GETTING STARTED GUIDE

ALCATEL-LUCENT RAINBOW™

ADFS Configuration guide

Ed 2

SEPTEMBER 2020

Author: Cloud Services

Alcatel·Lucent Enterprise

Disclaimer

This documentation is provided for reference purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this documentation is provided “as is” without any warranty whatsoever and to the maximum extent permitted.

In the interest of continued product development, ALE International reserves the right to make improvements to this document and the products it describes at any time without notice or obligation.

Copyright

Contents

Glossary

ALE: Alcatel-Lucent Enterprise

SSO: Single Sign On

ADFS: Active Directory Federation Service

SAML: Security assertion markup language

IDP: Identity Provider

1 Introduction

This guide provides technical description to configure ADFS Single Sign On (SSO) with Rainbow based on SAMLv2 protocol

2 Overview

Rainbow is able to use a third-party identity provider to make authentication. ADFS is a server deployed on customer premises and can be connected as identity provider on Rainbow based on SAMLv2 protocol. Once connected, all users of the company will be redirected to the ADFS login screen to connect to Rainbow.

3 History

Modifications	Date	Edition
Creation of document	13/02/2020	Ed 01
Page 6, replace der by pem format	22/09/2020	Ed 02

4 Related documents

None

5 Step 1: Configure Rainbow for ADFS

In the administration screen of Rainbow, in parameter, security tab, configure a SSO server based on SAMLv2 protocol.

Enter these parameters:

- Login URL: https://sso.adfs.your.domain.com/adfs/ls
- Logout URL (optional): let empty (restriction Rainbow side, when corrected, set it to https://sso.adfs.your.domain.com/adfs/ls) if SLO is required)
- Attribute ID : http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Attribute ID doesn't depend on the company should be always the same.

- Certificates: this certificate has to be downloaded from ADFS server:
  - On ADFS side, in the left menu,
    - Select ADFS -> Service -> Certificates
    - Select the "Token signing certificate" and click "view certificate" on the right.
    - On Details tab, click on "copy to file". Follow the wizard to export it in PEM format.
    - On rainbow side, copy the certificate content in base64 into Rainbow admin screen.

- Last step: downloads the metadata file to find the needed URLs to configure ADFS server.

6 Step 2: Configure ADFS for Rainbow using the Rainbow metadata

In ADFS home screen, on the left side, select "Relying party Trust" and "Add Relying party trust" on the right part of the screen.

6.1.1 In the creation Wizard.

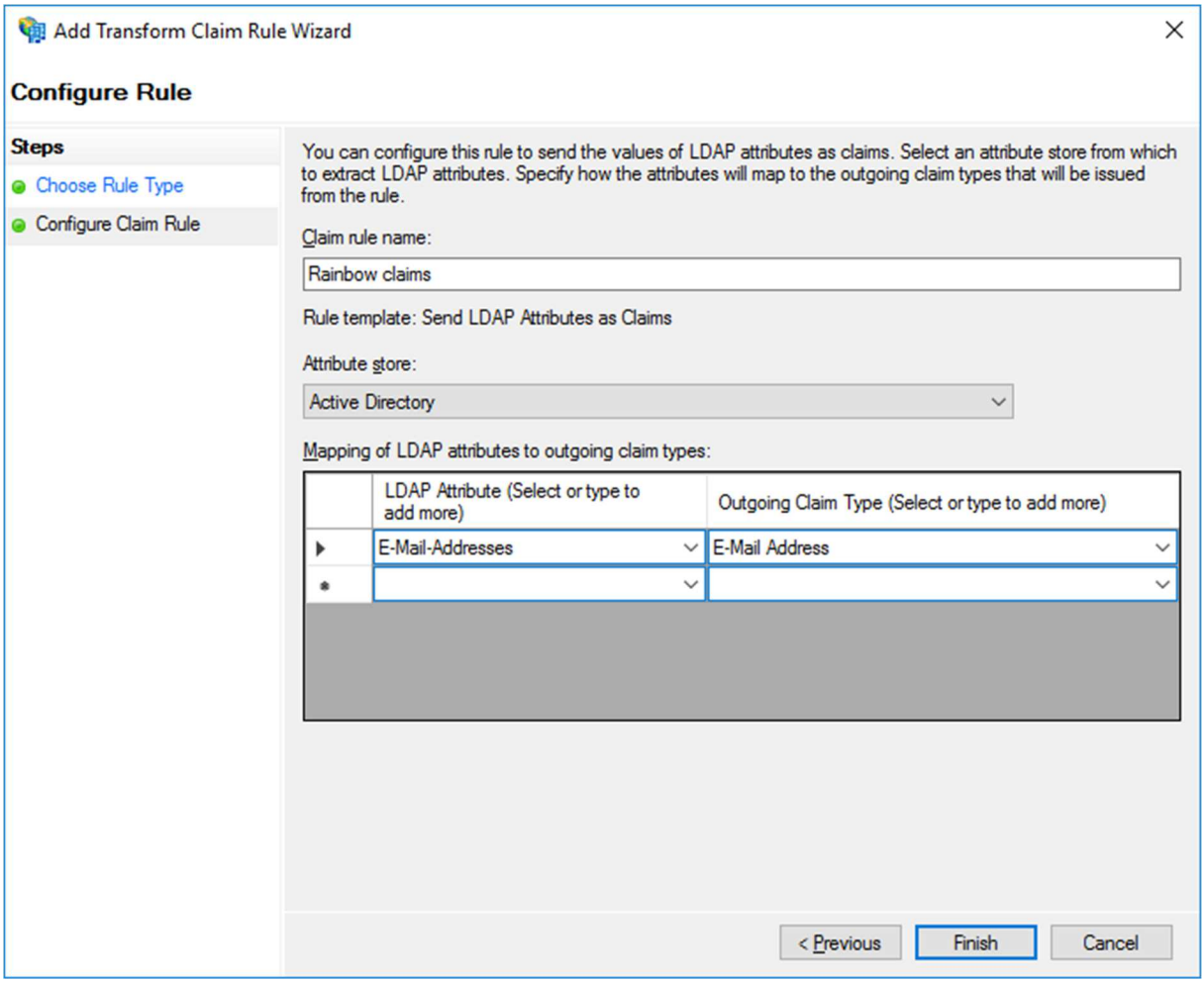
- Select "Claims aware entry"
- Select Import data about relying party from a file.
- Select the Rainbow metadata xml file.

6.1.2 Claims issuance

On the right, for the new Relying party trust just created, click on the "Edit claims issuance policy". Two rules have to be created: One for NameID and one for email.

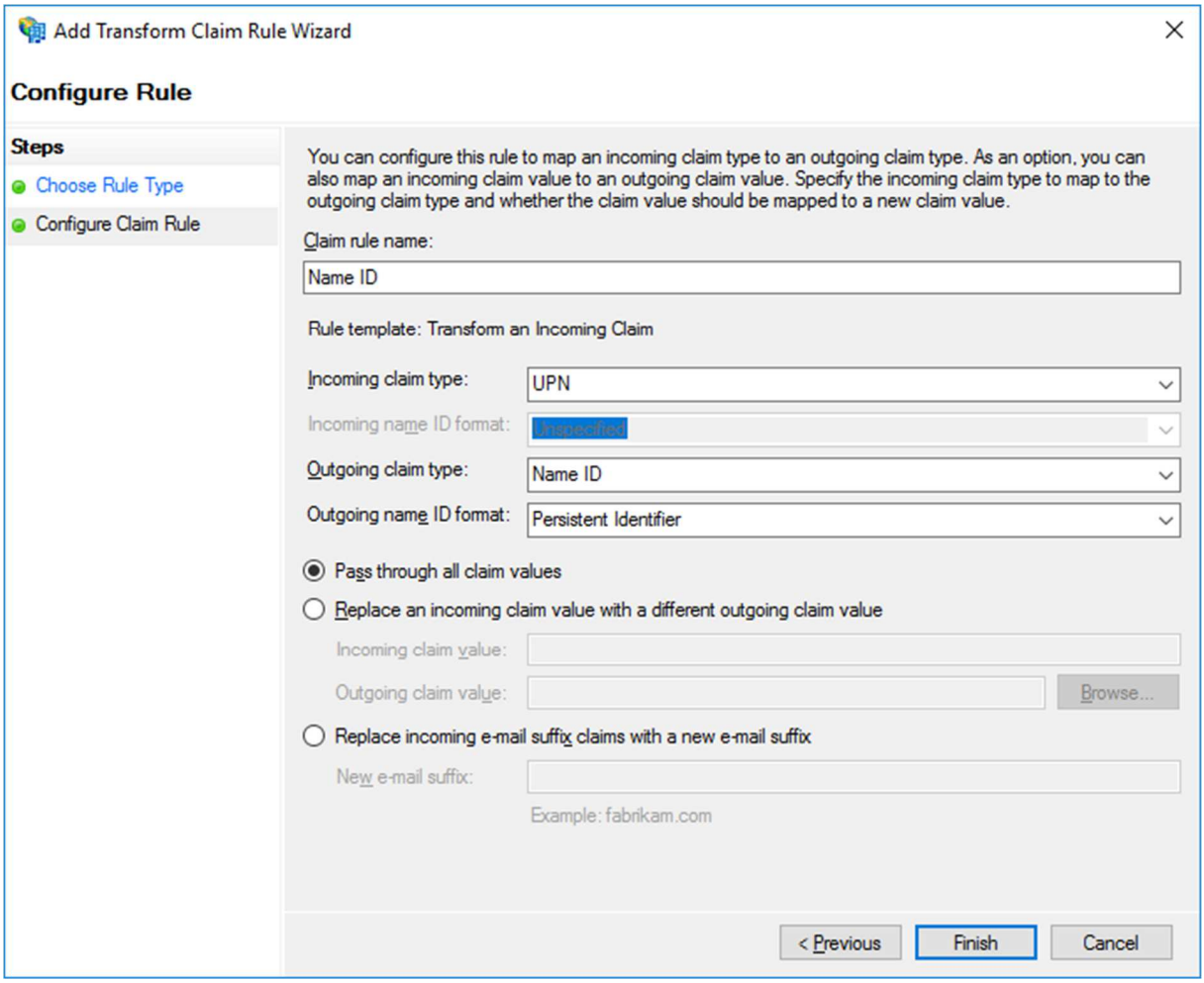
Email

- Click on "add rule".
- Select the "Send LDAP attribute as Claims"
- Set the name of the Rule as "Rainbow claims"
- Select the store as "Active Directory" and Select the email in both columns.



NameID

- Add rule
- Select “Transform an incoming claim”.
- Set the rule name as “NameID”
- Set the “Incoming claim type” to “UPN”
- Set the “Outgoing claim type” to “NameID”
- Set the “Outgoing name ID format” to “persistent”.



7 FAQ

Authentication fails with error seen on ADFS side: "*the revocation function was unable to check the revocation because the revocation server was offline*". Rainbow application displays a generic error as "*Unknown error, please contact your administrator*".

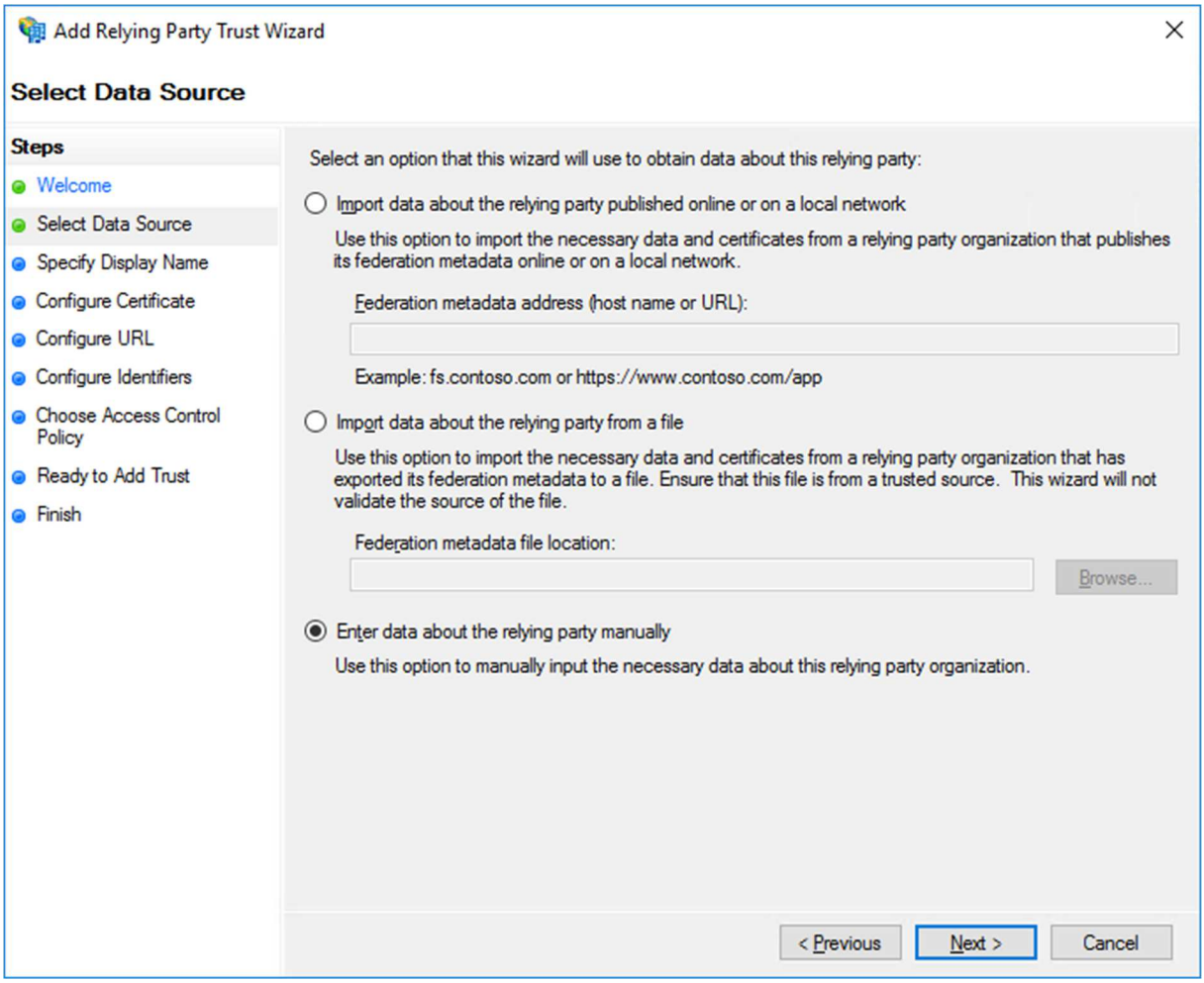
> Our production SAML certificate contains a CRL URL and should be accessible from the IDP. IDP must have access to http://crl.usertrust.com/GandiStandardSSLCA2.crl

8 Annexes

8.1 Manual configuration of the relying party trust.

It is possible to configure the relying party manually instead of importing the metadata xml file.

In step 2, in ADFS home screen, on the left side, select "Relying party Trust" and "Add Relying party trust" on the right part of the screen.



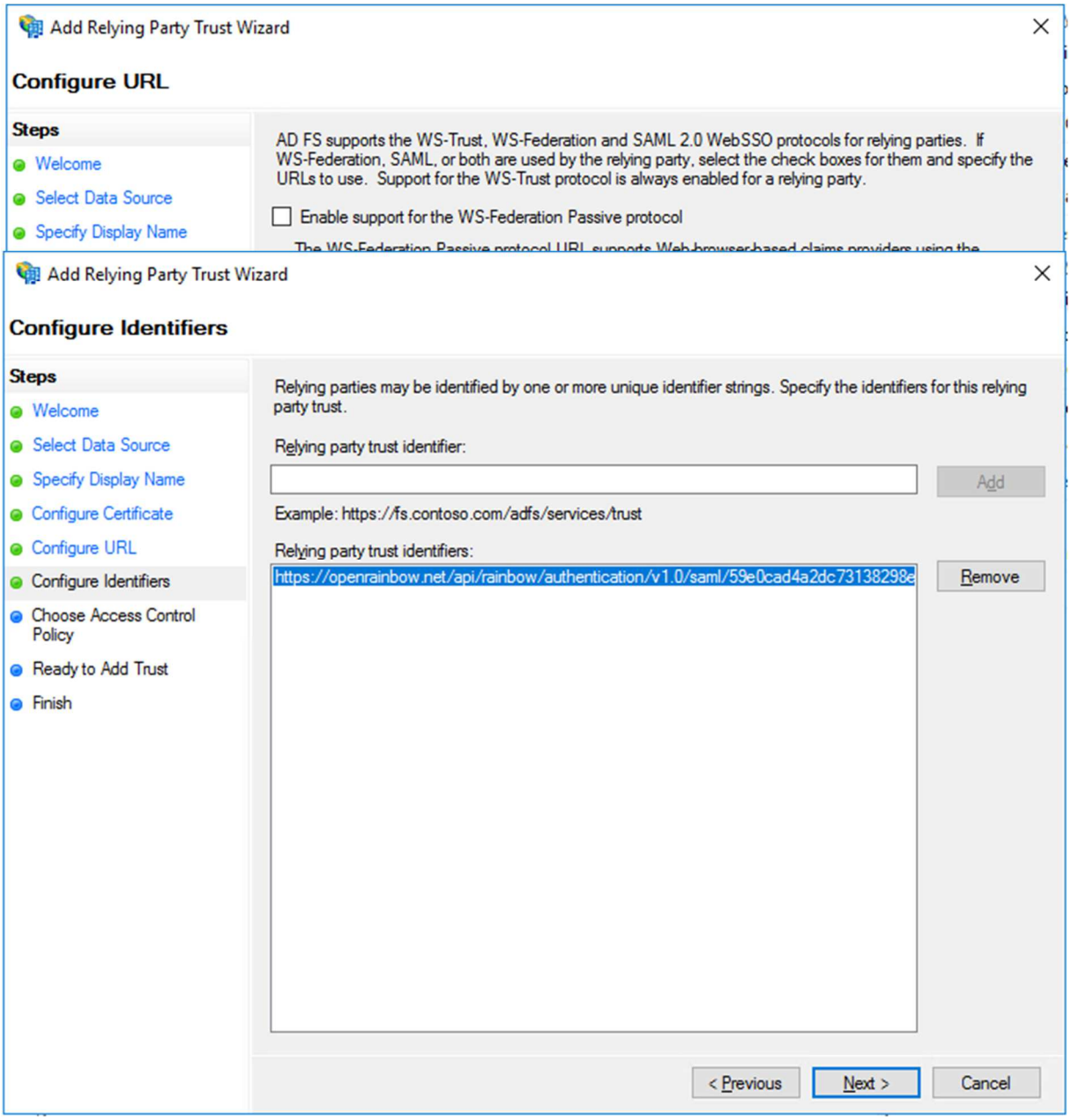
8.1.1 In the creation Wizard.

- Select “Claims aware entry”
- Select “Enter data about the relying party manually”

- Enter a display name as “Rainbow SSO”. It is only a description.
- Skip the step to configure an encryption certificate.
- Select SAML 2.0 and enter Relying party SAML 2.0 service URL:

https://openrainbow.net/api/rainbow/authentication/v1.0/saml/59e0cad4a2dc73138298e5af/assert.

This URL is specific for a customer. It can be found in the Rainbow metadata downloaded in the first step.



- In next step, set a replying trust identifier: https://openrainbow.net/api/rainbow/authentication/v1.0/saml/59e0cad4a2dc73138298e5af/metadata.xml.

This URL is specific for a customer. It can be found in the Rainbow metadata downloaded in the first step.

- In next step, choose Access Policy: select “Permit EveryOne”
- The next screen “Ready to add trust” permits to control the entered parameters.
- In the Finish screen, be sure to check the “Configure claims issuance policy for this application” to continue the configuration.

The Relying Party trust creation wizard is finished. But some further steps have to be done.

8.1.2 Certificates

The last step is to add the Rainbow signing certificate to ADFS:

In a text editor.

- add a first line:“-----BEGIN CERTIFICATE-----”
- Select the certificate in Rainbow metadata.xml, Copy paste it in a text editor
- add a last line: “-----END CERTIFICATE-----”
- Save the file.

In ADFS,

- On the right, for the Rainbow relying party just created, click on the “Properties”
- Open the “Signature” tab
- Import the Rainbow crt file.

8.2 Optional step to enable encryption

In ADFS,

- On the right, for the Rainbow relying party just created, click on the “Properties”
- Open the “Encryption” tab
- Import the Rainbow crt file also used for signature.

8.3 Optional step to let ADFS server to request Rainbow logout.

Add a logout URL in ADFS

- On the right, for the Rainbow relying party just created, click on the “Properties”
- Open the “Endpoint” tab
- Add a new endpoint:
    - Endpoint type: SAML logout
- Binding: Redirect
- Trusted URL: (same as login URL): https://openrainbow.net/api/rainbow/authentication/v1.0/saml/59e0cad4a2dc73138298e5af/assert

End of Document