SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for MS Azure AD



All information herein is either public information or is the property of and owned solely by Gemalto NV. 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.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. 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 Part Number: 007-013448-001, Rev. A Release Date: March 2016

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as MS Azure AD.

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 an 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. SafeNet's certificate-based tokens 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.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet's hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations' PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the SafeNet Authentication Manager Administrator Guide.

Azure Active Directory (Azure AD) is Microsoft's multi-tenant cloud-based directory and identity management service. Azure AD provides an easy-to-use solution to give employees and business partners single sign-on (SSO) access to thousands of cloud SaaS applications such as Office365, Salesforce.com, Dropbox, and Concur.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to MS Azure AD using SafeNet tokens.

It is assumed that the MS Azure AD environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

MS Azure AD can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

Applicability

The information in this document applies to:

 SafeNet Authentication Client (SAC)—SafeNet Authentication Client is the middleware that manages SafeNet's tokens.

Environment

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

- SafeNet Authentication Client (SAC)—Version 9.0
- MS Azure AD—On cloud
- AD FS—On Windows Server[®] 2012 R2

Audience

This document is targeted to system administrators who are familiar with MS Azure AD, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

CBA Flow using SafeNet Authentication Client

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



1. A user attempts to log on to MS Azure AD. The user is redirected to AD FS proxy server (WAP) for authentication.

- 2. After successful authentication, user is redirected to SafeNet Authentication Client (SAC) for a secondary authentication. The user uses the SafeNet token on which his certificate resides, and, when prompted, enters the token password.
- 3. The SAC authentication reply is sent back to AD FS, which returns a response to MS Azure AD, accepting or rejecting the user's authentication request.
- 4. The user is granted or denied access to MS Azure AD.

Prerequisites

Before implementing certificate-based authentication for MS Azure AD using SafeNet tokens, ensure the following:

- 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) should 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 SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (9.0) should be installed on all client machines.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of tokens that can be used as a second authentication factor for users who authenticate to MS Azure AD.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

SafeNet eToken Virtual

SafeNet Authentication Client: Integration Guide Using SafeNet Authentication Client CBA for MS Azure AD Document PN: 007-013448-001, Rev. A, Copyright © 2016 Gemalto, Inc., All rights reserved. • SafeNet eToken Rescue

Configuring MS Azure AD and AD FS

Configuring MS Azure AD and AD FS requires the following:

- Adding a Domain to Azure, page 7
- Syncing the Domain to Azure, page 10
- Verifying the Installation of AD Connect, page 14
- Enabling Azure AD Federated Domains, page 15
- Configuring the AD FS Authentication Policy, page 17

Adding a Domain to Azure

- 1. Log into the Microsoft Azure Management Portal.
- 2. On the **Microsoft Azure** window, in the left pane, click **ACTIVE DIRECTORY**, and then in the right pane click on your directory (for example **SFNTdemo**).

Microsoft Azure 🛛 🗸			CREDIT STATUS			nanerana Bela lanat ana cam
	active	directory				
🧀 🖫	DIRECTORY	ACCESS CONTROL NAMESPACES	MULTI-FACTOR AUTH PRO	VIDERS RIGHTS MANAGEM	ENT	
	NAME	STATUS	ROLE	SUBSCRIPTION	DATACENTER REGION	COUNTRY OR REGI D
	SFNTdemo	→ ✓ Active	Global Administrator	Shared by all SFNTdemo s	Asia, Europe, United States	Israel
STREAM ANALYTICS						
MANAGEMENT SERVICES						
ACTIVE DIRECTORY						
			DELETE			0

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

3. Click Add domain.



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

4. On the ADD DOMAIN window, in the DOMAIN NAME field, enter the domain name, and then click add.

ADD DOMAIN	×
Specify a domain name	
Enter the name of a domain that your organization owns.	
DOMAIN NAME	
I plan to configure this domain for single sign-on with my local Active Directory. 📀	
add	
	(\rightarrow)
	<u> </u>

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

5. On the **Microsoft Azure** window, in the right pane, the domain is added, but the **STATUS** is **Unverified**. To verify the domain, you will need to add some values to your DNS. Follow Microsoft's guidelines, and then click **VERIFY** when you are done.

Microsoft Azure 🛛 🗸		CREDIT-STATUS			g@nateriet-inicizon
<u></u>	sfntdemo	DOMAINS DIRECTORY IN	ITEGRATION CONFIGURE F	REPORTS LICENSES	
SFNTdemo	DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY D
	sintdema.com	Custom		Not Configured	No
6	authengineeringsaferetins onericristoff.com	Bric	V Atta	Not Avelable	Yes
<u>ک</u>					
_					
<>					
8					
\bigotimes					
					
8∞					
_					
•					
+ NEW		ADO VERIPY	DELETE		1 🙏 1 🔗 🔞

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

The new domain is now verified and ready for use.

Microsoft Azure 🗸 🗸		CREDIT STATUS			
<u></u>	sfntdemo	DOMAINS DIRECTORY IN	TEGRATION CONFIGURE F	LEPORTS LICENSES	
SFNTdemo	DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY D D
0	autorgrowing interesting	Tex.	of acces	Hot Research	78.0
Q	stridemo.com	Custom	Verified	Not Parmed	No
\$					
<u> </u>					
<i>⇒</i> 					

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

Syncing the Domain to Azure

1. On the **Microsoft Azure** window, in the left pane, click **ACTIVE DIRECTORY**, and then in the right pane, click on your directory (for example **SFNTdemo**).

Microsoft Azure		CREDIT STATUS	<u> </u>		ineering Exatenet and co	•
active d	lirectory					
	ACCESS CONTROL NAMESPACES	MULTI-FACTOR AUTH PROV	IDERS RIGHTS MANAGEMI	INT		
	STATUS	ROLE	SUBSCRIPTION	DATACENTER REGION	COUNTRY OR REGI	P
SCHEDULER SFNTdemo	→ ✓ Active	Global Administrator	Shared by all SFNTdemo s	Asia, Europe, United States	Israel	
TRAFFIC MANAGER						
MANAGEMENT SERVICES						
ACTIVE DIRECTORY						

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

2. Under Integrate with your local directory, click the Download Azure AD Connect link.

Microsoft Azure 🛛 🗸	CREDIT STATUS	
sf	ntdemo users groups applications domains directory integration configure reports	LICENSES
SFNTdemo		
0	Your directory is ready to use.	
	Here are a few options to get started.	
- -	Skip Quick Start the next time I visit	
<u> </u>		
<u>اللہ</u>	ANT TO Set Up Directory Manage Access Develop Applications	
G	ET STARTED	
1000 /	Improve user sign-in experience	
	Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.	
1		
(%)	Add domain	
	Integrate with your local directory	
	Use the same user accounts and groups in the cloud that you already use on premises.	
	Dominous Paulo Por Compas	
8∞	Get Azure AD Premium	
4	improve access management experiences for end users and administrators, including self service password reset, group management, sign in customization, and reporting.	
-	Try it now	
¥		
NEW		0

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

3. Install Azure AD Connect on a machine that is a part of the domain to connect to Azure. On the **Microsoft Azure Active Directory Connect** window, click **Continue**.



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

4. Click Use express settings.

🚸 Microsoft Azure Active 🛛	Directory Connect _ X
Microsoft Azure Active D Welcome Express Settings	Directory Connect X Express Settings X If you have a single Windows Server Active Directory forest, we will do the following: X • Configure synchronization of identities in the current AD forest of SFNTDEMO X • Configure password synchronization from on-premises AD to Azure AD X • Start an initial synchronization X • Synchronize all attributes X Learn more about express settings X If you would like different settings, click Customize. X
	Customize Use express settings

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

5. Enter your Azure AD administrator user name and password, and then click Next.

Microsoft Azure Active I	Directory Connect	_ ×
Welcome Express Settings Connect to Azure AD	Connect to Azure AD	
Connect to AD DS	USERNAME	
Configure	Juth angineering@salenetanc.com	
	PASSWORD	
	••••••	
	1	

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

6. Enter the domain administrator user name and password, and then click Next.

🚸 Microsoft Azure Active D	rectory Connect	-	×
Welcome Express Settings Connect to Azure AD Connect to AD DS Configure	Connect to AD DS Inter the Active Directory Domain Services enterprise administrator credentials: USERNAME Services PASWORD Total Services Se		
	Previous		

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

7. Click Install.



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

8. Click Exit.

🚸 Microsoft Azure Active D	irectory Connect –	×
Welcome Express Settings Connect to Azure AD Connect to AD DS Configure	Configuration complete Arure AD Connect configuration succeeded. The synchronization process has been initiated. The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. Learn more	
	Previous	

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

After the synchronization process is started, AD users will be able to log in to Azure.

Verifying the Installation of AD Connect

After you have successfully installed Azure AD Connect, you can verify that the synchronization process is started by signing in to the Azure portal. Also, you can check the last sync time.

- 1. Log in to the Microsoft Azure Management portal.
- 2. On the **Microsoft Azure** window, in the left pane, click **ACTIVE DIRECTORY**, and then in the right pane click on your directory (for example **SFNTdemo**).

Microsoft Azure 🛛 🗸			CREDIT STATUS		•	nsnage Minet in co	
	active direct	ory					
	NRECTORY ACCESS CO	ONTROL NAMESPACES	MULTI-FACTOR AUTH PROVIDE	RS RIGHTS MANAGEME	NT		
	NAME	STATUS	ROLE	SUBSCRIPTION	DATACENTER REGION	COUNTRY OR REGI	p
	SFNTdemo →	🗸 Active	Global Administrator	Shared by all SFNTdemo s	Asla, Europe, United States	Israel	
STREAM ANALYTICS							
MANAGEMENT SERVICES							
ACTIVE DIRECTORY							

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

3. Click the **DIRECTORY INTEGRATION** tab.



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

4. Under integration with local active directory, check the last sync time.

integration with local active directory				
DOMAINS VERIFIED FOR DIRECTORY SYNC	0			
DOMAINS PLANNED FOR SINGLE SIGN-ON	0			
DIRECTORY SYNC	ACTIVATED DEACTIVATED			
LAST SYNC	2 hours ago			

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

Enabling Azure AD Federated Domains

- 1. Log in to the AD FS server machine as a domain administrator.
- 2. Open Windows Azure AD Module for Windows PowerShell.
- 3. At the command prompt, type **Connect-MsolService**, and then press **Enter**.
- 4. On the Enter Credentials window, type your Azure AD administrator username and password, and then click OK.

Mathematical Administrator: Windows Azure A	ctive Directory Module	for Windows Po	werShell -	D X
PS C:\Users\Administrator\Desk	top> Connect-MsolSe	rvice		^ =
	Enter Credentials	? X		
Please enter cre	dentials			
User name:		m.orf V		
Password:	•••••			
				~
	OK	Cancel		

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

- 5. At the command prompt, perform the following steps:
 - a. Type the **Set-MsoIADFSContext -Computer <AD FS machine name>** command and then press **Enter**.
 - b. Type the **Convert–MsolDomainToFederated –DomainName <your domain name>** command and then press **Enter**.



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

- 6. Open the AD FS Management console.
- 7. In the left pane, under Console Root, click AD FS > Trust Relationships > Relying Party Trusts.

In the right pane, **Microsoft Office 365 Identity Platform** (currently, this is the Azure Relying Party's display name) should be listed as a trust.

Console Root	Display Name	Enabled	Туре	Identifier
AD FS	Device Registration Service	Yes	WS-T	um ma-drs sasdo safenetdemos.com
Service	Microsoft Office 365 Identity Platform	Yes	WS-T	um federation: MicrosoftOnline
a 🛅 Trust Relationships				
Claims Provider Trusts				
Relying Party Trusts				
Attribute Stores				
a 🛄 Authentication Policies				
Per Relving Party Trust				

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

Configuring the AD FS Authentication Policy

- 1. On the AD FS Management console, in the left pane, under AD FS, click Authentication Policies.
- 2. In the right pane, click Edit Global Primary Authentication.

AD FS	Authentication Policies		Actions			
3 Service	Authentication Pol	icies Over	ularu		Authentication Policies	
Authentication Policies	Addientication For				Edit Global Primary Authentication	1
Per Relying Party Trust	You can configure primary a	You can configure primary authentication and multi-factor authentication settings globally or per relying party trust.			Edit Global Multi-factor Authentica	
	Learn More				View	
	Configuing Authentical	ion Policies			New Window from Here	
	AD FS Help				C. Patrach	- 1
1						- 1
	Primary Authentica	Primary Authentication				
	Primary authentication is rec global and custom primary a	pured for all users uthentication sets	tying to access applications that use AD FS for authentication. You can use options below to nps.	configure		
	Global Settings					
	Authentication Methods	Extranel	Foma Authentication	Ede		
	Davids & Burlinster	Inhanet	Formulauthentication			
			and detailed			
	Custom Settings			105705		
	Per Balying Party			Manage		
	Web Application Provy			La		
	Multi-factor Auther	ntication				
	You can use options below authentication is required it	to configure multi- there is a match to	actor authentication settings based on users/groups, device, and location data. Multi-factor rany of the specified requirements.			
	Global Settings					
	Requirements	Users/Groups	Not configured	Ede		
		Device	Not configured	1.000		
	100 M 100	Location	Not configured			
	Authentication Methods	6.C	SafeNet Multi Factor Authentication (SMFA)			
	Custom Settings					
	Per Relying Party			Manage		
	Web Application Prov			Edit		

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

3. On the Edit Global Authentication Policy window, on the Primary tab, ensure that Forms Authentication is selected for both Extranet and Intranet.

	Edit Global Authentication Policy	
rimary	Multifactor	
Select users to	authentication methods. By selecting more than one authentication method, you er o have a choice of what method to authenticate with at sign in.	nable
f Integ authen	rated Windows authentication method is specified, it appears as the default tication method on browsers that support Integrated Windows authentication.	
Extran	net	
Intran	Certificate Authentication	
		_

Ø

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

NOTE: If you want to use CBA as the only authentication mechanism, ensure that only **Certificate Authentication** is selected for both **Extranet** and **Intranet**. Refer to "Appendix: Configuring AD FS with CBA for Single Authentication" on page 20.

- 4. Click the **Multi-factor** tab and then perform the following steps:
 - a. Under Users/Groups, add users and/or groups for which MFA will be required.
 - b. Under Locations, select Extranet and/or Intranet, according to your preferred configuration.
 - c. Select Certificate Authentication as an additional authentication method.
 - d. Click OK.

nimary	Multi-factor			
Configur	e multi factor a	uthentication (MFA) settin	gs.	
Users/	Groups			
MFA is	required for the	e following users and grou	ps:	
SFN	TDEMO\Doma	in Users		<u>A</u> dd
				Bemove
L				
Device	8			
MFA is	required for the	e following devices:		
Un	nregistered dev	ices		
Re	egistered devic	es		
Locatio	ons			
MFA is	required when	accessing applications fro	om the following location	าร:
✓ Ex	tranet			
🖌 Int	ranet			
Select a o enable	dditional authe e MFA:	ntication methods. You m	ust select at least one of	f the following method
✓ Certi	ficate Authenti	cation		
What is	multi-factor aut	hentication?		

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

Running the Solution

1. In a web browser, open the following URL:

https://account.activedirectory.windowsazure.com

2. On Azure Access Panel login window, enter your AD user name (for example, **bob@safenetdemos.com**), and then click **Continue**.

and a second as	
	Microsoft Azure
Cloud optimize your business	Type the email address of the account you want to sign in with.

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

3. You will be redirected to your organization's login page. Enter your AD password and then click **Sign in**.

adfs.sfntdemo.com
Sign in with your organizational account
bob@sfntdemo.com Þassword
Sign in

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

- 4. The browser displays all the certificates available on the machine. Select the end user certificate that is added on the SafeNet USB token.
- 5. On the **Confirm Certificate** window, click **OK**.

Windows Secu	rity
Confirm (Confirm this click Cancel.	Certificate certificate by clicking OK. If this is not the correct certificate,
	bob Issuer: sfntdemo-AD-CA Valid From: 10/21/2015 to 10/20/2016 Click here to view certificate prope]
	OK Cancel

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

6. On the SafeNet Authentication Client login window, enter the token password, and then click OK.

SafeNet	SafeNet	Authentication Client) 15664UGS 5160 1566455 616• 01 15 HS F 5
Enter the Token Pas	sword		
Token Name:		My Token	
Token Password:		[
		Current Language: EN	
This is an unlicer	sed copy for e	valuation use only.	

After successful authentication, you are redirected to access the Azure Access Panel.

You can now use the applications (for which access is given) without any further authentication (using the SSO abilities of Azure).

Microsoft Azure	bob@sfntdemo.com	SFNTdemo ?
applications	profile	
Salesforce	٩	
Showing 1 of 1		

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

Appendix: Configuring AD FS with CBA for Single Authentication

- 1. On the AD FS Management console, in the left pane, under AD FS, click Authentication Policies.
- 2. In the right pane, click Edit Global Primary Authentication.

AD FS	Authentication Policies				Actions
bervice Test Balationships Service Service	Authentication Poli		viow		Authentication Policies
 Authentication Policies Per Relying Party Trust 				Edit Global Primary Authentication	
	You can configure primary authentication and multi-factor authentication settings globally or per relying party trust.			Edit Global Multi-factor Authentica	
	Learn More			View	
	Configuring Authenticatio	n Policies			New Window from Here
	AD FS Help				Refresh
	<u>.</u>				
	Primary Authentica	tion			III Help
	Primary authentication is requi global and custom primary au	ired for all users (thentication setti	trying to access applications that use AD FS for authentication. You can use options below to ngs.	o configure	
	Global Settings	-	-	1	
	Authentication Methods	Extranet	Forms Authentication	Edit	
	Device Authentication	manor	Not enabled		
	Custom Cattings				
	Par Balving Partu			Managa	
	Web Application Proxy			Edit	
	Multi-factor Authen	tication	inster authantication nations based on unare lorsume classica, and location claim. Multifactors		
	authentication is required if th	ere is a match fo	r any of the specified requirements.		
	Global Settings				
	Requirements	Users/Groups	Not configured	Edit	
	19	Device	Not configured		
		Location	Not configured		
	Authentication Methods		SafeNet Multi Factor Authentication (SMFA)		
	Custom Settings				
	Per Relying Party			Manage	
	Web Application Proxy			Edit	

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

3. On the Edit Global Authentication Policy window, on the Primary tab, ensure that Certificate Authentication is selected for both Extranet and Intranet.

rimary	Multi-factor		
Select users to If Integ authen	authentication have a choin rated Window tication metho	methods. By selecting more than one authentication method, you ena ce of what method to authenticate with at sign in. s authentication method is specified, it appears as the default d on browsers that support integrated Windows authentication.	ble
	oms Authent	cation	-
~	Certificate Aut	nertication	
Intran	et		
Intran	et orms Authent	cation	
	et oms Authent Vindows Auth	cation entication enticstion	
	et Toms Authent Windows Auth Certificate Auth	cation entication mentication	
Intran	et orms Authent Vindows Auth Certificate Auth	cation entication ventication	

(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		
Address	Gemalto, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA		
Phone	United States	1-800-545-6608	
	International	1-410-931-7520	
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to nanage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.		