SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Exchange 2016 with ADFS



All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Number: 007-013762-001, Rev. A Release Date: May 2017

Contents

Third-Party Software Acknowledgement	4
Description	4
Applicability	5
Environment	5
Audience	5
CBA Flow using SafeNet Authentication Client	6
Prerequisites	7
Supported Tokens and Smart Cards in SafeNet Authentication Client	7
Configuring Exchange 2016 with ADFS	8
ADFS Configuration	8
Configuring AD FS Authentication Policy:	22
Exchange Configuration	23
Running the Solution	24
Support Contacts	27

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Exchange 2016 with ADFS.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

PKI is and effective strong authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. Gemalto's certificate-based tokens and smart cards provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Exchange 2016 with ADFS using Gemalto's tokens and smart cards.

It is assumed that the Exchange 2016 with ADFS environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

Exchange 2016 with ADFS can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

Applicability

The information in this document applies to:

- SafeNet Authentication Client (SAC) Typical installation mode SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto's tokens and smart cards.
- SafeNet Authentication Client (SAC) IDGo800 Compatible mode DGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

For more details about different SAC installation modes, please refer to the Customization section in SafeNet Authentication Client Administrator Guide.

- Microsoft AD FS 2012 R2
- Microsoft Exchange server 2016 Installed on Server 2012 R2.

Environment

The integration environment that was used in this document is based on the following software versions:

- SafeNet Authentication Client (SAC) 10.3
- Microsoft Exchange server 2016
- Microsoft AD FS 2012 R2
- Microsoft Active Directory & Certificate authority

Audience

This document is targeted to system administrators who are familiar with Exchange 2016 with ADFS, and are interested in adding certificate-based authentication capabilities using Gemalto tokens and smart cards. See Supported Tokens and Smart Cards in SafeNet Authentication Client, on page 7.

CBA Flow using SafeNet Authentication Client

The diagram below illustrates the flow of certificate-based authentication:



- 1. A user attempts to connect to the Exchange 2016 with ADFS server using the Exchange 2016 with ADFS URL
- 2. The user is redirected to an ADFS authentication page, and is prompted to enter the Domain user name and password. After successfully entering the Domain user name and password, the user is prompted to enter the Token/Smart card password on which the certificate resides.
- 3. After successful authentication, the user is allowed to access to the Exchange portal.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificatebased authentication for Exchange 2016 with ADFS using Gemalto tokens and smart cards:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, Token Policy Object (TPO) must be configured with MS CA Connector. For further details, refer to the section "Connector for Microsoft CA" in the *SafeNet Authentication Manager Administrator's Guide*.
- Users must have a Gemalto token or smart card with an appropriate certificate enrolled on it.
- AD FS is set-up as described: https://technet.microsoft.com/en-us/library/dn635116(v=exchg.150).aspx
- It is assumed that the environment is configured and working with domain users user name password authentication.
- SafeNet Authentication Client (10.3) must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.3) supports the following tokens and smart cards:

Certificate-based USB tokens

- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards

- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For a list of all supported devices, refer to SafeNet Authentication Client Customer Release Notes.

Configuring Exchange 2016 with ADFS

ADFS Configuration

Creating a relying party trust for Outlook Web App and EAC

1. In Server Manager, click Tools, and then select AD FS Management.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

2. In AD FS snap-in, under AD FS\Trust Relationships, right-click Relying Party Trusts, and then click Add Relying Party Trust to open the Add Relying Party Trust wizard.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. On the Welcome page, click Start.

Add Relying Party Trust Wizard
Velcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard. Previous Start

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. On the Select Data Source page, click Enter data about the relying party manually, and then click Next.

Add Relying Party Trust Wizard		
Select Data Source		
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Multi-factor Authentication Now? Choose Issuance Authentication News Ready to Add Trust Finish	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 address (host name or URL): 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: Browse (e) Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization. 	
	< Previous Next > Cancel	

(The screen image above is from Microsoft[®] software. Trademarks are the property of their respective owners.)

5. On the **Specify Display Name** page, in the **Display Name** box, type **Outlook Web App** or **OWA**, and then under **Notes**, you can type a description for this relying party trust (such as **This is a trust for https://** exchange.integ.com/owa) and then click **Next**.

Ŵ	Add Relying Party Trust Wizard	×
Specify Display Nan	ne	
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	OWA	
Specify Display Name	Notes:	
Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish		< >
	< Previous Next > Can	cel

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

6. On the Choose Profile page, click AD FS profile, and then click Next.

\$	Add Relying Party Trust Wizard	x
Choose Profile		
Steps Welcome Select Data Source Specify Display Name Configure Certificate Configure URL Configure Multi-factor Authentication Now? Choose Issuance Authentication 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.	
	< Previous Next > Cance	el

(The screen image above is from Microsoft[®] software. Trademarks are the property of their respective owners.)

7. On the **Configure Certificate** page, click **Next**.

%	Add Relying Party Trust Wizard	x
Configure Certificate		
Configure Certificate Steps • Welcome • Select Data Source • Specify Display Name • Choose Profile • Configure Certificate • Configure URL • Configure URL • Configure Multi factor Authentication Now? • Choose Issuance Authonization Rules • Ready to Add Trust • Finish	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	
	< Previous Next > Cancel	

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

8. On the Configure URL page, **click Enable support for the WS-Federation Passive protocol**, and then under **Relying party WS-Federation Passive protocol URL**, type your OWA's URL (for example, https://exchange.integ.com/owa/), and then click **Next**.

\$	Add Relying Party Trust Wizard
Configure URL	
Steps Welcome Select Data Source Specify Display Name Choose Profile Corfigure Cetificate Corfigure URL Configure Mulifactor Authentication Now? Choose Issuance Authoritication Rules Ready to Add Trust Finish	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-Trust protocol WS-trust protocol The WS-Federation Passive protocol URLs upports Web-browser-based claims providers using the WS-Federation Passive protocol URL: https://exchange.integ.com/owa/ Example: https://fs.cortoso.com/adfs/ls/ Cample: https://signigie-sign-on (SSO) service URL supports Web-browser-based claims providers using 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 <u>S</u> AML 2.0 SSO service URL: Example: https://www.contoso.com/adfs/ls/ Example: https://www.contoso.com/adfs/ls/
	< Previous Next > Cancel

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

9. On the **Configure Identifiers** page, specify one or more identifiers for this relying party, click **Add** to add them to the list, and then click **Next**.

\$ #	Add Relying Party Trust Wizard
Configure Identifiers	
Steps Welcome Select Data Source	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.
Specify Display Name	
Choose Profile Configure Certificate	Example: https://fs.contoso.com/adfs/services/trust Relvino.party trust identifiers:
Configure URL	https://exchange.integ.com/owa/ Remove
Configure Identifiers	
Configure Multi-factor Authentication Now?	
 Choose Issuance Authorization Rules 	
Ready to Add Trust	
 Finish 	
	< Previous Next > Cancel

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

10. On the **Configure Multi-factor Authentication Now?** Page, leave the default configuration (we will configure MFA later on) and then click **Next**.

\$	Add	Relying Party T	rust Wizard		X
Steps Welcome Select Data Source	Configure multi-factor a there is a match for an	authentication setting y of the specified req	s for this relying party trust. Multi-factor auti uirements.	nentication is required	d if
 Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi factor Authentication Now? Choose Issuance Authonization Rules Ready to Add Trust Finish 	Multifactor Auther Requirements I do not want to co Configure multifact You can also configure Authentication Policie	tication Users/Groups Device Location nfigure multi-factor au or authentication set e multi-factor authe s node. For more in	INTEG\Domain Users Not configured Extranet, Intranet thentication settings for this relying party tru- tings for this relying party trust. ntication settings for this relying party tru formation, see <u>Configuring Authentication</u>	Global Settings ust at this time. Ist by navigating to t	the
			< Previous Nex	t > Cancel	

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

11. On the Choose Issuance Authorization Rules page, select Permit all users to access this relying party, and then click next.



(The screen image above is from Microsoft[®] software. Trademarks are the property of their respective owners.)

12. On the **Ready to Add Trust** page, review the settings, and then click **Next** to save your relying party trust information.

\$	Add Relying Party Trust Wizard
Ready to Add Trust	
Steps Welcome Select Data Source Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure URL Configure Identifiers Configure Identifiers Configure MultiFactor Authentication New? Choose leasance Authorization Rules Ready to Add Trust Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database. Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Not < > Specify the monitoring settings for this relying party trust. Relying party's federation metadata URL: Monitor relying party: Accematically update relying party This relying party's federation metadata data was last checked on: < (never > This relying party was last updated from federation metadata on: < (never >
	< Previous Next > Cancel

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

13. On the Finish page, verify that Open the Edit Claim Rules dialog for this relying party trust when the wizard closes is unchecked, and click Close.

\$	Add Relying Party Trust Wizard	x
Finish		
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Cettificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap in Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	
	Close	

(The screen image above is from Microsoff[®] software. Trademarks are the property of their respective owners.)

- 14. To create a relying party trust for EAC, repeat steps 1-13 with the following differences:
 - In step 5, enter EAC for the display name instead of Outlook Web App. For the description, you can enter, for example, This is a trust for the Exchange Admin Center.
 - In step 8, the Relying party WS-Federation Passive protocol URL is ECP's URL (for example, https://exchange.integ.com/ecp/).

The ADFS Relying Party Trusts pane should now include two new trusts (OWA and ECP):

Image: Service Image: Service Actions Image: Service Image: Service No WS-T	la .	AD FS
AD FS Daplay Name Enabled Type Identifier Ad Resime Provider Truts Daplay Name Enabled Type Identifier Ad Resime Provider Truts Daplay Name Enabled Type Identifier Ad Resime Provider Truts Daplay Name Enabled Type Identifier Ad Relying Party Truts Daplay Truts Add Relying Party Truts Add Relying Party Truts Add Relying Party Truts Daplay Identifier No WS-T Https://doi:rtip.ou/mail.pdf Integration Service Yee WS-T https://doi:rtip.ou/mail.pdf Add Non-Claims-A Integration Service Yee WS-T https://doi:rtip.ou/mail.pdf No Integration Service Yee WS-T https://doi:rtip.ou/mail.pdf No Integration Service WS-T https://doi:r	File Action View Window Help	
 Service Trut Relationships Claims Provider Truts Relying Party Truts Relying Party Truts Authentication Policies Display Name Enabled Type Identifier Relying Party Truts Display Truts Display Truts Display Truts Display Truts Relying Party Truts Display Truts Display Truts Relying Party Truts Display Truts </td <td>🗭 🖤 🛛 🕅 🖬 🔟 🔟</td> <td>ng Party Trusts Actions</td>	🗭 🖤 🛛 🕅 🖬 🔟 🔟	ng Party Trusts Actions
< m >	 Envice Trust Beltinships Claims Provider Trusts Relying Party Trusts Athibut Stores Authentication Policies 	Japiday Name Enabled Type Identifier Jevice Registration Service No WS-T ummed add uriting com/app 1/ WS-T Add Relying Party Trus Japiday Name Yes WS-T https://dx.https:

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Adding ADFS claim rules for OWA and EAC

In a claims-based identity model, the function of Active Directory Federation Services (AD FS) as a federation service is to issue a token that contains a set of claims. Claims rules govern the decisions in regard to claims that AD FS issues. Claim rules and all server configuration data are stored in the AD FS configuration database.

You must create three claim rules:

- Active Directory user SID
- Active Directory group SID
- Active Directory UPN

To add the required claims:

1. In Server Manager, click Tools, and then click AD FS Management.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

2. In the console tree, under AD FS\Trust Relationships, click the Relying Party Trusts, and then right-click the Outlook Web App trust, and then click Edit Claim Rules.

🕨 🐟 😰 🔝 🖬 📰	Relving Party Trusts	_		-	_	Actions
 AD FS Service Tuxt Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies 	Relying Party Trusts Deploy Name Derice Registration Servic https://citikg.com/app https://citikg.com/app https://citikg.com/app	os 1/ Update from Federatio Edit Claim Rules Disable Properties Delete Help	Enabled No Yes Ver In Metadata	Type WS-T WS-T WC-T	Mantfler ummende die Integ com https://doi.integ.com/apo/1/ app//containue at die doningy https://exchane at die doningy https://exchane at die doningy	Actions Relying Party Trusts Add Rehing Party Trus. Add Non-Claims-Awar View New Window from Here Refersh Help https://exchane.integ Update from Federatio Edit Claim Rules Disable Properties Delete Help Help

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. In the **Edit Claim Rules** window, on the **Issuance Transform Rules** tab, click **Add Rule** to start the Add Transform Claim Rule Wizard.

suance Transform Rules	Issuance Authorization Rul	es Delegation Authorizat	ion Rules
The following transform	rules specify the claims that w	vill be sent to the relying pa	rty.
Order Rule Name		Issued Claims	
Add Rule Edit	Rule		

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. On the Select Rule Template page, under Claim rule template, select Send Claims Using a Custom Rule, and click Next.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

5. On the Configure Rule page, in the Choose Rule Type step, under Claim rule name, enter the name for the claim rule. Use a descriptive name for the claim rule, for example, ActiveDirectoryUserSID. Under Custom rule, enter the following claim rule language syntax:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types = ("http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"), query = ";objectSID;{0}", param = c.Value);

Edit Rule - ActiveDirectoryUserSID)
You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an ssuance statement using the AD FS claim rule language.	
Calin fore name. ActiveDirectoryUserSID	_
Rule template: Send Claims Using a Custom Rule	
Custom rule:	
<pre>c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount mme", Issuer == "AD AUTHORITY"]</pre>	< .
	~
OK Cancel	-

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

- 6. On the **Configure Rule** page, click **OK**.
- 7. In the Edit Claim Rules window, on the Issuance Transform Rules tab, click Add Rule to start the Add Transform Claim Rule Wizard.

suance 1	ransform Rules	Issuance Authorization R	ules Delegation Authori:	zation Rules
The follo	wing transform n	ules specify the claims that	will be sent to the relying	party.
Order	Rule Name		Issued Claims	
1	ActiveDirectory	UserSID	<see claim="" rule=""></see>	
				*
Add F	ule	Rule		

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

8. On the Select Rule Template page, under Claim rule template, select Send Claims Using a Custom Rule, and then click Next.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

9. On the **Configure Rule** page, on the **Choose Rule Type** step, under **Claim rule name**, enter the name for the claim rule. Use a descriptive name for the claim rule, for example, **ActiveDirectoryGroupSID**. Under **Custom rule**, enter the following claim rule language syntax for this rule:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",	
Issuer == "AD AUTHORITY"]	

=> issue(store = "Active Directory", types =
 ("http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid"), query =
 ";tokenGroups(SID);{0}", param = c.Value);

Edit Rule - ActiveDirectoryGroupSID	×
You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extract claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.	s
Claim rule name:	
ActiveDirectoryGroupSID	
Rule template: Send Claims Using a Custom Rule	
Custom rule:	
<pre>c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount name", Issuer == "AD AUTHORITY"] => issue(store = "Active Directory", types = ("http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid"), query = ";tokenGroups(SID);{0}", param = c.Value);</pre>	<
OK Cancel	

(The screen image above is from Microsoft[®] software. Trademarks are the property of their respective owners.)

10. On the **Configure Rule** page, click **OK**.

11. In the Edit Claim Rules window, on the Issuance Transform Rules tab, click Add Rule to start the Add Transform Claim Rule wizard.



(The screen image above is from Microsoff® software. Trademarks are the property of their respective owners.)

ance]	Fransform Rules	Issuance Authorizat	ion Rules Delegat	ion Authorization	Rules
he f <mark>ol</mark> lo	wing transform n	ules spec <mark>ify</mark> the claim	s that will be sent to	the relying party.	
Order	Rule Name		Issued Cla	ims	1
1	ActiveDirectory	UserSID	<see clain<="" td=""><td>n rule></td><td></td></see>	n rule>	
2	ActiveDirectory	GroupSID	<see clain<="" td=""><td>n rule></td><td></td></see>	n rule>	
					1
					•
Add F	tule Edit f	Rule	Rule		

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

12. On the Select Rule Template page, under Claim rule template, select Send Claims Using a Custom Rule, and then click Next.

\$	Add Issuance Authorization Claim Rule Wizard
Select Rule Templa	te
Steps	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.
Configure Claim Rule	Claim rule template:
	Send Claims Using a Custom Rule 🗸 🗸
	Claim rule template description:
	Using a custom rule, you can creater urles that can't be created with a nule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include: • Sending claims from an LDAP attribute store using a custom LDAP filter • Sending claims from a custom attribute store • Sending claims only when 2 or more incoming claims are present • Sending claims only when a nic noming claim value matches a complex pattern • Sending claims only with complex changes to an incoming claim value • Creating claims for use only in later rules
	< Previous Next > Cancel

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

13. On the Configure Rule page, on the Choose Rule Type step, under Claim rule name, enter the name for the claim rule. Use a descriptive name for the claim rule, for example, ActiveDirectoryUPN. Under Custom rule, enter the following claim rule language syntax for this rule:

c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]

=> issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query = ";userPrincipalName;{0}", param = c.Value);

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions a	extracts and an
issuance statement using the AD FS claim rule language.	
Claim rule name:	
ActiveDirectoryUPN	
Rule template: Send Claims Using a Custom Rule	
Custom rule:	
c:[Type ==	
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsacc	count
=> issue(store = "Active Directory", types =	
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), ques	ry =
";userFrincipaiName;{U}", param = c.value);	

(The screen image above is from Microsoff® software. Trademarks are the property of their respective owners.)

- 14. Click OK.
- 15. In the Edit Claim Rules window, click Apply, and then OK.

suance 1	Fransform Rules	Issuance Authorization F	Rules Delegation Authori	zation Rules
The follo	wing transform n	ules spec <mark>i</mark> fy the claims tha	t will be sent to the relying	party.
Order	Rule Name		Issued Claims	
1	ActiveDirectory	UserSID	<see claim="" rule=""></see>	
2	ActiveDirectory	GroupSID	<see claim="" rule=""></see>	
				1
Add F	tule Edit F	Rule Remove Rule		

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Configuring AD FS Authentication Policy:

- 1. In the ADFS Management window, right click on the Authentication Policies and choose to Edit Global Primary Authentication.
- 2. In the **Primary** tab, make sure **Form Authentication** is checked both for Extranet and Intranet.
- 3. In the Multi-factor tab:
 - a. Add the users/groups to be controlled by the MFA.
 - b. Choose Extranet/Intranet (or both) according to your preferred configuration.
 - c. Make sure **Certificate Authentication** is checked as additional authentication methods.
 - d. Press ok.



(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Exchange Configuration

In this step, after configuring AD FS to use claims-based authentication with Outlook Web App and EAC, it is needed to enable AD FS on the exchange side:

- 1. Copy signing certificate thumbprint From AD FS Server
- 2. **ON ADFS Server** Locate the AD FS token signing certificate thumbprint by using Windows PowerShell on the AD FS server.
 - a. Open Windows PowerShell and enter: Get-ADFSCertificate -CertificateType "Token-signing"
 - b. Copy the signing certificate thumbprint
- 3. On **Exchange Server**, using the Exchange Management Shell enter and run (see the example and paste the signing certificate thumbprint where needed):

Example:

Open Exchange Management Shell and enter:

\$uris = @(" https://exchange.integ.com/owa/","https://exchange.integ.com/ecp/")
Set-OrganizationConfig -AdfsIssuer "https://adfs.integ.com/adfs/ls/" -AdfsAudienceUris \$uris AdfsSignCertificateThumbprint"88970C64278A15D642934DC2987D9CCA5E65DS3B"

4. Enable ADFS authentication on the virtual directories.

- 5. **On the Exchange Server** using the Exchange Management Shell Enable ADFS authentication enter and run following:
 - a. For ECP Open Windows PowerShell and enter:

Get-EcpVirtualDirectory | Set-EcpVirtualDirectory -AdfsAuthentication \$true -BasicAuthentication \$false -DigestAuthentication \$false -FormsAuthentication \$false -WindowsAuthentication \$false

b. For OWA Open Windows PowerShell and enter:

Get-OwaVirtualDirectory | Set-OwaVirtualDirectory -AdfsAuthentication \$true -BasicAuthentication \$false -DigestAuthentication \$false -FormsAuthentication \$false -WindowsAuthentication \$false - OAuthAuthentication \$false

Note: ECP virtual directory must be configured before OWA

6. Perform IIS Reset.

Running the Solution

After ADFS and Exchange is configured to use authentication (through ADFS), users can log on to Exchange 2016 using Multi Factor Authentication.

Prerequisites:

- SafeNet Authentication Client is installed
- Token/smart card with smart card user certificate is connected.

To run the solution:

1. The administrator browses to the exchange URL **Example**: https://exchange.integ.com/ecp/ and is redirected to the organization's ADFS login page.

ADFS Gemalto
Sign in with your organizational account
safenetdemos\administrator
•••••••
Sign in
© 2013 Microsoft

(The screen image above is from Microsoff[®] software. Trademarks are the property of their respective owners.)

- 2. The administrator enters AD credentials and clicks Sign in.
- 3. After successful login, when prompted to confirm certificate, the administrator clicks OK.

A	DFS Gemalto
Windows Security	
Confirm Certificate Confirm this certificate by clicking OK. If this is not the correct certificate, click Cancel.	ome SAFENETDEMOS\administrator urity reasons, we require additional information y your account
Administrator Issue: safenetdemos-SERVER2008R Valid From: 1/26/2017 to 1/26/2018 Click here to view certificate prope	a certificate that you want to use for tication. If you cancel the operation, please our browser and try again.
OK	
© 20	113 Microsoft

(The screen image above is from Microsoft[®] software. Trademarks are the property of their respective owners.)

4. After certificate confirmation, the smart card logon window opens. The user enters the token/smart card password and clicks **OK**.

		ADFS Ge	emalto
S Token Logon	ation Client		ENETDEMOS\administrator
Enter the Token Password	My Token	Security tobe the	punt that you want to use for
Token Name:	Current Language: EN		er and try again.
This is an unlicensed copy	for evaluation use only.	OK Cancel	
		© 2013 Microsoft	

(The screen image above is from Microsoft[®] software. Trademarks are the property of their respective owners.)

5. After another successful login, the user is redirected to the organization's Exchange server (in this example: https://exchange.integ.com/ecp/)

recipients	mailboyes group	s resources contacts	shared migration	
recipients	indiboxes group	s resources contacts	shared migration	
Dermissions				
compliance management	+-/ = 23			
organization	DISPLAY NAME	 MAILBOX TYPE 	EMAIL ADDRESS	
protection	Administrator	User	Administrator@safenetdemos.com	Administrator
orotection				User mailbox
mail flow				Administrator@safenetdemos.com
mobile				Title:
0.0.10.10				Work phone:
oublic folders				
unified messaging				Phone and Voice Features
				Unified Messaging: Disabled
ervers				Enable
nybrid				Mobile Devices
				Disable OWA for Devices
0013				View details
				In Direct Archive
				In-Place Archive

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com