8x8, Inc.

8x8 SAML Single Sign On

Configuring 8x8 SAML SSO with Microsoft ADFS

Version 1.0

Copyright © 2015, 8x8, Inc. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

8x8® is a registered trademark of 8x8, Inc.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owner/s. All other brands and/or product names are the trademarks (or registered trademarks) and property of their respective owner/s.

TABLE OF CONTENTS

Using this Document

This document is designed for IT administrators who need to configure Single Sign-on between Microsoft ADFS and 8x8 Virtual Office apps.

Overview

Configuring 8x8 SAML with Microsoft ADFS involves:

- Installation of Microsoft Active Directory Federation Service (ADFS) 3.0
- Configuration of Microsoft ADFS
- General ADFS Setup
- Configuration of 8x8 Account Manager
- Creation of ADFS Relying Party Trust
- Configuration of ADFS Claim Rules
- Logging into ADFS

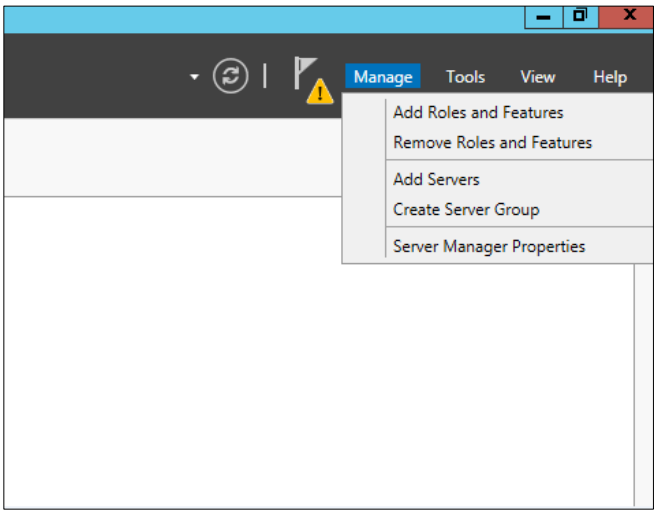
ADFS is an identity provider for Windows, so it provides a ***Security Token Service (STS)*** that creates and issues **SAML tokens** to authenticated users. Claims based authentication is an industry standard security protocol to authenticate users.

Install ADFS on Windows Server 2012 R2

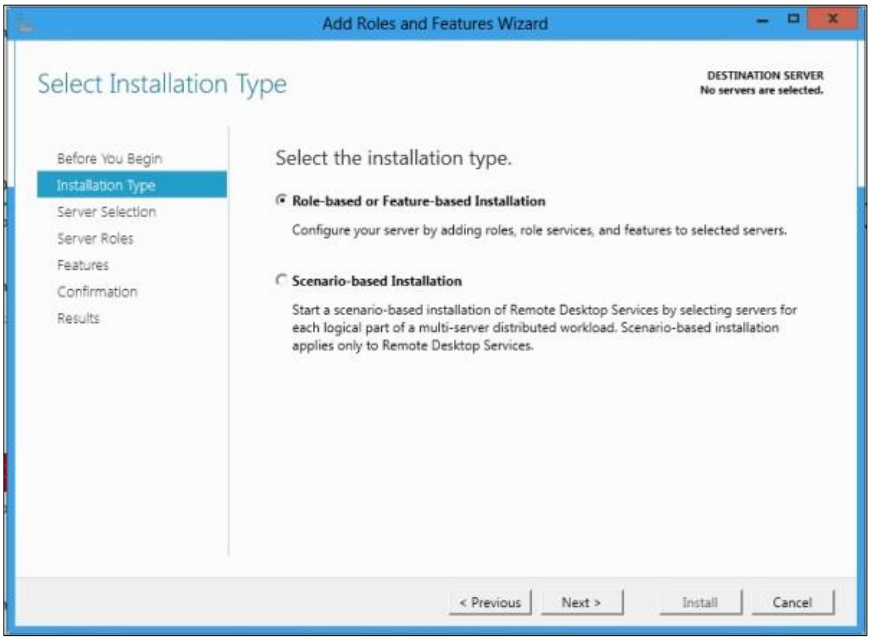
ADFS installs as a Windows Server 2012 R2 server role and does not require any additional download. The installation uses the “Add Roles and Features Wizard”.

To start the Add Roles and Features Wizard:

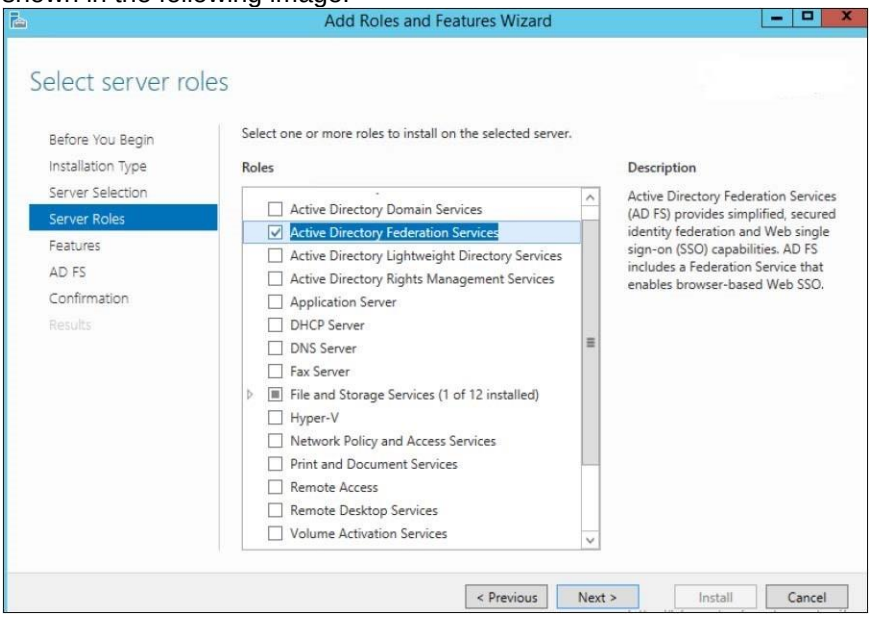
1. Open the Server Manager on the server. Under Manage menu, select **Add Roles and Features**.



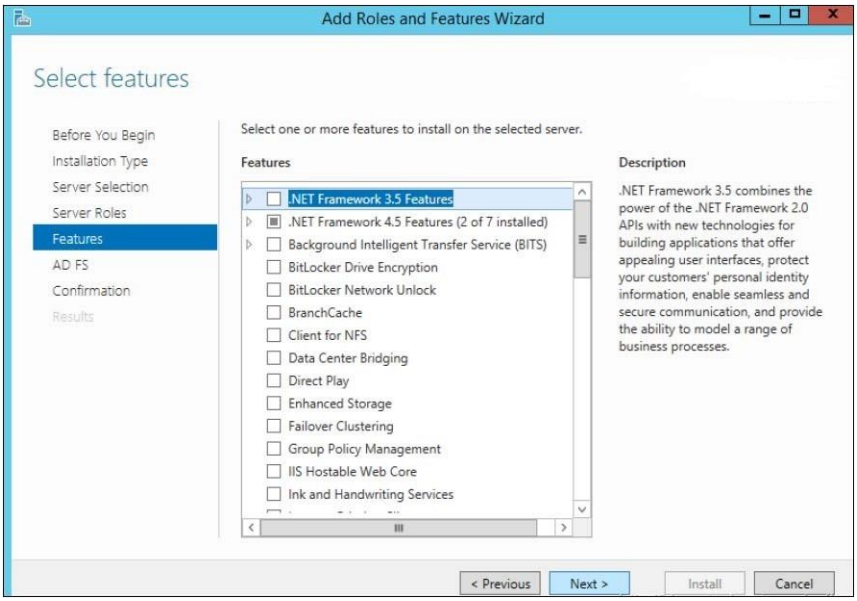
2. The wizard initiates by opening **Before you begin** Dialog box. Click **Next** to proceed to **Installation Type** page.
3. Select **Role-based or Feature-based Installation** as shown below.



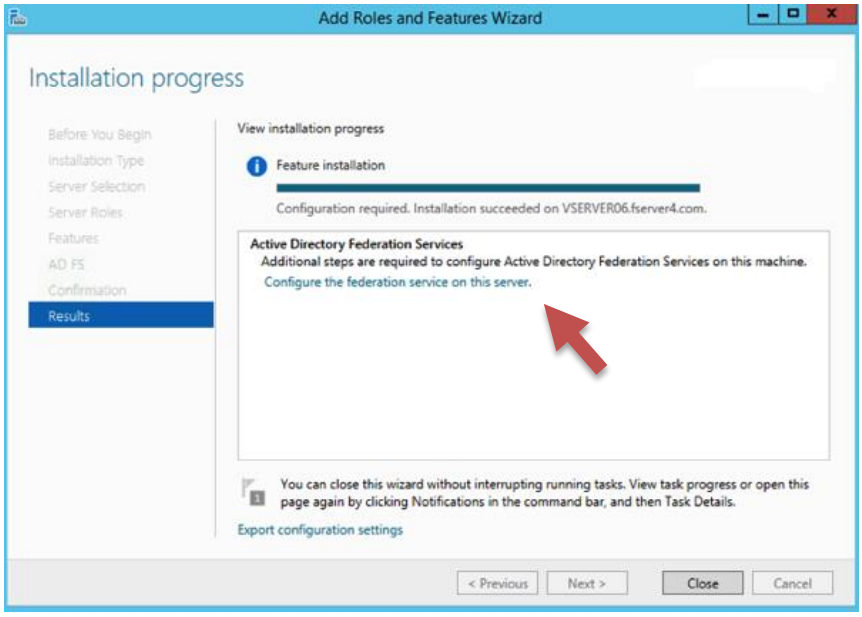
4. On the **Select Server Roles** page, check the box for **Active Directory Federation Services**, as shown in the following image.



5. You do not need to add any additional features. Remember that the IIS dependency was removed in ADFS 2012 R2



6. Once the feature installation is complete, proceed to the configuration of the ADFS service **Configure the federation service on this server**.



Configuration of ADFS 3.0

To configure ADFS 3.0, we need to configure the ADFS server and create the identity provider Security Token Service (STS).

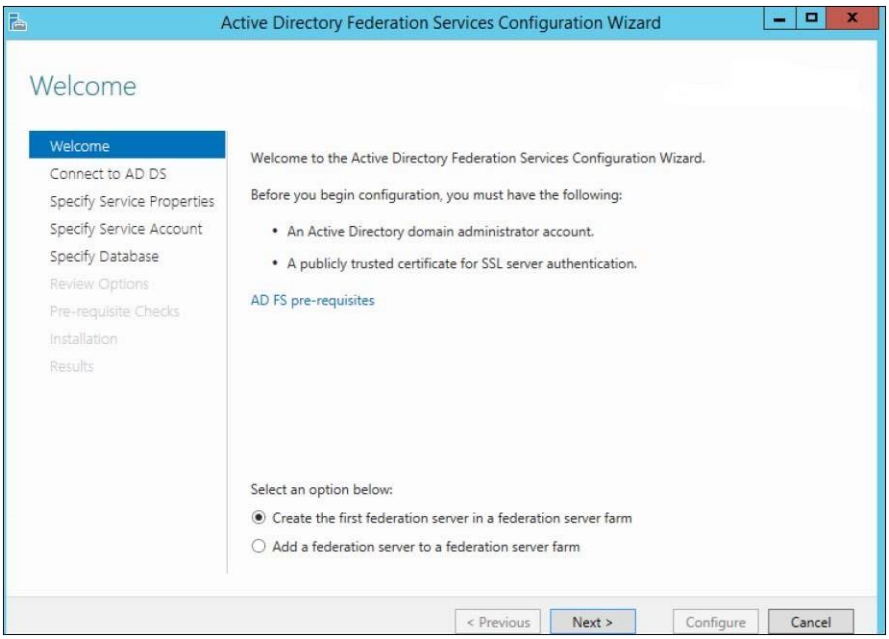
Before you begin the ADFS configuration wizard, you must have the following:

- Access to Domain Admin Credentials.
- Installed the 3rd party certificate for SSL server authentication.

Additionally a group managed service account is also pre-created.

You have two options:

- Create the first federation server in a federation server farm.
- Add a federation server to a federation server farm.

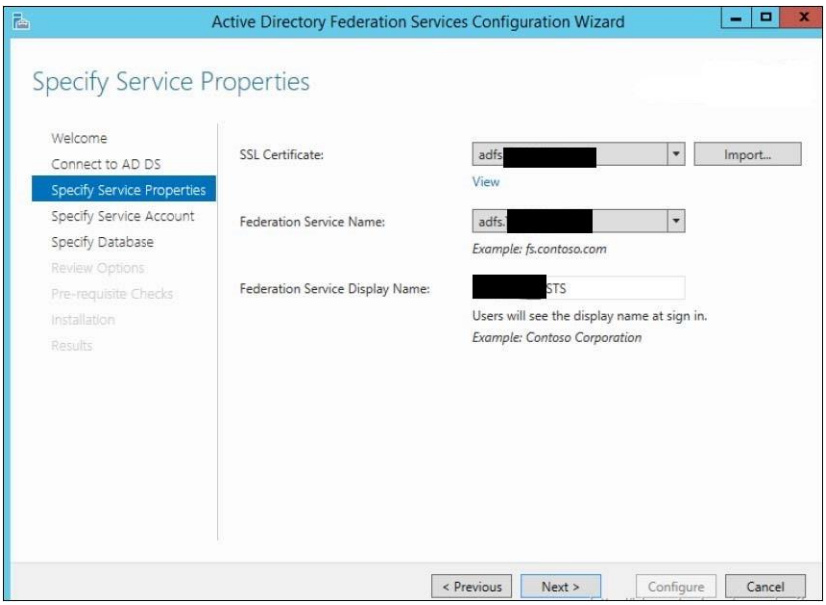


1. In the first panel of the ADFS Configuration Wizard, specify the AD account that has permissions to perform the federation service configuration.
   Note: This account must be of the type domain administrator.

2. Use Domain\Administrator account.

3. Select the SSL certificate that you will use and also provide the ADFS name selected in the design process. In this case the name is adfs.example.com. Clients will use the same name on the Intranet and Internet to locate ADFS. Provide your chosen display name and click **Next**.

4. You can also use a GMSA (Group Managed Service Account) as the ADFS service account. GMSA will automatically update the service account's credentials.

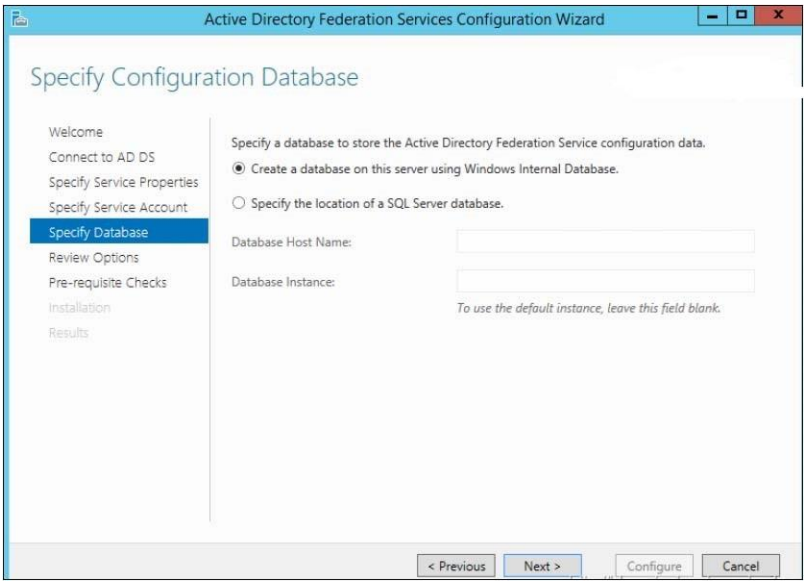


5. In the next step, we specify a service account for the ADFS service. This should be a domain user account and requires no special permissions.

6. You may get a warning that you cannot use a Group Managed Service Account. This is because your test domain is not currently configured to support them. For more information about Group Managed Service Accounts, check out this link. http://blogs.technet.com/b/askpfeplat/archive/2012/12/17/windows-server-2012-group-managed-service-accounts.aspx.

7. Select the type of database you would like to use from the following options:
    a. Create a database on this server using Windows Internal Database
    b. Specify the location of the SQL Server database.

    Note: If you choose to use the Windows Internal Database, you can migrate the configuration and artifact databases to SQL at a later point in time.

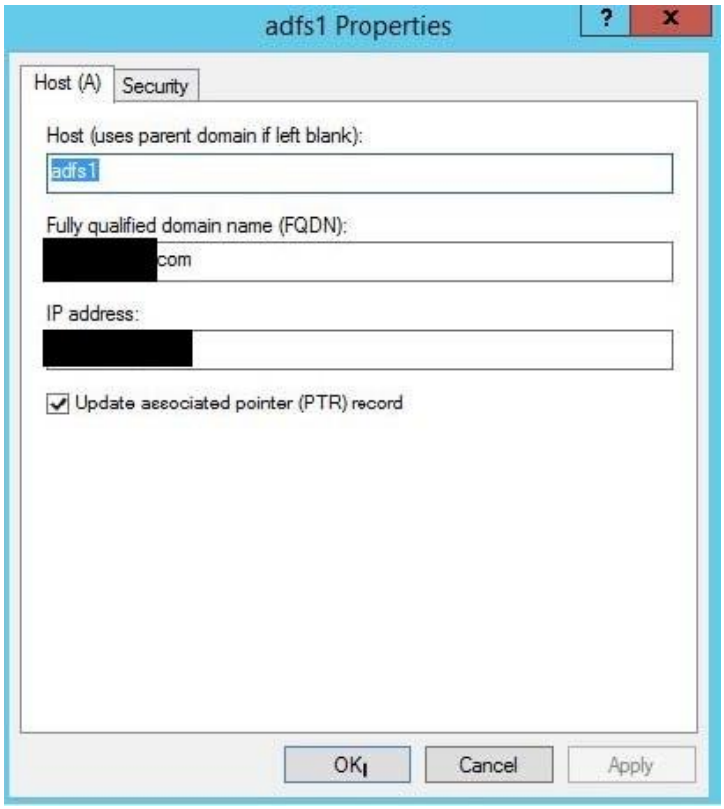


8. Review the options and ensure the ADFS pre-requisite checks are done before proceeding with the configuration.

Create a DNS A Record

To configure Microsoft ADFS, you must create a DNS A record to support the Federation Service name. In this case you will need an "**A**" record that points to your federation service, https://adfs.example.com, at the ADFS server IP address x.x.x.x.

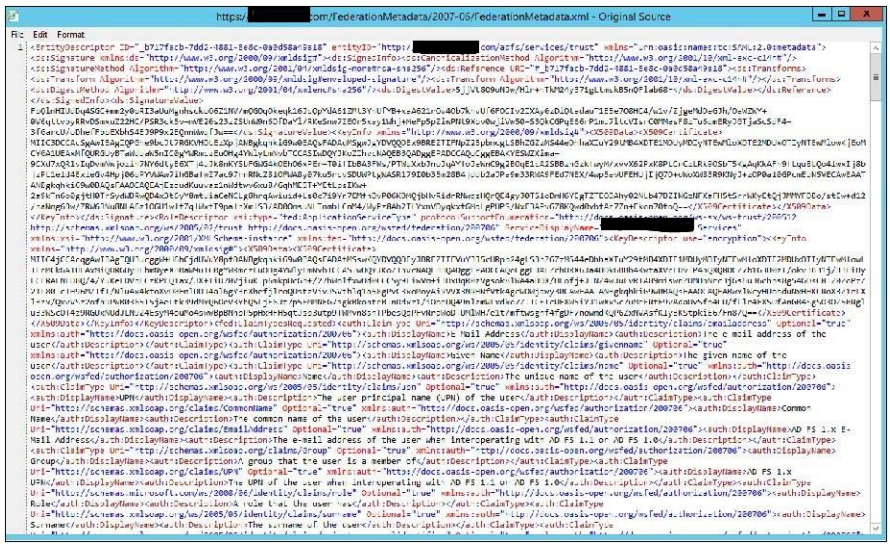
You must create the DNS record for the ADFS instance. This maps to the ADFS namespace that we previously planned. Create this A record in your internal DNS infrastructure. Once the DNS record has been created and propagated ensure that it resolves correctly.



Verify Federation Service Metadata

1. Open Internet Explorer from Web Application Proxy or any Server on the Domain and navigate to your ADFS server's federation metadata URL.

2. Change the FQDN to match your environment.
   https://adfs.example.com/federationmetadata/2007-06/federationmetadata.xml

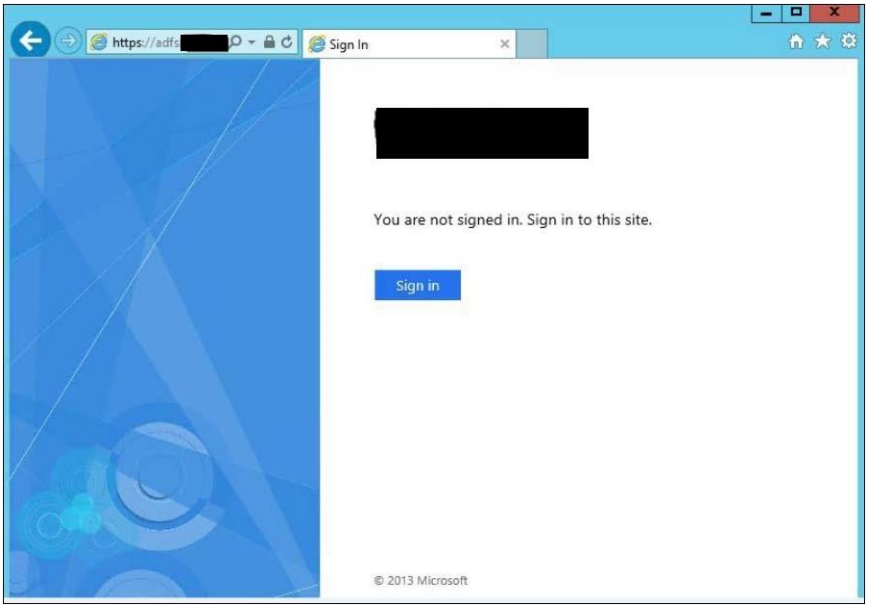


Verify ADFS Sign-In Page

1. Browse to the ADFS sign-in page and test that you are able to authenticate.

2. The URL will be similar to what is shown below. Change the FQDN to match your organization.
   https://adfs.example.com/adfs/ls/idpinitiatedsignon.htm

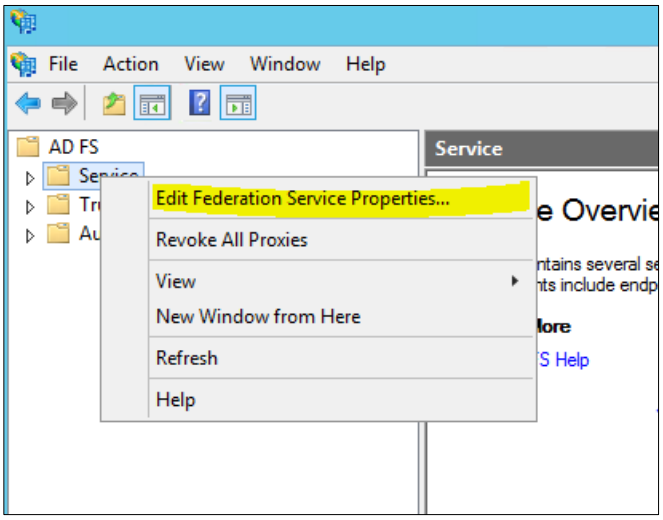
3. At the prompt, click **Sign in**.



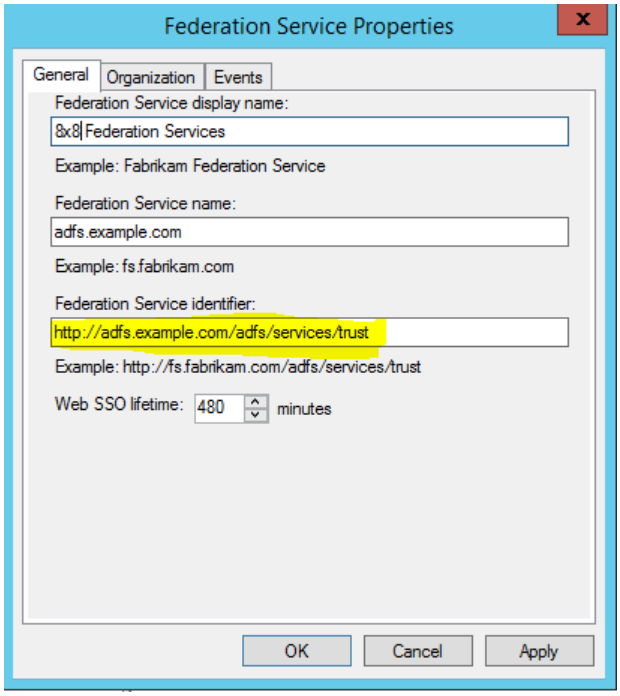
General ADFS Setup

This procedure uses ADFS 3.0 and shows adfs.example.com as the ADFS website. Replace this with your ADFS website address.

1. Log into the ADFS server and open the management console.
2. Right-click **Service** and choose ***Edit Federation Service Properties***.



3. Confirm that the General settings match your ***DNS*** entries and certificate names. Take note of the ***Federation Service Identifier***, since that is used in the **8x8 SAML 2.0** configuration settings.



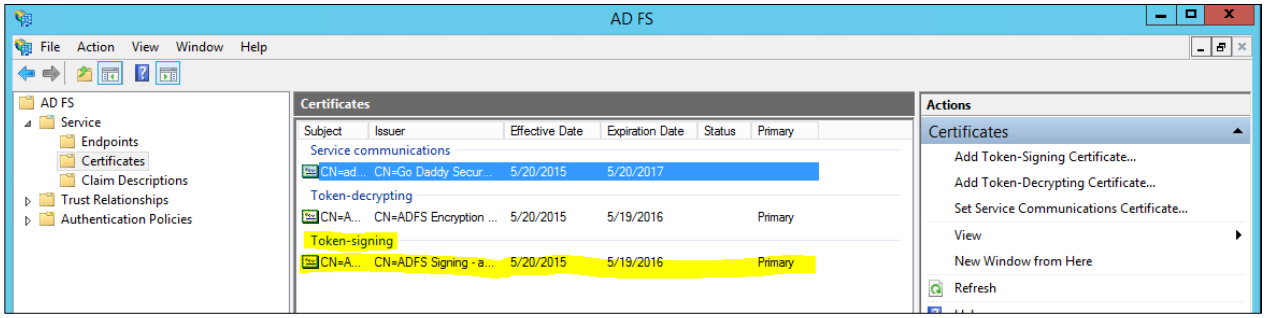
4. Browse to the certificates and export the **Token-Signing certificate**.
    a. Right-click the certificate and select **View Certificate**.
    b. Select the **Details** tab.

c. Click **Copy to File**.

5. The Certificate Export Wizard launches.
   a. Select Next.
   b. Ensure **No, do not export the private key** is selected, and then click **Next**.
   c. Select ***DER encoded binary X.509 (.cer)***, and then click **Next**.
   d. Select where you want to save the file and give it a name. Click **Next**.
   e. Select **Finish**.

8x8 Account Manager requires that this certificate be in **PEM** format. You can convert this certificate using client tools or even online tools such as:

SSL Shopper (https://www.sslshopper.com/ssl-converter.html).
Use the DER/Binary certificate we just created and export it to Standard PEM format.



Set up SAML 2.0 in Account Manager

Setting up Single Sign-On in Account Manager: If not already active, contact **8x8 Virtual Office Administrator** to activate the SAML 2.0 Single Sign-On plugin.

The admin must set up Single Sign-On and specify the **Identity Provider** used by the company.

Defining Federated ID in User Profiles—is an optional step. If the 8x8 user name is not a unique email address, then you must add Federation ID (for SAML).

Customers with Identity Management Systems like Microsoft ADFS require their employees to be able to authenticate to 8x8 apps using their company user name instead of an 8x8 user name and password.

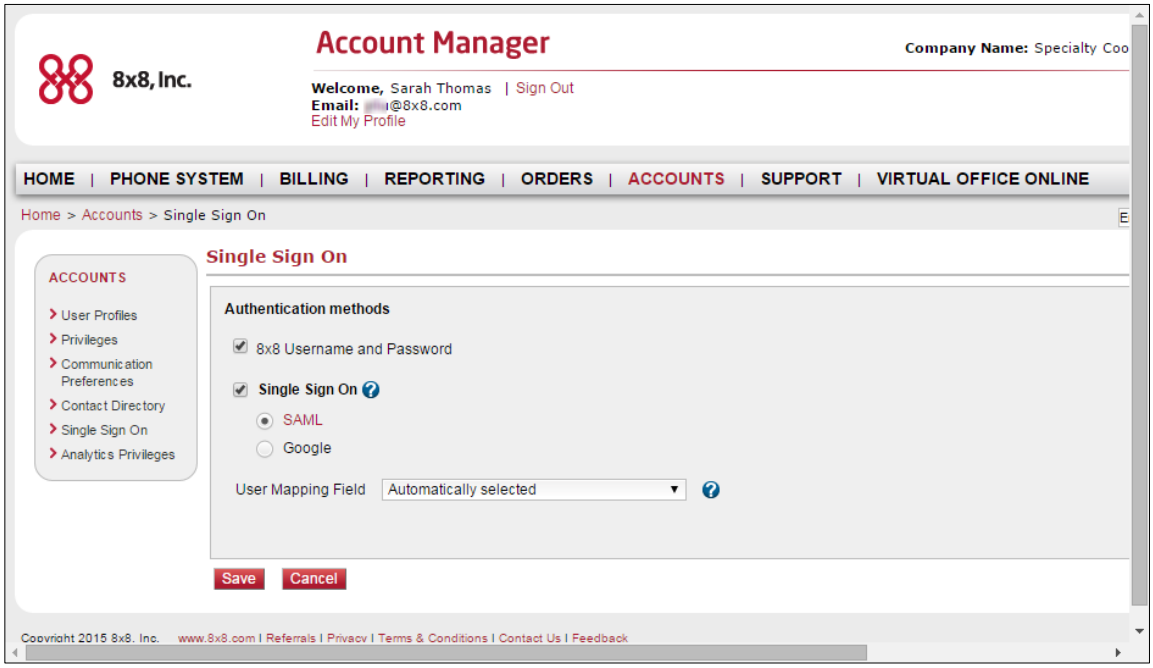
In this release, we support SAML 2.0. Single Sign-On (SSO) for the following 8x8 applications that use the shared 8x8 login web page.

- Virtual Office Online
- Virtual Office Desktop
- Virtual Office Mobile
- Virtual Contact Center
- Account Manager
- Switchboard Pro
- Virtual Office Analytics

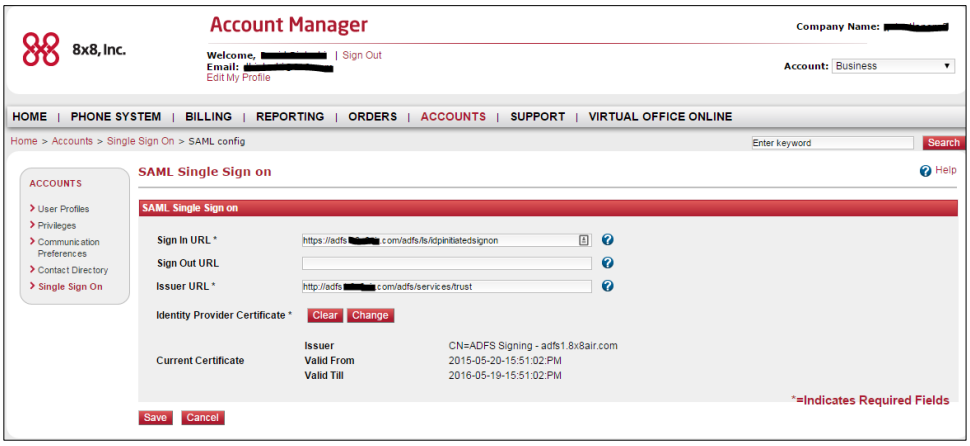
With support for federated SSO, users can log in to 8x8 applications through their company's identity management system.

Setting up Single Sign-On for ADFS

1. Log in to Account Manager.
2. Navigate to **Accounts** tab.
3. Select **Single Sign-On** option from the navigation menu.



4. Select an Identity Provider.
5. Select **SAML**: Allows users to log in to 8x8 applications by signing via SAML Identity Provider.
6. **Select the User Mapping Field** that maps each user from your SAML Identity Provider directory to 8x8.The system begins by matching via 8x8 Username.
   8x8 Username: The system maps via 8x8 **Username**.
7. **Federation ID:** For SAML, 8x8 maps via **Federation ID.**
8. **Save these settings.**
   If you selected **SAML**, you must specify the following:
9. **Sign in URL**: Enter the User authentication URL provided by Identity Provider (IDP).
   For ADFS this is (https://adfs.example.com/adfs/ls/idpinitiatedsignon.aspx).
10. **Sign-Out URL**: User sign out URL provided by IDP. This is the landing page when you log off from an 8x8 application. The input for this field is **optional**.
11. Issuer URL: IDP identifier: This is the *Federation Service Identifier* from the Federation Service Properties in ADFS Management Services under the General Tab.
    (**http://adfs.example.com/adfs/services/trust**).
12. **Identity Provider Certificate**: You may receive this information from the Identity Management.
    Token-Signing certificate in **PEM** format.
13. Browse to locate the certificate file and upload.



The certificate file is validated and notifies you of any errors.

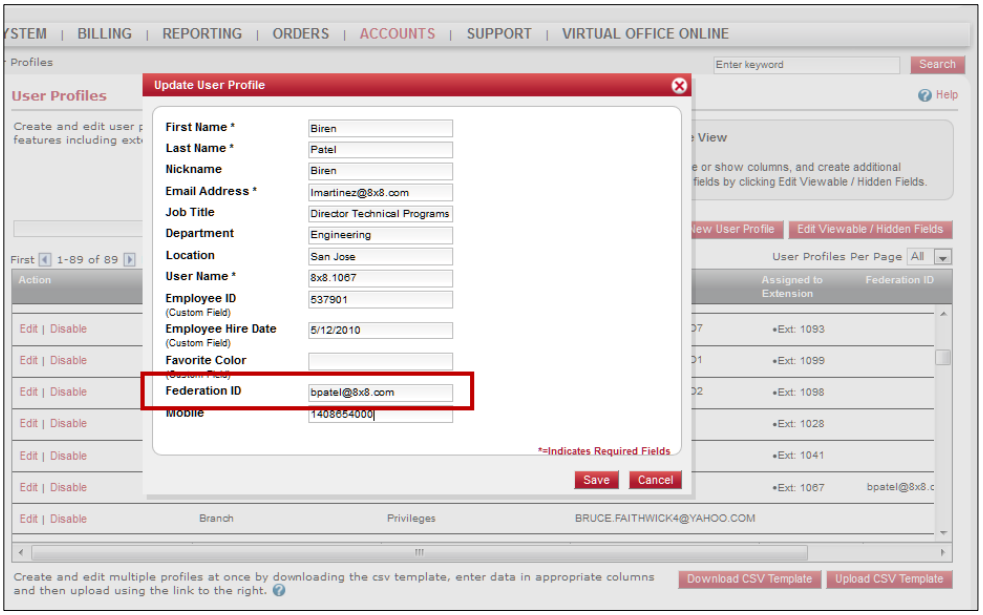
14. **Save the settings**. This completes the configuration of **SAML 2.0 Federated SSO**.

Defining Federated ID

If your company does not use unique email addresses for 8x8 username, you must map Virtual Office User with the Identity Provider using **Federated ID**.

After selecting the Identity Provider during Single Sign-On configuration, navigate to **user profiles** and populate the required mapping field in the user profile.

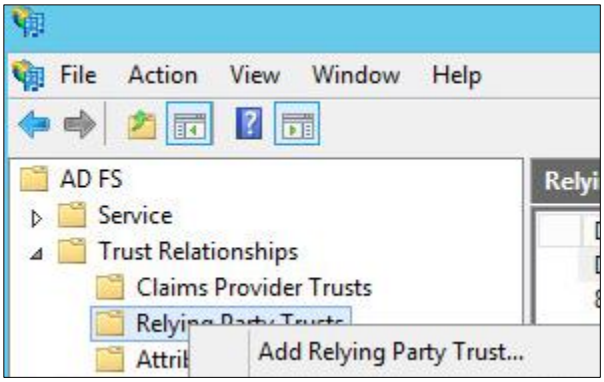
1. Navigate to **Accounts**.
2. Select to view **User Profiles**.
3. Based on the choice of identity provider, the corresponding mapping field shows.
4. For SAML, Federated ID is added.
5. From the list, edit the desired user profile to add the mapping field data.
6. For SAML, populate Federated ID.



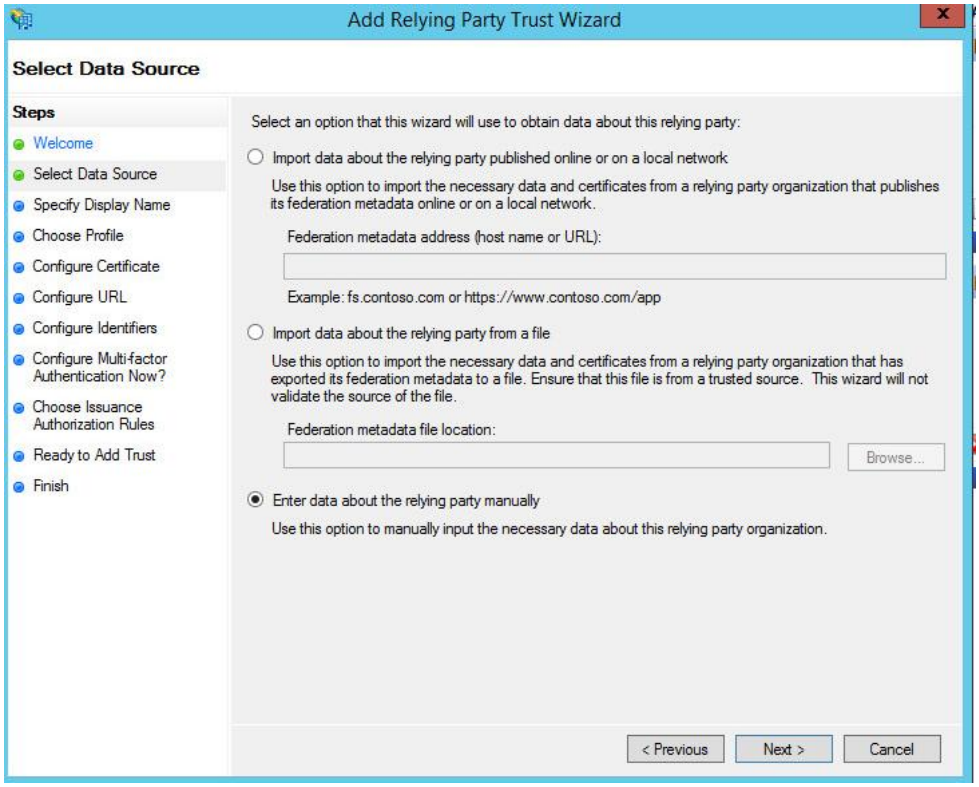
Add a Relying Party Trust to ADFS

Manual configuration of the relying party appears to be easier to implement for 8x8 SAML 2.0.

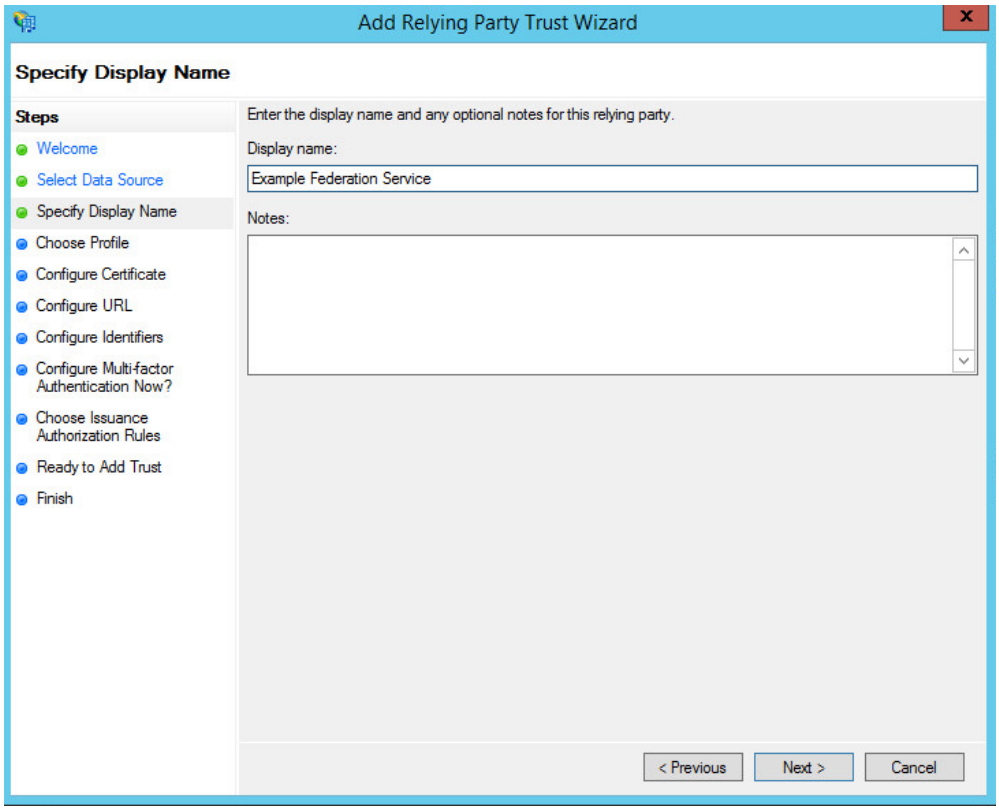
1. Open the ADFS Management console and select **Relying Party Trusts**.



2. Select **Add Relying Party Trust…** from the top right corner of the window.
3. The add wizard appears.
4. Click **Start** to begin.
5. Select **Enter Data about Relying Party manually**. Click **Next**.

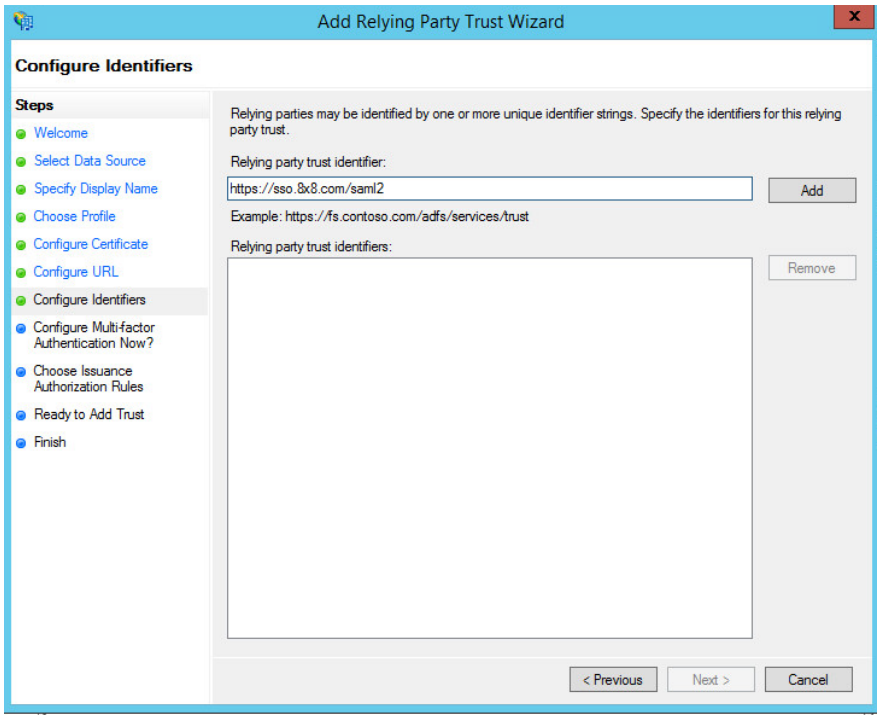


6. Add a display name such as **“8x8 Federation Service”** and enter any notes you want.

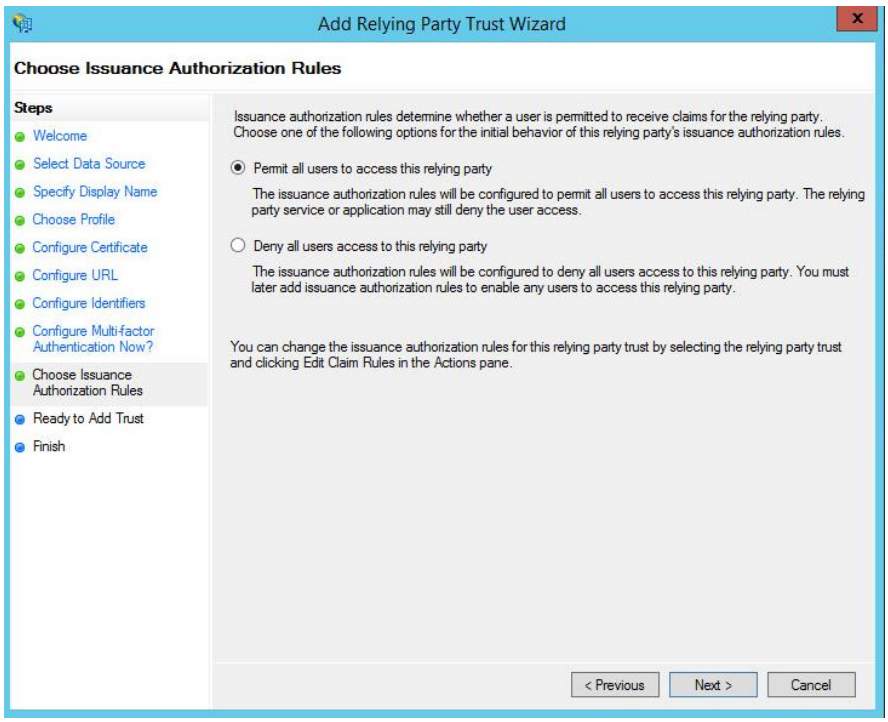


7. Click **Next**.
8. Select **ADFS 2.0/3.0 Profile**.
9. Do *not* select a token encryption certificate.
   It will use the certificate that is defined on the service that has already been exported. Defining a certificate here will prevent proper communication with 8x8 Account Manager.
10. Do *not* enable any settings on the **Configure URL**.

11. Enter the 8x8 web site to which you connected as the Relying Party trust identifier. In this case use https://sso.8x8.com/saml2 and click **Add**.



12. In the next step, select **Permit all users to access this relying party**.



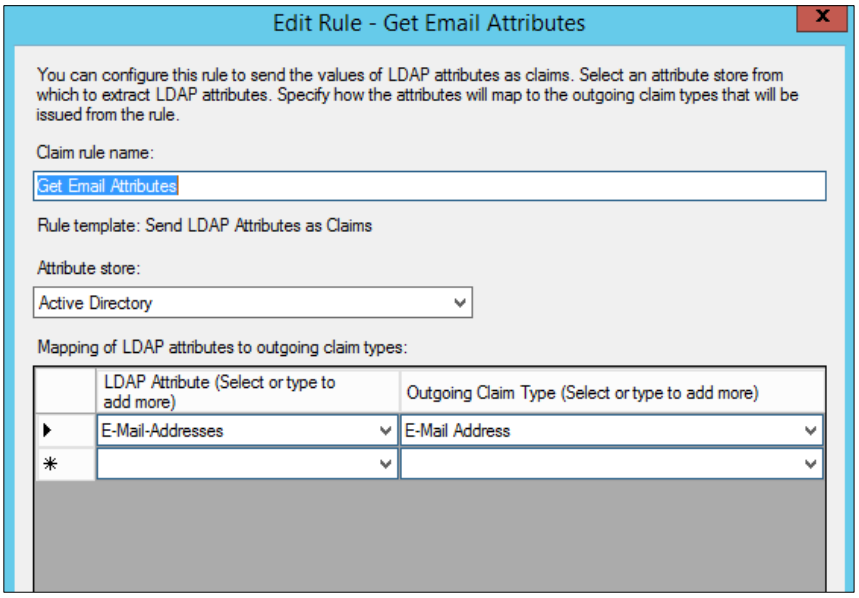
13. Click **Next** and clear the **Open the Claims when this finishes** check box.
14. Close this page. The new relying party trust appears in the window.
15. Right-click on the relying party trust and select **Properties**.
16. Browse to the **Advanced** tab and set the **Secure hash algorithm** to SHA-1.

17. Browse to the **Endpoints** tab and add a **SAML Assertion Consumer** with a **Post** binding and a URL of https://sso.8x8.com/saml2
18. Click **OK** to complete the setup.

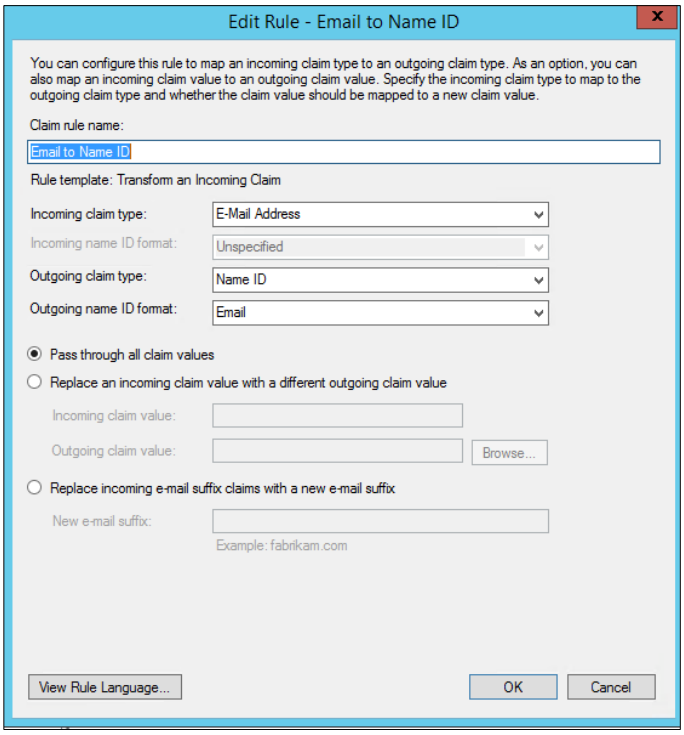
Configure ADFS Relying Party Claim Rules

Edit the Claim rules to enable proper communication with Service-Now.

1. Right-click on the relying party trust and select **Edit Claim Rules…**.
2. On the Issuance Transform Rules tab select **Add Rules…**.
3. Select **Send LDAP Attribute as Claims** as the claim rule template to use.
4. Give the claim a name such as **8x8 Claims App**.
5. Set the Attribute Store to **Active Directory**, the LDAP Attribute to **E-Mail-Addresses**, and the Outgoing Claim Type to **E-mail Address** for mapping.



6. Select **Finish**.
7. Select **Add Rule…**
8. Select **Transform an Incoming Claim** as the claim rule template to use. Click **Next**.
9. Give it a name such as **Email to Name ID**.
10. Specify the Incoming claim type. It should be **E-mail Address** (it must match the **Outgoing Claim Type in rule #1**. The Outgoing claim type is **Name ID** (this is requested in 8x8 Account Manager policy **urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress**) and the Outgoing name ID format is **Email**. Pass through all claim values.
11. Click **Finish.**



Log into ADFS

1. Open Internet Explorer and browse to *https://adfs.example.com/adfs/ls/idpinitiatedsignon.aspx*.
   This opens a generic page with a drop down list of all Relying Party Trusts configured.
2. Select the one you want to log in to and click **Continue to Sign In**.
   This only works if you have enabled SSO on the 8x8 Account Manager web page. If the configuration is complete, you are logged in.