



# ALCATEL-LUCENT RAINBOW™

## ADFS Configuration guide

Ed 2

SEPTEMBER 2020

*Author: Cloud Services*



**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**

©2020 ALE International. Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for a commercial purpose is prohibited unless prior permission is obtained from Alcatel-Lucent.

Alcatel-Lucent, OmniPCX, and OpenTouch and Rainbow are either registered trademarks or trademarks of Alcatel-Lucent.

All other trademarks are the property of their respective owners.

## Contents

<b>Glossary</b> .....	<b>4</b>
<b>1 Introduction</b> .....	<b>5</b>
<b>2 Overview</b> .....	<b>5</b>
<b>3 History</b> .....	<b>5</b>
<b>4 Related documents</b> .....	<b>5</b>
<b>5 Step 1: Configure Rainbow for ADFS</b> .....	<b>6</b>
<b>6 Step 2: Configure ADFS for Rainbow using the Rainbow metadata</b> .....	<b>6</b>
6.1.1 In the creation Wizard. ....	6
6.1.2 Claims issuance .....	6
<b>7 FAQ</b> .....	<b>8</b>
<b>8 Annexes</b> .....	<b>8</b>
8.1 Manual configuration of the relying party trust. ....	8
8.1.1 In the creation Wizard. ....	9
8.1.2 Certificates .....	11
8.2 Optional step to enable encryption .....	11
8.3 Optional step to let ADFS server to request Rainbow logout. ....	11

## Glossary

---

<b>ALE:</b>	Alcatel-Lucent Enterprise
<b>SSO:</b>	Single Sign On
<b>ADFS:</b>	Active Directory Federation Service
<b>SAML:</b>	Security assertion markup language
<b>IDP:</b>	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.

The screenshot shows the 'Add Transform Claim Rule Wizard' dialog box, specifically the 'Configure Rule' step. The 'Steps' pane on the left shows 'Configure Claim Rule' as the active step. The main area contains the following configuration options:

- Claim rule name:** Rainbow claims
- 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)
▶	E-Mail-Addresses	E-Mail Address
*		

At the bottom right, there are three buttons: '< Previous', 'Finish', and 'Cancel'.

## 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”.

**Add Transform Claim Rule Wizard**

**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: Name ID

Rule template: Transform an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Name ID

Outgoing claim type: Name ID

Outgoing name ID format: Persistent Identifier

Pass through all claim values  
 Replace an incoming claim value with a different outgoing claim value  
 Incoming claim value:   
 Outgoing claim value:  Browse...  
 Replace incoming e-mail suffix claims with a new e-mail suffix  
 New e-mail suffix:   
 Example: fabrikam.com

< Previous Finish Cancel

## 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.

The screenshot shows the 'Add Relying Party Trust Wizard' dialog box. The title bar reads 'Add Relying Party Trust Wizard' with a close button (X) on the right. The main heading is 'Select Data Source'. On the left, a 'Steps' pane lists the following steps: Welcome, Select Data Source (highlighted), Specify Display Name, Configure Certificate, Configure URL, Configure Identifiers, Choose Access Control Policy, Ready to Add Trust, and Finish. The main area contains three radio button options for selecting data source information:

- 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. Below this is a text box for 'Federation metadata address (host name or URL):' with an 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. Below this is a text box for 'Federation metadata file location:' with a 'Browse...' button to its right.
- Enter data about the relying party manually. Use this option to manually input the necessary data about this relying party organization.

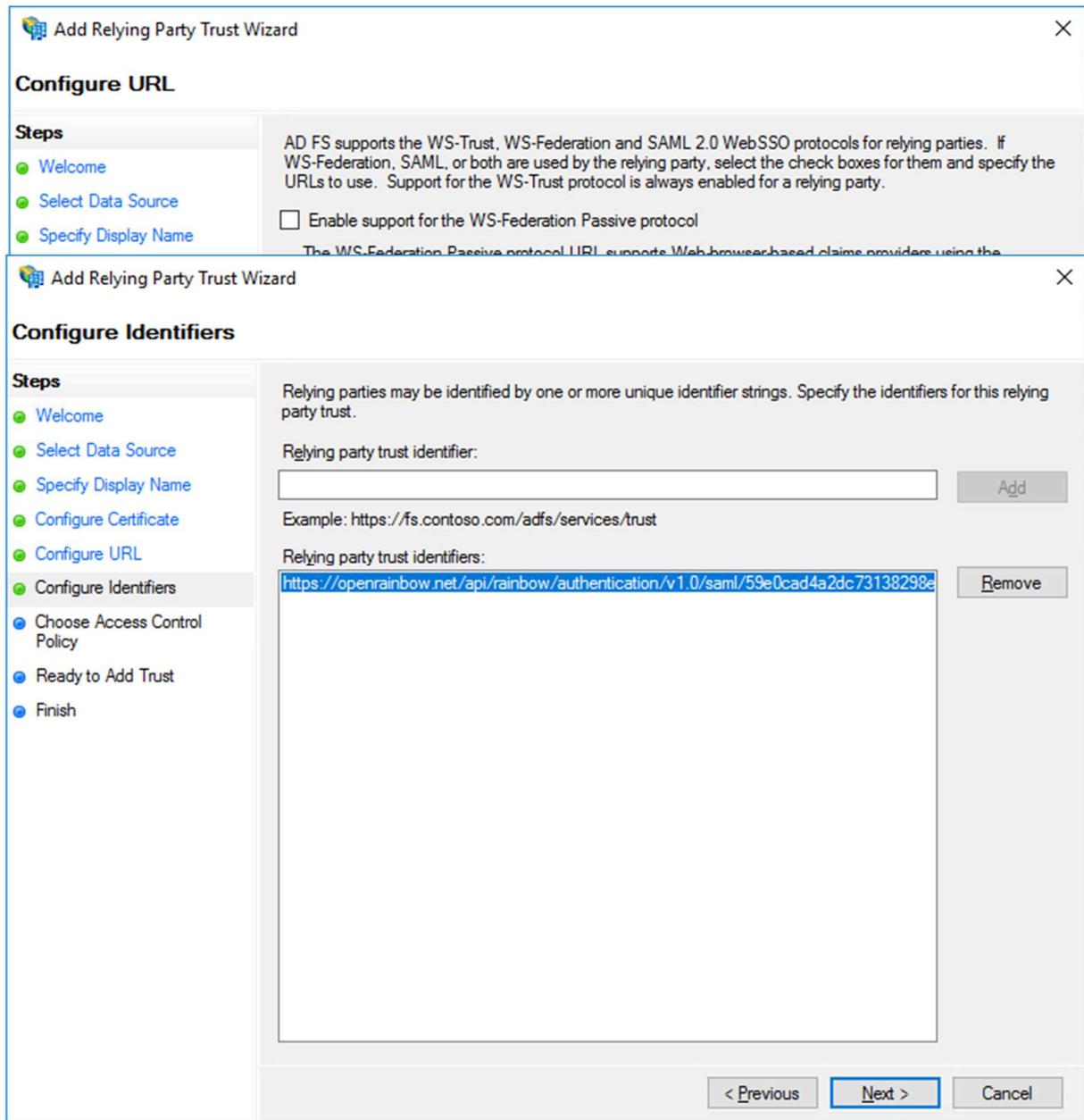
At the bottom right, there are three buttons: '< Previous', 'Next >' (highlighted with a blue border), and 'Cancel'.

### 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*