

1. SSO - Admin Guide	2
1.1 Setting up Global SSO	2
1.1.1 Configuring IDP	2
1.1.1.1 ADFS configuration	2
1.1.1.1.1 Configuring ADFS for SSO	2
1.1.1.1.2 ADFS - Preparing certificate for SAML SSO Client	15
1.1.1.1.3 ADFS - configuring SAML sign-out	17
1.1.2 Step 1: Performing prerequisites check	19
1.1.3 Step 2: Preparing and configuring SAML SSO Client	19
1.1.4 Step 3: Installing and configuring Atlassian SSO add-ons	20
1.1.4.1 Configuring JIRA SSO add-on	21
1.1.4.2 Configuring Confluence SSO add-on	23
1.1.4.3 Configuring Bamboo SSO add-on	25
1.1.4.4 Configuring Bitbucket SSO add-on	27
1.1.4.5 Configuring FishEye SSO add-on	27

# SSO - Admin Guide

The content is intended for IDP Admins, Atlassian System Admins, thus we are assuming that the audience has sufficient and relevant technical knowledge.

The following pages describe how to prepare IDP, set up and configure Global SSO:

- [Setting up Global SSO](#)
  - [Configuring IDP](#)
    - [ADFS configuration](#)
  - [Step 1: Performing prerequisites check](#)
  - [Step 2: Preparing and configuring SAML SSO Client](#)
  - [Step 3: Installing and configuring Atlassian SSO add-ons](#)
    - [Configuring JIRA SSO add-on](#)
    - [Configuring Confluence SSO add-on](#)
    - [Configuring Bamboo SSO add-on](#)
    - [Configuring Bitbucket SSO add-on](#)
    - [Configuring FishEye SSO add-on](#)
- [Upgrading Atlassian tools that have Global SSO](#)

## Setting up Global SSO

To set up cPrime's Global SSO, perform the following operations:

1. [Configure IDP](#)
2. [Step 1: Perform prerequisites check](#)
3. [Step 2: Prepare and configure SAML SSO Client](#)
4. [Step 3: Install and enable the Atlassian authenticators](#)

## Configuring IDP

Depending on how your IDP is set up, the IDP Admin should work on one of the following IDP configurations in order to work with cPrime Global SSO:

- [ADFS configuration](#)
- [OneLogin configuration](#)
- [Centrify configuration](#)

We will use ADFS as an example to explain how to configure ADFS to work with Global SSO.

### ADFS configuration

If you have ADFS IDP, here is additional information for ADFS configuration:

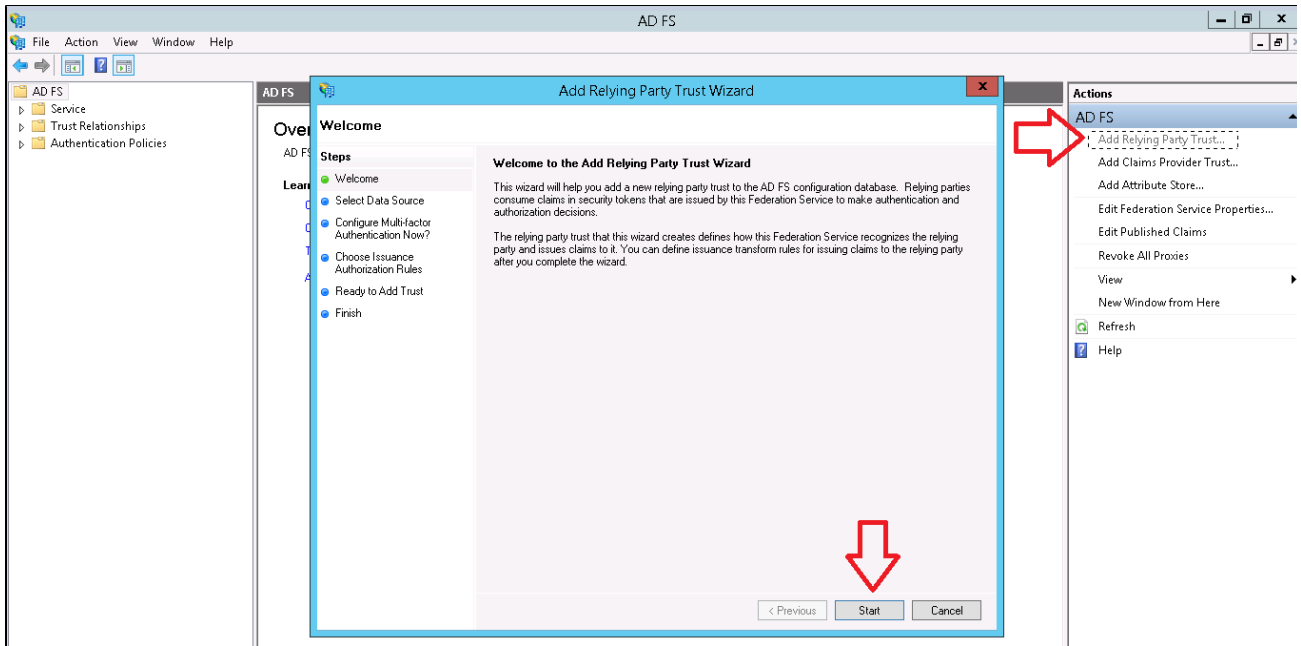
1. [Configuring ADFS for SSO](#)
2. [ADFS - Preparing certificate for SAML SSO Client](#)
3. [ADFS - configuring SAML sign-out](#)

After you are done with ADFS configuration, proceed with [Step 1 for SSO setup - prerequisites check](#).

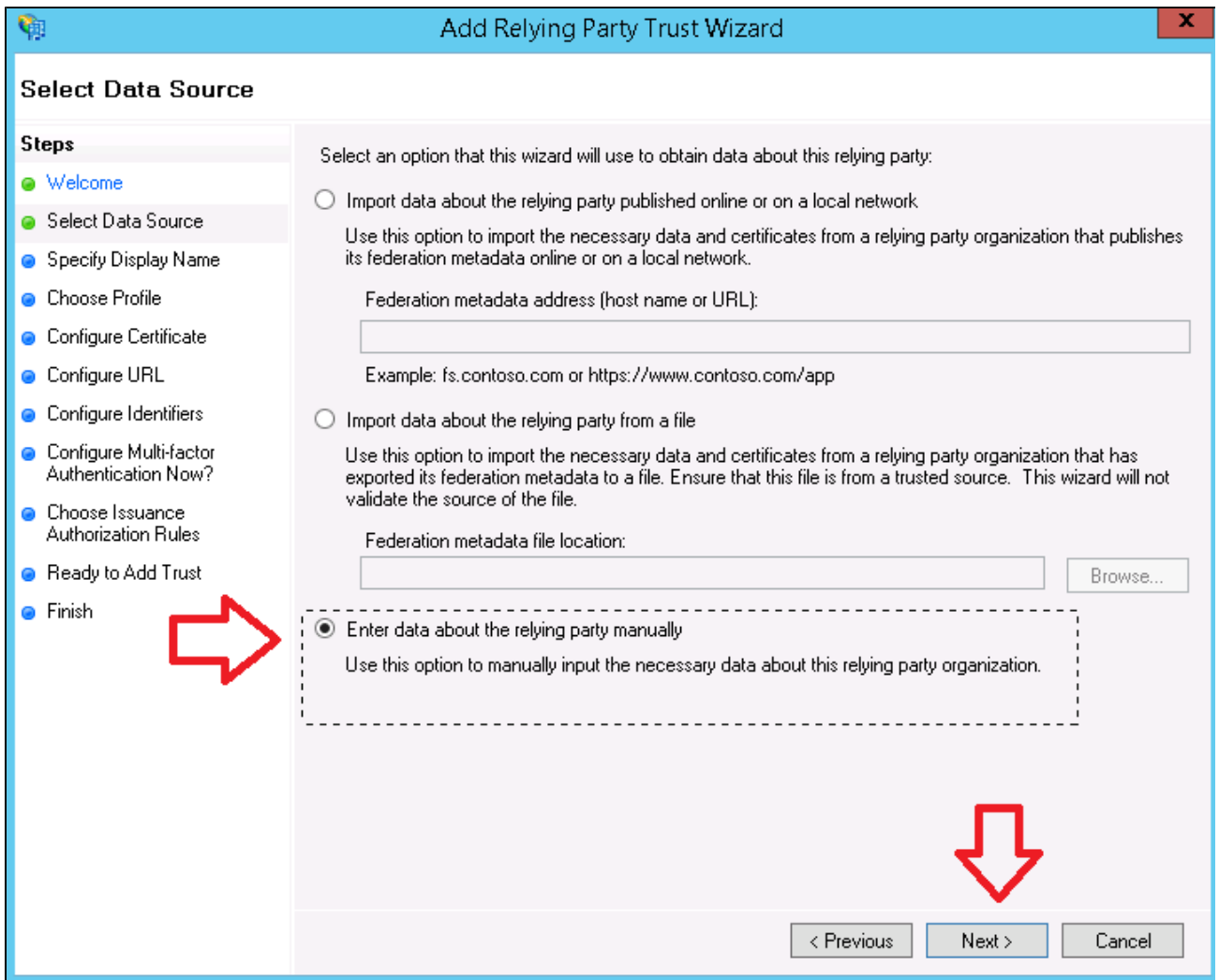
### Configuring ADFS for SSO

On Your AD FS Server, perform the following operations:

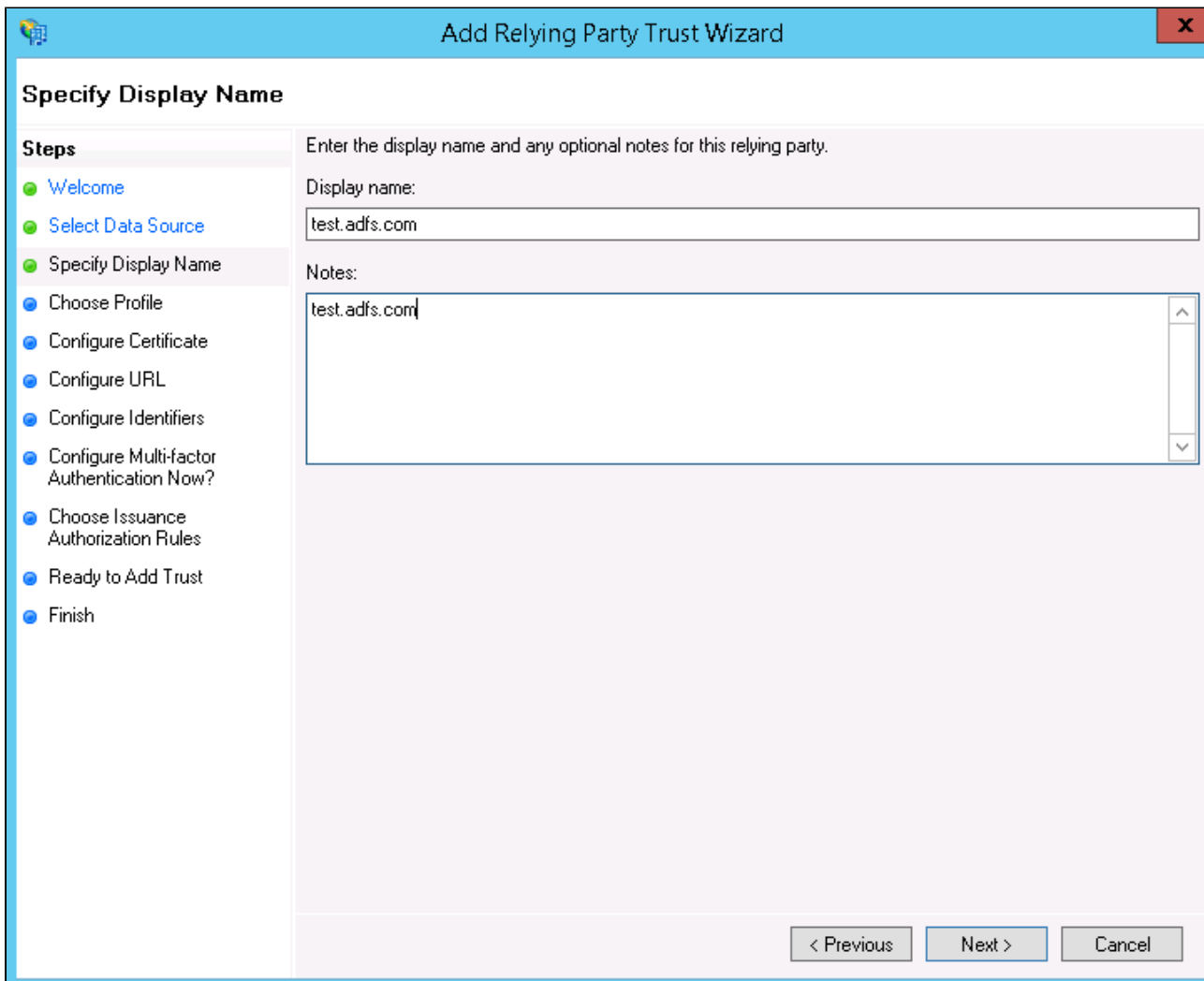
1. Open the AD FS Management console.
2. In the Actions pane, click **Add Relying Party Trust**.
3. On the wizard introduction page, click **Start**.



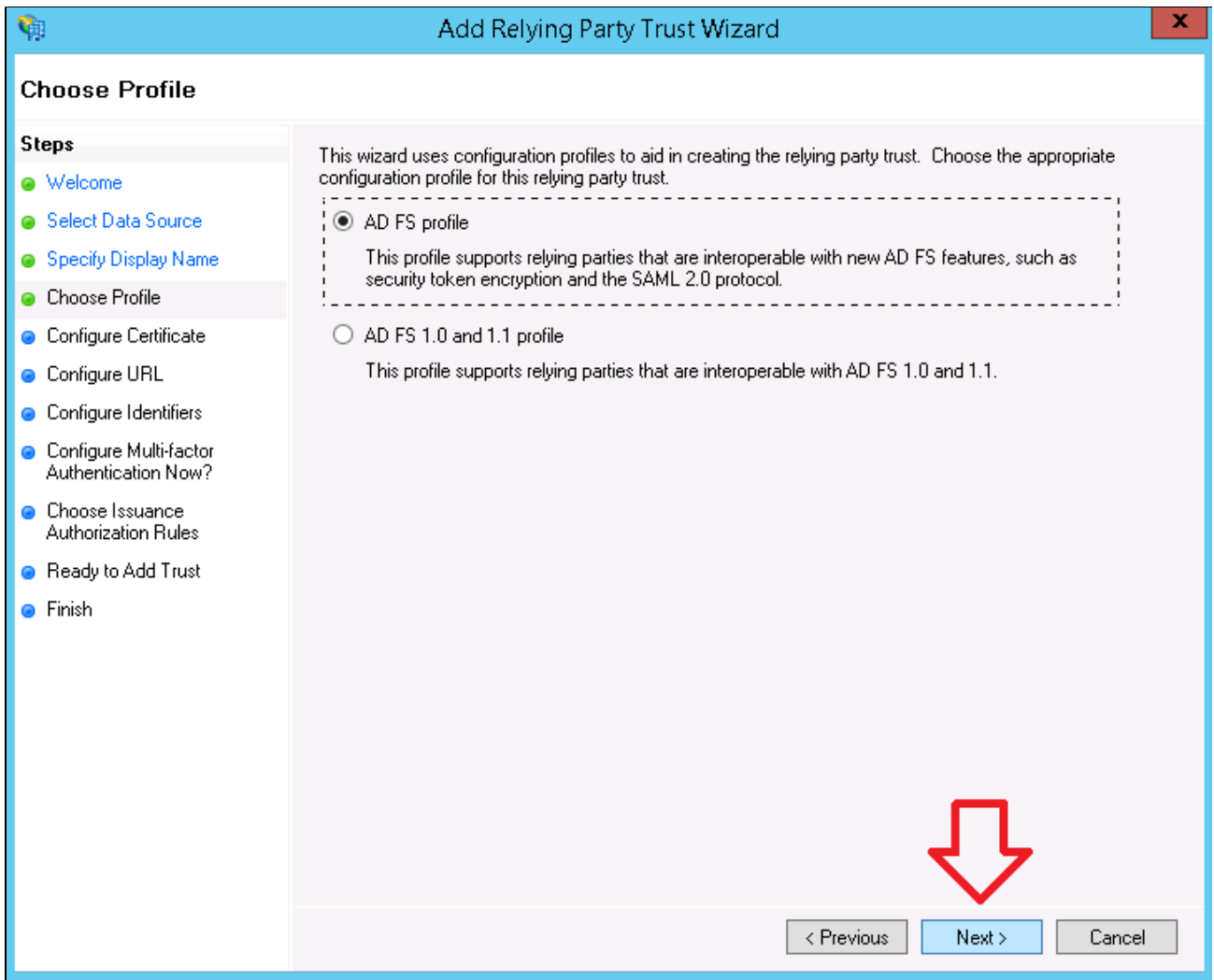
4. Select **Enter data about the relying party manually** and click **Next**.



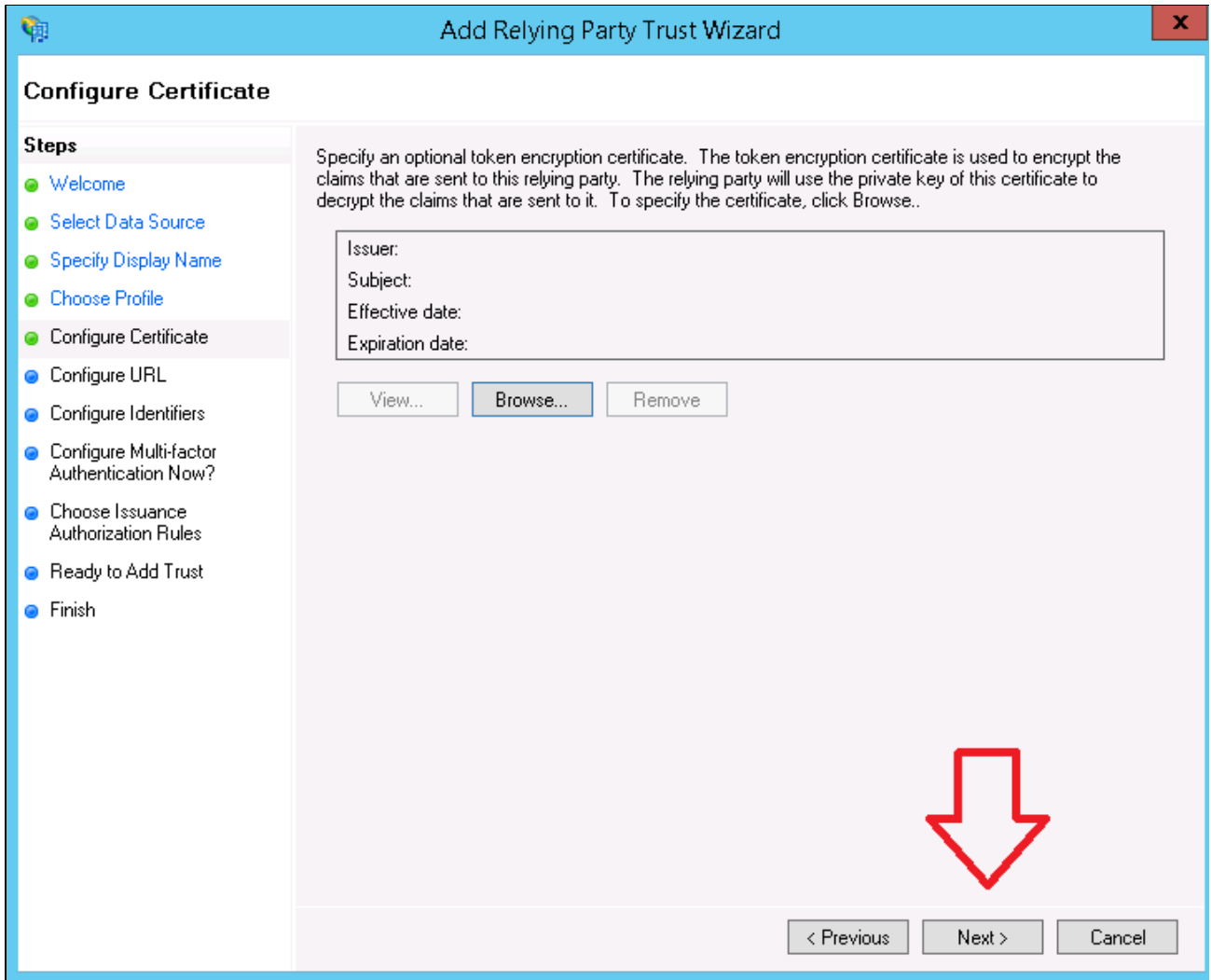
5. Fill in the **Display name** field and click **Next**.



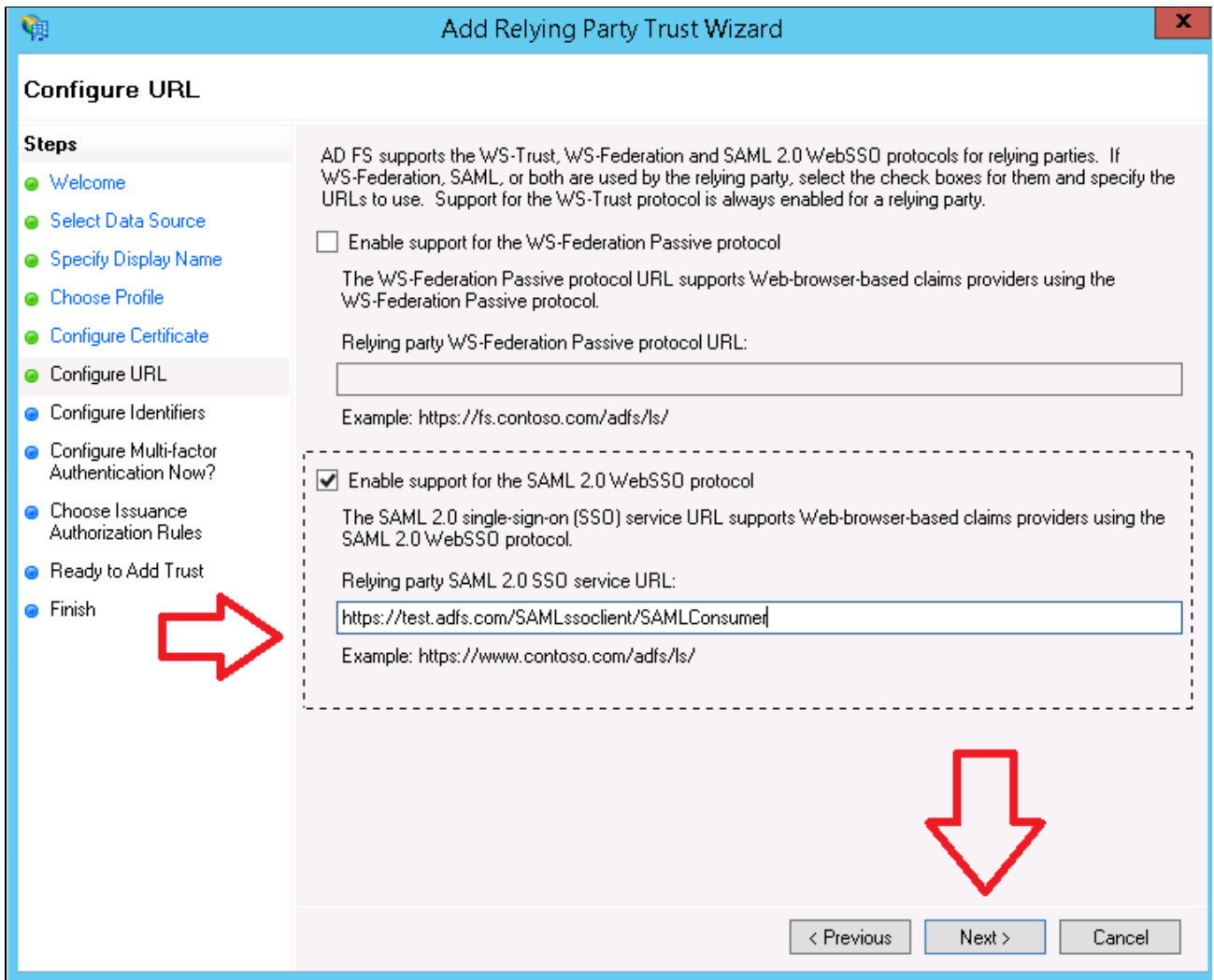
6. Select the **AD FS profile** option and click **Next**.



7. You will not need a token encryption certificate, so click **Next** to continue.



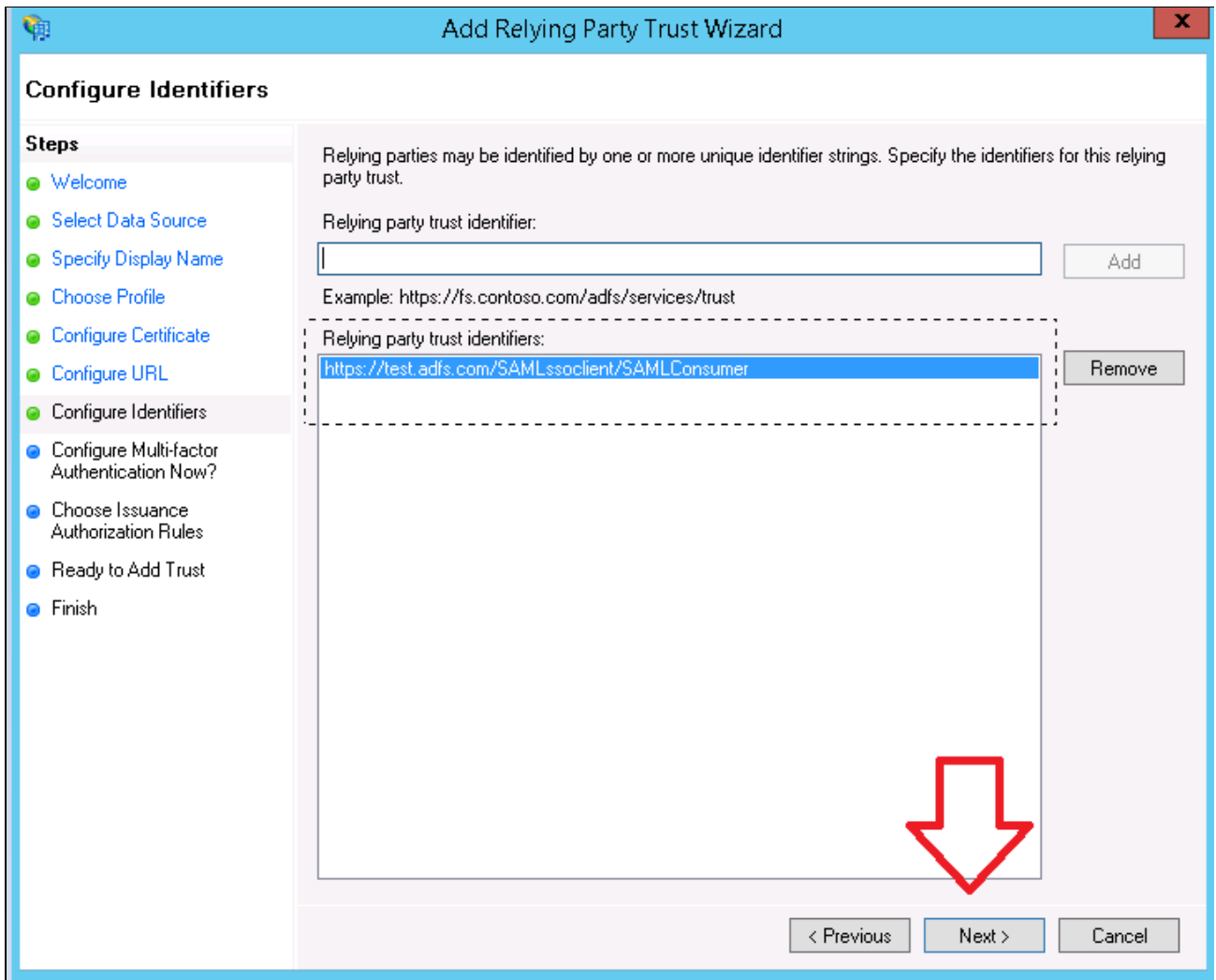
8. Select **Enable support for the SAML 2.0 WebSSO protocol**, paste the URL of your SAML Consumer service, and click **Next**. Example: <https://test.adfs.com/SAMLssoclient/SAMLConsumer>.



9. In the **Relying party trust identifiers** field, enter the same URL (example: <https://test.adfs.com/SAMLssoclient/SAMLConsumer>).



Ensure that you include `https://` here, and that you omit a slash at the end of the URL. Otherwise the integration will not work.

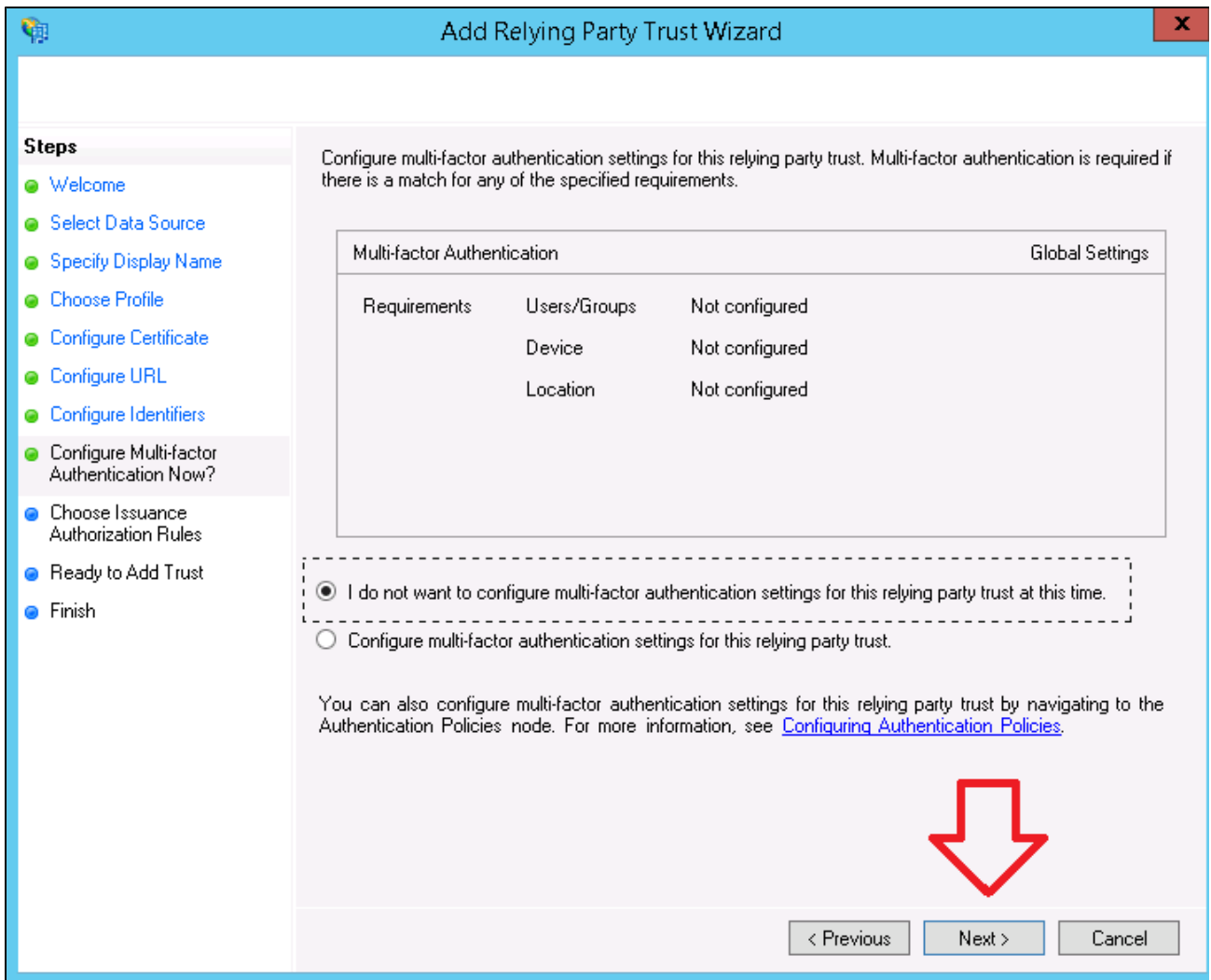


10. Select your desired multi-factor authentication option for users and click **Next**.

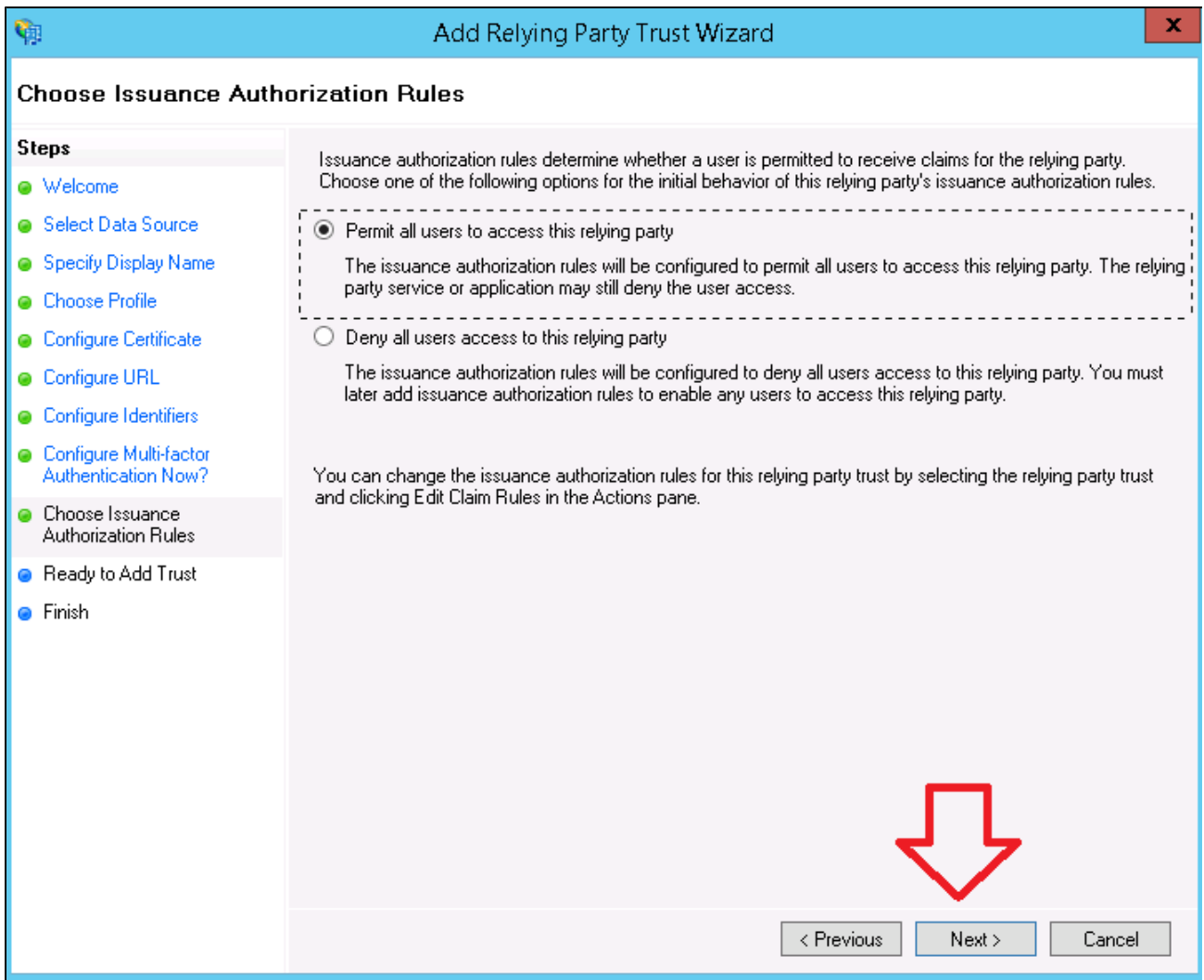


Enabling multi-factor authentication requires additional steps that are outside the scope of this guide.

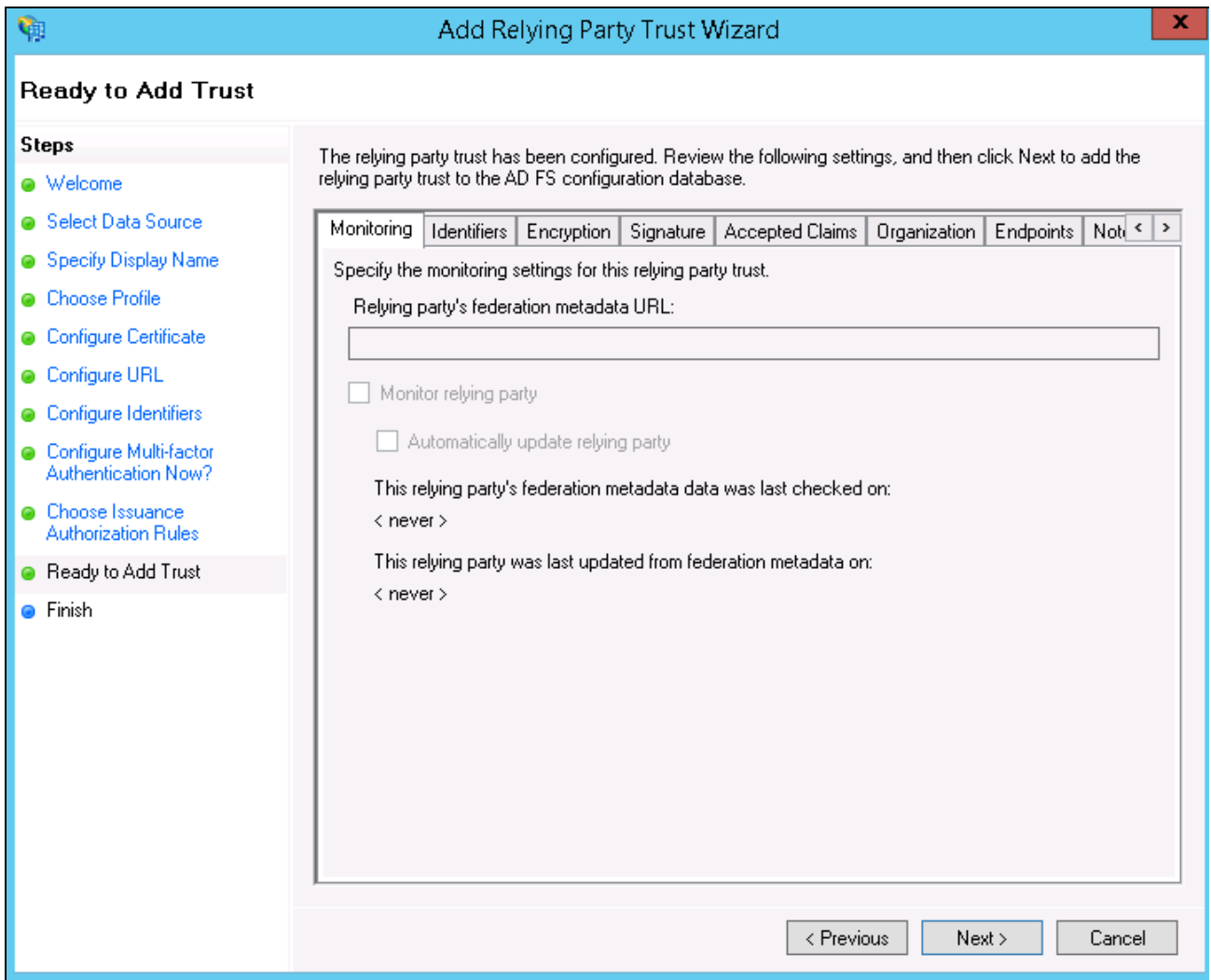




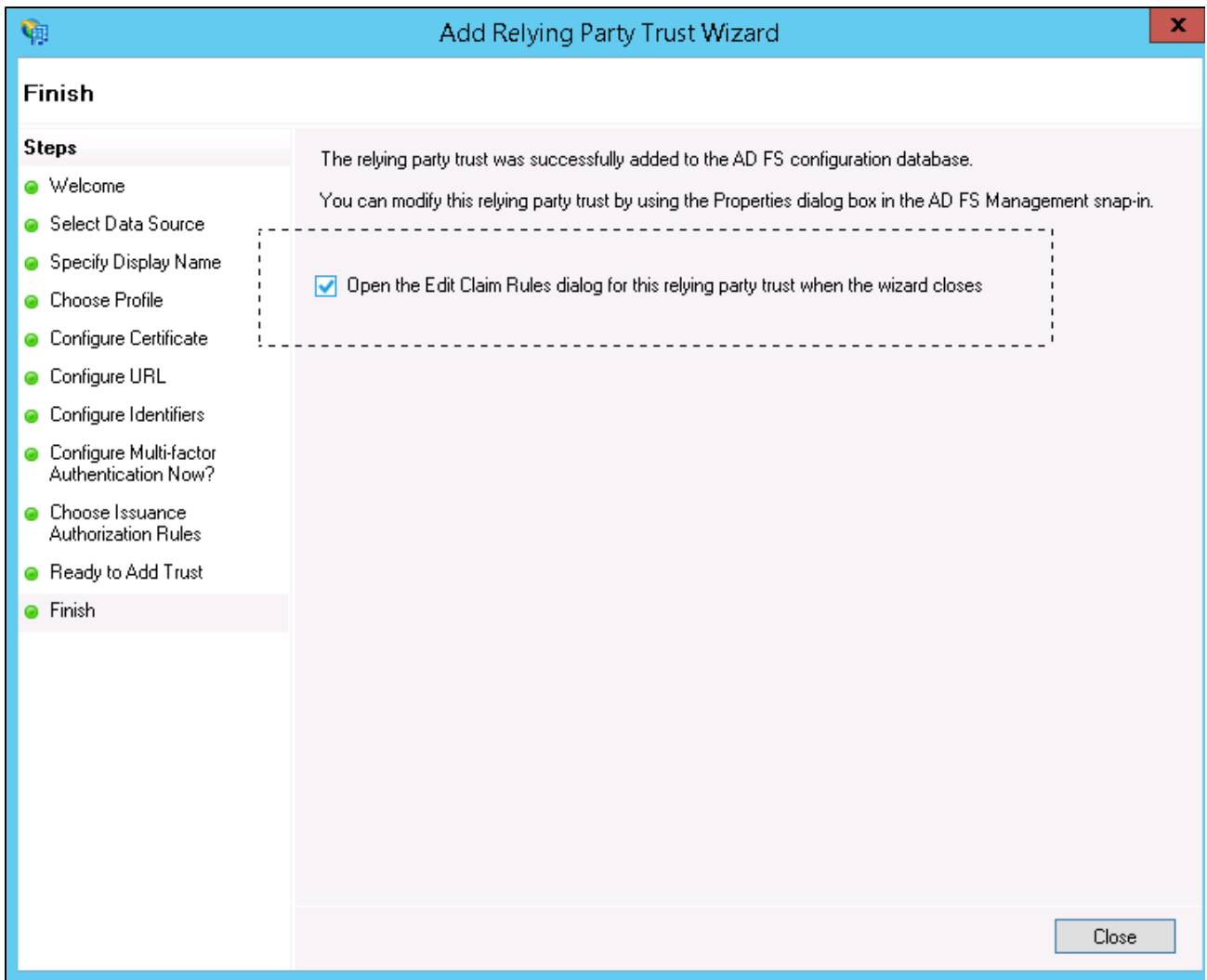
11. Select **Permit all users to access this relying party** and click **Next**.



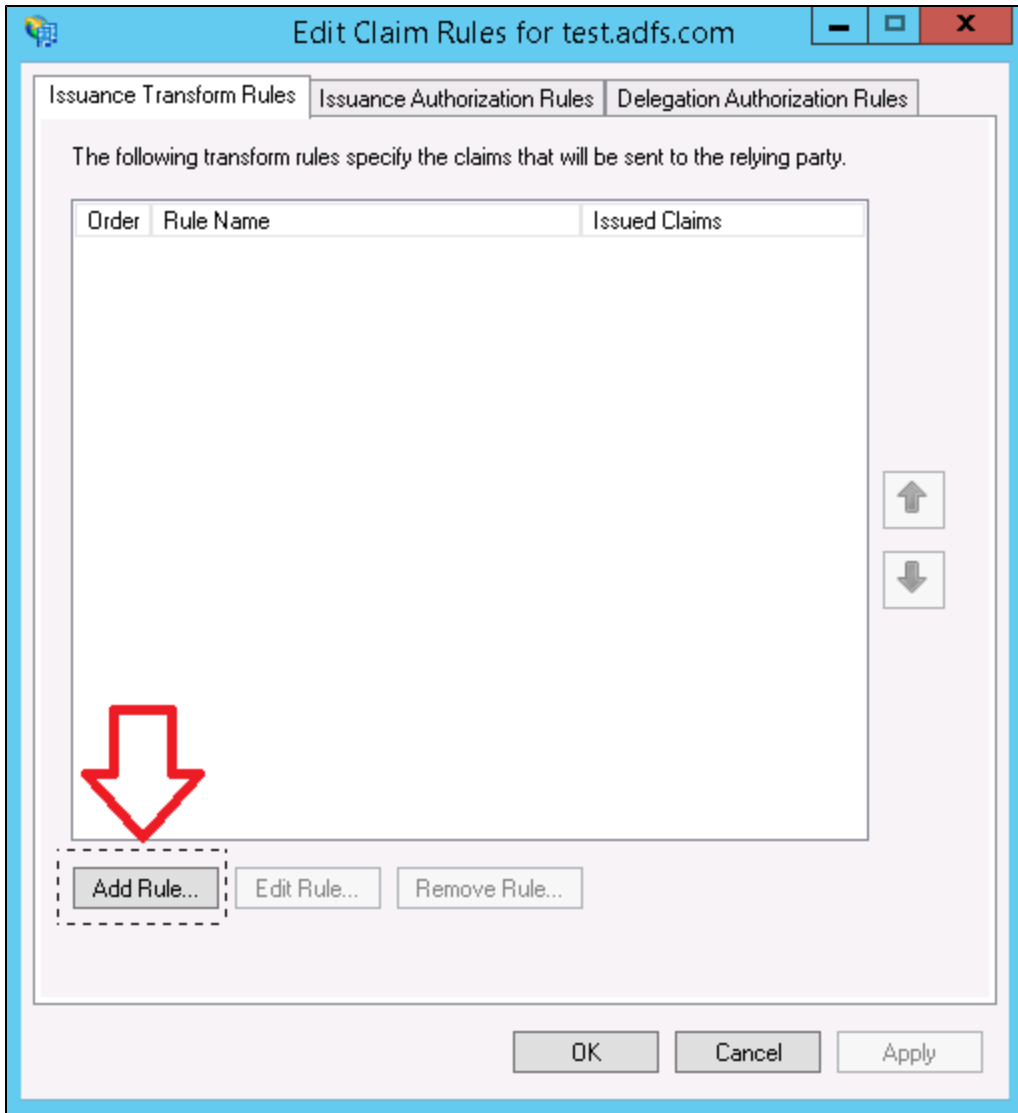
12. Review your settings and click **Next**.



13. To exit the wizard, click **Close**.



14. In the **Issuance Transform Rules** tab of the dialog, click **Add Rule**.



15. Configure the **Send LDAP Attributes as Claims** rule and click **Next**.

**Edit Rule - Username** ✕

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:

Rule template: Send LDAP Attributes as Claims

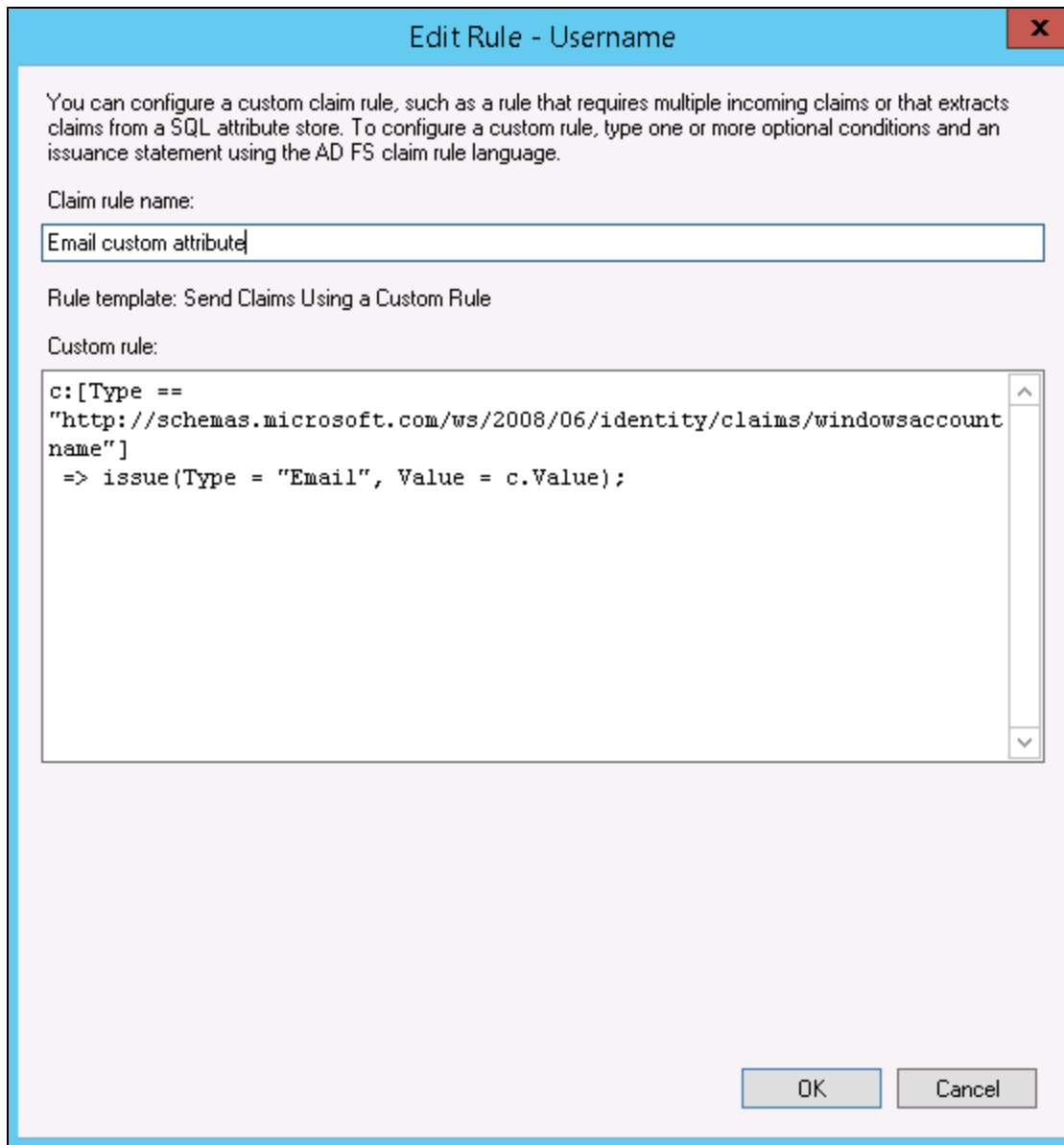
Attribute store:

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)
	Employee-ID	Name ID
▶*		

16. In this case we will send the "Email" attribute to our consumer, so click **Add Rule** again, select "Send Claims Using a Custom Rule", and put in the following rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccou
ntname"]
=> issue(Type = "Email", Value = c.Value);
```



After these steps, proceed with [configuring SAML sign-out](#).

## ADFS - Preparing certificate for SAML SSO Client

To prepare the certificate for SAML SSO Client, perform the following operations:

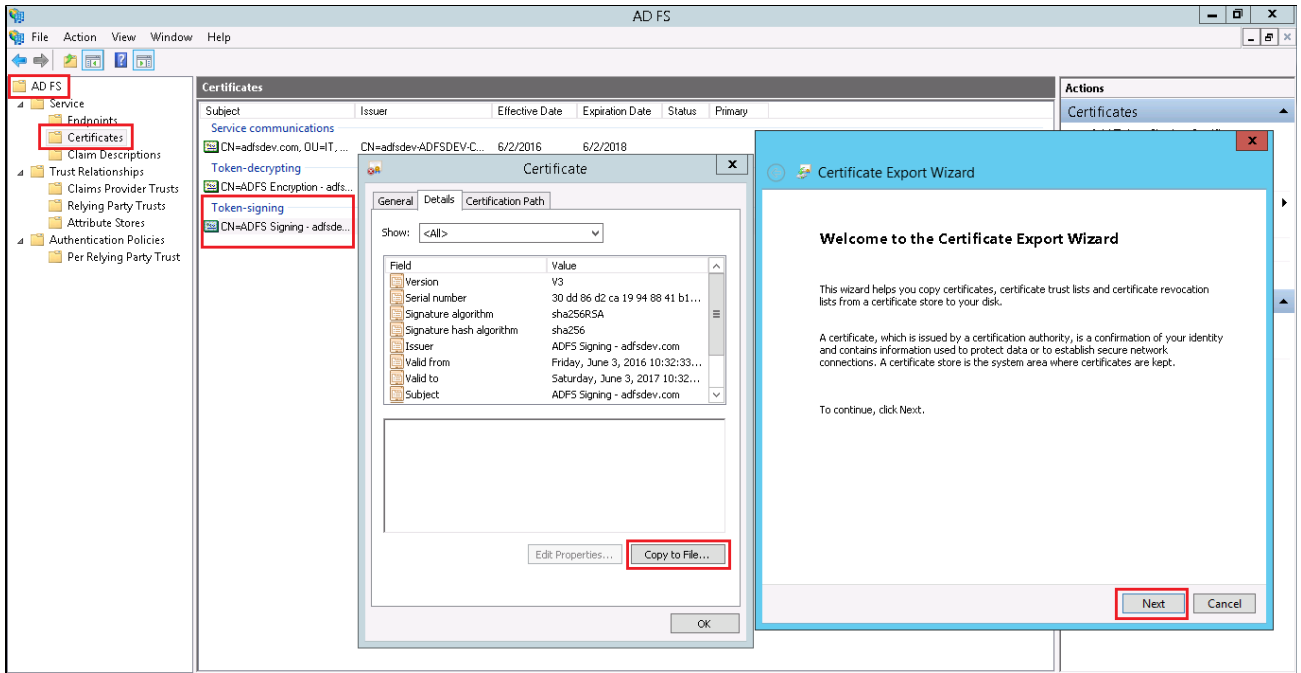
1. [Export the Token Signing Certificate](#)
2. [Convert this certificate for our SAML SSO Client](#)

### Exporting the Token Signing Certificate

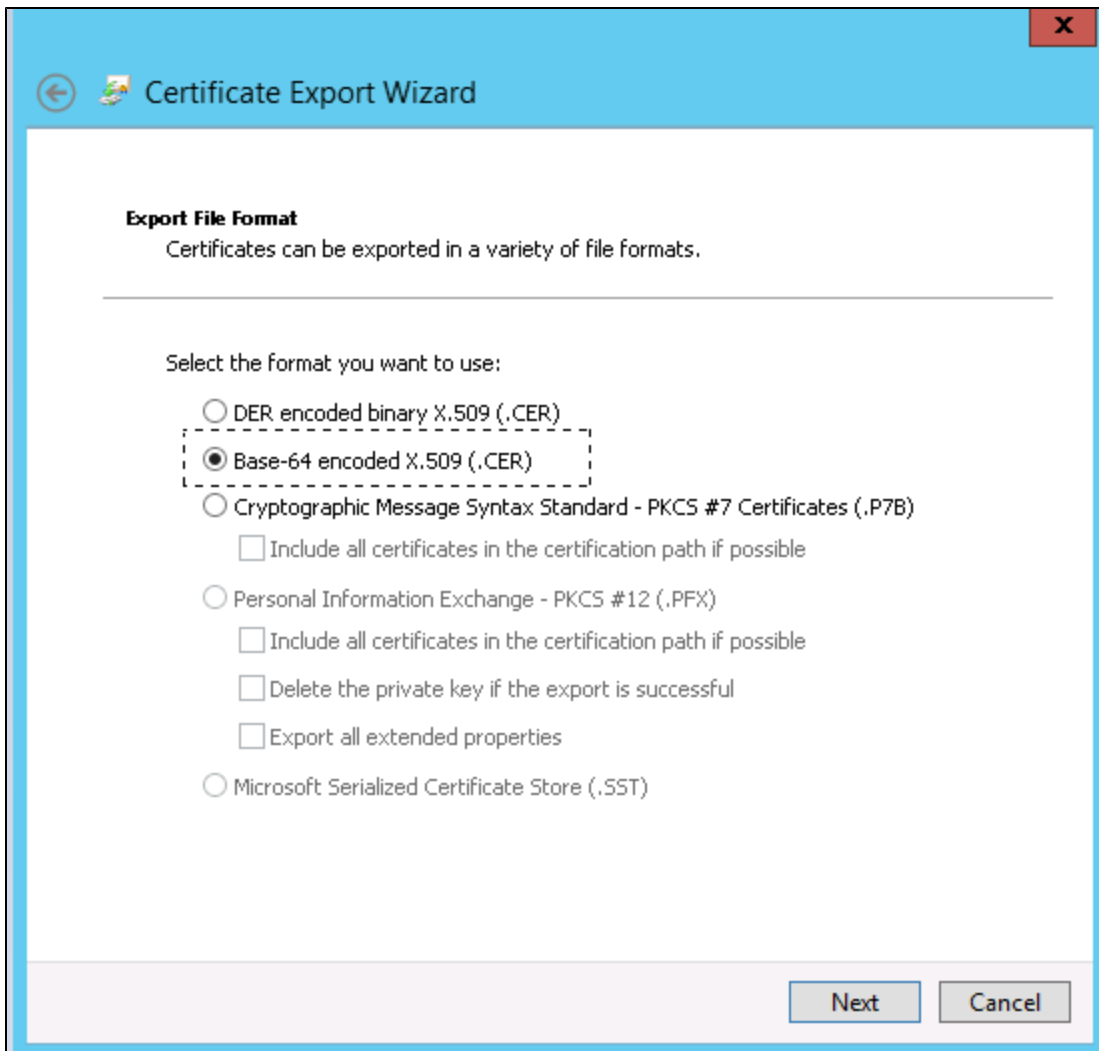
The Token Signing Certificate can be exported from the ADFS 2.0 Management, Services snap-in.

To export the Token Signing Certificate:

1. Go to ADFS Management.
2. Click **Services** to open the **Service Snap-in**.
3. In the **Services Snap-in**, click **Certificates**.
4. In **Token-signing** of the **Certificates** pane, select the Certificate and open it.
5. In the **Details** tab of the **Certificate** window, click **Copy to File**.
6. Click **Next**.



7. Select **Base-64 encoded X.509 (.CER)**, click **Next**, and save it.





## Converting the certificate for our SAML SSO Client

After these steps, convert this certificate for our SAML SSO Client. There are two ways to implement it:

### 1. Executing Linux command for converting

```
openssl enc -base64 -A -in Example.cer -out finalBase64.ser
```

### 2. Using a link

Use the following link for converting: <http://www.mobilefish.com/services/base64/base64.php>.

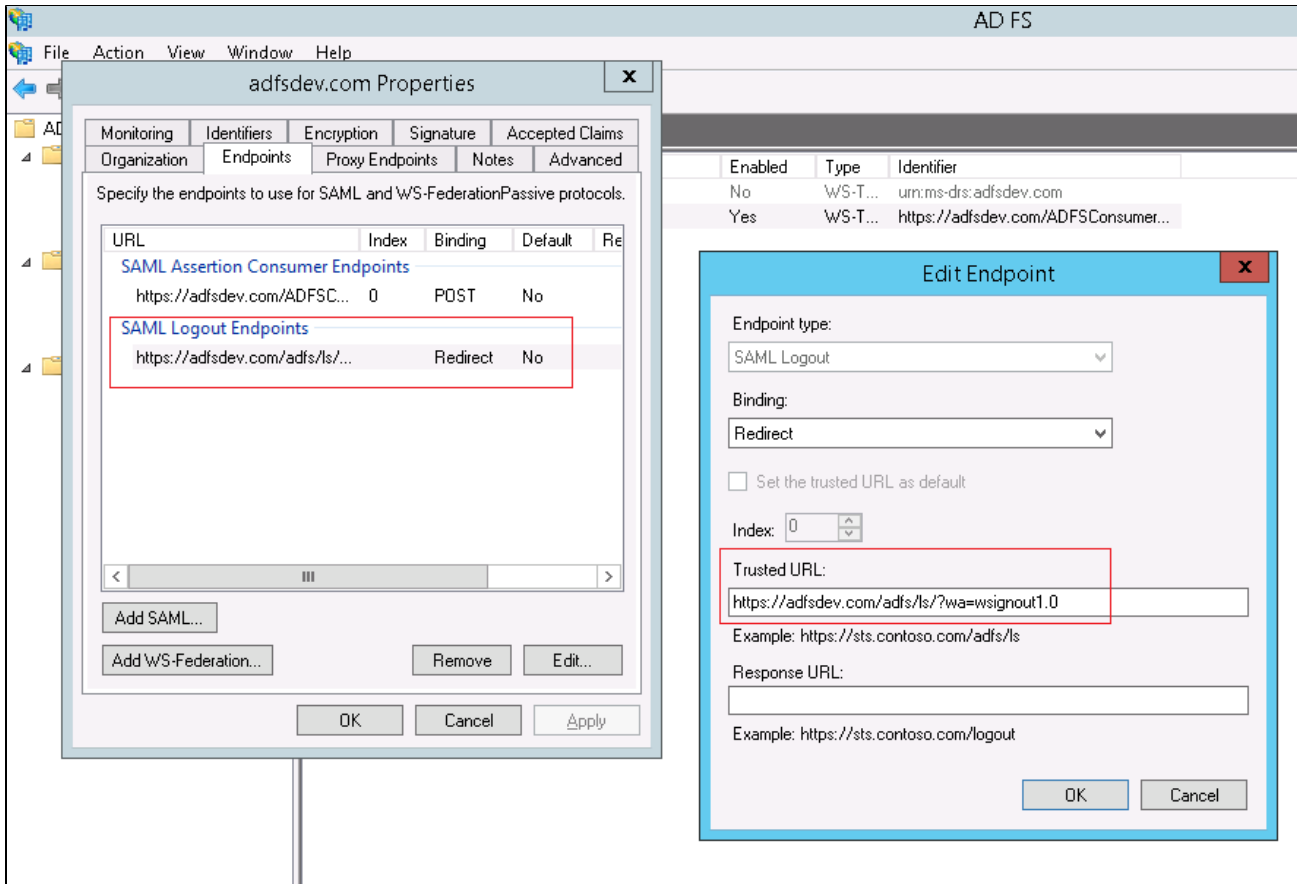
The screenshot shows a web browser window with the URL [www.mobilefish.com/services/base64/base64.php](http://www.mobilefish.com/services/base64/base64.php). The page features a sidebar on the left with various utility links such as 'vCard generator', 'European clothing standard EN 13402 pictogram generator', 'Favicon generator', 'File checksum calculator', 'Find the BIC numbers for Dutch IBAN numbers', 'Free game sound effects', 'Free game textures', 'Free online practice exams', 'Free online SEPA XML validation', 'Generate Dutch bank account numbers and Dutch citizen service numbers', 'Google toolbar custom button code generator', 'Google maps (API v2) code generator', 'Google map distance calculator', 'Hide email address', 'HTML escape and unescape tool', 'Hieroglyphs generator', and 'IBAN checker'. The main content area is titled 'Input base64 encoder and decoder:' and contains a large text input field for 'Enter source data \*'. Below this is a file upload section with a button 'Выберите файл' and a file name 'base64.cer'. The 'Conversion method \*' dropdown is set to 'Encode to Base64 string'. The 'Output to file' dropdown is set to 'Output to file'. The 'Max characters per line \*' is set to '999'. A CAPTCHA 'YxN' is displayed, and a text input field for the CAPTCHA is shown. The 'Convert' and 'Clear' buttons are at the bottom.

## ADFS - configuring SAML sign-out

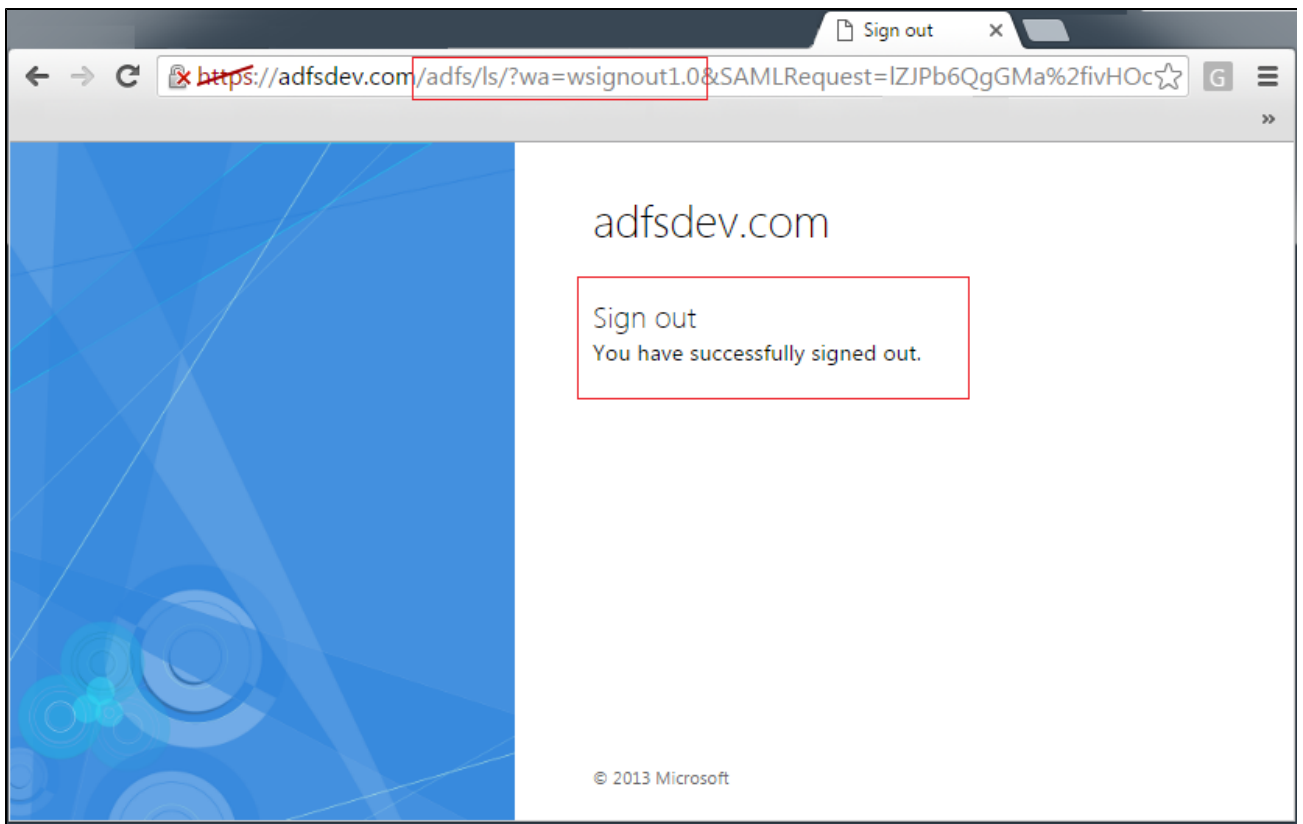
Inside your SaaS SSO configuration, define a sign-out URL.  
Example: <https://test-ads.com/ads/ls/?wa=wsignout1.0>.

1. On the ADFS side, go to **RP trust** for your app.
2. Configure a SAML logout endpoint.

Example:



When configured, a proper logout will look like this:



After you are done with ADFS configuration, proceed with [step 1 for SSO setup](#).

## Step 1: Performing prerequisites check

### Prerequisites before setting up Global SSO

1. For Global SSO, the Atlassian products [must be accessible via HTTPS only](#).
2. SSO should only accept HTTPS SAML URL's.
3. IDP should support SAML 2.0 Assertions.
4. Global SSO works on the server implementations only.
5. We will need to have a signing certificate from IDP and will need to convert it to a Base64 encrypted string in preparation for our SAML SSO Client configuration.

After you are done with the prerequisites, proceed with [SAML SSO Client configuration](#).

## Step 2: Preparing and configuring SAML SSO Client

To prepare and configure SAML SSO Client, perform the following operations:

1. [Generate a public/private key pair](#)
2. [Convert the certificate from IDP to base64 string](#)
3. [Configure SAML SSO Client](#)
4. [Configure logout for the Atlassian applications](#)

### 1. Generating a public/private key pair

To generate a public/private key pair, execute the following commands in the Linux console:

1. `openssl genrsa -out mykey.pem 2048`
2. `openssl pkcs8 -topk8 -inform PEM -outform PEM -in mykey.pem -out private_key.pem -nocrypt`
3. `openssl rsa -in mykey.pem -pubout -outform DER -out public_key.der`

### 2. Converting the certificate from IDP to base64 string

**WARNING!** In openssl, the base64 line length is limited to 76 characters by default. To be able to decode a base64 line without a line feed that exceeds the 76 characters, use `-A` option:

```
openssl enc -base64 -A -in Example.cer -out finalBase64.ser  
and put this certificate in the ./SAMLssoclient/WEB-INF/classes/ directory
```

### 3. Configuring SAML SSO Client

1. Deploy the **SAMLssoclient.war** directly to a new Tomcat instance or to any Atlassian application.
2. [Configure IDP](#).
3. Configure SAML SSO Client by using one of the following options:
  - a. Using SAML SSO Client Admin page: <https://yourdomain.com/SAMLssoclient/SsoUpdate>
  - b. Manually, by using a config file on your server: **./SAMLssoclient/WEB-INF/classes/config.properties**

### config.properties

```
unauthorizedPage=403.html
EncryptionPrivateKey=..\path_to_your\private_key.pem
assertionConsumerServiceUrl=http\://domain.com/SAMLConsumer/SAML
Consumer
errorPage=error.html
idpServerUrl=https\://domain.com/idpinitiatedsignon
NameAttribute=Email
certificate=converted_certificate.ser
cookiePath=/
loggingLevel=DEBUG
cookieDomain=domain.com
```

#### Where:

Name (admin page)	Attribute(config.properties)	Description
—	unauthorizedPage	User failed validation page for redirecting
Private key	EncryptionPrivateKey	Full path to our private key for encryption
Assertion Consumer Service URL	assertionConsumerServiceUrl	Link to our SAML SSO Client page
Name Attribute	NameAttribute	Attribute name which we use for username encoding and then put to an SSO cookie
Certificate	certificate	Put your converted certificate to a folder, for example " <b>..\Tomcat 8.0\webapps\SAMLssoclient\WEB-INF\classes\</b> ", and enter the name of this certificate here.
—	errorPage	SAML error page for redirecting.
—	cookiePath	URL path for saving the SSO cookie
Log Level	loggingLevel	The logging level can be DEBUG, INFO, or ERROR
Cookie Domain	cookieDomain	Your server's domain
IDP Server URL	idpServerUrl	Link to your IDP
Issuer Application URL	issuerUrl	Issuer Application URL
Default target service	default.target.service	Default target service

## 4. Configuring logout for the Atlassian applications

As a result, you can have one logout for all Atlassian applications:

To implement logout, set the cookiePath property ( `..\SAMLssoclient\WEB-INF\classes\config.properties` file):  
**cookiePath=**



Note that the same value for path property should be set in all SSO authenticators.

## Step 3: Installing and configuring Atlassian SSO add-ons

This step describes how to configure and enable the following Atlassian SSO add-ons:

- JIRA
- Confluence
- Bitbucket
- Bamboo
- FishEye

## Configuring JIRA SSO add-on

This article describes how to configure SSO authenticator for JIRA.

**WARNING!** If you entered wrong parameters, use a "back door" functionality in order to avoid cyclic redirects and to access application bypass SSO.

Just add a GET parameter `sso=off` to the needed URL. Example: <https://some.jira.com/?sso=off>.

To configure SSO for JIRA:

1. Install JIRA SSO add-on.

The screenshot shows the JIRA Add-Ons management interface. The top section is for the 'Authentication-Redirect-Filters' add-on, which is in a trial state. It includes a 'Buy now' button and a warning that the trial expires on 08/Jun/16. Below this, there are buttons for 'Buy now', 'Uninstall', and 'Disable'. The main content area displays the following details:

No screenshots available	Version: 1.0.0-SNAPSHOT	14 of 14 modules enabled
	Vendor: cPrime	
	Add-on key: com.cprime.labs.jira.Authentication-Redirect-Filters	
	License details: Evaluation, Unlimited-user testing license, Standard, expires 08/Jun/16	
	License status: Valid	
	License SEN: Unknown	
	License key: AAAClg00DA...	

Below the main details, there is a list of other installed add-ons:

- > Entity property conditions
- > Filter Deletion Warning Plugin
- > HipChat for JIRA UPDATE AVAILABLE Update
- > JIRA Feature Keys
- > Soy Function Plugin
- > Support Tools Plugin UPDATE AVAILABLE Update

At the bottom, there are links for 'Audit log', 'JIRA update check', 'Settings', and 'Enter safe mode'.

2. Go to **Administration > Add-Ons**.
3. In the **FILTERS** section, click **Global SSO**.  
The **Global SSO Configuration** page opens.
4. Fill in the fields on this page. The field description is provided in the [table below](#).

The screenshot shows the JIRA Administration interface for Global SSO Configuration. The left sidebar contains navigation links for Application Links, Behaviours, Builds, JIRA Agile, Issue Collectors, JIRA.AGNICIENT.COM, Monitoring, Admin Helper, and Filters. The main content area is titled 'Global SSO Configuration' and contains the following fields:

- Login URL:** `https://aag0677.my.centify.com/applogin/appKey/8980f085-4d24-48a7-a701-bb13c4e90b0f/customerId/AAG0677`
- Logout URL:** `https://aag0677.my.centify.com/applogout`
- Cookie Domain:** `.cprime.com`
- Time Expiry:** `14400`
- Path:** `/`
- Exclude paths:** `/applinks;/auth;/rest;/oauth;/rpc;/xml;LinkConfluencePage;ManageRating;LinkJiraIssue;AjaxIssueEditAction`
- Public Key:** `/var/atlassian/application-data/jira/public_key.der`
- Exclude IP addresses:** `107.170.234.49;127.0.0.1`

Buttons for 'Save' and 'Test SSO' are located at the bottom of the form.

**Field description for the Global SSO Configuration page**

Attribute	Description
Login URL	IDP Login Page Examples: <ul style="list-style-type: none"> <li><code>https://adfs-test.com/adfs/ls/idpinitiatedsignon</code></li> <li><code>https://aag0677.my.centify.com/applogin/appKey/8980f085-4d24-48a7-a701-bb13c4e90b0f/customerId/AAG0677</code></li> </ul>
Logout URL	IDP Logout Page Examples: <ul style="list-style-type: none"> <li><code>https://aag0677.my.centify.com/applogout</code></li> <li><code>https://adfs-test.com/adfs/ls/?wa=wsignout1.0</code></li> </ul>
Cookie Domain	Domain of your applications for SSO cookie
Path	Your application path. If you need to have one logout from all applications, enter "/" for this field.
Exclude paths	You can disable SSO from URLs which contain custom pieces of URL (semicolon separated values). Example: <b><code>/rest/usermanagement;/rest/api</code></b>  Another case is to open REST API for using.
Public Key	Full path to your public key file for decrypting the SSO username
Exclude IP addresses	To support deep linking between applications, specify a list of application's IP addresses for linking
Time Expiry	Life length of SSO Token (cookie) for authentication in seconds. Default value is 14400 (4 hours).

You can test your SSO cookie by using the **Test SSO** button:

Exclude IP addresses for filter(semicolon separated values)).

Save

Test SSO



### Info!

SSO login is - telcorp-admin | Cookie will expire in 232(minutes).

## Configuring Confluence SSO add-on

This article describes how to configure SSO authenticator for Confluence.

**WARNING!** If you entered wrong parameters, use a "back door" functionality in order to avoid cyclic redirects and to access application bypass SSO.

Just add a GET parameter `sso=off` to the needed URL. Example: <https://some.confluence.com/?sso=off>.

To configure SSO for Confluence:

1. Install Confluence SSO add-on.

The screenshot shows the Confluence administration interface. The left sidebar contains a navigation menu with categories like CONFIGURATION, ATlassian Marketplace, and Users & Security. The main content area is titled 'Manage add-ons' and features a message about the Atlassian Marketplace server. Below this, there are filters for 'Filter visible add-ons' and 'User-installed'. The 'User-installed add-ons' section displays the 'Authentication-Redirect-Filters' add-on, which is highlighted with a red border. The add-on details include a 'Free trial' button, version information (1.0.0-SNAPSHOT), vendor (cPrime), add-on key (com.cprime.labs.confluence.Authentication-Redirect-Filters), license details (Unlicensed), and a license key field. There is also an 'Update' button at the bottom of the add-on details.

2. Go to **Administration > Add-Ons**.
3. In the **CONFIGURATION** section, click **Global SSO**.  
The **Configuration page for SSO** opens.
4. Fill in the fields on this page. The field description is provided in the [table below](#).

The screenshot shows the 'Configuration page for SSO' in Confluence. The left sidebar contains a navigation menu with categories like CONFIGURATION, CPRIIME GOOGLE ADDON, CONFIGURE JIRA USER, ATLASSIAN MARKETPLACE, and SCRIPT RUNNER. The main content area has the following fields:

- Login URL:**  (SSO Login URL)
- Logout URL:**  (SSO Logout URL)
- Cookie Domain:**  (SAMLssoclient Cookie Domain)
- Time Expiry:**  (Live of SSO Token for authentication in seconds. Default value is 14400(4 hours).)
- Path:**  (Application Path)
- Exclude paths:**  (Exclude Paths or part of URLs for filter(semicolon separated values). Example: /rest/usermanagement;/rest/api etc.)
- Public Key:**  (Please enter the full path to your public key file on server.)
- Exclude IP addresses:**  (Exclude IP addresses for filter(semicolon separated values).)

Buttons:

**Info!** SSO login is - telcorp-admin | Cookie will expire in 217(minutes).

**Field description for the Global SSO Configuration page**

Attribute	Description
Login URL	IDP Login Page Examples: <ul style="list-style-type: none"> <li>https://adfs-test.com/adfs/ls/idpinitiatedsignon</li> <li>https://aag0677.my.centify.com/applogin/appKey/8980f085-4d24-48a7-a701-bb13c4e90b0f/customerId/AAG0677</li> </ul>
Logout URL	IDP Logout Page Examples: <ul style="list-style-type: none"> <li>https://aag0677.my.centify.com/applogout</li> <li>https://adfs-test.com/adfs/ls/?wa=wsignout1.0</li> </ul>
Cookie Domain	Domain of your applications for SSO cookie
Path	Your application path. If you need to have one logout from all applications, enter "/" for this field.
Exclude paths	You can disable SSO from URLs which contain custom pieces of URL (semicolon separated values). Example: <b>/rest/usermanagement;/rest/api</b>  Another case is to open REST API for using.
Public Key	Full path to your public key file for decrypting the SSO username
Exclude IP addresses	To support deep linking between applications, specify a list of application's IP addresses for linking
Time Expiry	Live of SSO Token for authentication in seconds. Default value is 14400(4 hours).



You can test your SSO cookie by using the **Test SSO** button.

## Configuring Bamboo SSO add-on

This article describes how to configure SSO authenticator for Bamboo.

**WARNING!** before installing this add-on, check whether you can receive the SSO cookie.

To configure SSO for Bamboo:

1. Install Bamboo SSO add-on.

The screenshot shows the Jira Add-Ons page for the 'Authentication-Redirect-Filters' plugin. The page is titled 'Authentication-Redirect-Filters' and includes a 'TRIAL EXPIRING' badge and a 'Buy now' button. Below the title, there is a description: 'This is the com.cprime.labs.jira.Authentication-Redirect-Filters plugin for Atlassian Jira.' and a warning: 'Your trial is expiring on 08/Jun/16. Buy a license for this add-on.' There are three buttons: 'Buy now', 'Uninstall', and 'Disable'. A table displays the following information:

No screenshots available	Version: 1.0.0-SNAPSHOT	14 of 14 modules enabled
	Vendor: cPrime	
	Add-on key: com.cprime.labs.jira.Authentication-Redirect-Filters	
	License details: Evaluation, Unlimited-user testing license, Standard, expires 08/Jun/16	
	License status: Valid	
	License SEN: Unknown	
	License key: AAAClg00DA...	

Below the table, there are several other add-ons listed with expandable arrows and update buttons:

- > Entity property conditions
- > Filter Deletion Warning Plugin
- > HipChat for JIRA UPDATE AVAILABLE Update
- > JIRA Feature Keys
- > Soy Function Plugin
- > Support Tools Plugin UPDATE AVAILABLE Update

At the bottom, there are links for 'Audit log', 'JIRA update check', 'Settings', and 'Enter safe mode'.

2. Go to **Administration > Add-Ons**.
3. Click **Global SSO** on the left panel.  
The **Configuration page for Global SSO** opens.
4. Fill in the fields on this page. The field description is provided in the table below.  
**WARNING!** Before you enter login / logout URL, test your SSO!

Bamboo administration

**BUILD RESOURCES**

- Agents
- Agent matrix
- Executables
- JDKs
- Server capabilities
- Global variables
- Linked repositories
- Shared credentials
- Repository settings

**ELASTIC BAMBOO**

- Configuration

**PLANS**

- Concurrent builds
- Quarantine settings
- Expiry
- Bulk action
- Build monitoring
- Remove plans
- Move plans
- Bulk edit plan permissions

**SECURITY**

- Users

### Configuration page for Global SSO

Login URL:  SSO Login URL

Logout URL:  SSO Logout URL

Cookie Domain:  SAMLssoclient Cookie Domain.

Path:  Application Path.

Exclude paths:  Exclude Paths or part of URLs for filter(semicolon separated values). Example: /rest/usermanagement;/rest/api etc.

Public Key:  Please enter the full path to your public key file on server.

Exclude IP addresses:  Exclude IP addresses for filter(semicolon separated values).

**Info!**  
SSO login is - telcorp-admin

You can test your SSO cookie by using the **Test SSO** button:

**Info!**  
SSO login is - username

**Field description for the Global SSO Configuration page**

Attribute	Description
Login URL	IDP Login Page Examples: <ul style="list-style-type: none"> <li>https://adfs-test.com/adfs/ls/idpinitiatedsignon</li> <li>https://aag0677.my.centify.com/applogin/appKey/8980f085-4d24-48a7-a701-bb13c4e90b0f/customerId/AAG0677</li> </ul>
Logout URL	IDP Logout Page Examples: <ul style="list-style-type: none"> <li>https://aag0677.my.centify.com/applogout</li> <li>https://adfs-test.com/adfs/ls/?wa=wsignout1.0</li> </ul>
Cookie Domain	Domain of your applications for SSO cookie

Path	Your application path. If you need to have one logout from all applications, enter "/" for this field.
Exclude paths	You can disable SSO from URLs which contain custom pieces of URL (semicolon separated values). Example: <b>/rest/usermanagement;/rest/api</b>  Another case is to open REST API for using.
Public Key	Full path to your public key file for decrypting the SSO username
Exclude IP addresses	To support deep linking between applications, specify a list of application's IP addresses for linking

## Configuring Bitbucket SSO add-on

To configure Bitbucket SSO Authenticator, perform the following operations:

1. Install the Bitbucket SSO add-on.
2. Configure the **BITBUCKET\_WORK\_DIR/shared/bitbucket.properties** file.

As a result, you will have a configuration like this:

```

bitbucket.properties
...
plugin.global-sso.login.url=https://aag0677.my.centriify.com/applogin/
appKey/6c7c624e-b80d-447d-8b0a-c9e9ef31c73c/customerId/AAG0677
plugin.global-sso.logout.url=https://aag0677.my.centriify.com/applogout
plugin.global-sso.public.key.file=/var/atlassian/application-data/bit
bucket/public_key.der
plugin.global-sso.path=/
plugin.global-sso.domain=.cprime.com
plugin.global-sso.expiry.time=14400

```

Where:

Property	Description
plugin.global-sso.login.url	IDP Login URL.
plugin.global-sso.logout.url	IDP Logout URL.
plugin.global-sso.public.key.file	Full path to the public key on the server(for decryption the cookie).
plugin.global-sso.path	Cookie path.
plugin.global-sso.domain	Cookie domain.
plugin.global-sso.expiry.time	Live of SSO Cookie for authentication in seconds. Default value is 14400(4 hours).

3. Generate **public\_key.der** and specify a path to this key.
4. Restart Bitbucket instance.
5. Install the **Bitbucket-SSO-Authenticator** add-on.

## Configuring FishEye SSO add-on

Content in development, please wait a bit.