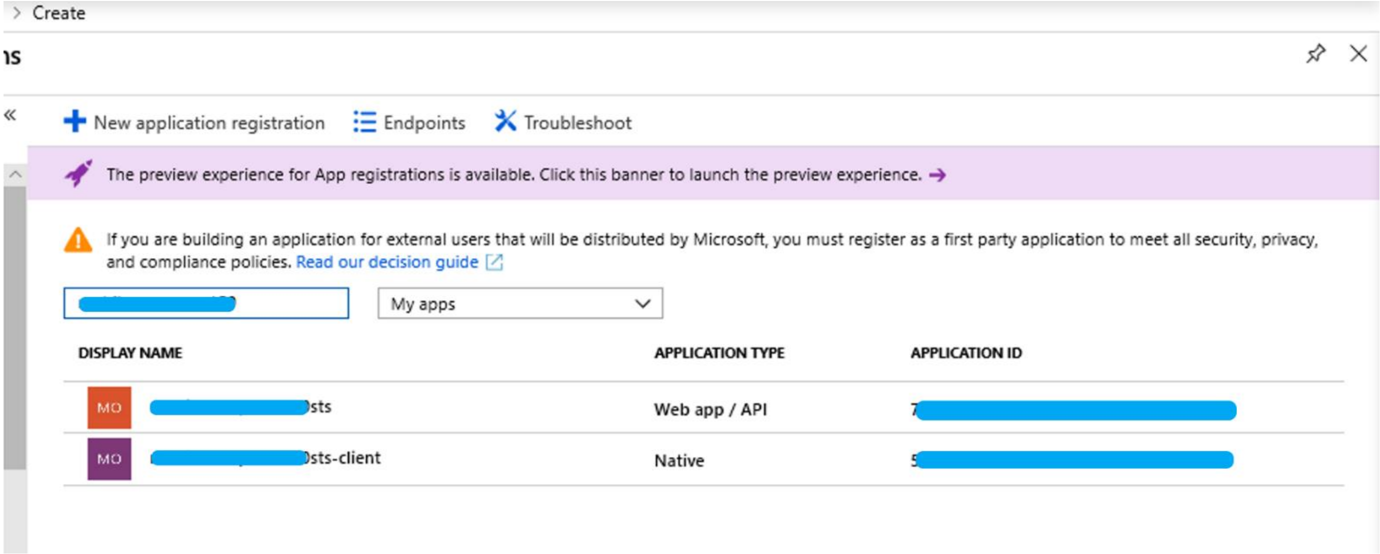
Application type

Native

* Redirect URI

https://[redacted]sts.azurewebsit ✓

8 After you've created the new identity, go to **App registrations** to find the Native app registration in the list and click on the display name to open the Settings view.



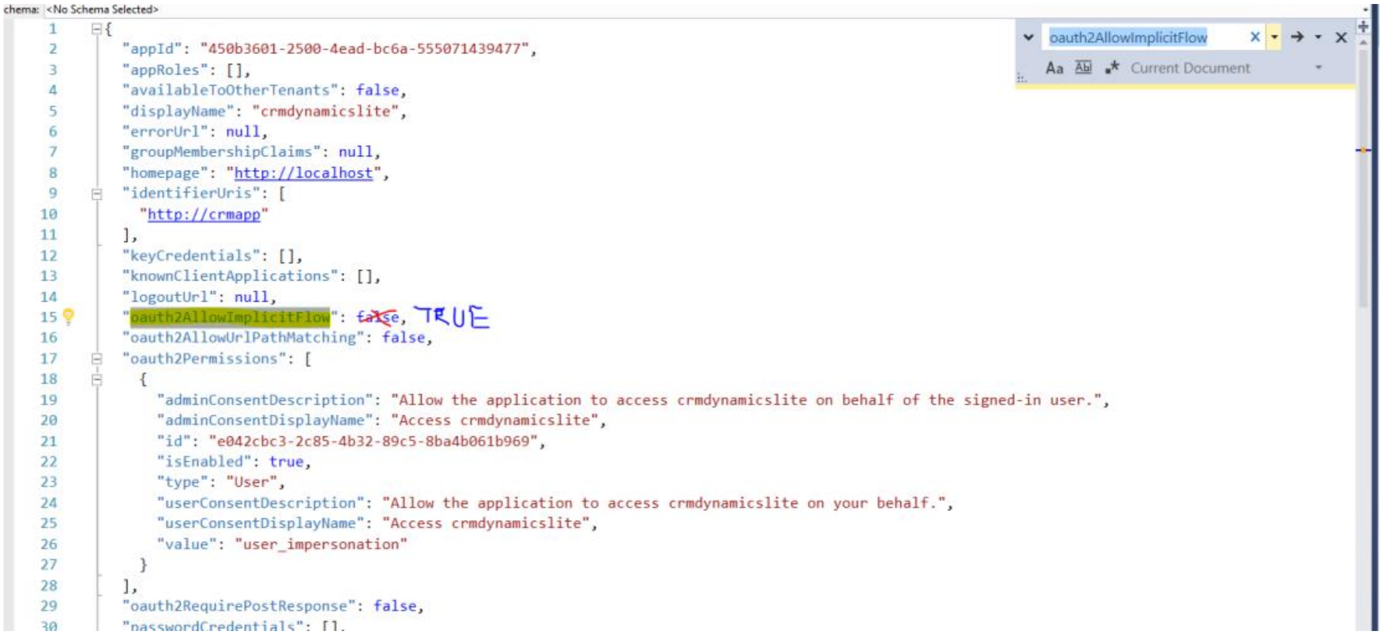
The preview experience for App registrations is available. Click this banner to launch the preview experience. →

If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. Read our decision guide

[redacted] My apps

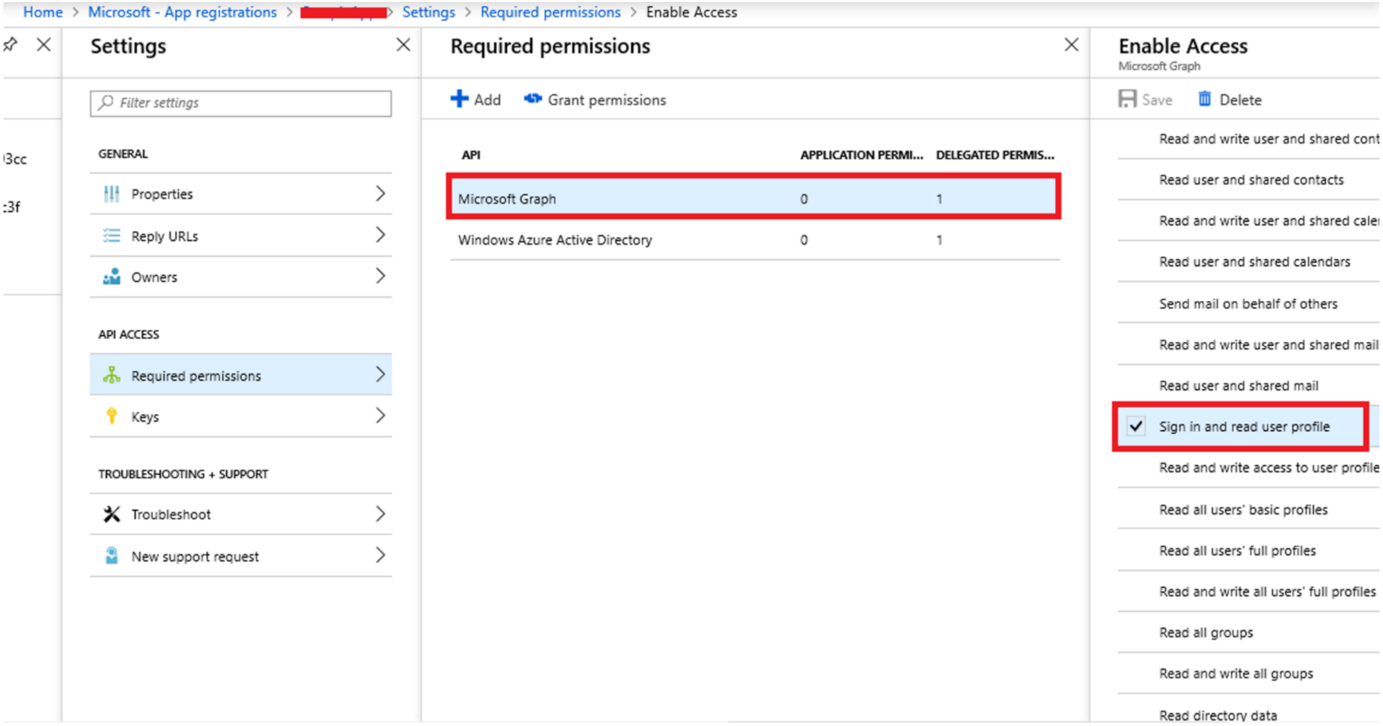
DISPLAY NAME	APPLICATION TYPE	APPLICATION ID
MO [redacted]sts	Web app / API	[redacted]
MO [redacted]sts-client	Native	[redacted]

9. Click the **Manifest** button to open the manifest file with a text editor for the newly created client application. Search for the ***oauth2AllowImplicitFlow*** property. By default, it is set to false; change it to ***true*** and save the file.



```
{
  "appId": "450b3601-2500-4ead-bc6a-555071439477",
  "appRoles": [],
  "availableToOtherTenants": false,
  "displayName": "crmdynamicslite",
  "errorUrl": null,
  "groupMembershipClaims": null,
  "homepage": "http://localhost",
  "identifierUris": [
    "http://crmapp"
  ],
  "keyCredentials": [],
  "knownClientApplications": [],
  "logoutUrl": null,
  "oauth2AllowImplicitFlow": ~~false~~, TRUE
  "oauth2AllowUrlPathMatching": false,
  "oauth2Permissions": [
    {
      "adminConsentDescription": "Allow the application to access crmdynamicslite on behalf of the signed-in user.",
      "adminConsentDisplayName": "Access crmdynamicslite",
      "id": "e042cbc3-2c85-4b32-89c5-8ba4b061b969",
      "isEnabled": true,
      "type": "User",
      "userConsentDescription": "Allow the application to access crmdynamicslite on your behalf.",
      "userConsentDisplayName": "Access crmdynamicslite",
      "value": "user_impersonation"
    }
  ],
  "oauth2RequirePostResponse": false,
  "passwordCredentials": [],
```

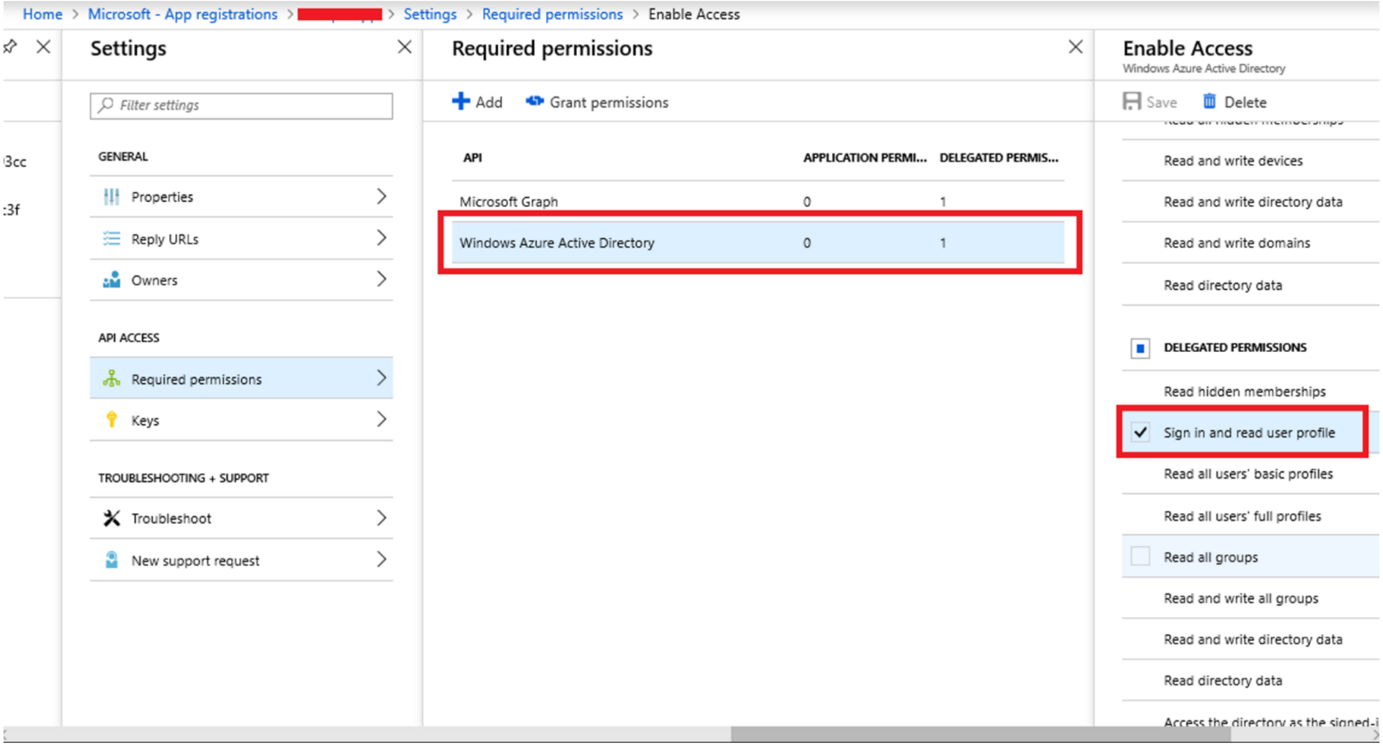
9 Switch to the **Required Permissions** blade. Add and enable the required permissions for the Microsoft Graph API, Windows Azure Active Directory API and STS application, as shown below.



Home > Microsoft - App registrations > [redacted] > Settings > Required permissions > Enable Access

API	APPLICATION PERMI...	DELEGATED PERMIS...
Microsoft Graph	0	1
Windows Azure Active Directory	0	1

- Read and write user and shared cont
- Read user and shared contacts
- Read and write user and shared cale
- Read user and shared calendars
- Send mail on behalf of others
- Read and write user and shared mail
- Read user and shared mail
- ☑ Sign in and read user profile
- Read and write access to user profile
- Read all users' basic profiles
- Read all users' full profiles
- Read and write all users' full profiles
- Read all groups
- Read and write all groups
- Read directory data



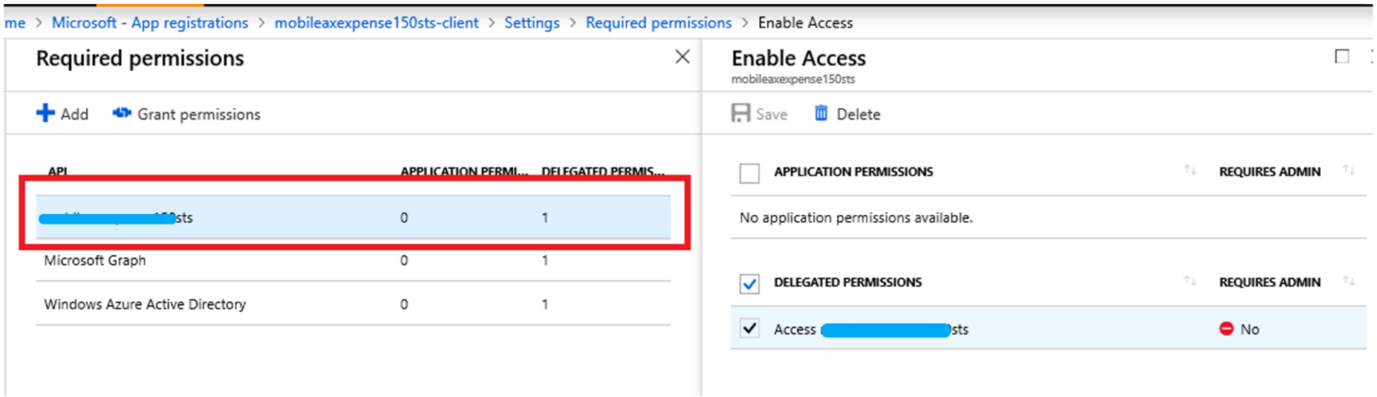
Home > Microsoft - App registrations > [redacted] > Settings > Required permissions > Enable Access

API	APPLICATION PERMI...	DELEGATED PERMIS...
Microsoft Graph	0	1
Windows Azure Active Directory	0	1

- Read and write devices
- Read and write directory data
- Read and write domains
- Read directory data

■ DELEGATED PERMISSIONS

- Read hidden memberships
- ☑ Sign in and read user profile
- Read all users' basic profiles
- Read all users' full profiles
- □ Read all groups
- Read and write all groups
- Read and write directory data
- Read directory data
- Access the directory as the signed-i



me > Microsoft - App registrations > mobileaxexpense150sts-client > Settings > Required permissions > Enable Access

Required permissions

API	APPLICATION PERMI...	DELEGATED PERMIS...
[redacted]sts	0	1
Microsoft Graph	0	1
Windows Azure Active Directory	0	1

Enable Access

mobileaxexpense150sts

□ APPLICATION PERMISSIONS	REQUIRES ADMIN
No application permissions available.	

☑ DELEGATED PERMISSIONS	REQUIRES ADMIN
✓ Access [redacted]sts	⛔ No

10 You need to provide the redirect URI's for the client application to be able to redirect back after the SAS token authentication.

Go to the **Redirect URIs** blade, and provide the redirect URI's for the applications in different platforms, such as Windows desktop, Android, and iOS.

For the Windows desktop expense app

ms-app://S-1-15-2-3928788700-3789986351-3052964962-3352193189-1654392005-971744669-2270453158/

For the Windows desktop timesheet app

ms-app://s-1-15-2-1686823218-3869368799-4003585847-1074717996-2718656644-2639155508-3087402168

For the Windows desktop approvals app

ms-app://s-1-15-2-256616160-1993905071-509288680-1590138783-827304346-2645043696-2039586845

For the Google Android app

msauth://microsoft.dynamicsax/azvBvNWkMH4gNvJYX3ssUoXXqDI=

For the Apple iOS app

x-msauth-dynamicsax://com.microsoft.dynamics.ax

You have now completed the setup required for AAD authentication. Got to the “Configure the on-premises server with AX 2012 and the connector” section.

Configure the on-premises server with AX 2012 and the connector

Update Microsoft Dynamics AX 2012 R2

Note that this fix is no longer published as a KB since it is included with Microsoft Dynamics AX 2012 R3.

Set up unreconciled expenses

Deploy the TrvUnreconciledExpense service

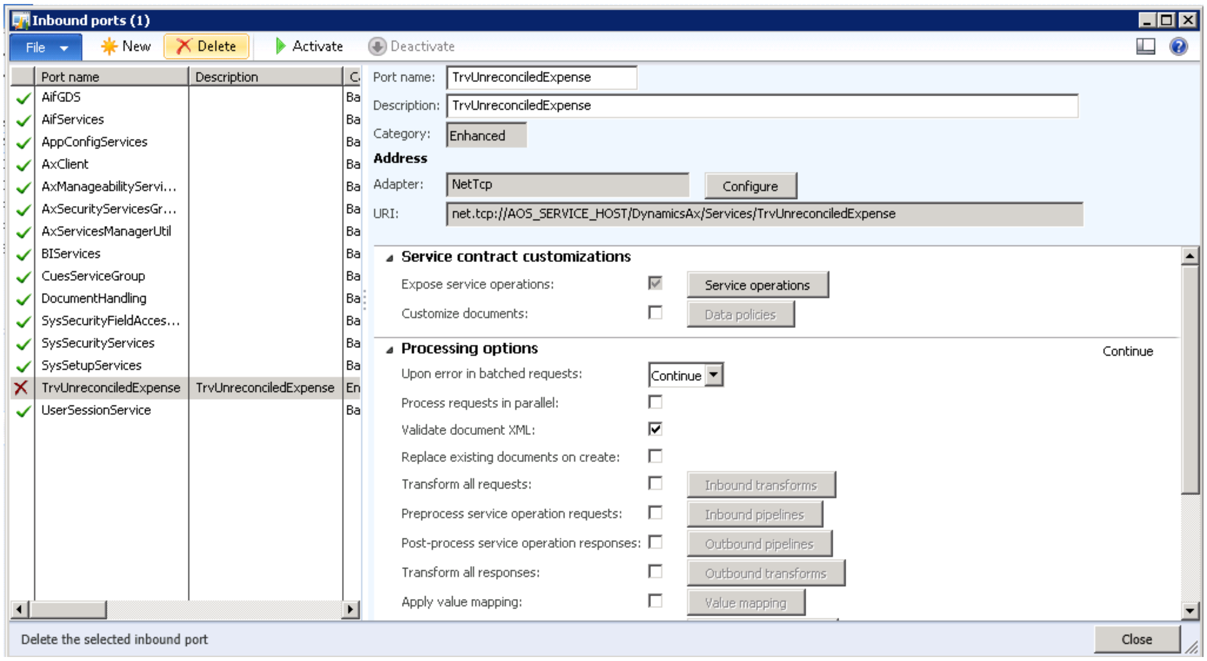
- In the Developer Workspace, click **Services** > **TrvUnreconciledExpense**. Right-click, and then select **Add ins** > **Register service**.

Set up inbound ports

1 In Microsoft Dynamics AX, click **System Administration** > **Services and Application integration framework** > **Inbound ports.**

2 Create a new port, and enter a name and description.

3 On the **Service contract customizations** FastTab, click **Service operations**. The Web Services Description Language (WSDL) URI is filled in.



	Port name	Description	C.
✓	AifGDS		Ba
✓	AifServices		Ba
✓	AppConfigServices		Ba
✓	AxClient		Ba
✓	AxManageabilityServi...		Ba
✓	AxSecurityServicesGr...		Ba
✓	AxServicesManagerUtil		Ba
✓	BIServices		Ba
✓	CuesServiceGroup		Ba
✓	DocumentHandling		Ba
✓	SysSecurityFieldAcces...		Ba
✓	SysSecurityServices		Ba
✓	SysSetupServices		Ba
✗	TrvUnreconciledExpense	TrvUnreconciledExpense	En
✓	UserSessionService		Ba

Port name: TrvUnreconciledExpense

Description: TrvUnreconciledExpense

Category: Enhanced

Address

Adapter: NetTcp [Configure]

URI: net.tcp://AOS_SERVICE_HOST/DynamicsAx/Services/TrvUnreconciledExpense

Service contract customizations

Expose service operations: ☑ [Service operations]

Customize documents: □ [Data policies]

Processing options Continue

Upon error in batched requests: Continue

Process requests in parallel: □

Validate document XML: ☑

Replace existing documents on create: □

Transform all requests: □ [Inbound transforms]

Preprocess service operation requests: □ [Inbound pipelines]

Post-process service operation responses: □ [Outbound pipelines]

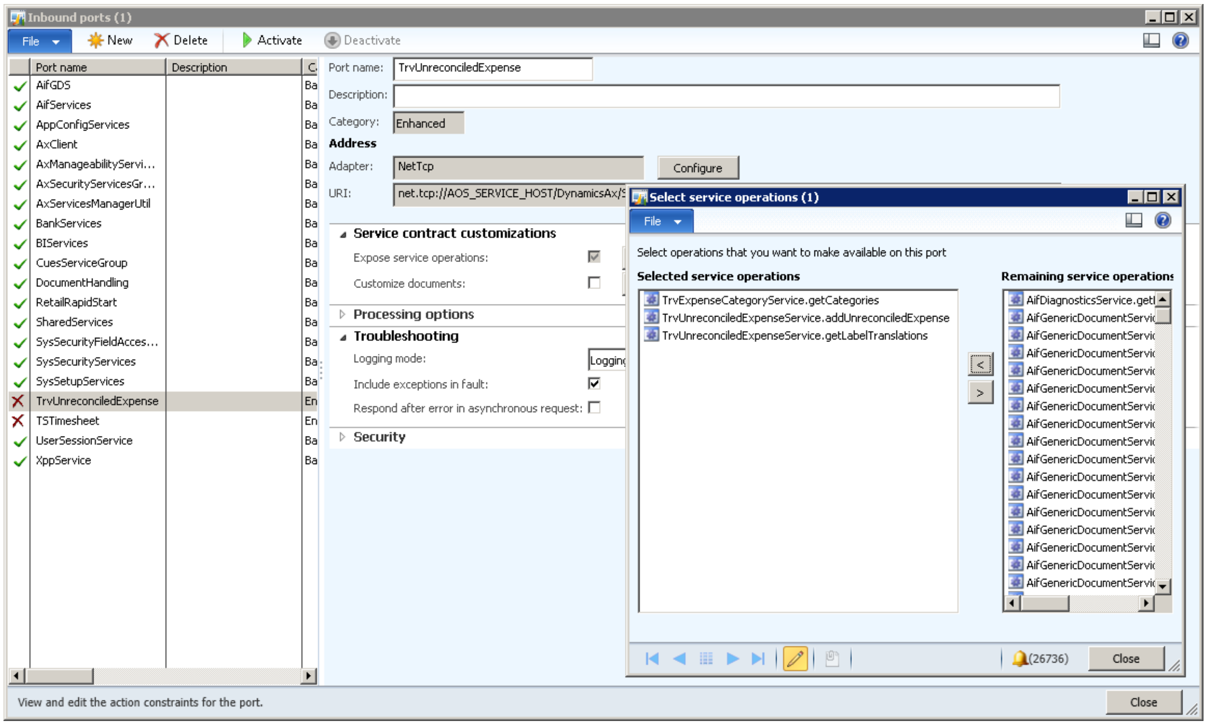
Transform all responses: □ [Outbound transforms]

Apply value mapping: □ [Value mapping]

Delete the selected inbound port

4 In the **Select service operations** form, in the **Remaining service operations** list, select the following service operations, and then click the left arrow button (**<**) to add them to the **Selected service operations** list:

- TrvExpenseCategoryService.getCategories
- TrvUnreconciledExpenseService.addUnreconciledExpense
- TrvUnreconciledExpenseService.getLabelTranslations



	Port name	Description	C
✓	AifGDS		Ba
✓	AifServices		Ba
✓	AppConfigServices		Ba
✓	AxClient		Ba
✓	AxManageabilityServi...		Ba
✓	AxSecurityServicesGr...		Ba
✓	AxServicesManagerUtil		Ba
✓	BankServices		Ba
✓	BIServices		Ba
✓	CuesServiceGroup		Ba
✓	DocumentHandling		Ba
✓	RetailRapidStart		Ba
✓	SharedServices		Ba
✓	SysSecurityFieldAcces...		Ba
✓	SysSecurityServices		Ba
✓	SysSetupServices		Ba
✗	TrvUnreconciledExpense		En
✗	TSTimesheet		En
✓	UserSessionService		Ba
✓	XppService		Ba

Port name: TrvUnreconciledExpense

Description:

Category: Enhanced

Address

Adapter: NetTcp

URI: net.tcp://AOS_SERVICE_HOST/DynamicsAx/S

Service contract customizations

Expose service operations: ☑

Customize documents: ☐

Processing options

Troubleshooting

Logging mode: Loggin

Include exceptions in fault: ☑

Respond after error in asynchronous request: ☐

Security

Select operations that you want to make available on this port

Selected service operations

- TrvExpenseCategoryService.getCategories
- TrvUnreconciledExpenseService.addUnreconciledExpense
- TrvUnreconciledExpenseService.getLabelTranslations

Remaining service operations

- AifDiagnosticsService.getI
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic
- AifGenericDocumentServic

View and edit the action constraints for the port.

5 Close the **Select service operations** form.

6 On the **Troubleshooting** FastTab, select the **Include exceptions in fault** check box, and then click **Activate**.

Set up timesheets

Deploy the TSTimesheetService service

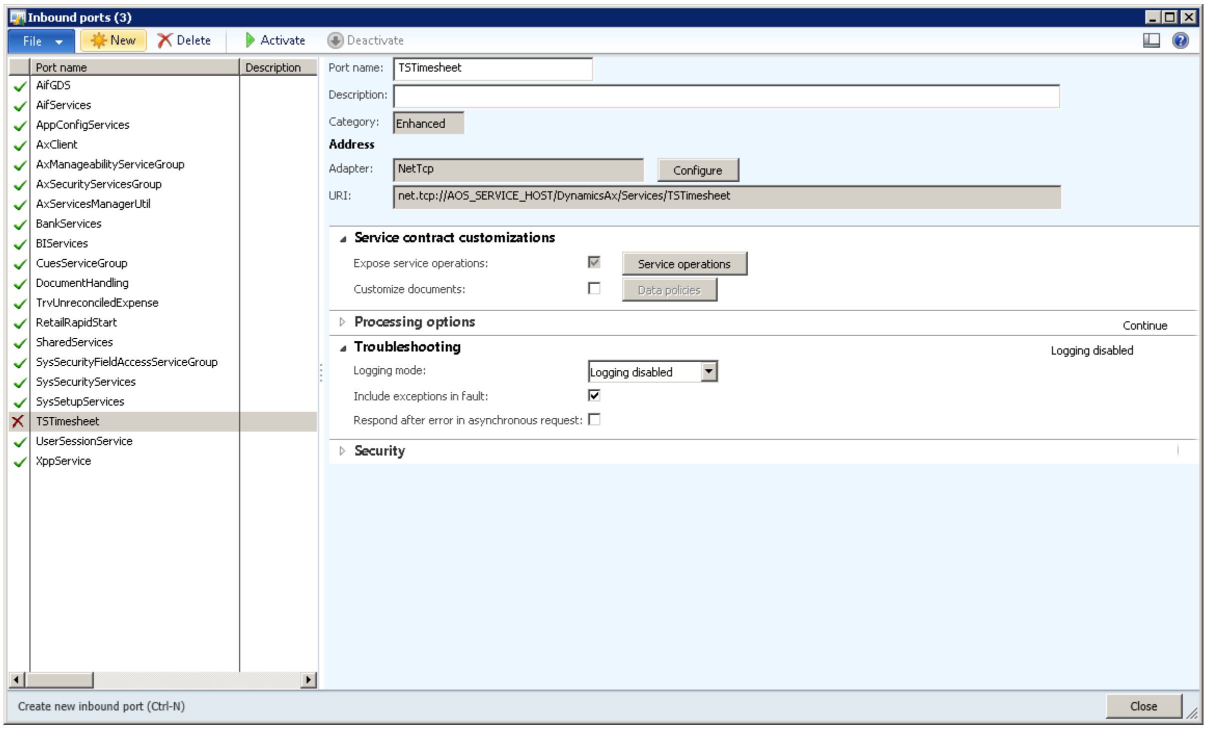
- In the Developer Workspace, click **Services** > **TSTimesheetService**. Right-click, and then select **Add ins** > **Register service**.

Set up inbound ports

1 In Microsoft Dynamics AX, click **System Administration** > **Services and Application integration framework** > **Inbound ports**.

2 Create a new port, and enter a name and description.

3 On the **Service contract customizations** FastTab, click **Service operations**. The WSDL URI is filled in.



Port name	Description
✓ AifGDS	
✓ AifServices	
✓ AppConfigServices	
✓ AxClient	
✓ AxManageabilityServiceGroup	
✓ AxSecurityServicesGroup	
✓ AxServicesManagerUtil	
✓ BankServices	
✓ BIServices	
✓ CuesServiceGroup	
✓ DocumentHandling	
✓ TrvUnreconciledExpense	
✓ RetailRapidStart	
✓ SharedServices	
✓ SysSecurityFieldAccessServiceGroup	
✓ SysSecurityServices	
✓ SysSetupServices	
✗ TSTimesheet	
✓ UserSessionService	
✓ XppService	

Port name: TSTimesheet
Description:
Category: Enhanced

Address

Adapter: NetTcp
URI: net.tcp://AOS_SERVICE_HOST/DynamicsAx/Services/TSTimesheet

Service contract customizations

Expose service operations: ☑
Customize documents: □

Processing options Continue

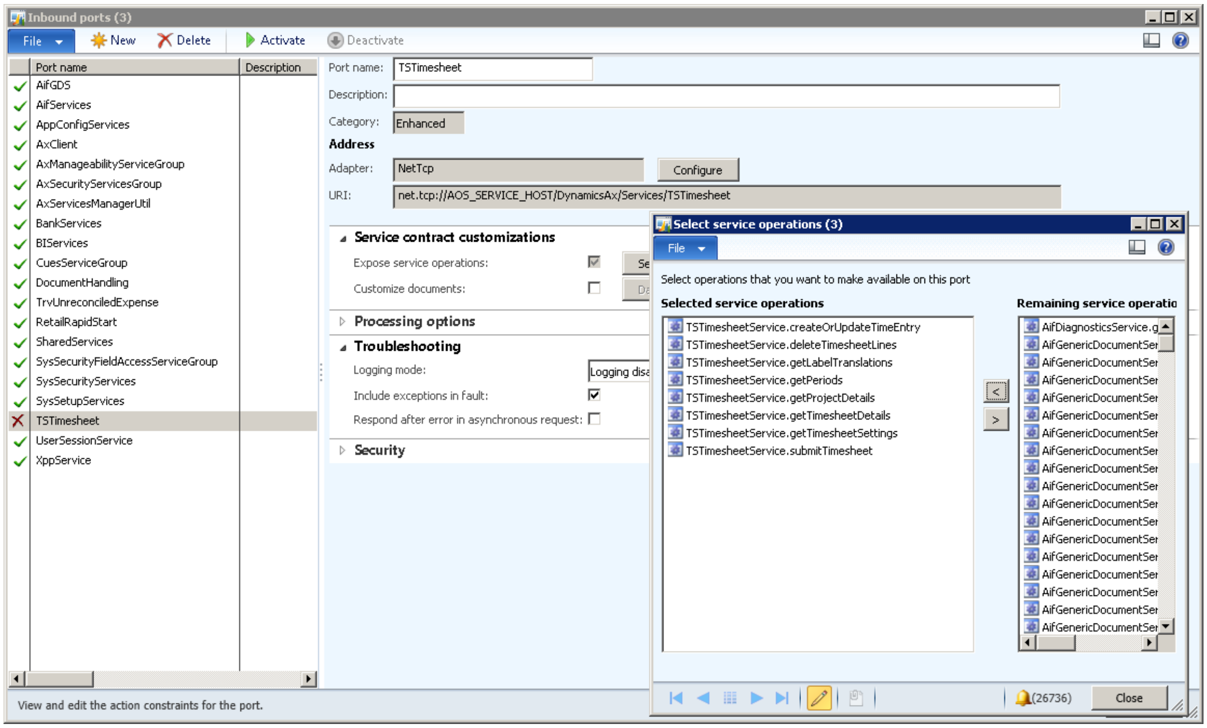
Troubleshooting Logging disabled

Logging mode: Logging disabled
Include exceptions in fault: ☑
Respond after error in asynchronous request: □

Security

Create new inbound port (Ctrl-N)

4 In the **Select service operations** form, in the **Remaining service operations** list, select all eight operations for the TSTimesheetService service, and then click the left arrow button (**<**) to add them to the **Selected service operations** list.



Port name: TSTimesheet
Category: Enhanced
Adapter: NetTcp
URI: net.tcp://AOS_SERVICE_HOST/DynamicsAx/Services/TSTimesheet

Select operations that you want to make available on this port

Selected service operations

- TSTimesheetService.createOrUpdateTimeEntry
- TSTimesheetService.deleteTimesheetLines
- TSTimesheetService.getLabelTranslations
- TSTimesheetService.getPeriods
- TSTimesheetService.getProjectDetails
- TSTimesheetService.getTimesheetDetails
- TSTimesheetService.getTimesheetSettings
- TSTimesheetService.submitTimesheet

Remaining service operatio

- AifDiagnosticsService.g
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer
- AifGenericDocumentSer

View and edit the action constraints for the port.

5 Close the **Select service operations** form.

6 On the **Troubleshooting** FastTab, select the **Include exceptions in fault** check box, and then click **Activate**.

Set up the Microsoft Dynamics AX Connector for Mobile Applications service

You can find the updated installer (version 8.2.387 or newer) at https://mbs.microsoft.com/customersource/northamerica/AX/news-events/news/MSDYN_MobileAppsAX.

Use the following procedure to install and configure the connector.

Prerequisites

- The Microsoft Dynamics AX Connector for Mobile Applications service should be deployed or run as a user account of the .NET Business Connector proxy account. For more information about how to create and set up the .NET Business Connector proxy account, see Specify the .NET Business Connector proxy account [AX 2012].

  If Enterprise Portal is deployed on the server, it will use the .NET Business Connector proxy account.

  Important: You must add the .NET Business Connector proxy user account as an admin on the computer that runs the Microsoft Dynamics AX Connector for Mobile Applications service.

  Also note the following guidance for the .NET Business Connector proxy account:

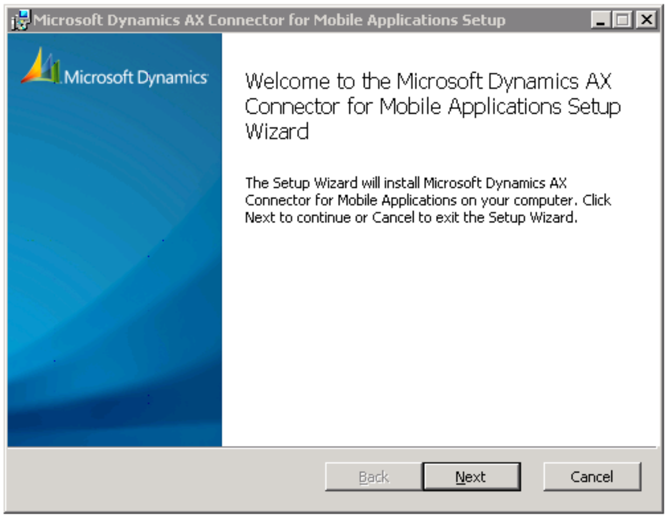
  - It must be a Windows domain account.
  - It must be a dedicated account (that is, it must be used only by .NET Business Connector).
  - It must have a password that doesn’t expire.
  - It must not have interactive sign-in rights.
  - It must not be a Microsoft Dynamics AX user.

  To check which .NET Business Connector proxy user account has been configured, in Microsoft Dynamics AX, click **System administration**> **System service accounts**.

- Only one instance of the connector can be deployed to run on a computer.

Installation

1 Click **Start** > **All Programs** > **Microsoft Dynamics AX Connector for Mobile Applications**, and start the Microsoft Dynamics AX Connector for Mobile Applications Setup Wizard.

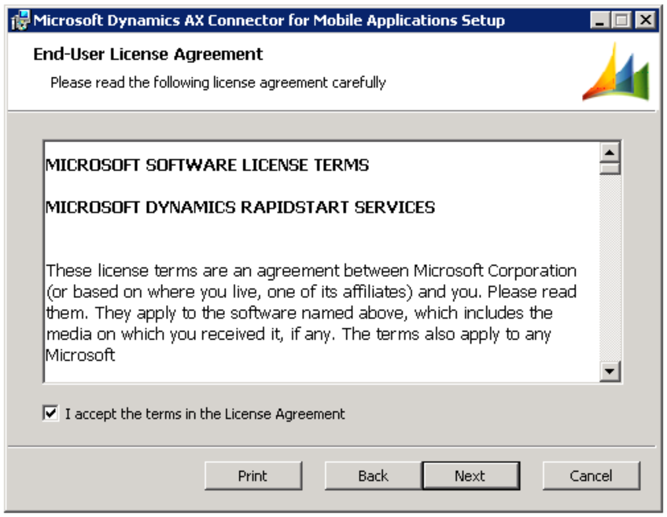


Microsoft Dynamics AX Connector for Mobile Applications Setup

Welcome to the Microsoft Dynamics AX Connector for Mobile Applications Setup Wizard

The Setup Wizard will install Microsoft Dynamics AX Connector for Mobile Applications on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

2 On the **End-User License Agreement** page, select the **I accept the terms in the License Agreement** check box, and then click **Next**.



Microsoft Dynamics AX Connector for Mobile Applications Setup

End-User License Agreement

Please read the following license agreement carefully

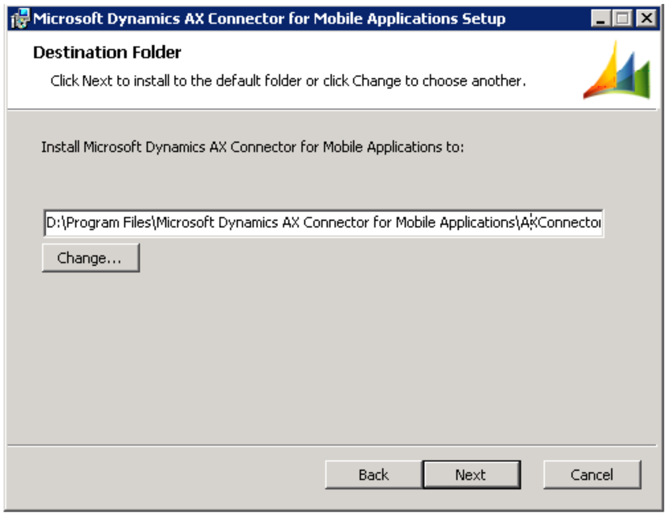
MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT DYNAMICS RAPIDSTART SERVICES

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

☑ I accept the terms in the License Agreement

3 On the **Destination Folder** page, accept the default folder location for the connector, or click **Change** to select another location. Then click **Next**.



Microsoft Dynamics AX Connector for Mobile Applications Setup

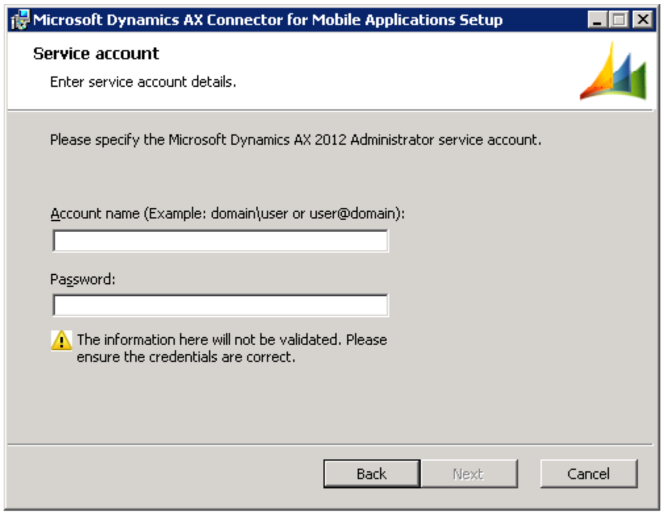
Destination Folder

Click Next to install to the default folder or click Change to choose another.

Install Microsoft Dynamics AX Connector for Mobile Applications to:

D:\Program Files\Microsoft Dynamics AX Connector for Mobile Applications\AXConnector

4 On the **Service account** page, in the **Account name** and **Password** fields, enter the name and password for the .NET Business Connector proxy user account that you previously created, and then click **Next**.



Microsoft Dynamics AX Connector for Mobile Applications Setup

Service account

Enter service account details.

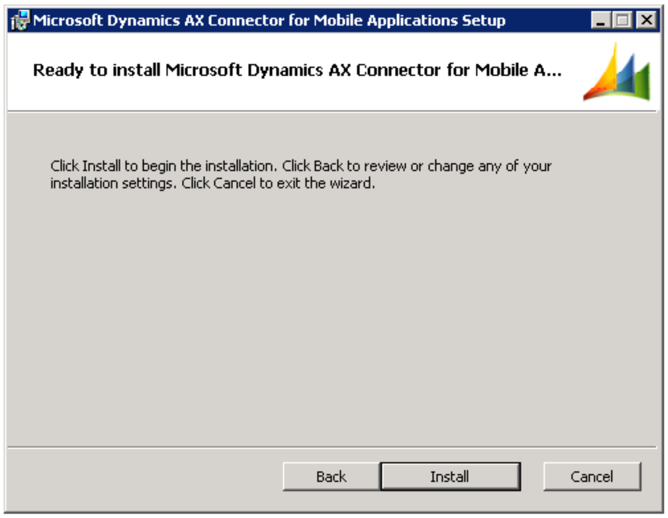
Please specify the Microsoft Dynamics AX 2012 Administrator service account.

Account name (Example: domain\user or user@domain):

Password:

The information here will not be validated. Please ensure the credentials are correct.

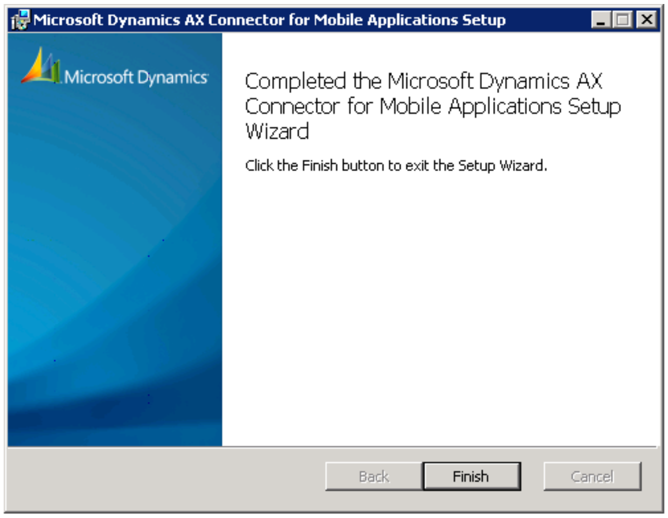
5 Click **Install**.


Microsoft Dynamics AX Connector for Mobile Applications Setup

Ready to install Microsoft Dynamics AX Connector for Mobile A...

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

6 Click **Finish**.

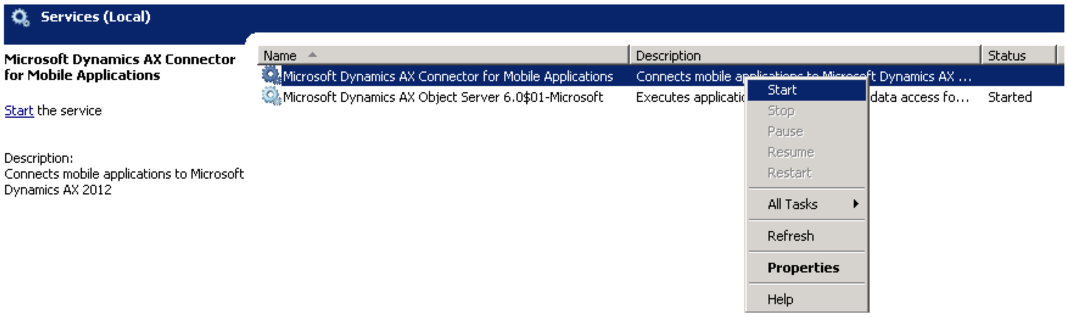

Microsoft Dynamics AX Connector for Mobile Applications Setup

Completed the Microsoft Dynamics AX Connector for Mobile Applications Setup Wizard

Click the Finish button to exit the Setup Wizard.

7 Click **Start** > **Administrative Tools** > **Service** to open the Windows Services list.

8 Click **Start** to start the Microsoft Dynamics AX Connector for Mobile Applications service. The service will run under the context of the service user account.


Services (Local)

Microsoft Dynamics AX Connector for Mobile Applications

Start the service

Description:
Connects mobile applications to Microsoft Dynamics AX 2012

Name	Description	Status
Microsoft Dynamics AX Connector for Mobile Applications	Connects mobile applications to Microsoft Dynamics AX ...	
Microsoft Dynamics AX Object Server 6.0$01-Microsoft	Executes applicati... data access fo...	Started

9 On the **Start** menu, click the **Microsoft Dynamics AX Connector for Mobile Applications** shortcut. The graphical user interface (GUI) for configuring the connector parameters is started.

10 Use the information in the following table to configure the connector parameters if you are using AD FS.

Parameter	**Configuration**
Azure service namespace	Enter the service namespace that you set up in the Create a new Service Bus namespace and shared access policies section, and then click **Save**.
Azure service identity name	Enter the service identity name that you set up in the Create a new Service Bus namespace and shared access policies section. For example, sendlisten.
Azure service identity password	Enter the 256-bit symmetric key for the service identity that was generated in the Create a new Service Bus namespace and shared access policies section.
Thumbprint of X.509 certificate used to sign SAML token	You can find information about the thumbprint value in the Add and configure the token signing certificate section.
Endpoint URI of ExpenseServices (if using Expenses applications)	The following text is preconfigured in this field: **net.tcp://<AOS_MACHINE_NAME>:8201/DynamicsAx/Services/TrvUnreconciledExpense** Replace **<AOS_MACHINE_NAME>** with the name of the computer that hosts Microsoft Dynamics AX Application Object Server (AOS). Replace the default AOS port number, 8201, if a different port is used.
Endpoint URI of TSTimesheetService (if using Timesheets applications)	The following text is preconfigured in this field: **net.tcp://<AOS_MACHINE_NAME>:8201/DynamicsAx/Services/TSTimesheet** Replace **<AOS_MACHINE_NAME>** with the name of the computer that hosts AOS. Replace the default AOS port number, 8201, if a different port is used.
Endpoint URI of ApprovalsServices (if using the Approvals application)	The following text is preconfigured in this field: **net.tcp://<AOS_MACHINE_NAME>:8201/DynamicsAx/Services/EmailApprovalsServices** Replace **<AOS_MACHINE_NAME>** with the name of the machine that hosts AOS. Replace the default AOS port number, 8201, if a different port is used.

Parameter	**Configuration**
Endpoint URI of EmailApprovalsServices (if using Email approvals	The following text is preconfigured in this field: **net.tcp://<AOS_MACHINE_NAME>:8201/DynamicsAx/Services/EmailApproalsServices** Replace **<AOS_MACHINE_NAME>** with the name of the machine that hosts AOS. Replace the default AOS port number, 8201, if a different port is used.
ADFS URL	ADFS machine URL, for example https://contosoadfs.com
ADFS Metadata	https://contosoadfs.com/FederationMetadata/2007-06/FederationMetadata.xml, refer to the Save AD FS metadata.xml file step
ADFS Metadata security protocol type	ADFS Metadata security protocol typically set to **default** **TLS12** can also be optionally entered if required. See LCS Issue search 300809 for more information.
Enable AAD authentication	**False**
Web resource URL	Identifier name from the relying party trust that you created in the "Add relying party trust" (Step 7), for example *http://DynamicsADFSNative.contoso.com*
Expenses app registration Native app Id	Enter any GUID For example: **abcd-123-efgh-4567** See the Create AD FS clients section.
Timesheets app registration Native app Id	Enter any GUID For example: **bcde-123-efgh-4567** See the Create AD FS clients section. Connector version of 8.2.388.0 or above is required

Parameter	Configuration
Approvals app registration Native app Id	Enter any GUID For example: **cdef-123-efgh-4567** See the Create AD FS clients section. Connector version of 8.2.388.0 or above is required
Android ADFS native app Id	For example: **abcd-123-efgh-9123** See the Create AD FS clients section.
IOS ADFS Native App Id	For example: **abcd-123-efgh-8709** See the Create AD FS clients section.
Support Email	The contact email address that is shown to mobile users, and that they can use in the event of any issues, such as **support@contoso.com**.

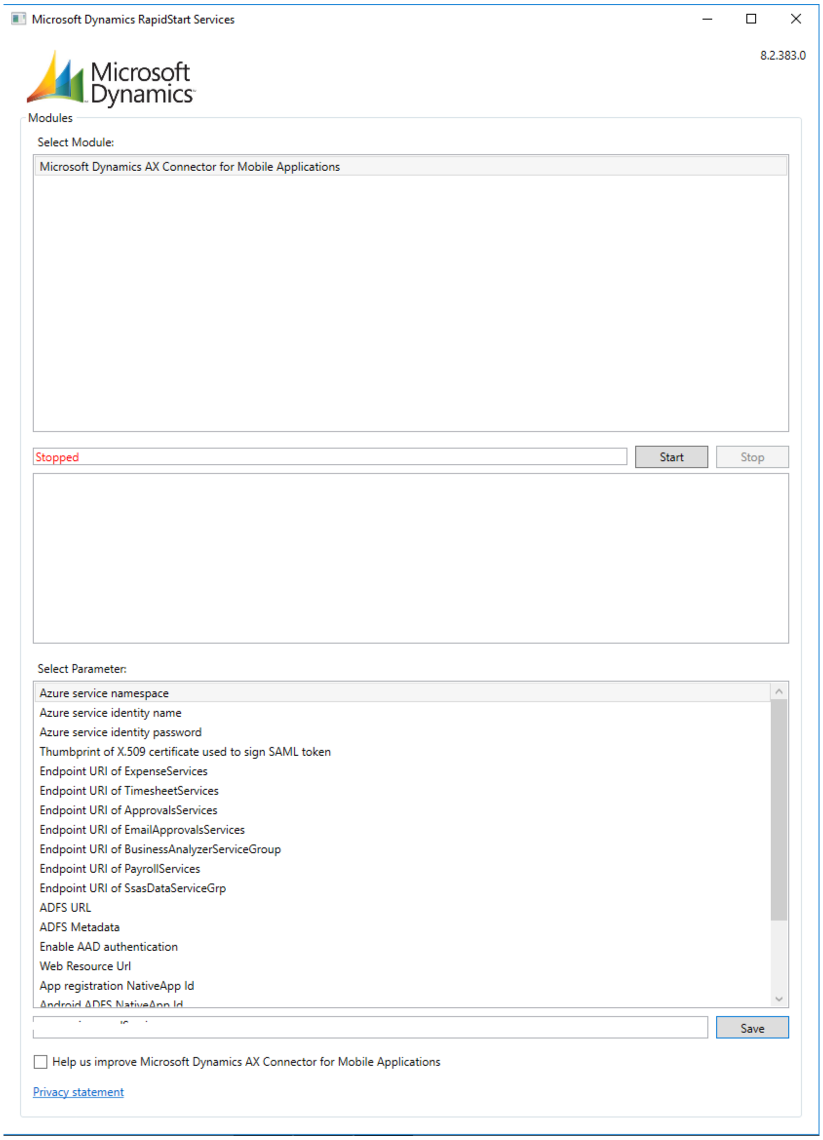
11 Use the information in the following table to configure the connector parameters if using Azure Active Directory

Parameter	Configuration
Azure service namespace	Enter the service namespace that you set up in the Create a new Service Bus namespace and shared access policies section, and then click **Save**.
Azure service identity name	Enter the service identity name that you set up in the Create a new Service Bus namespace and shared access policies section. For example, sendlisten.
Azure service identity password	Enter the 256-bit symmetric key for the service identity that was generated in the Create a new Service Bus namespace and shared access policies section.
Thumbprint of X.509 certificate used to sign SAML token	<Empty>

Parameter	Configuration
Endpoint URI of ExpenseServices (if using Expenses applications)	The following text is preconfigured in this field: **net.tcp://<AOS_MACHINE_NAME>:8201/DynamicsAx/Services/TrvUnreconciledExpense** Replace **<AOS_MACHINE_NAME>** with the name of the computer that hosts Microsoft Dynamics AX Application Object Server (AOS). Replace the default AOS port number, 8201, if a different port is used.
Endpoint URI of TSTimesheetService (if using Timesheets applications)	The following text is preconfigured in this field: **net.tcp://<AOS_MACHINE_NAME>:8201/DynamicsAx/Services/TSTimesheet** Replace **<AOS_MACHINE_NAME>** with the name of the computer that hosts AOS. Replace the default AOS port number, 8201, if a different port is used.
Endpoint URI of ApprovalsServices (if using the Approvals application)	Azure Active Directory implementation is not supported for approvals. Use AD FS instead.
Endpoint URI of EmailApprovalsServices (if using Email approvals)	he following text is preconfigured in this field: **net.tcp://<AOS_MACHINE_NAME>:8201/DynamicsAx/Services/EmailApproalsServices** Replace **<AOS_MACHINE_NAME>** with the name of the machine that hosts AOS. Replace the default AOS port number, 8201, if a different port is used.
ADFS Metadata	<Empty>
Enable AAD authentication	**True**
Web resource URL	https://graph.windows.net
Expenses app registration Native app Id	Application Id of the native app (client app) from App registrations that was created in **Setting up authorization** section (step 8)

Parameter	Configuration
Android ADFS native app Id	**Not applicable**
IOS ADFS Native App Id	**Not applicable**
AAD Authorization Endpoint	https://login.windows.net/<TENANT_ID>/oauth2/authorize , Replace the TenantID with your organization tenant id in azure portal. This can be easily found if you hover over your login details in Azure portal in top right corner.
AAD End Session Endpoint	https://login.windows.net/<TENANT_ID>/oauth2/logout
AAD Signed-in Information URL	https://graph.windows.net/<TENANT_ID>/me?api-version=1.6
AAD Token Issuer URL	https://sts.windows.net/<TENANT_ID>/
AAD URI for token keys validation	https://login.microsoftonline.com/common/discovery/keys
Support Email	The contact email address that is shown to mobile users, and that they can use in the event of any issues, such as **support@contoso.com**.

Note that the **Endpoint URI** parameters for the expense and time services are optional. If you don't configure one of those services, leave the field blank, and click **Save**. When the Microsoft Dynamics AX Connector for Mobile Applications service is started, you will notice that the URL for that service doesn't appear, and the Microsoft Dynamics AX mobile application won't show the corresponding feature.



Select Module:

Microsoft Dynamics AX Connector for Mobile Applications

Stopped

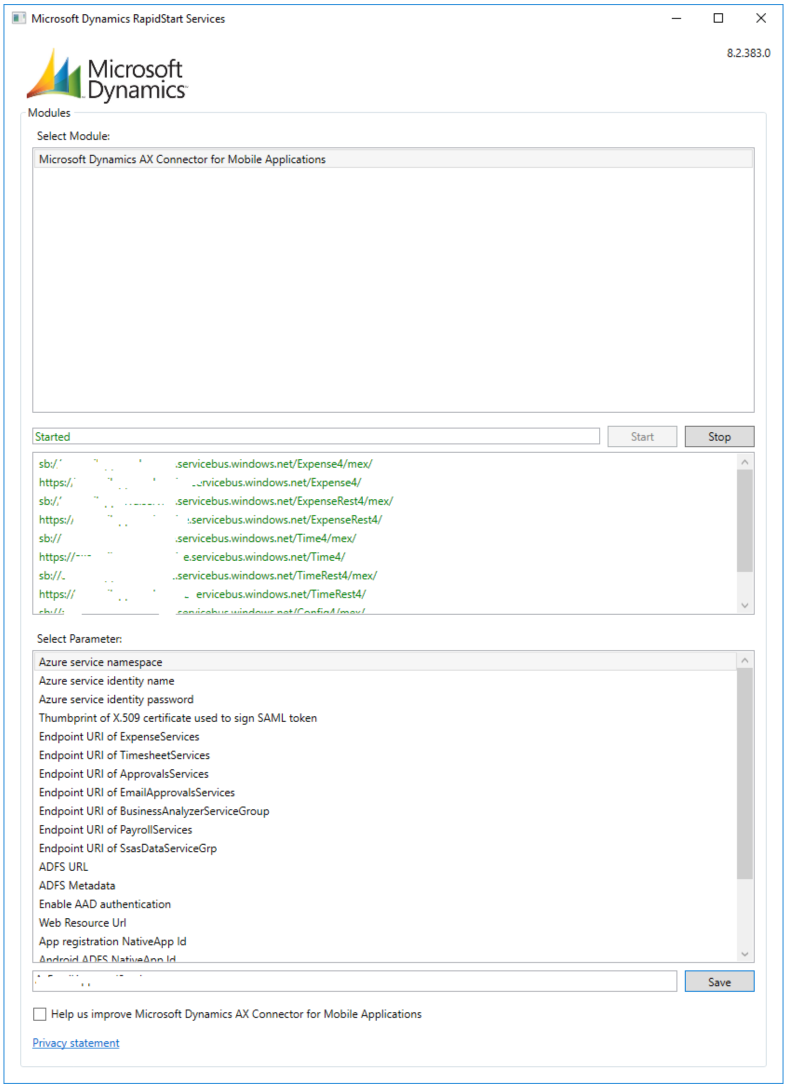
Select Parameter:

Azure service namespace
Azure service identity name
Azure service identity password
Thumbprint of X.509 certificate used to sign SAML token
Endpoint URI of ExpenseServices
Endpoint URI of TimesheetServices
Endpoint URI of ApprovalsServices
Endpoint URI of EmailApprovalsServices
Endpoint URI of BusinessAnalyzerServiceGroup
Endpoint URI of PayrollServices
Endpoint URI of SsasDataServiceGrp
ADFS URL
ADFS Metadata
Enable AAD authentication
Web Resource Url
App registration NativeApp Id
Android ADFS NativeApp Id

□ Help us improve Microsoft Dynamics AX Connector for Mobile Applications

12 When you've finished entering values for the parameters, click **Save**.

13 After the connector parameters are saved, click **Start** in the dialog box. You can see that the status has changed to **Started**, and that the Microsoft Dynamics AX Connector for Mobile Applications service is now running and listening on the Service Bus.



Select Module:

Microsoft Dynamics AX Connector for Mobile Applications

Started

```
sb://[redacted].servicebus.windows.net/Expense4/mex/
https://[redacted]ervicebus.windows.net/Expense4/
sb://[redacted].servicebus.windows.net/ExpenseRest4/mex/
https://[redacted].servicebus.windows.net/ExpenseRest4/
sb://[redacted].servicebus.windows.net/Time4/mex/
https://[redacted]e.servicebus.windows.net/Time4/
sb://[redacted].servicebus.windows.net/TimeRest4/mex/
https://[redacted]ervicebus.windows.net/TimeRest4/
sb://[redacted].servicebus.windows.net/Config4/mex/
```

Select Parameter:

Azure service namespace
Azure service identity name
Azure service identity password
Thumbprint of X.509 certificate used to sign SAML token
Endpoint URI of ExpenseServices
Endpoint URI of TimesheetServices
Endpoint URI of ApprovalsServices
Endpoint URI of EmailApprovalsServices
Endpoint URI of BusinessAnalyzerServiceGroup
Endpoint URI of PayrollServices
Endpoint URI of SsasDataServiceGrp
ADFS URL
ADFS Metadata
Enable AAD authentication
Web Resource Url
App registration NativeApp Id
Android ADFS NativeApp Id

[redacted]

☐ Help us improve Microsoft Dynamics AX Connector for Mobile Applications

Privacy statement

Configure the Microsoft Dynamics AX mobile application

When you notify users that the solution is available, they must provide their domain credentials and the service connection name to use the Microsoft Dynamics AX mobile application on their phone.

When users open the Microsoft Dynamics AX mobile application for the first time, they are directed to a sign-in page that has the following fields:

- **User name**
- **Password**
- **Service connection name** – The value is the name of the Service Bus namespace that you set up in the Create a new Service Bus namespace and shared access policies section.

After users enter the information and click **sign in**, the data is synced from the server, and the users can start to use the application.

Appendix A: Migrate from ACS to SAS

The following changes have been made to support SAS instead of ACS for the November 7, 2018, deprecation of ACS

- The requirements have been increased to require AD FS 3.0 or later. The previous version required AD FS 2.0.
- A new version of the connector must be installed. The new version isn't backward compatible with ACS.
- A new Service Bus namespace is required.
- Shared access policies must be created.
- ACS configuration is no longer required.

Appendix B: Configure the Approvals App

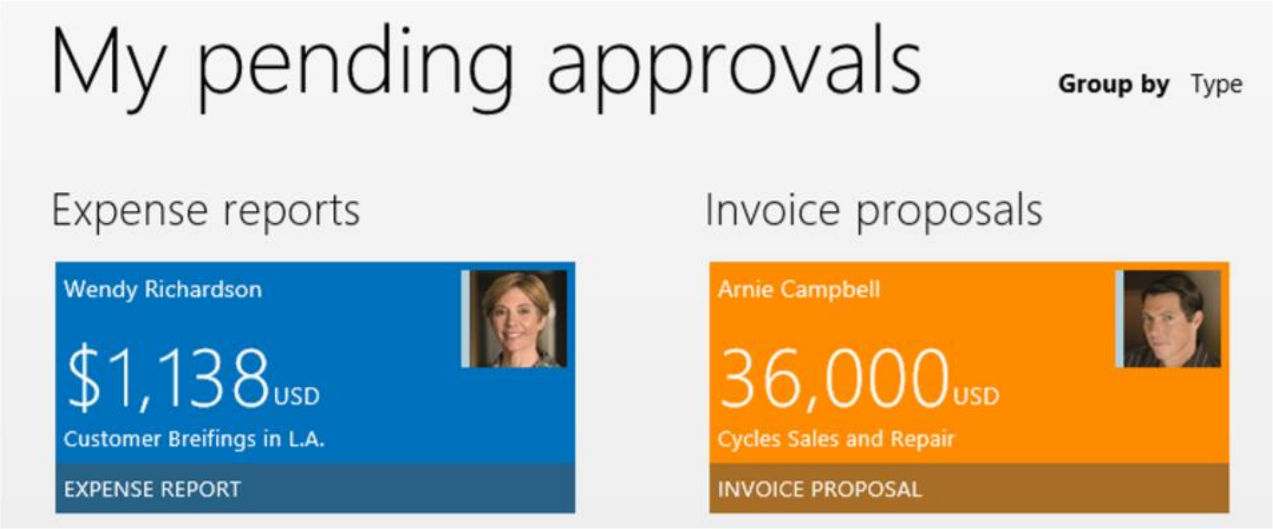
Viewing recent approval items

The Approvals app provides a way for users to view all the workflow approval items assigned to them, and to approve or reject them. After the workflow generates the approval, the approver will be able to view the details, attachments, comments, and other information for that approval. For example, if an approver rejects a particular version of a timesheet, and that approval is later re-routed by workflow and assigned to a different employee, the timesheet document, including the subsequent changes, will still be visible to the original approver.

Configuring the Approvals app

The Approvals app provides a way for users to view all the workflow approval items assigned to them, and to approve or reject them. To help users determine which action to take, basic information about the approval is shown on the tiles, and more detailed information is shown when one of the tiles is opened. Even more information about the approval item can be shown by using attachments. For approvals of timesheets and expenses, the app also includes extended context, such as the list of expenses or time entries, receipts, and visual breakdowns of the impact of the expenditures on current project budgets. The following illustrations show each of these approaches.

Contextual information shown on tiles



My pending approvals

Group by Type

Expense reports

Wendy Richardson

$1,138 USD

Customer Breifings in L.A.

EXPENSE REPORT

Invoice proposals

Arnie Campbell

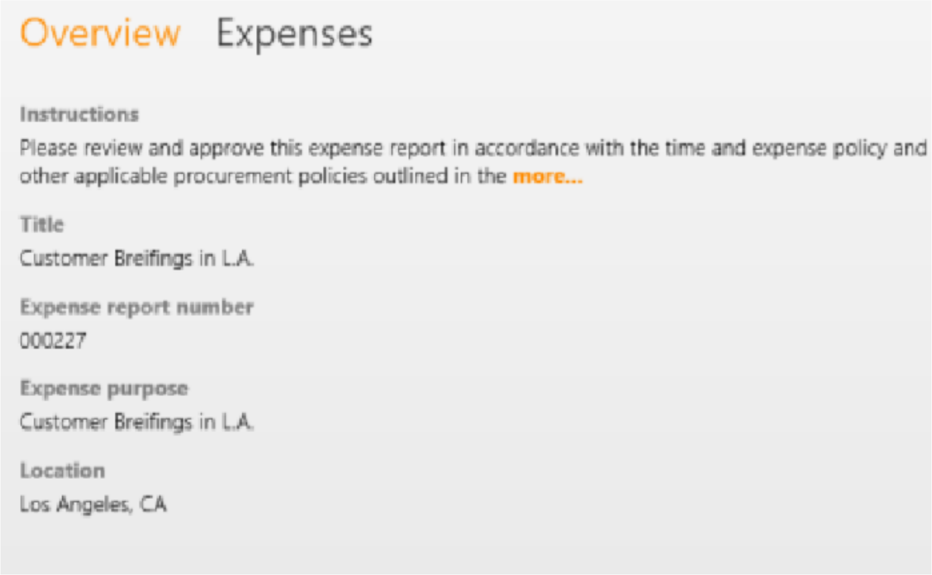
36,000 USD

Cycles Sales and Repair

INVOICE PROPOSAL

Figure A1: Screen capture of the contextual information shown on tiles

Contextual information shown on the Overview tab



Instructions

Please review and approve this expense report in accordance with the time and expense policy and other applicable procurement policies outlined in the more...

Title

Customer Breifings in L.A.

Expense report number

000227

Expense purpose

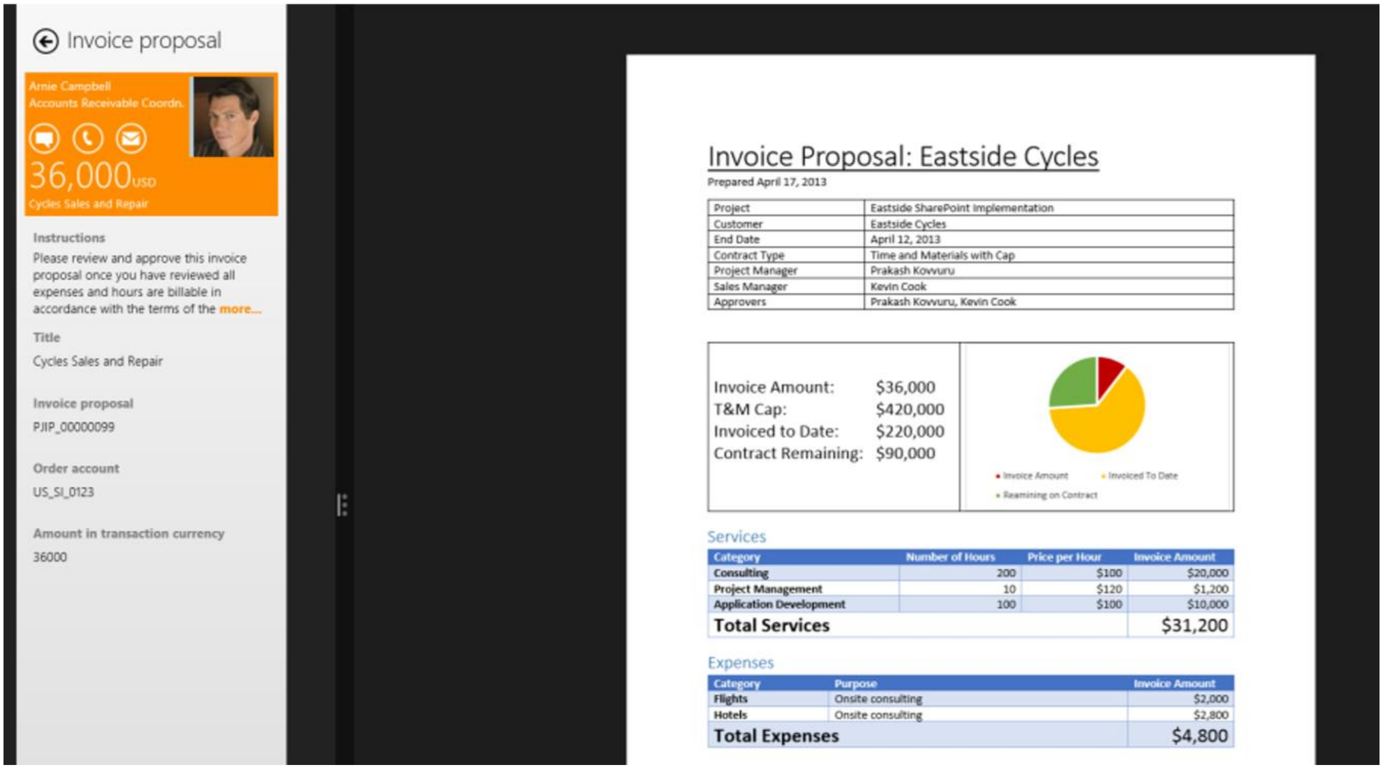
Customer Breifings in L.A.

Location

Los Angeles, CA

Figure A2: Screen capture of the contextual information shown on the Overview tab

Contextual information shown as an attachment



Invoice proposal

Arnie Campbell
Accounts Receivable Coordn.

36,000USD
Cycles Sales and Repair

Instructions
Please review and approve this invoice proposal once you have reviewed all expenses and hours are billable in accordance with the terms of the more...

Title
Cycles Sales and Repair

Invoice proposal
PJIP_00000099

Order account
US_SI_0123

Amount in transaction currency
36000

Invoice Proposal: Eastside Cycles

Prepared April 17, 2013

Project	Eastside SharePoint Implementation
Customer	Eastside Cycles
End Date	April 12, 2013
Contract Type	Time and Materials with Cap
Project Manager	Prakash Kovvuru
Sales Manager	Kevin Cook
Approvers	Prakash Kovvuru, Kevin Cook

Invoice Amount:	$36,000
T&M Cap:	$420,000
Invoiced to Date:	$220,000
Contract Remaining:	$90,000

Services

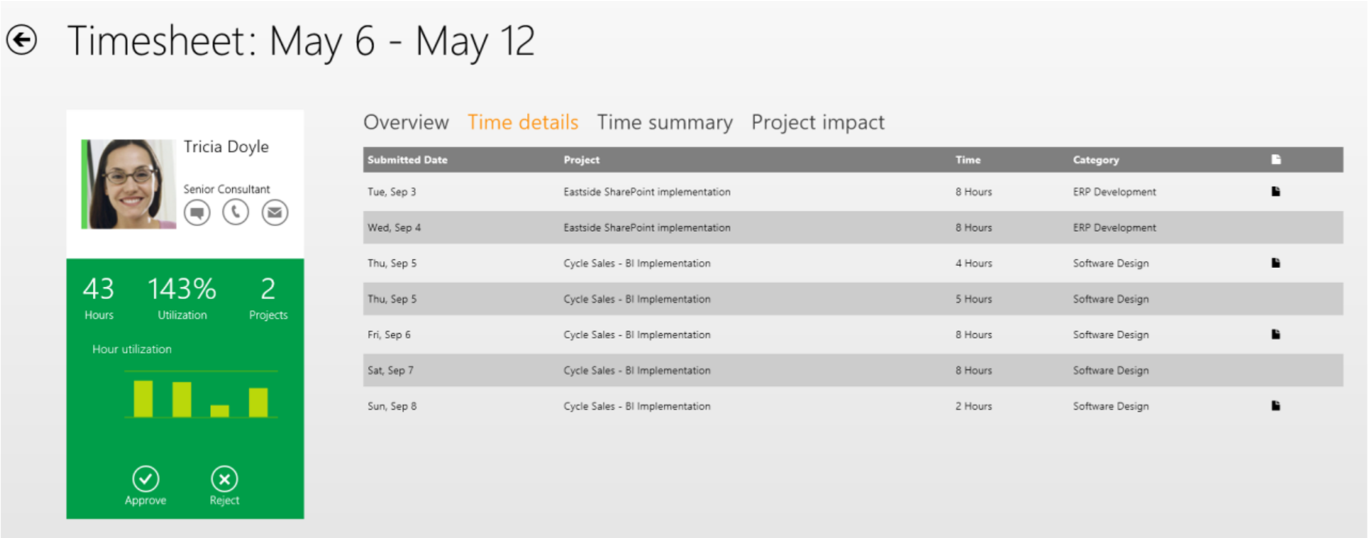
Category	Number of Hours	Price per Hour	Invoice Amount
Consulting	200	$100	$20,000
Project Management	10	$120	$1,200
Application Development	100	$100	$10,000
Total Services			$31,200

Expenses

Category	Purpose	Invoice Amount
Flights	Onsite consulting	$2,000
Hotels	Onsite consulting	$2,800
Total Expenses		$4,800

Figure A3: Screen capture of the contextual information shown as an attachment

Extended context for a timesheet (Time details, Time summary, and Project impact tabs)



Timesheet: May 6 - May 12

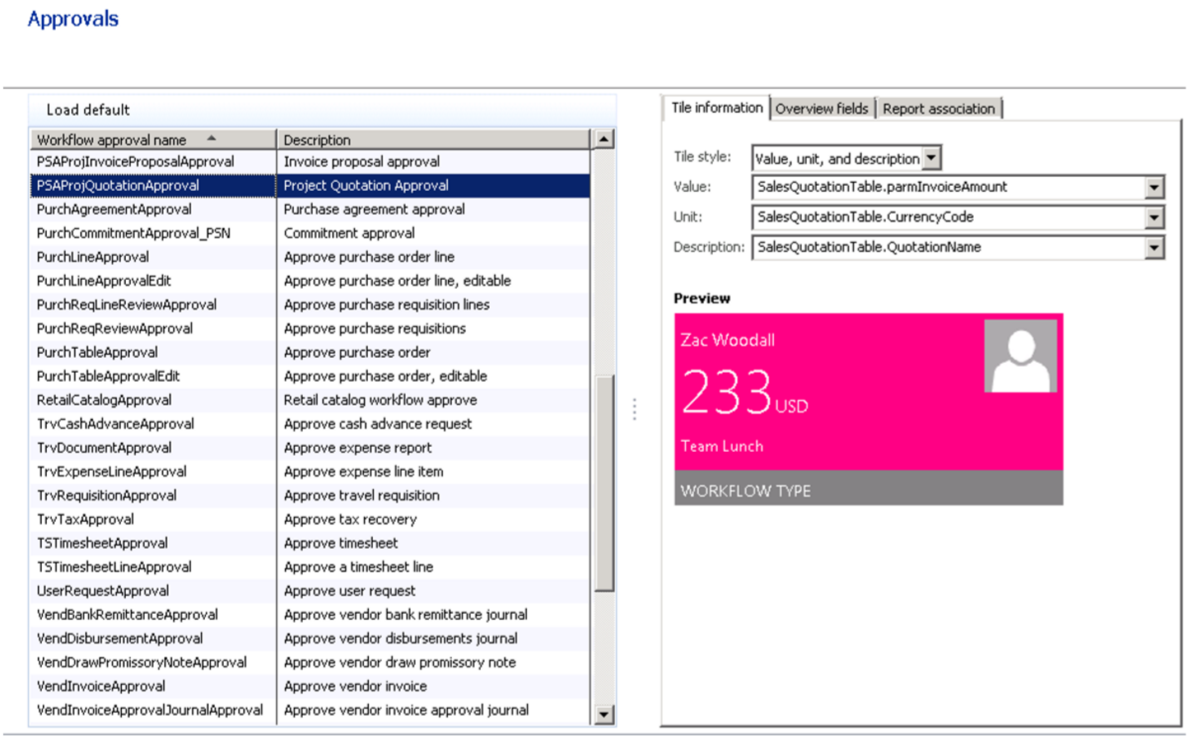
Tricia Doyle
Senior Consultant

43 Hours 143% Utilization 2 Projects

Submitted Date	Project	Time	Category	📄
Tue, Sep 3	Eastside SharePoint implementation	8 Hours	ERP Development	📄
Wed, Sep 4	Eastside SharePoint implementation	8 Hours	ERP Development	
Thu, Sep 5	Cycle Sales - BI Implementation	4 Hours	Software Design	📄
Thu, Sep 5	Cycle Sales - BI Implementation	5 Hours	Software Design	
Fri, Sep 6	Cycle Sales - BI Implementation	8 Hours	Software Design	📄
Sat, Sep 7	Cycle Sales - BI Implementation	8 Hours	Software Design	
Sun, Sep 8	Cycle Sales - BI Implementation	2 Hours	Software Design	📄

Figure A4: Screen capture of a timesheet and other contextual information

Although the extended context for timesheets and expenses is built into the app and can't be provided for other approval types, all the other contextual information, such as context on a tile, context on the **Overview** tab, and attachments, can be customized to meet the requirements of your organization by making configurations on the server. All customizations are performed in the following form, which is accessible in the Microsoft Dynamics AX client under **System Administration > Setup > Windows Store > Windows application store setup.**



Approvals

Load default

Workflow approval name	Description
PSAProjInvoiceProposalApproval	Invoice proposal approval
PSAProjQuotationApproval	Project Quotation Approval
PurchAgreementApproval	Purchase agreement approval
PurchCommitmentApproval_PSN	Commitment approval
PurchLineApproval	Approve purchase order line
PurchLineApprovalEdit	Approve purchase order line, editable
PurchReqLineReviewApproval	Approve purchase requisition lines
PurchReqReviewApproval	Approve purchase requisitions
PurchTableApproval	Approve purchase order
PurchTableApprovalEdit	Approve purchase order, editable
RetailCatalogApproval	Retail catalog workflow approve
TrvCashAdvanceApproval	Approve cash advance request
TrvDocumentApproval	Approve expense report
TrvExpenseLineApproval	Approve expense line item
TrvRequisitionApproval	Approve travel requisition
TrvTaxApproval	Approve tax recovery
TSTimesheetApproval	Approve timesheet
TSTimesheetLineApproval	Approve a timesheet line
UserRequestApproval	Approve user request
VendBankRemittanceApproval	Approve vendor bank remittance journal
VendDisbursementApproval	Approve vendor disbursements journal
VendDrawPromissoryNoteApproval	Approve vendor draw promissory note
VendInvoiceApproval	Approve vendor invoice
VendInvoiceApprovalJournalApproval	Approve vendor invoice approval journal

Tile style: Value, unit, and description

Value: SalesQuotationTable.parmInvoiceAmount

Unit: SalesQuotationTable.CurrencyCode

Description: SalesQuotationTable.QuotationName

Preview

Figure A5: Screen capture Approvals page and Tile information tab

Configuring the tiles

Tiles can be rendered in two different formats, as specified by the **Tile style** field. When this field is set to **Value, unit, and description**, three fields can be chosen and will be shown on the tile. This style communicates a quantity and unit, such as **USD 233**, on an expense report or timesheet, and then provide additional information, such as the summary **Team Lunch**. If your approval does not have a value overview, you can use **the Title and description** format, which has just two options. Developers can extend the set of fields and values that is available for inclusion on tiles. The set of available fields is determined by the corresponding workflow template's class. For example, the following steps show how to add the quotation amount to the quotation approval, because this is likely the value that you would want to show in the app:

1) In the Application Object Tree (AOT), click **Workflows > Approvals > PSAQuotationApproval**. Note the value of the **Document** property, which in this case is **PSAProjQuotationDocument**. In the AOT, click **Classes > PSAPRojQuotationDocument**. Add the following code to the class. This code will return the value of a display method that is already on the class and that contains the value that we want to show the user:
2)

```
public AmountCur parmInvoiceAmount(
          CompanyId _companyId,

           tableId   _tableId,

           RecId     _recId)

 {

     SalesQuotationTable t;

if(_tableId == tableNum(SalesQuotationTable))

  {       t = SalesQuotationTable::findRec(_recId);

          return t.invoiceAmount();

   }

   return 0;

   }
```

Complete an Incremental CIL compilation.

Return to the Windows Store App configuration screen, and select **Value** as the new field to show on the tile.

To customize the tile color, double-click the example tile, and then select the color from the color palette.

Configuring the Overview tab

The list of fields that shown on the **Overview** tab of a specific approval is determined by the fields that selected on the **Overview fields** tab of the Windows Store App configuration screen. By default, this list is populated with the fields that are typically shown in the Microsoft Dynamics AX client, which are determined by the field group specified on the workflow approval item in the AOT. To modify this list, click on the **Overview** tab and use the same process described earlier for customizing the information on **the Tile information** tab.

Adding reports

You can build reports to customize the information that an approver will receive in the Approval app, and then associate the reports with the workflow template. For example, a new report might show all the details of the quotation that is being approved. When an approval work item is generated, the report that displays the quotation information is rendered and included as an attachment in the email message to the approver. The approver can then open and view the report. The following steps must be completed if you want to include a custom report:

1) **Author a new report:** The new report must use a query-based data source whose root is the same table as the workflow template's document. **Continuing the example with PSASalesQuotation** from the previous sections, the new report must be based on a query whose root table is SalesQuotationTable. This enables the context of the quotation that is being approved to be passed to the report when it is executed.

Create a menu item: Create a new display menu item that references your new report. In order to associate the report with the workflow template, you must complete these steps:
1. Verify that the configuration key matches the configuration key of the workflow template.
2. Use the same prefix for the menu item and the report. The prefix refers to the first three letters of the element name in the AOT.
Pick the menu item: On the **Report association** tab of the Windows Store App configuration screen, select the newly created menu item. After you have completed these steps, the report will be rendered when an approver clicks **view** on the approval item in the attachments section of the application.

Using Microsoft Lync integration

If your organization uses Lync for communications and collaboration, the Approvals app can show pictures of submitters and indicate their availability. This will help the approver know whether they can contact a submitter by using Lync. If Lync is not available, pictures will be retrieved from Microsoft

Dynamics AX, but no presence indicators will be included. Lync integration in the Approvals app utilizes the new UCWA protocol and therefore can be used only with on-premises deployments of Lync 2013 CU1. Additionally, the domain of your users will need to be added to the “Allowed List,” as described in this document: http://ucwa.lync.com/documentation/ITAdmin-Configuration.

Update history

Date	Update
May 2019	• Removed broken link to the KB for Microsoft Dynamics AX 2012 R2. • Added redirect URIs for approval and timesheet apps for Azure Active Directory. • Added Appendix for approvals app configuration
March 2019	• Added clarification around CA signing requirements • Added support for connector 8.2.389.0 to enable ADFS Metadata security protocol type of default or TLS12. • Added updated steps for supporting multiple mobile apps with updated parameters for the three windows desktop apps rather than the generic app registration native app Id for all three apps. New parameters added as of Connector 8.2.388.0

Send feedback.

Microsoft Dynamics is a line of integrated, adaptable business management solutions that enables you and your people to make business decisions with greater confidence. Microsoft Dynamics works like and with familiar Microsoft software, automating and streamlining financial, customer relationship, and supply chain processes in a way that helps you drive business success.

United States and Canada toll-free: (888) 477-7989

Worldwide: (1) (701) 281-6500

dynamics.microsoft.com

This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.