Overview and Walkthrough: Single sign-on with AD FS and SAP SuccessFactors

Author : Robert Michelsen

Date : April 8, 2015

This article walks through setting up SAML 2.0 SSO between AD FS and SAP SuccessFactors.

It explains what needs to be to done from a customer/admin perspective for a complete SSO implementation. If the customer is experienced enough and feels confident to do these steps without assistance, its not required to involve an implementation partner. This example setup will be the most simple way to implement SAML SSO. SuccessFactors allows many advanced configuration options, which will be covered in a later article. This article is intended as an overview and to provide hands on experience with configuring SuccessFactors SSO.

The SSO configuration on the SuccessFactors side is done in backend tools ("Provisioning tool") which only SuccessFactors employees and SuccessFactors implemenation partners have access to. A customer who wants to implement SSO needs to relay the needed info to either of them.

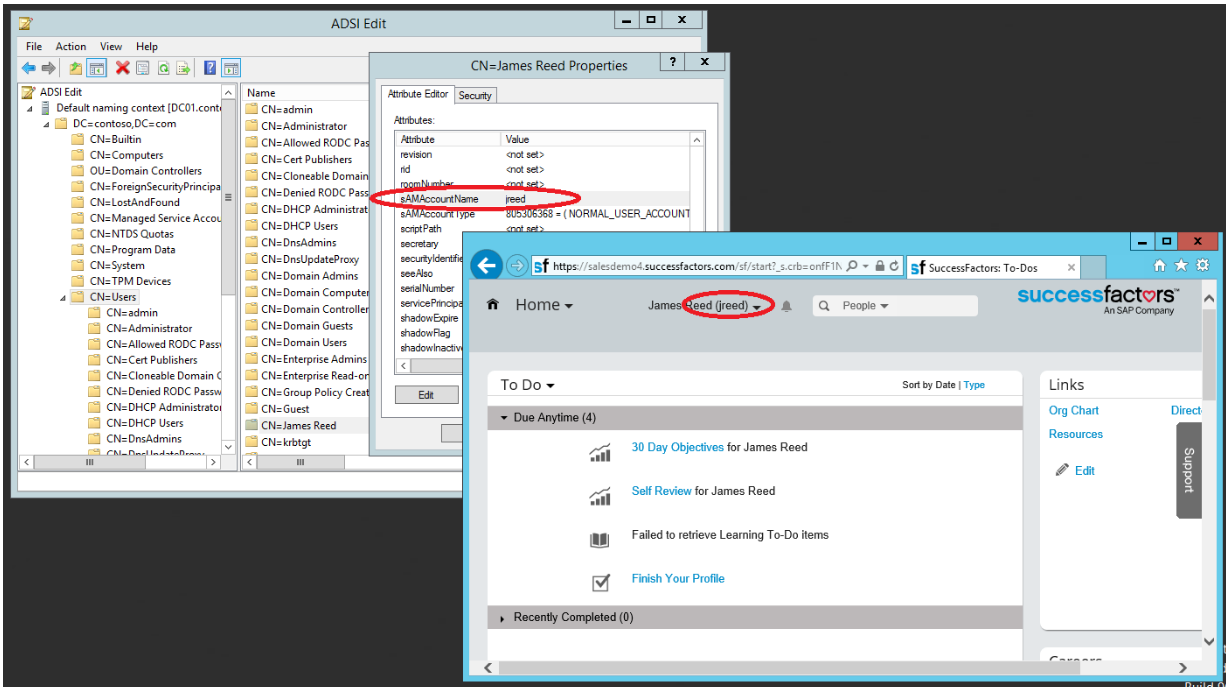
It is possible to setup SSO with salesdemo instances, however in this case it is required that the instance was requested by a partner and is associated with the partners Provisioning account. This is because SuccessFactors will not make any changes to salesdemo instances. It will not work with a salesdemo instance requested from the www.successfactors.com homepage, as they are not associated with a provisioning account of a partner.

This article uses AD FS as an example, but the information here can be applied to SSO middleware like Okta or SiteMinder as well.

Overview of the setup

This example setup assumes:

- The username in SuccessFactors is the same as the sAMAccountName of the user in Active Directory. The sAMAccountName is actually the familiar Domain***LogonName***. The Active Directory and SuccessFactors accounts need to be prepared accordingly. Note that SuccessFactors uses userid as well as username. The username is the name Successfactors users use to login without SSO. A good way way to confirm username is via Admin Tools - Update User Information - Employee Export.



Attribute	Value
revision	<not set>
rid	<not set>
roomNumber	<not set>
sAMAccountName	jreed
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
scriptPath	<not set>
secretary	
securityIdentifie	
seeAlso	
serialNumber	
servicePrincipa	
shadowExpire	
shadowFlag	
shadowInactiv	

Due Anytime (4)

30 Day Objectives for James Reed

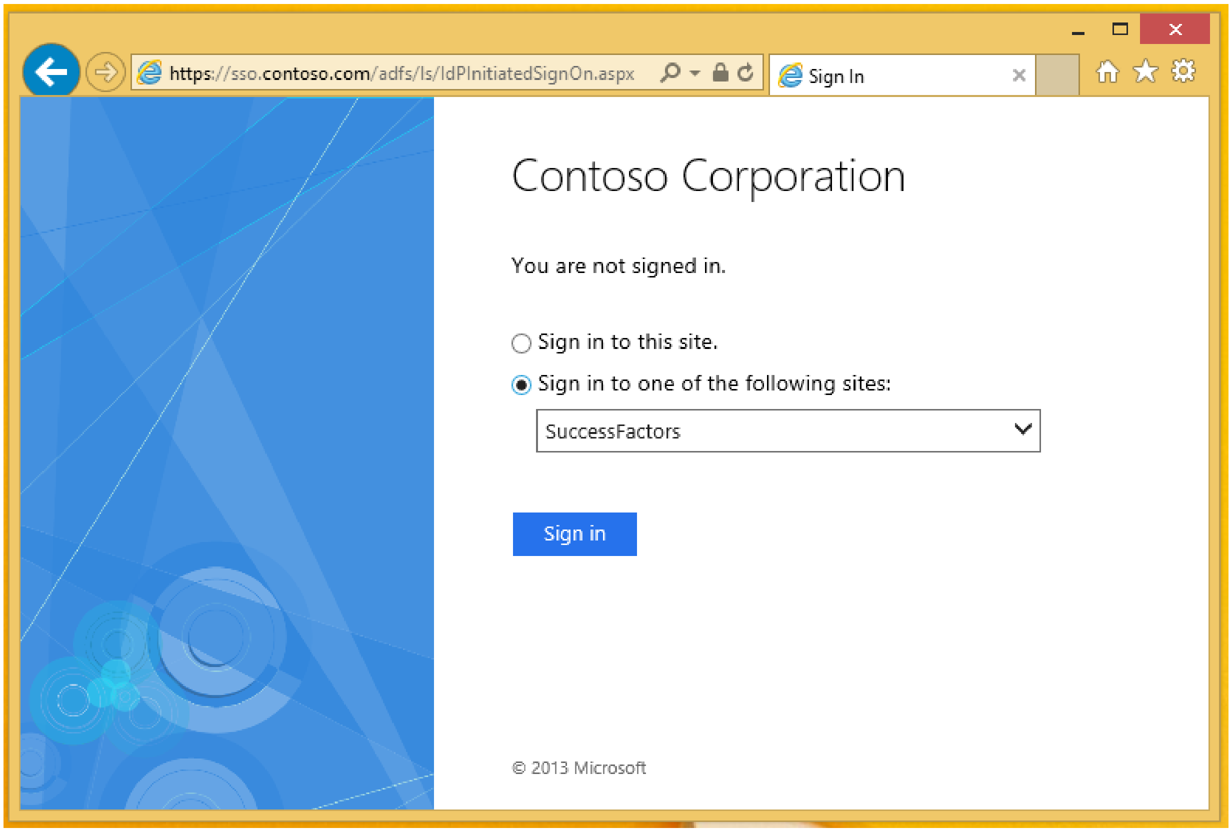
Self Review for James Reed

Failed to retrieve Learning To-Do items

Finish Your Profile

Recently Completed (0)

- Users will navigate to the AD FS IdP login page to login to the SF application (IdP initiated login).



Contoso Corporation

You are not signed in.

○ Sign in to this site.

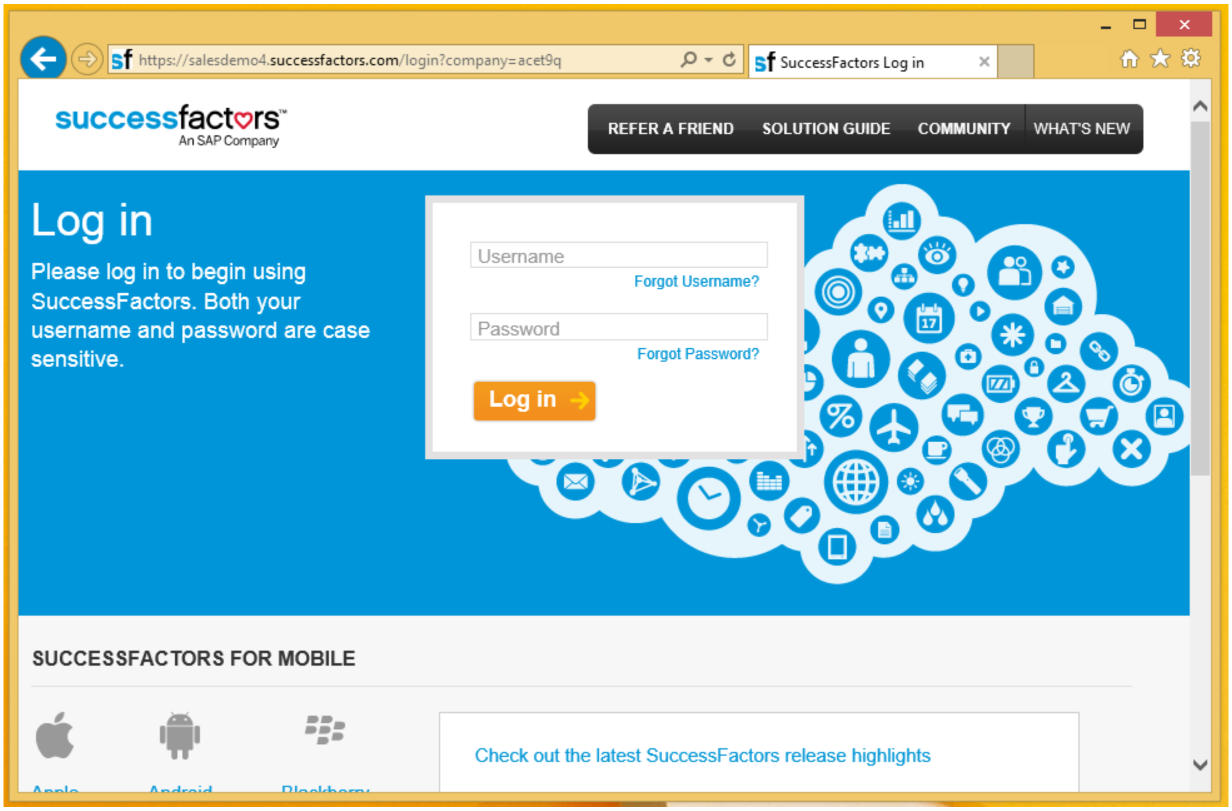
● Sign in to one of the following sites:

SuccessFactors

Sign in

© 2013 Microsoft

- Password login will be disabled for all users. The SuccessFactors login page (with the company ID parameter) will still be available, but users won't be able to login there with their SuccessFactors credentials anymore. Before setting up SSO, an admin account is already configured in SuccessFactors, and a matching Active Directory account exists. This is important, as else you will be locked out of your instance, and need to contact SF/Partner to deactivate SSO to get access again.



https://salesdemo4.successfactors.com/login?company=acet9q

Log in

Please log in to begin using SuccessFactors. Both your username and password are case sensitive.

Check out the latest SuccessFactors release highlights

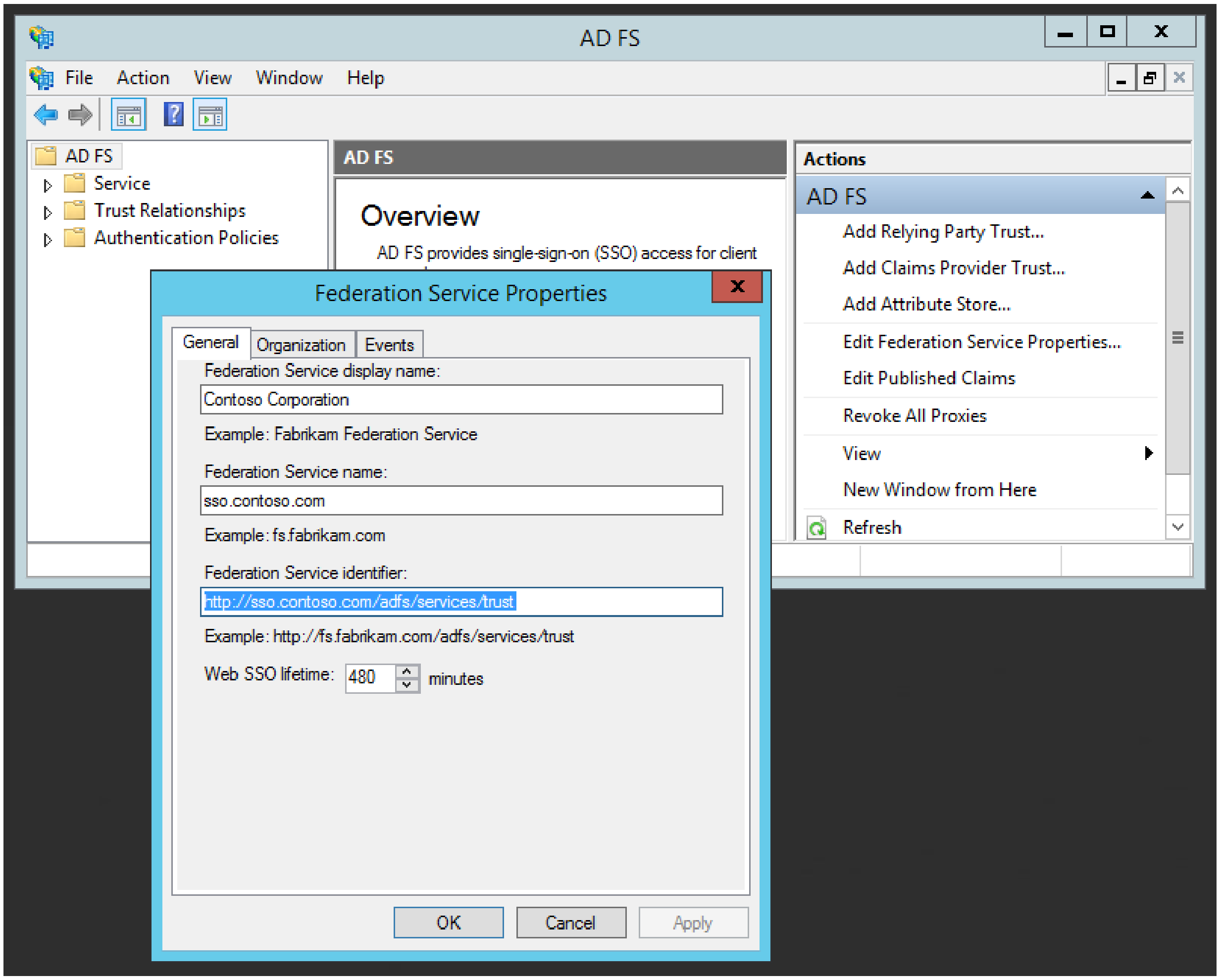
Information the customer needs to provide to SuccessFactors or Partner

The following info needs to be provided to be configured in the backend for your instance:

- Company ID and performancemanager domain
- Request to set token based SSO to activated ("activate SSO")
- new SAML asserting party to be added with the following two parameters:
  - SAML issuer
  - token signing certificate (Base 64 format)

Performancemanager Domain and company ID are for example:
https://***salesdemo4.successfactors.com***/login?company=***acet9q***
https://***performancemanager4.successfactors.com***/login?company=***contoso***

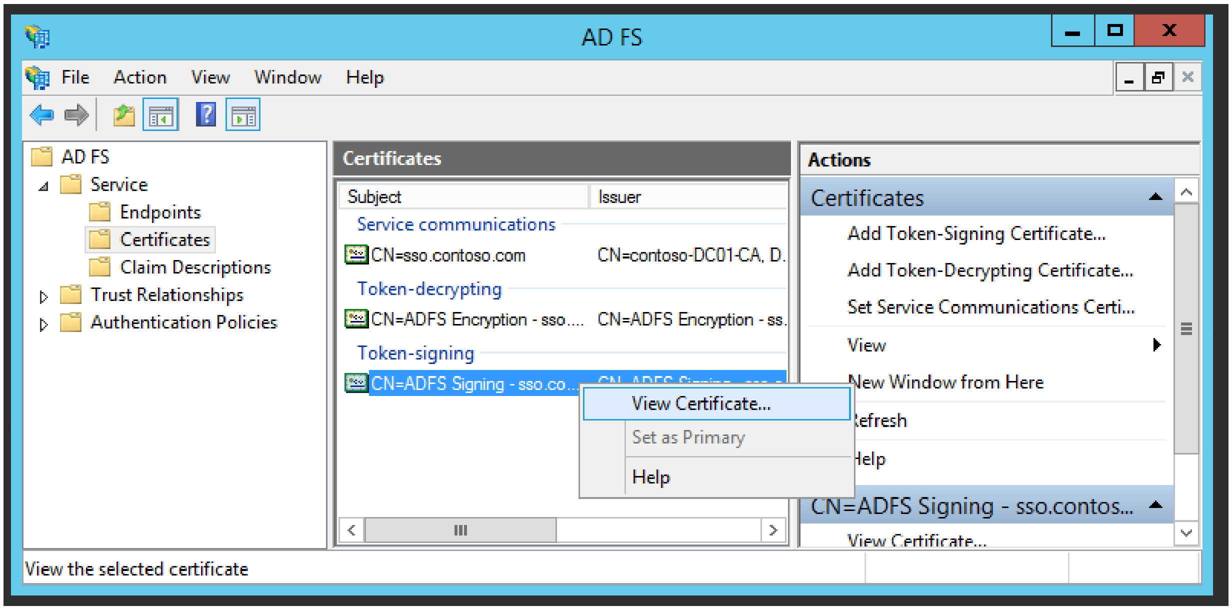
SAML issuer
This is the ID of the Federation Service that the IdP sends to SuccessFactors. It is a parameter that is "global" for the Federation Service, and not a parameter of an individual asserting party. You can therefore provide it even before setting up the Relying Party for SuccessFactors. It is often a URL, but can also be just a name. In AD FS, it is called "Federation Service Identifier", and can be found under Edit Federation Service Properties…



Overview
AD FS provides single-sign-on (SSO) access for client

Federation Service display name: Contoso Corporation
Example: Fabrikam Federation Service
Federation Service name: sso.contoso.com
Example: fs.fabrikam.com
Federation Service identifier: http://sso.contoso.com/adfs/services/trust
Example: http://fs.fabrikam.com/adfs/services/trust
Web SSO lifetime: 480 minutes

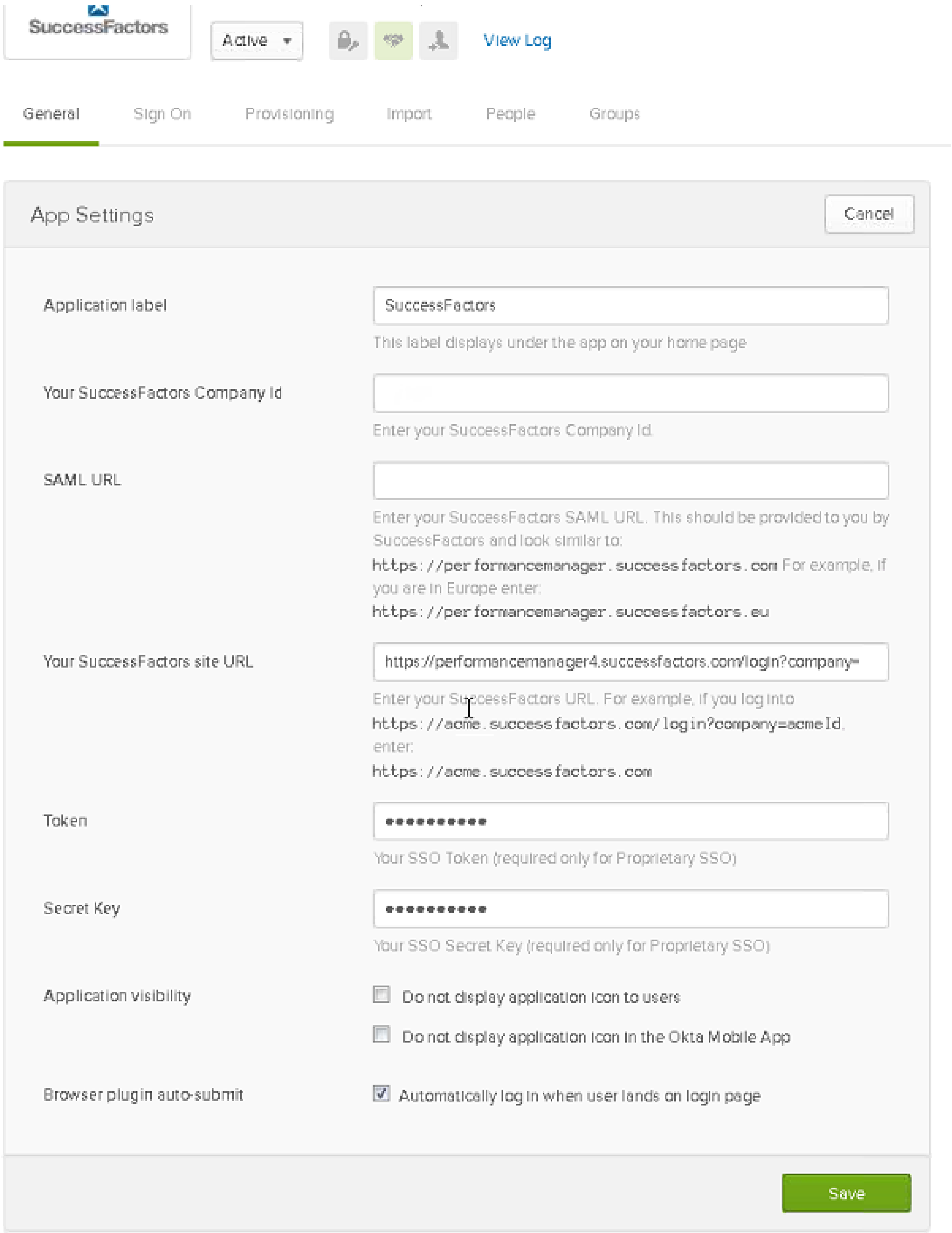
The token signing certificate is global for the Federation Service as well, and can be found under Service - Certificates Folder in AD FS. The certificate needs to be provided in base 64 format (right click, View Certificate..., Details tab, Copy to File..., Base-64 encoded X.509 (.CER)



Subject	Issuer
Service communications	
CN=sso.contoso.com	CN=contoso-DC01-CA, D.
Token-decrypting	
CN=ADFS Encryption - sso....	CN=ADFS Encryption - ss.
Token-signing	
CN=ADFS Signing - sso.co...	CN=ADFS Signing - sso.c

Information the customer needs to enter on his IdP

It’s a little known fact that the info to be entered on the IdP side does not need to be "provided" by SuccessFactors. Instead, everything can be derived from company ID and performancemanger domain. This is for example reflected in the predefined Okta SuccessFactors app, which generates all necessary info based on that:



App Settings

Application label: SuccessFactors

This label displays under the app on your home page

Your SuccessFactors Company Id:

Enter your SuccessFactors Company Id.

SAML URL:

Enter your SuccessFactors SAML URL. This should be provided to you by SuccessFactors and look similar to: `https://performancemanager.successfactors.com` For example, if you are in Europe enter: `https://performancemanager.successfactors.eu`

Your SuccessFactors site URL: https://performancemanager4.successfactors.com/login?company=

Enter your SuccessFactors URL. For example, if you log into `https://acme.successfactors.com/login?company=acmeId`, enter: `https://acme.successfactors.com`

Token: ●●●●●●●●●●●

Your SSO Token (required only for Proprietary SSO)

Secret Key: ●●●●●●●●●●●

Your SSO Secret Key (required only for Proprietary SSO)

Application visibility:

□ Do not display application icon to users

□ Do not display application icon in the Okta Mobile App

Browser plugin auto-submit:

☑ Automatically log in when user lands on login page

The following URLs will need to be generated:

Relying party SAML 2.0 SSO service URL, with your domain, and company ID, for example:
https://***salesdemo4.successfactors.com***/saml2/SAMLAssertionConsumer?company=***acet9q***
https://
performancemanager4.successfactors.com
/saml2/SAMLAssertionConsumer?company=***contoso***

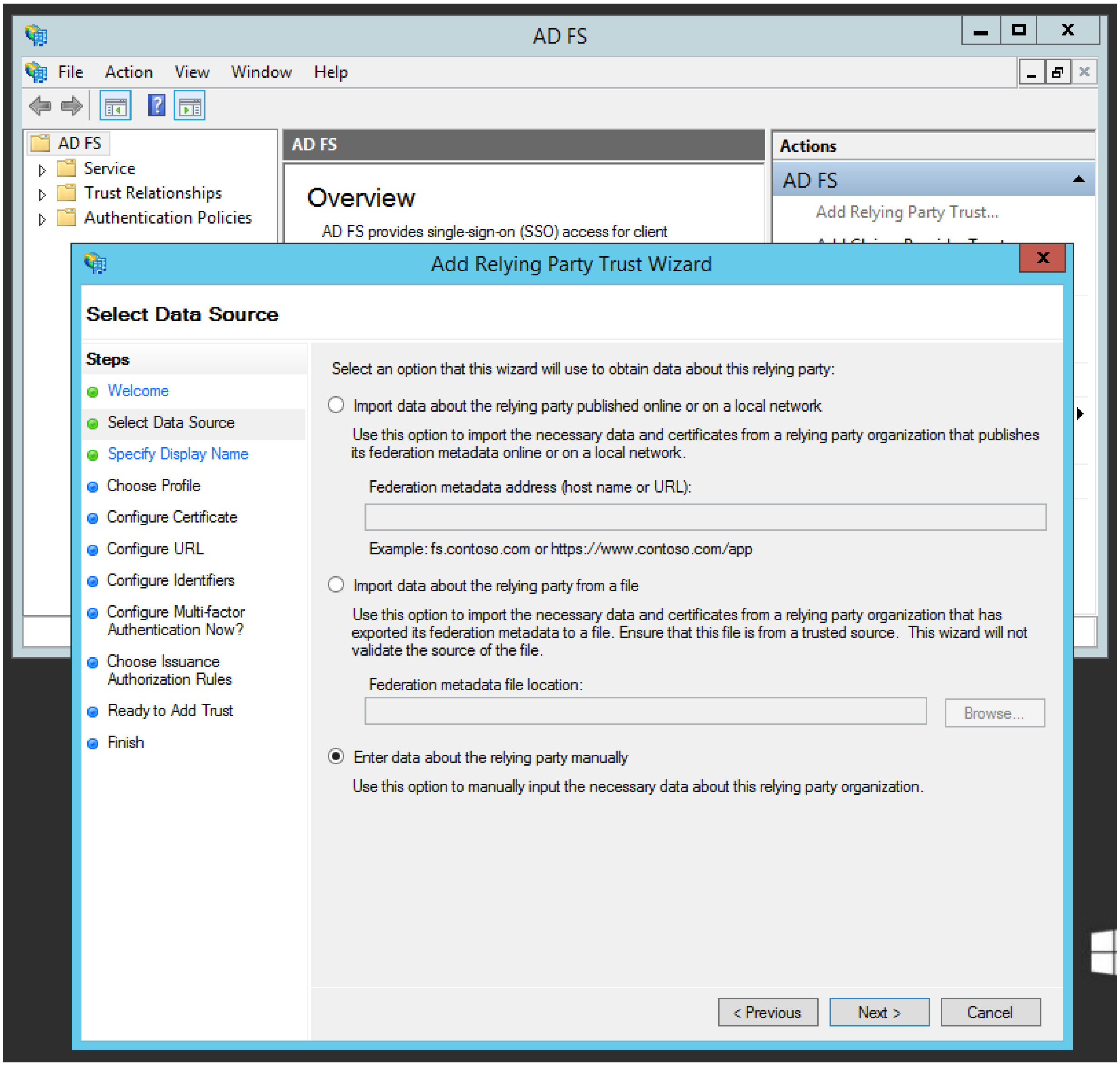
Relying Party Trust Identifier, with your company ID, for example:
https://www.successfactors.com/***acet9q***
https://www.successfactors.com/***contoso***

These two URLs are basically all the data you need. The next section shows how to setup the Relying Party Trust using these URLs.

Adding the Relaying Party Trust for SuccessFactors in AD FS

To setup SSO on the IDP, a Relaying Party Trust needs to be added in AD FS:

Choose Add new Relaying Party, and select Enter Data Source Manually. SuccessFactors does not publish or provide a federation metadata file.



Overview

AD FS provides single-sign-on (SSO) access for client

Select Data Source

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.

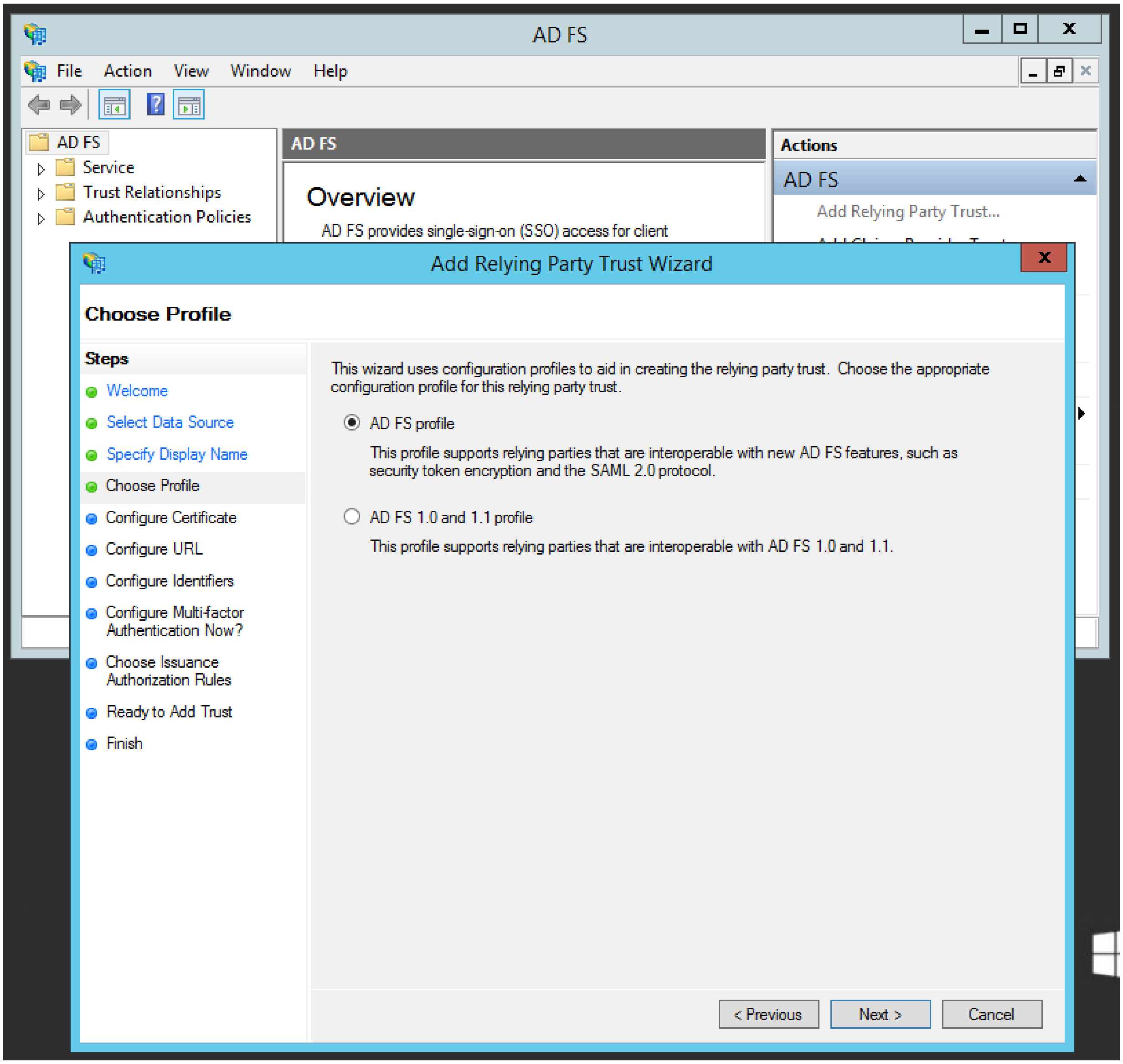
Federation metadata file location:

● Enter data about the relying party manually

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

Enter a displayname of your choice, which shows up as name for the Relying Party in the AD FS console, and for the users as the service name to login on the AD FS IdP initiated login page.

For profile, choose AD FS profile, for SAML 2.0 support:


AD FS
File Action View Window Help
AD FS
Service
Trust Relationships
Authentication Policies
AD FS
Overview
AD FS provides single-sign-on (SSO) access for client
Actions
AD FS
Add Relying Party Trust...

Add Relying Party Trust Wizard

Choose Profile

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

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

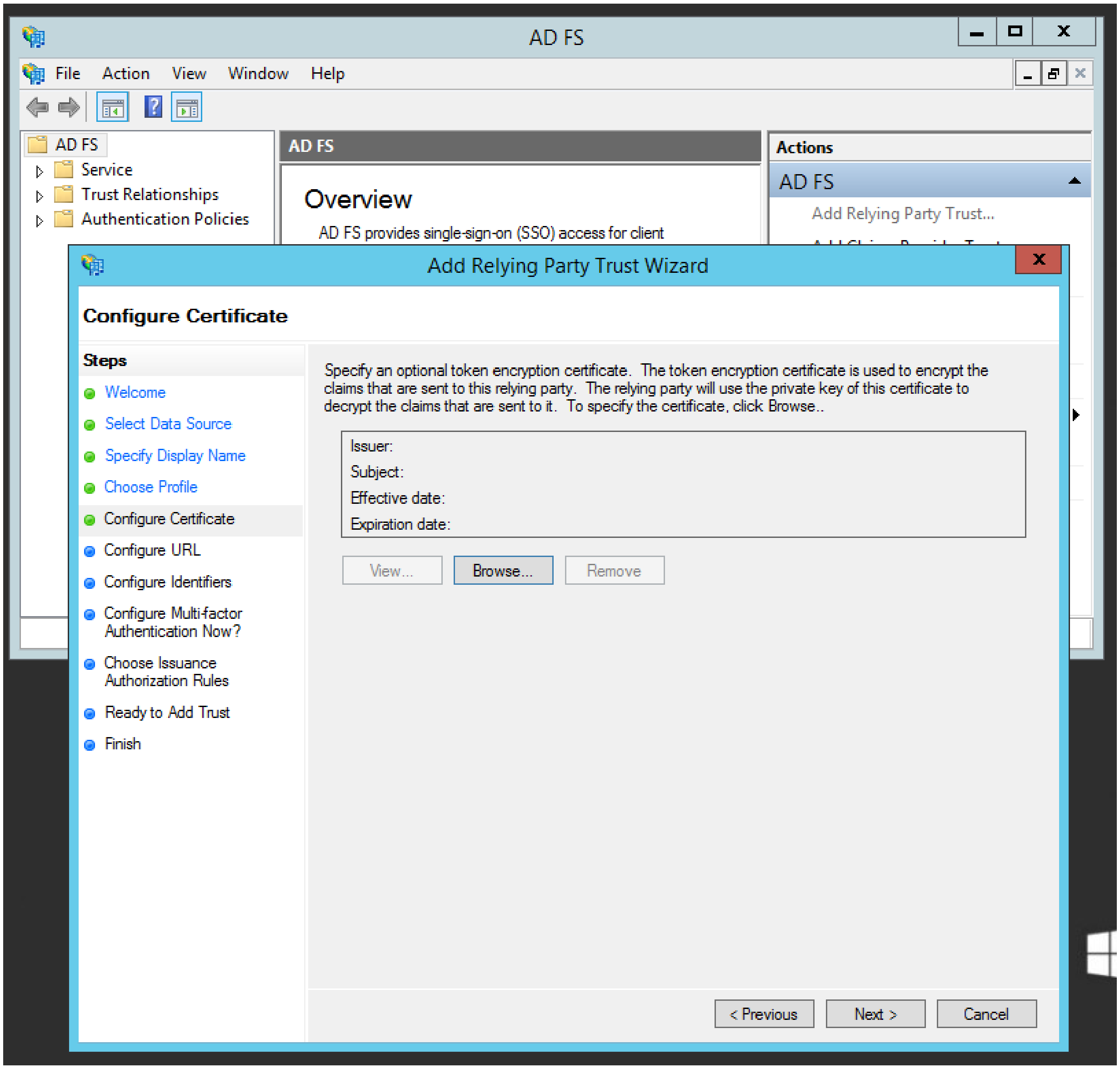
● AD FS profile

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.

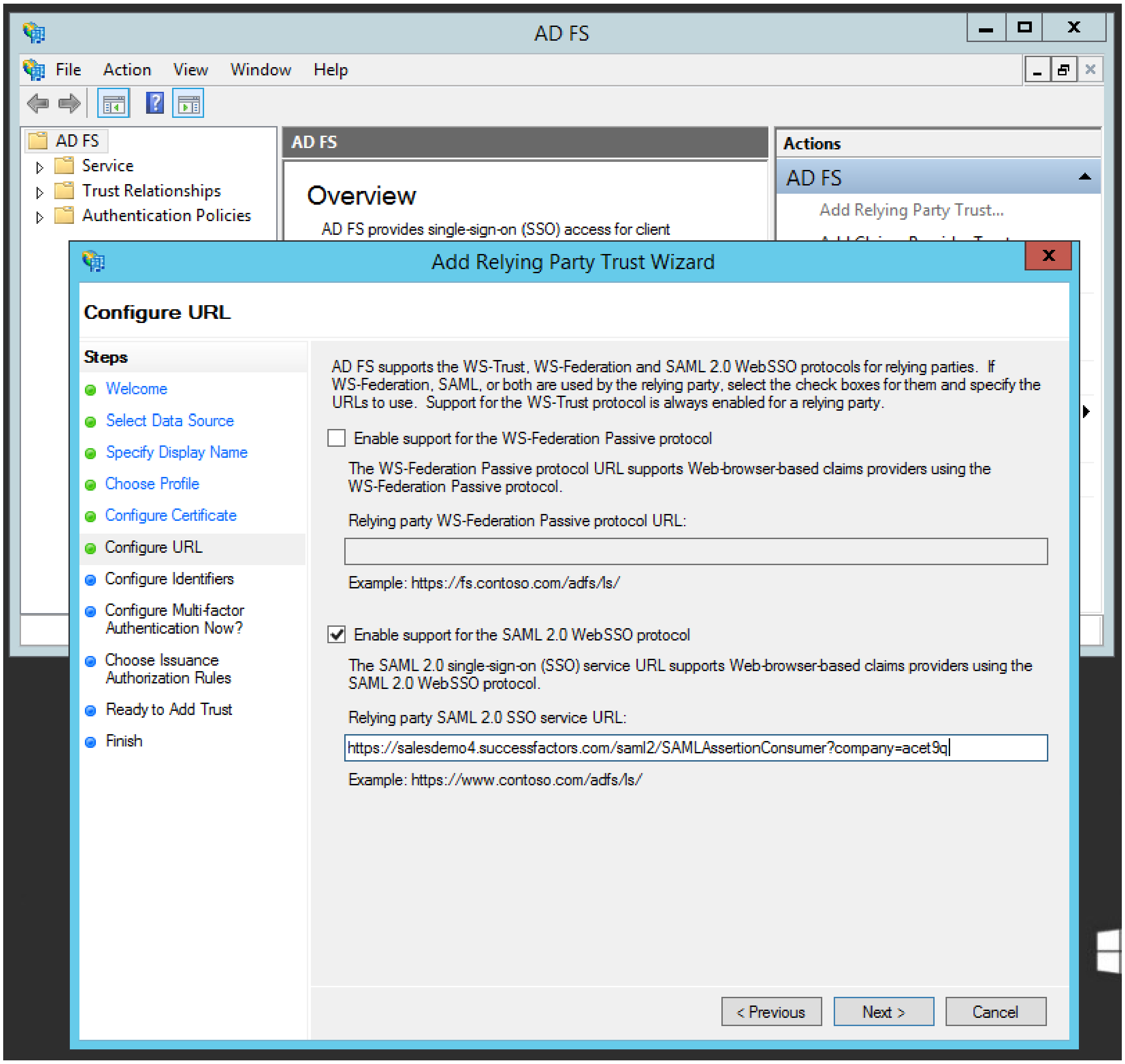
Don’t select a token encryption certificate. Note that this setting has nothing to do with the token signing certificate.



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:

Enter the Relying Party Service URL:



Overview

AD FS provides single-sign-on (SSO) access for client

Configure URL

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

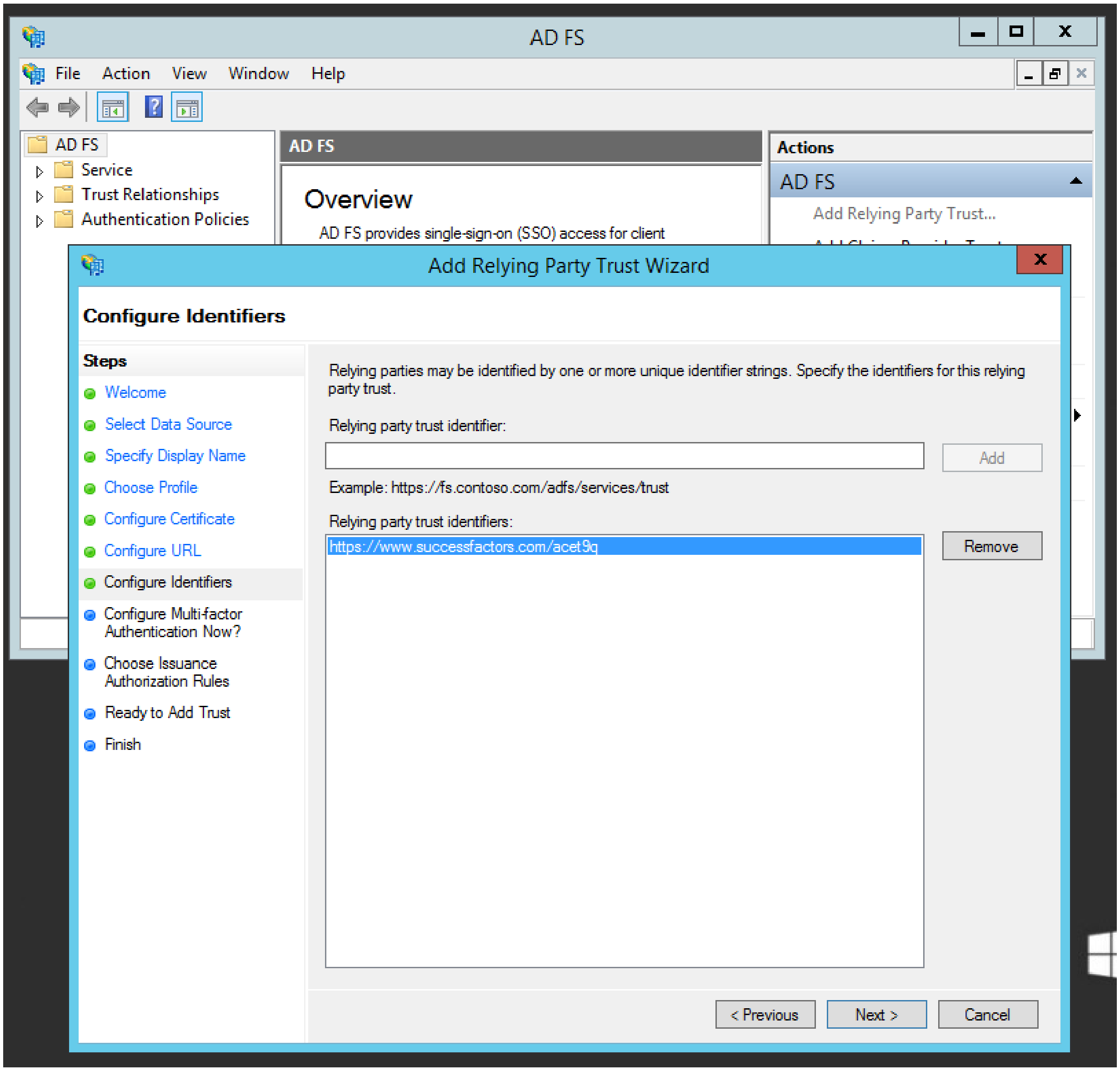
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://salesdemo4.successfactors.com/saml2/SAMLAssertionConsumer?company=acet9q

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

Configure Relying party trust identifier:



Overview

AD FS provides single-sign-on (SSO) access for client

Configure Identifiers

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:

https://www.successfactors.com/acet9q

In the next screens, do not configure multi factor authentication, permit all users access to this relying party, and finish the wizard.

The asserting party will show up under Relying Party Trusts folder.

Claims configuration

The claims are the values that identify the user that wants to login which are sent to the relying party. SuccessFactors logs in the user that is specified with the NameID parameter. We will configure the claims so that the value of sAMAccountName of the logged in user will be sent as value for the NameID parameter. In other words, we will configure the claims so that in the SAML assertion under subject it will read for example NameID=jreed, if user James Reed wants to login.

Here is where it gets a bit tricky:

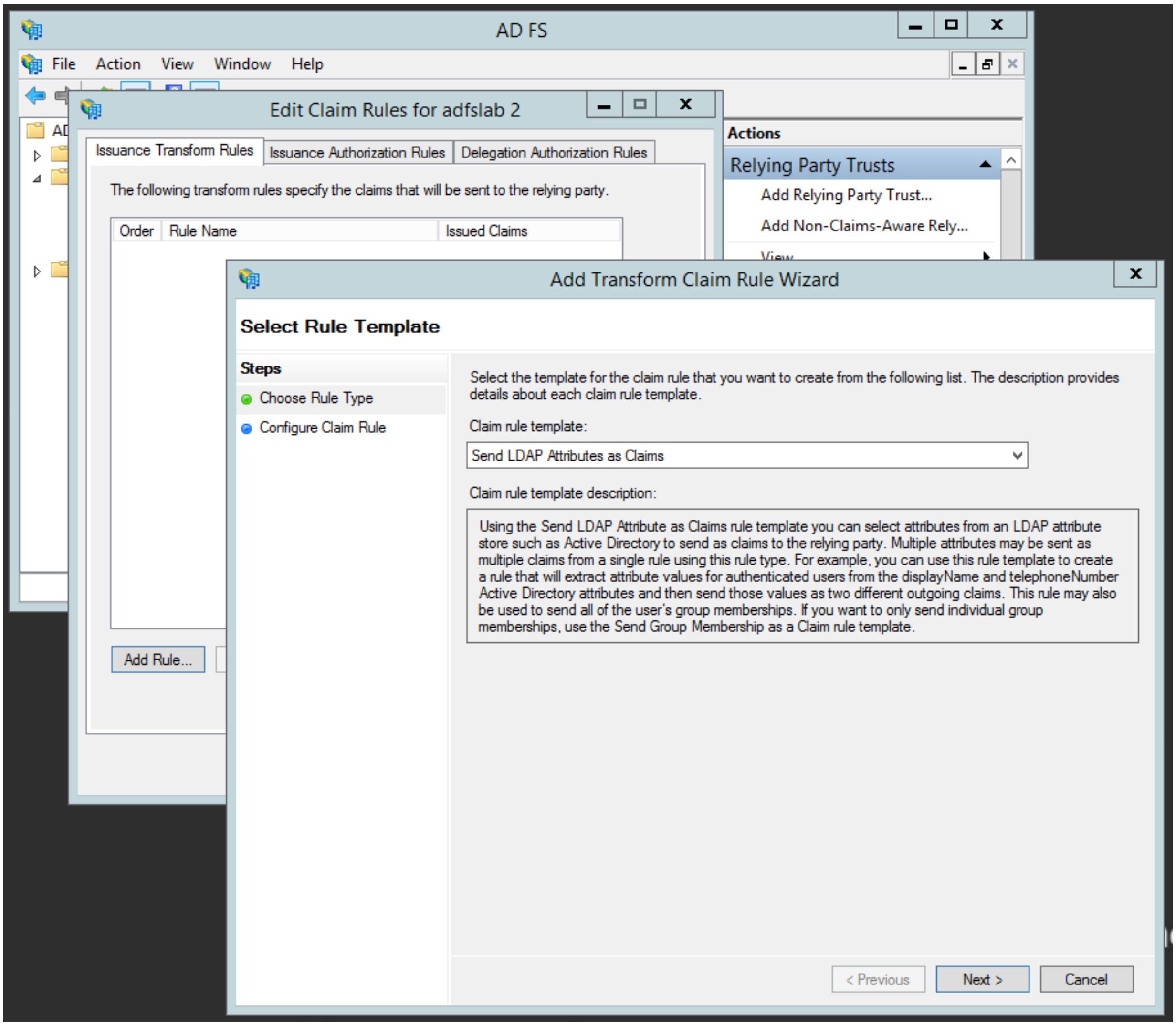
It would make sense to create a claim rule to map the incoming claim "sAMAccountname" to outgoing claim type "NameID", via "Send LDAP attribute as Claims" template.

For some reason, this does not work though. Apparently, "sAMAccountName" cannot be mapped directly to "NameID" in this step. The subject section in the SAML assertion will be empty, possibly due to an internal error in the AD FS server or with the claim rule templates. I still need to research this more.

The way to work around this is to send the LDAP attribute "sAMAccountName" to a dummy claim e.g. "Given Name" first, and then add a second rule to transform this "Given Name" claim to "NameID".

To do so, follow these steps:

In the Edit Claim Rules dialog for the Relying Party trust, click Add Rule... and select Send LDAP Attributes as claims:



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

Select Rule Template

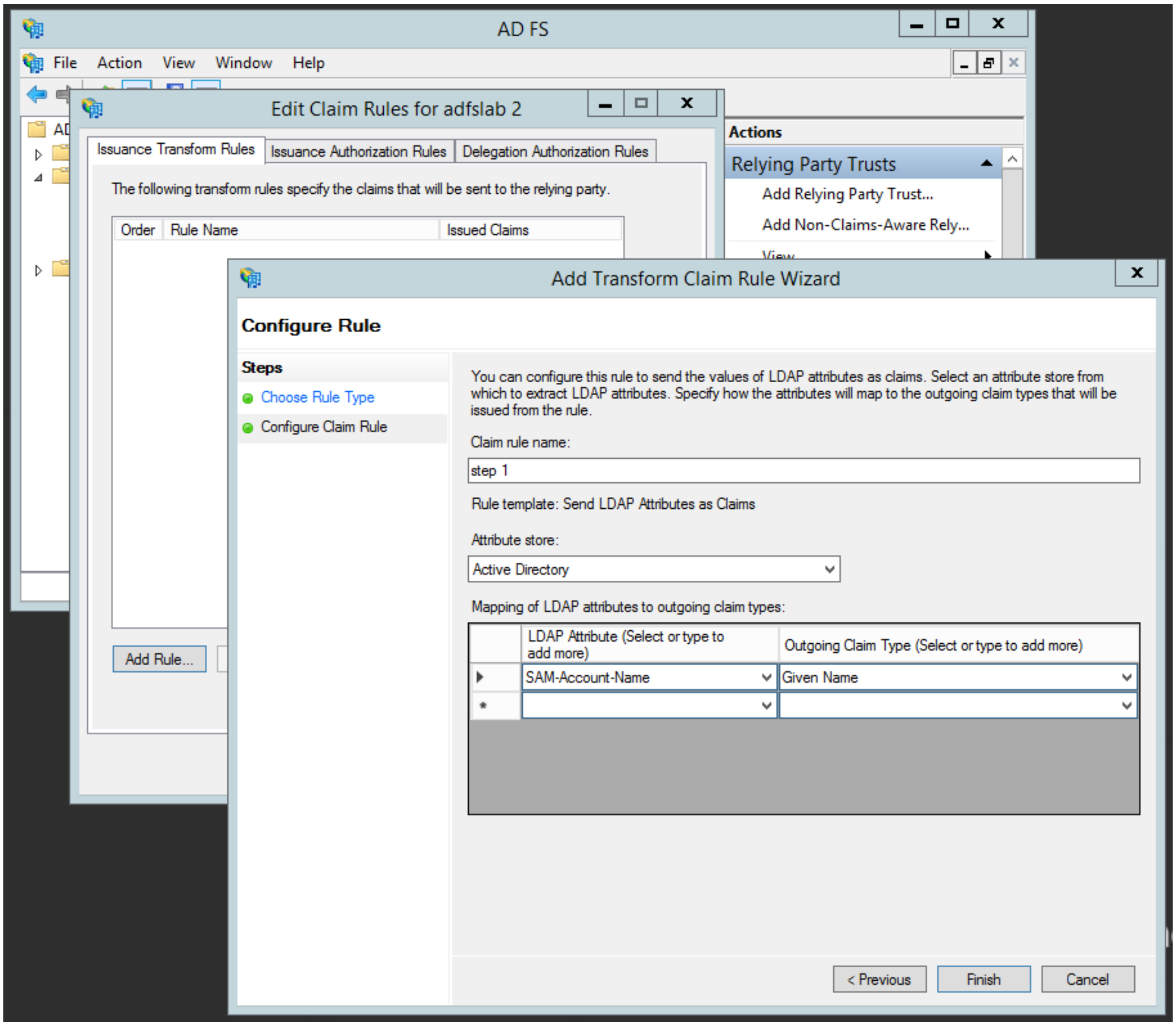
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

Enter a Claim rule name, select attribute store Active Directory, select LDAP Attribute "SAM-Account-Name" and Outgoing Claim Type "Given Name".



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

Configure Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: step 1

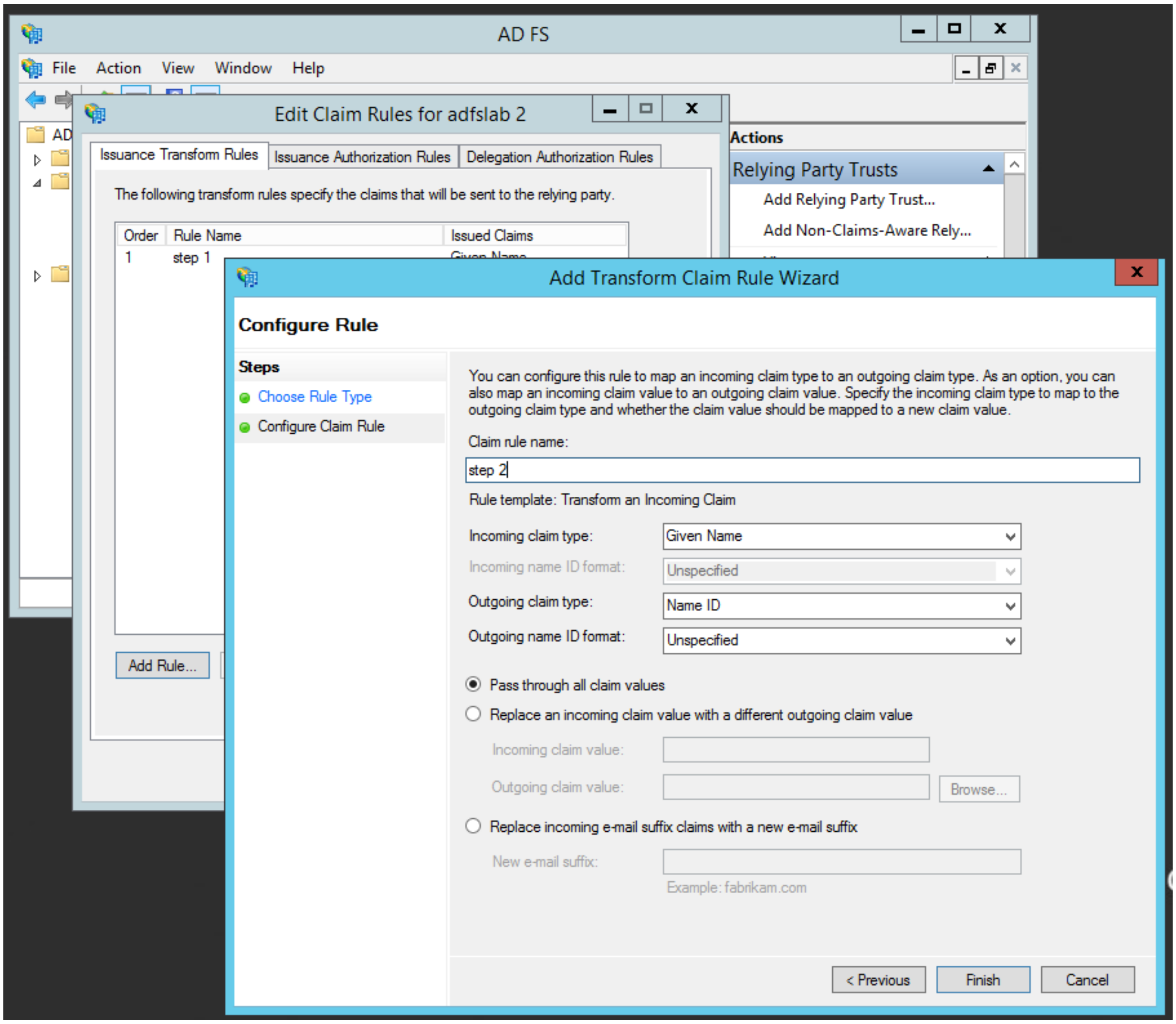
Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	SAM-Account-Name	Given Name
*		

Add a second Rule, select Claim rule template "Transform an Incoming Claim". Select Incoming claim type: Given Name, Outgoing claim type: Name ID, Outgoing name ID format: Unspecified, Pass through all claim values.


AD FS
File
Action
View
Window
Help
AD
Edit Claim Rules for adfslab 2
Issuance Transform Rules
Issuance Authorization Rules
Delegation Authorization Rules
Actions
Relying Party Trusts
Add Relying Party Trust...
Add Non-Claims-Aware Rely...
Add Rule...
Add Transform Claim Rule Wizard
< Previous
Finish
Cancel
Browse...

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

Order	Rule Name	Issued Claims
1	step 1	Given Name

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: step 2

Rule template: Transform an Incoming Claim

Incoming claim type: Given Name

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Unspecified

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

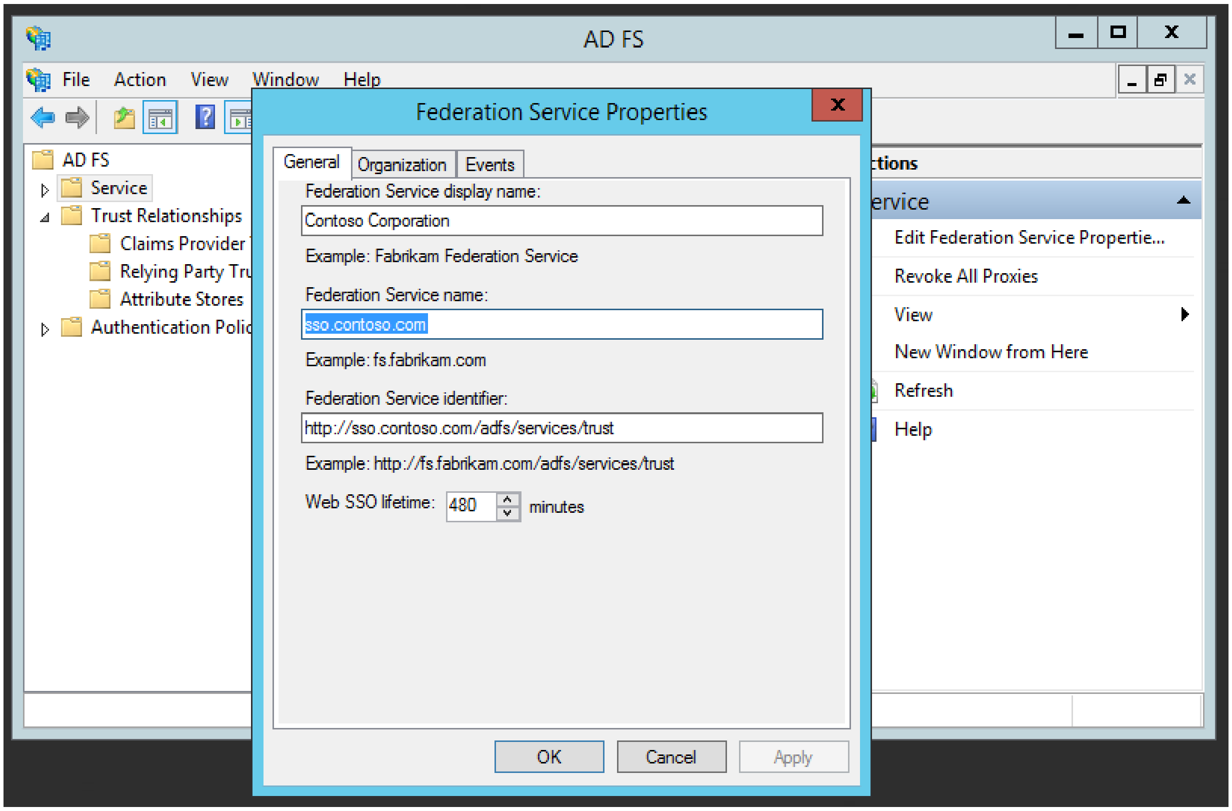
○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Logging in

Users login by navigating to the AD FS IdP initiated signin page which is hosted by AD FS under:
https://sso.contoso.com/adfs/ls/IdPInitiatedSignOn.aspx
Replace sso.contoso.com with the Federation Service name:



Federation Service Properties

Federation Service display name: Contoso Corporation

Example: Fabrikam Federation Service

Federation Service name: sso.contoso.com

Example: fs.fabrikam.com

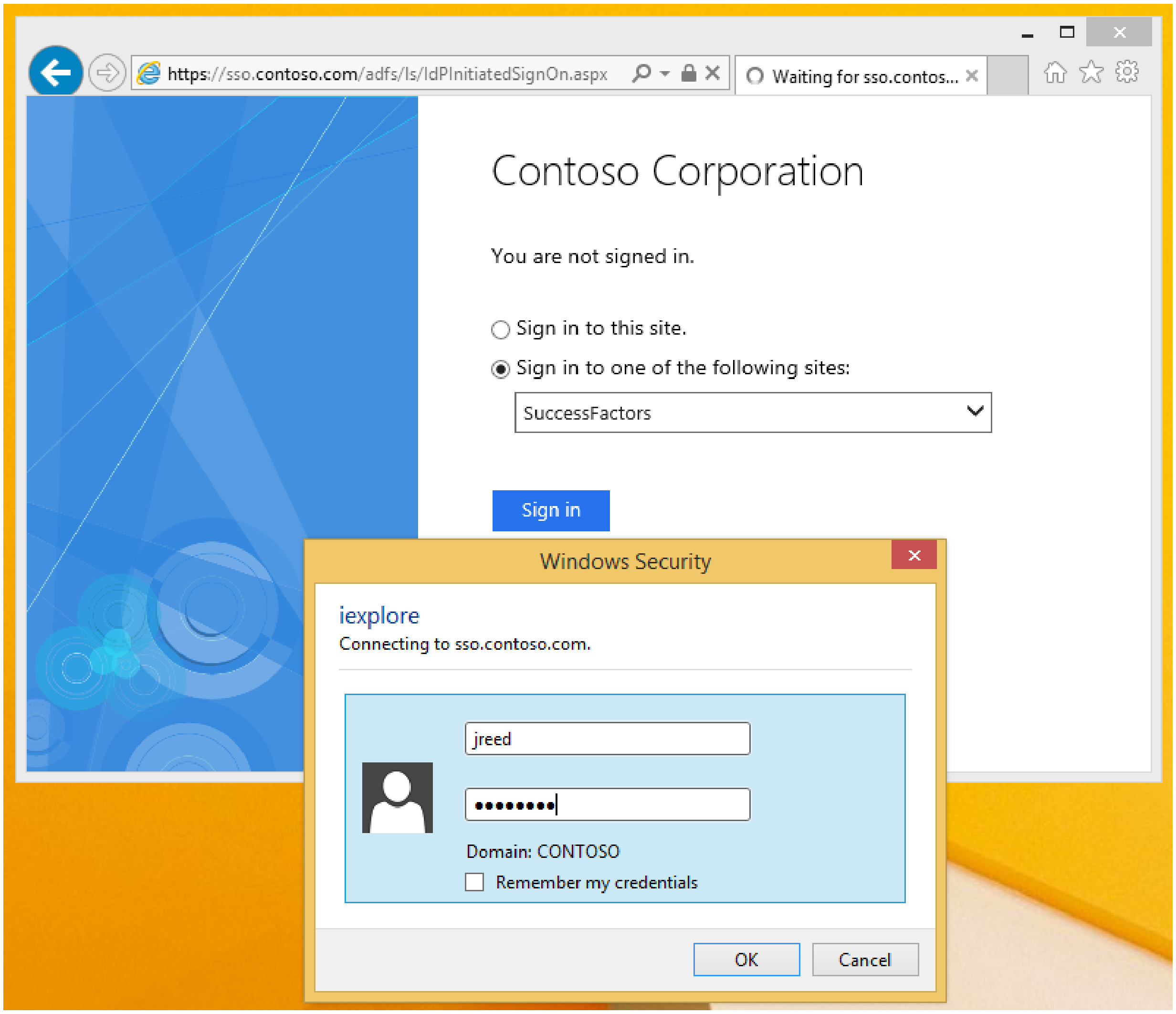
Federation Service identifier: http://sso.contoso.com/adfs/services/trust

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

Web SSO lifetime: 480 minutes

Make sure that DNS and network settings allow clients to connect to the AD FS server.

This is how the login looks like for the user:



https://sso.contoso.com/adfs/ls/IdPInitiatedSignOn.aspx

Waiting for sso.contos...

Contoso Corporation

You are not signed in.

○ Sign in to this site.

● Sign in to one of the following sites:

SuccessFactors

Windows Security

iexplore

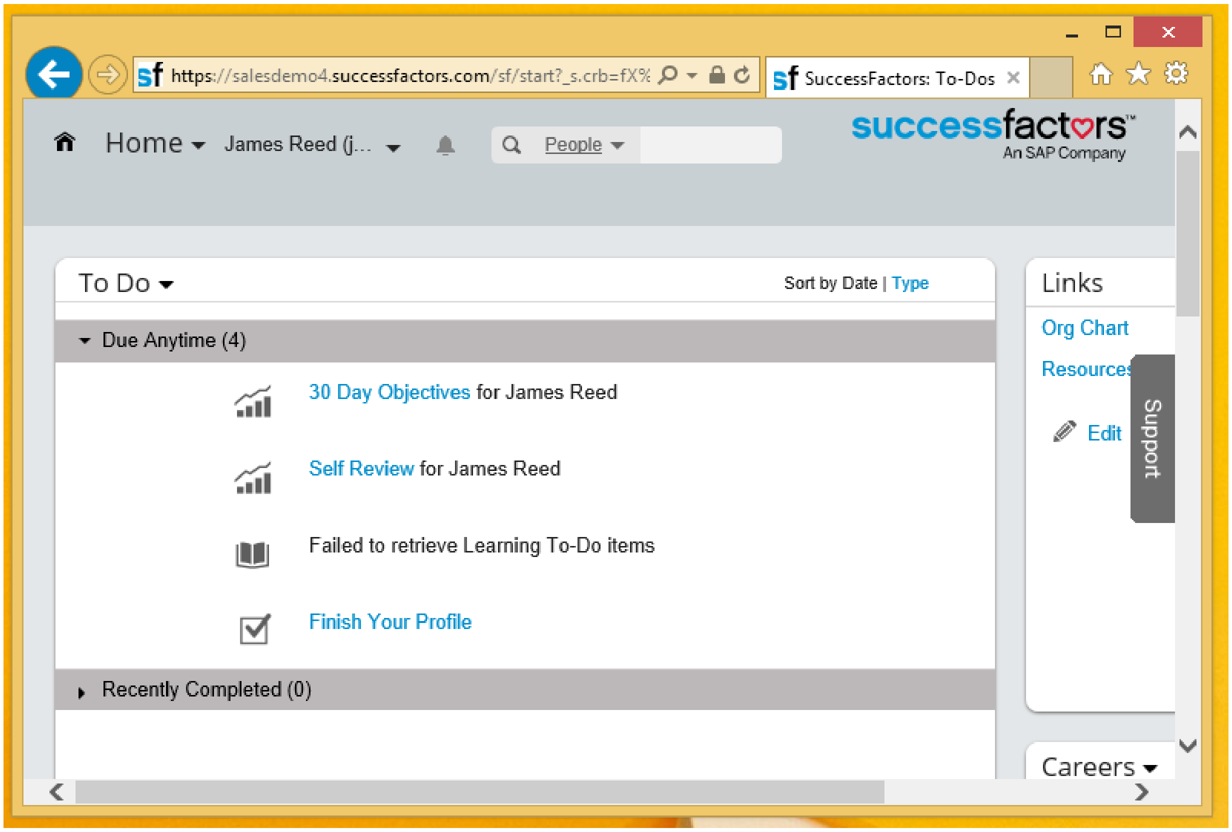
Connecting to sso.contoso.com.

jreed

••••••••

Domain: CONTOSO

□ Remember my credentials



To Do

Sort by Date | Type

Due Anytime (4)

30 Day Objectives for James Reed

Self Review for James Reed

Failed to retrieve Learning To-Do items

Finish Your Profile

Recently Completed (0)