SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for MS Azure AD

gemalto
security to be free

Document Part Number: 007-013448-001, Rev. A

Release Date: March 2016

Contents

Third-Party Software Acknowledgement 4
Description 4
Applicability 5
Environment 5
Audience 5
CBA Flow using SafeNet Authentication Client 5
Prerequisites 6
Supported Tokens in SafeNet Authentication Client 6
Configuring MS Azure AD and AD FS 7
    Adding a Domain to Azure 7
    Syncing the Domain to Azure 10
    Verifying the Installation of AD Connect 14
    Enabling Azure AD Federated Domains 15
    Configuring the AD FS Authentication Policy 17
Running the Solution 18
Appendix: Configuring AD FS with CBA for Single Authentication 20
Support Contacts 21

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:

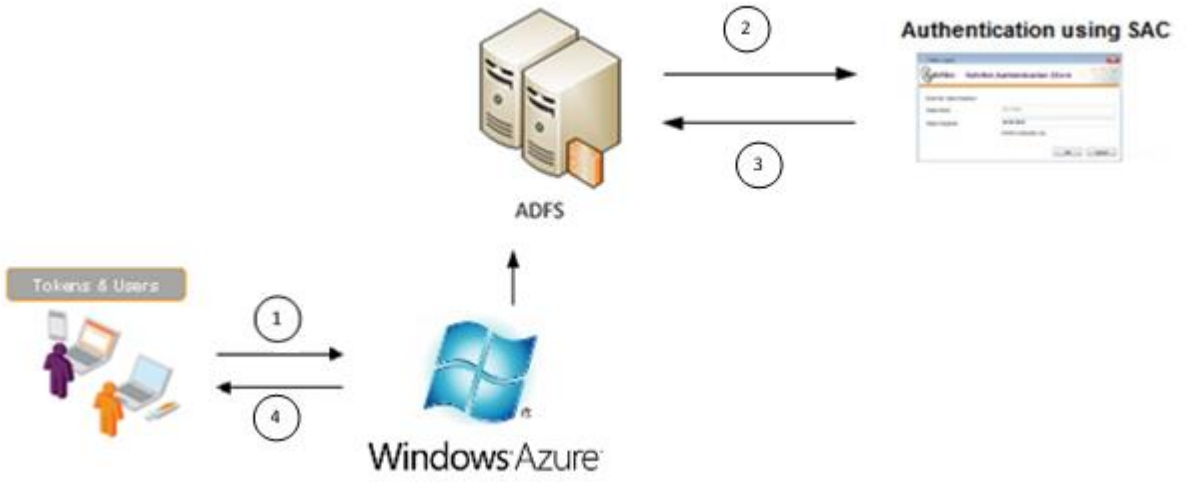
- **SafeNet Authentication Client (SAC)**—Version 9.0
- **MS Azure AD**—On cloud
- **AD FS**—On Windows Server® 2012 R2

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 eToken Rescue

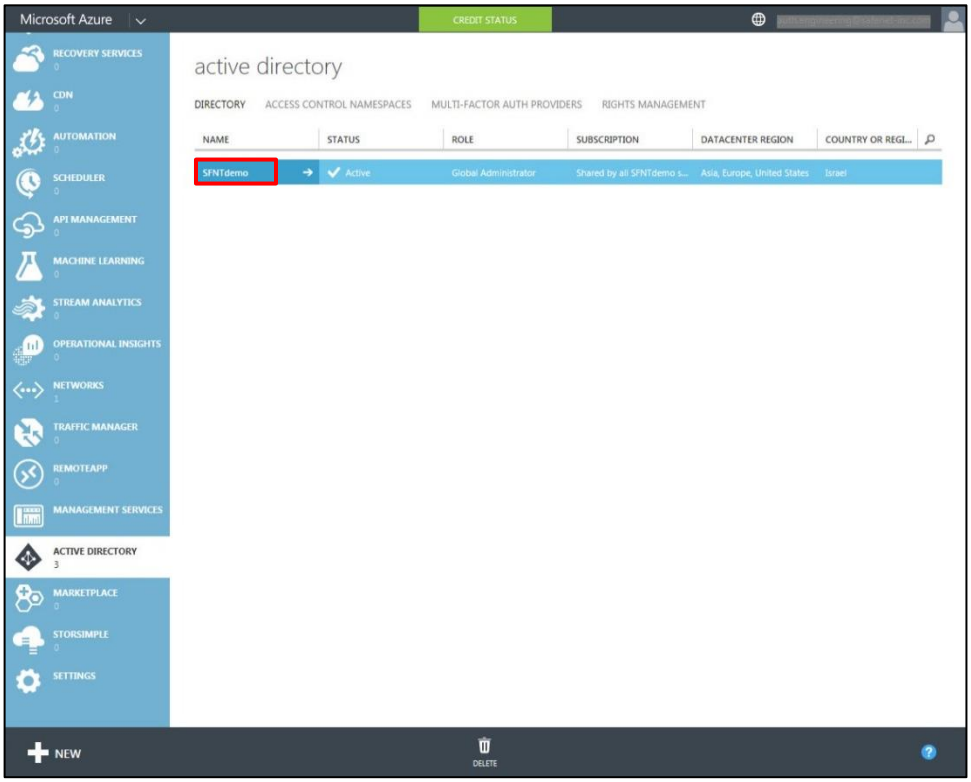
Configuring MS Azure AD and AD FS

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

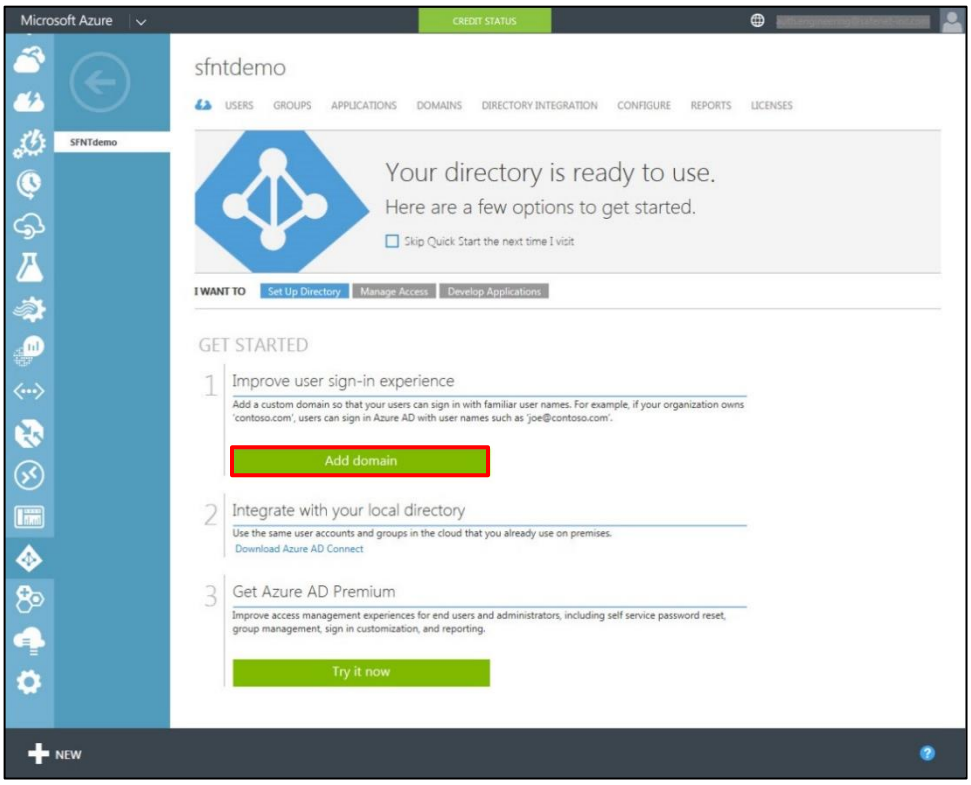
Adding a Domain to Azure

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**).



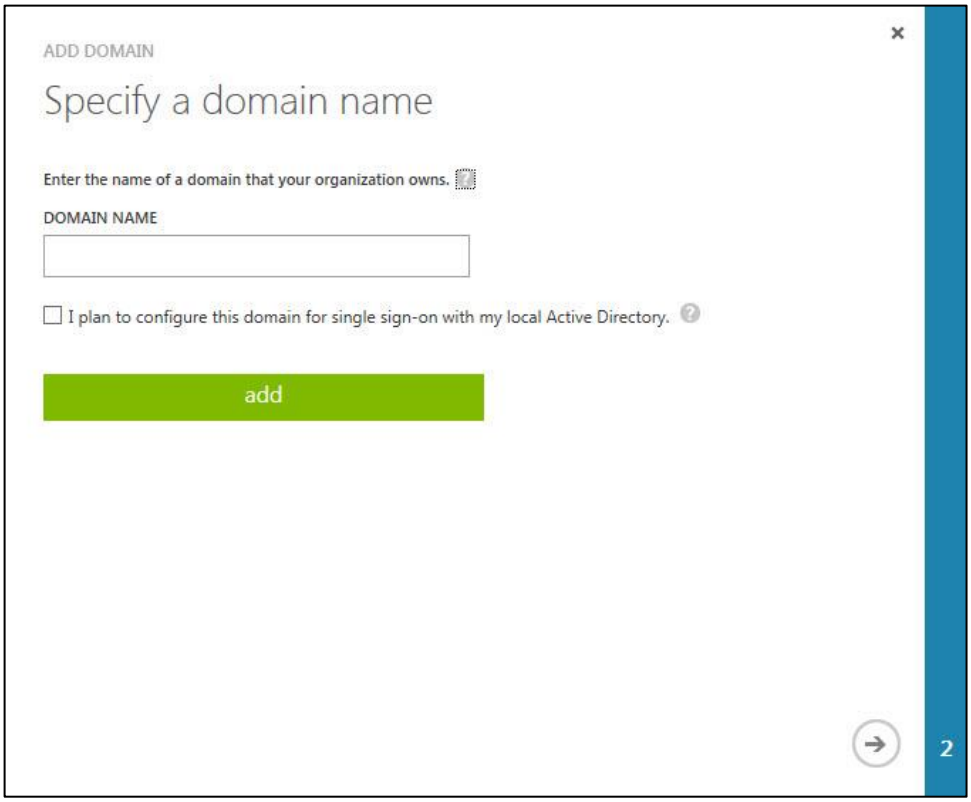
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. Click **Add domain**.



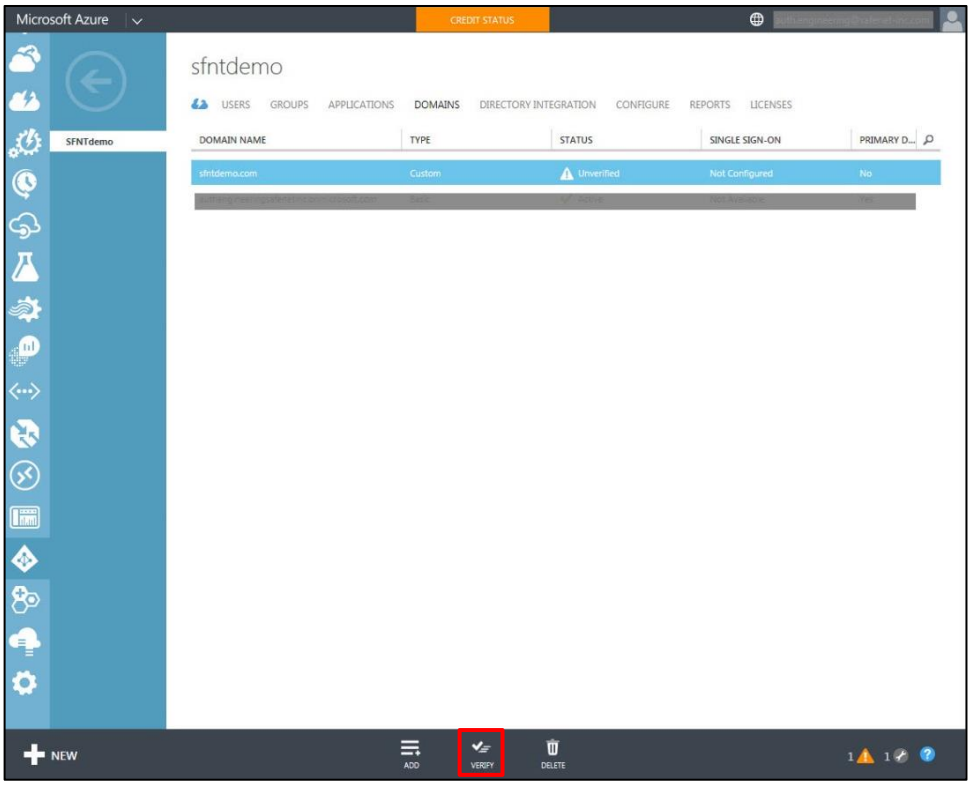
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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



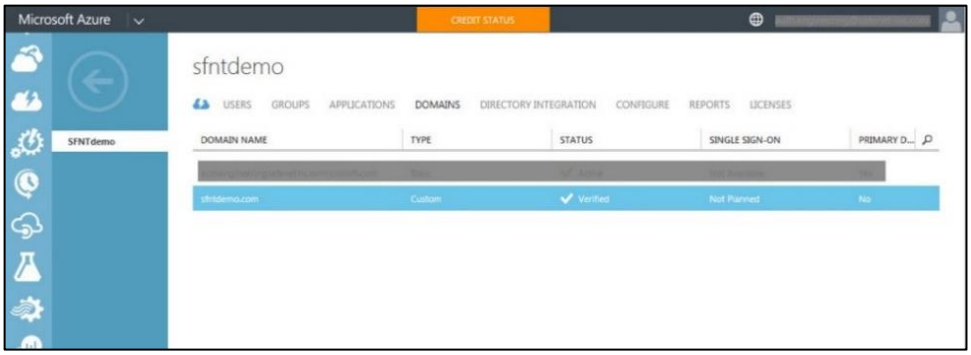
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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.



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

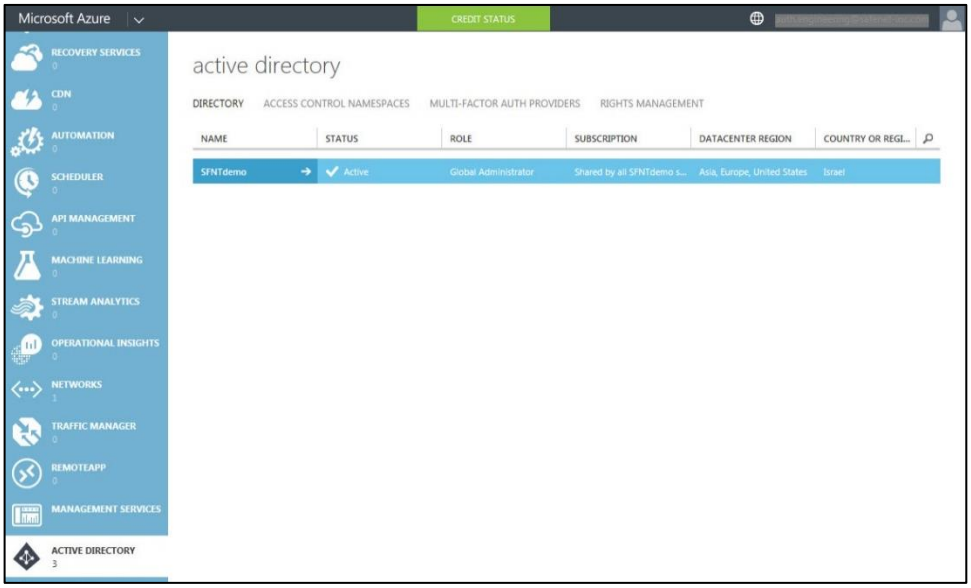
The new domain is now verified and ready for use.



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

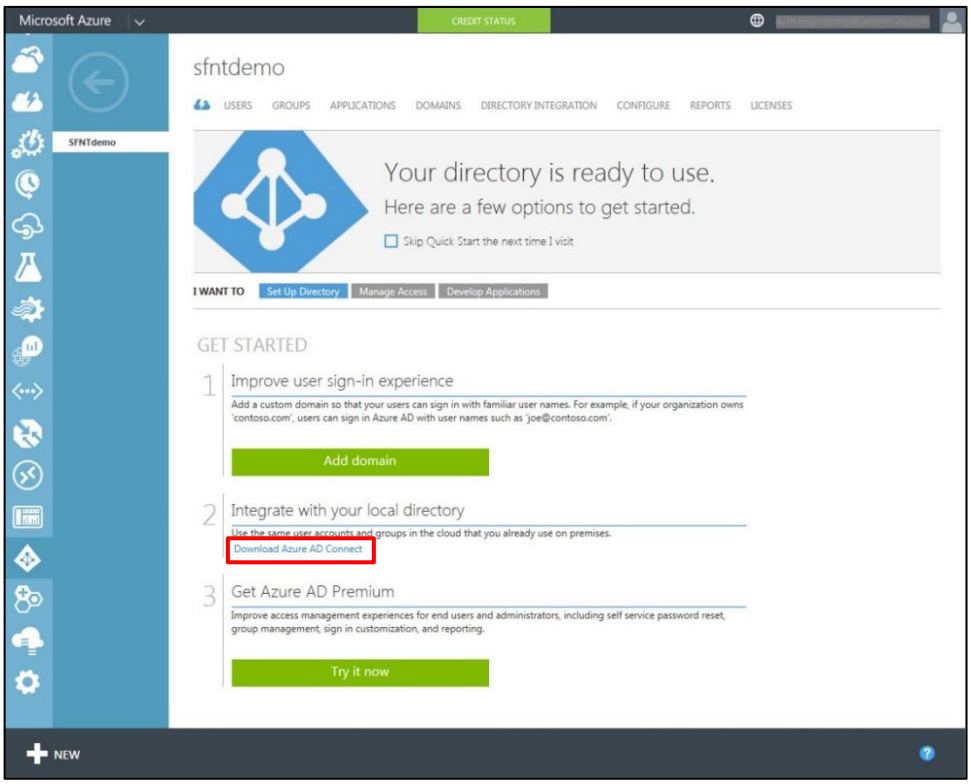
Syncing the Domain to Azure

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**).



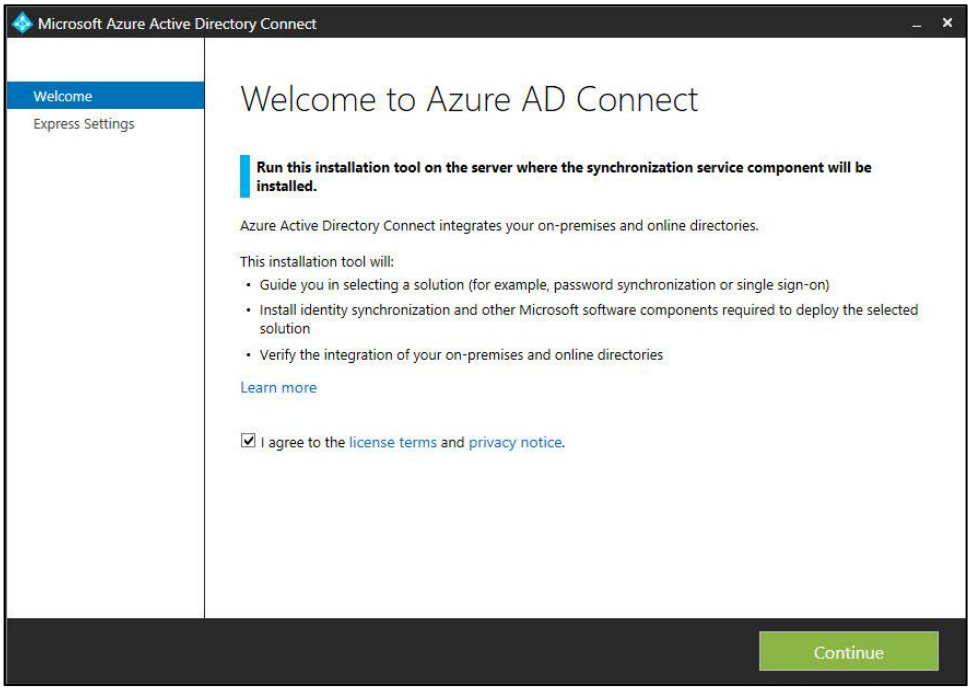
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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



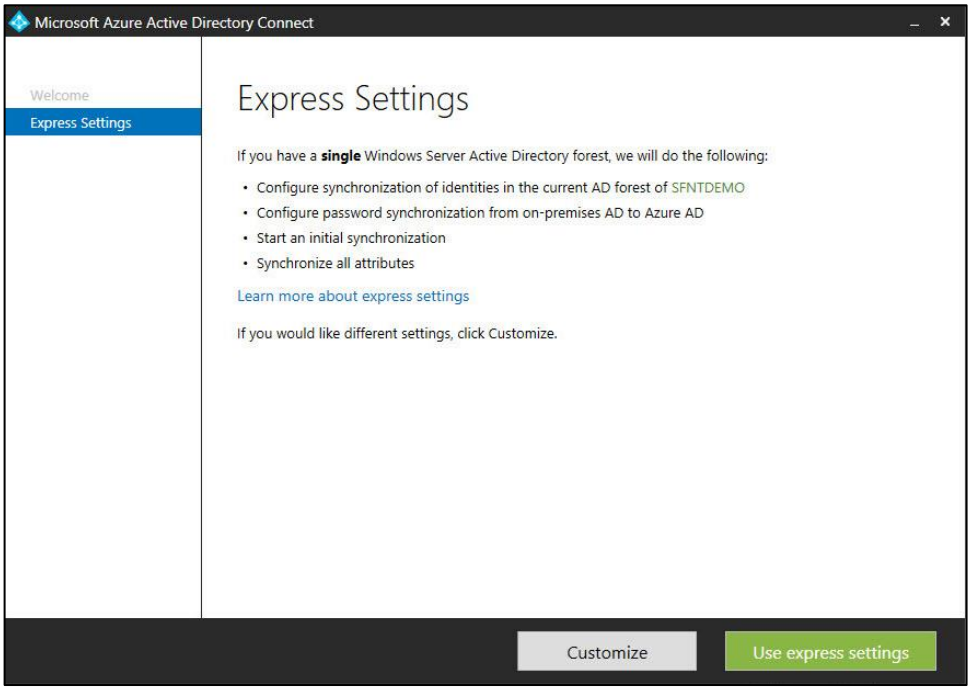
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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**.



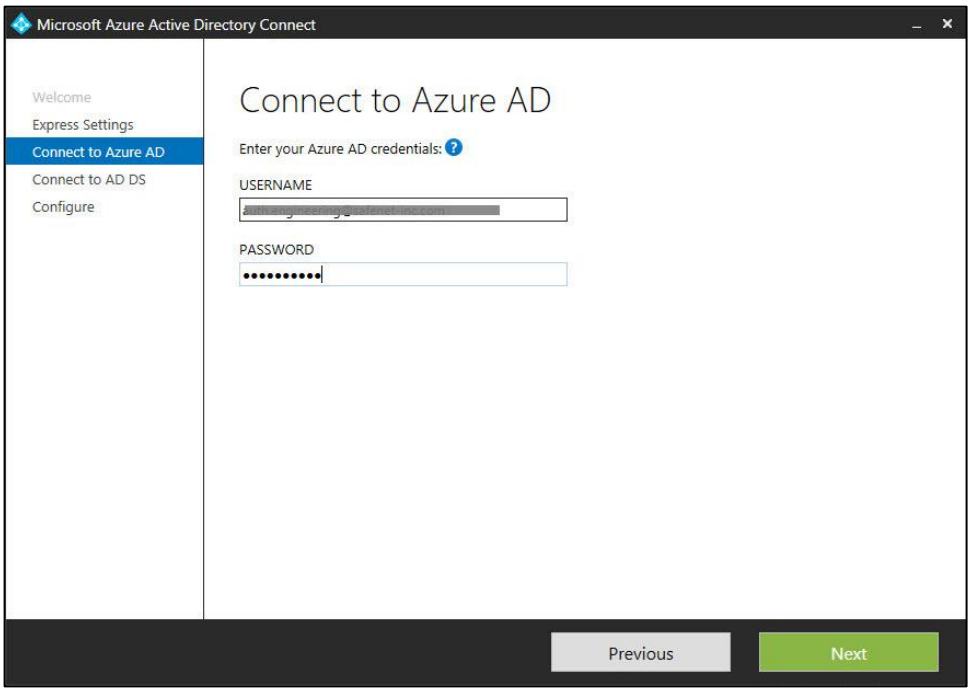
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. Click **Use express settings**.



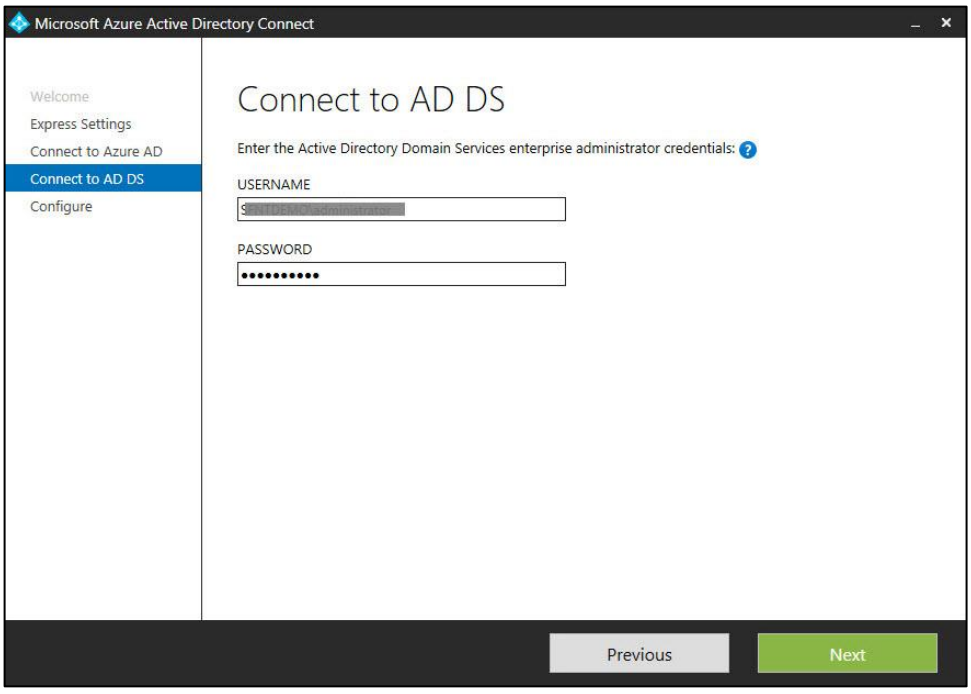
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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



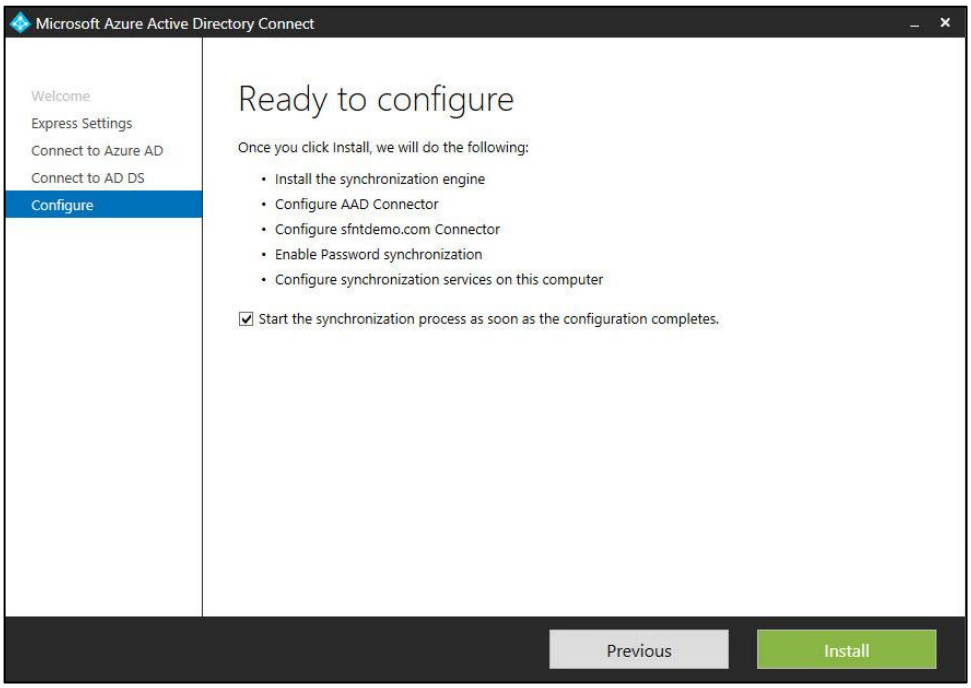
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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



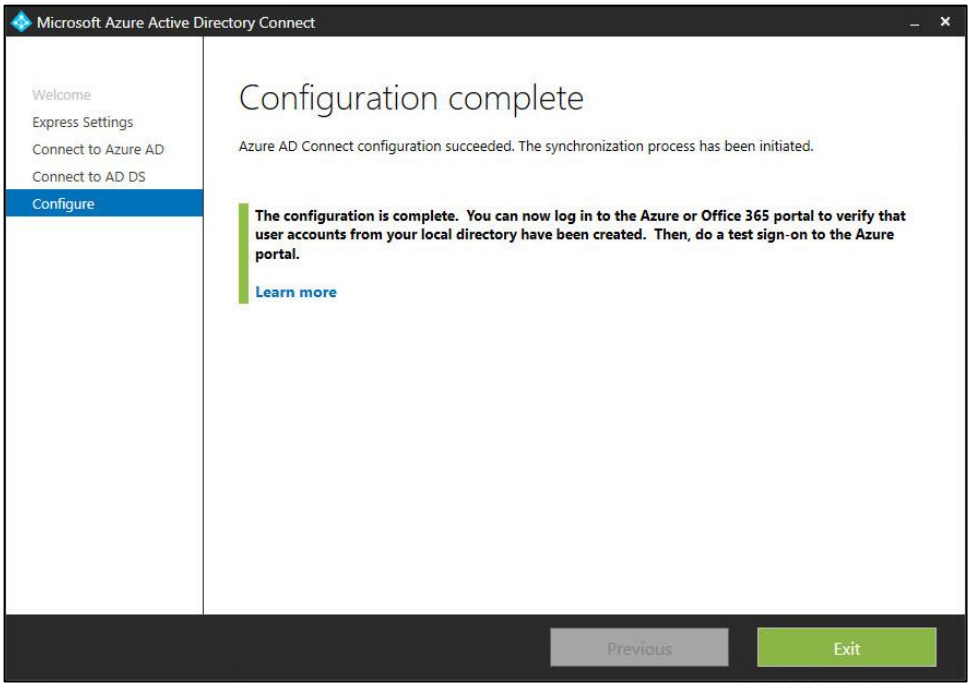
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

7. Click **Install**.



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

8. Click **Exit**.



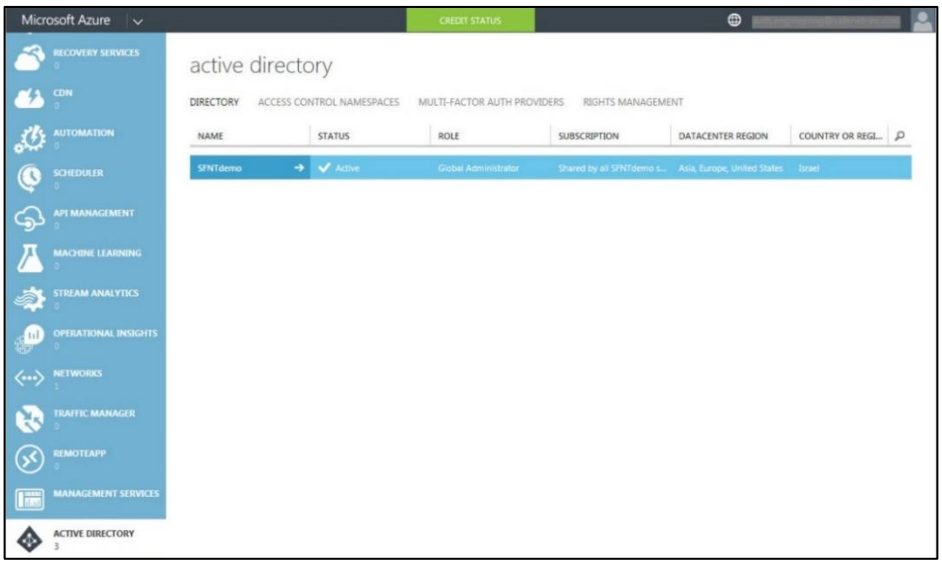
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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

Verifying the Installation of AD Connect

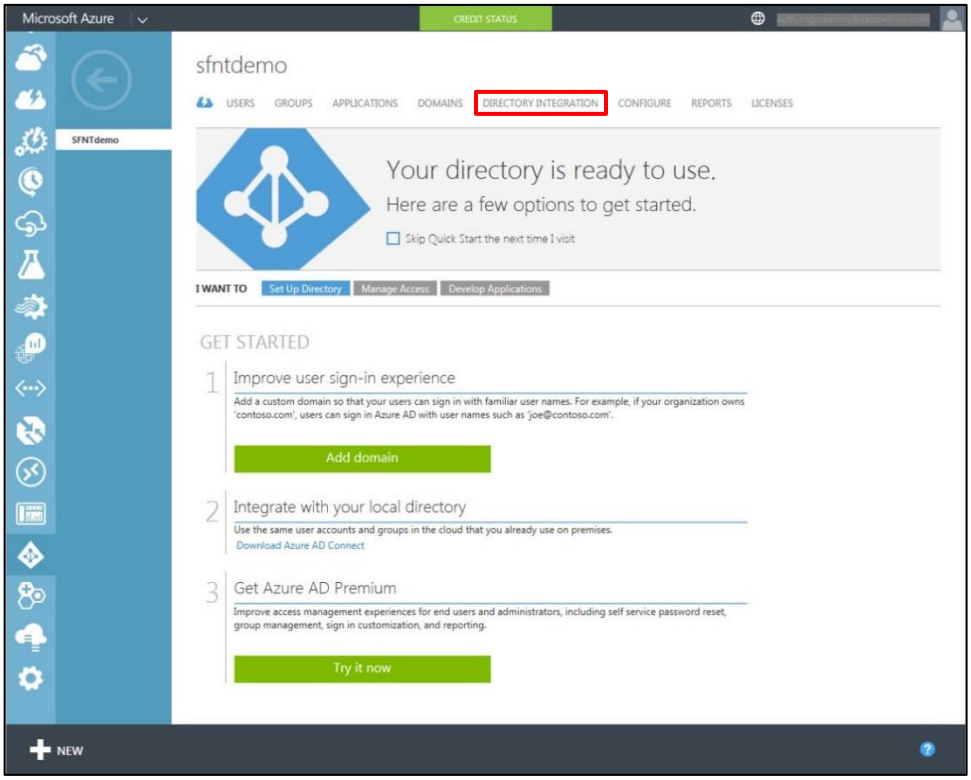
After you have successfully installed Azure AD Connect, you can verify that the synchronization process is started by signing in to the Azure portal. Also, you can check the last sync time.

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**).



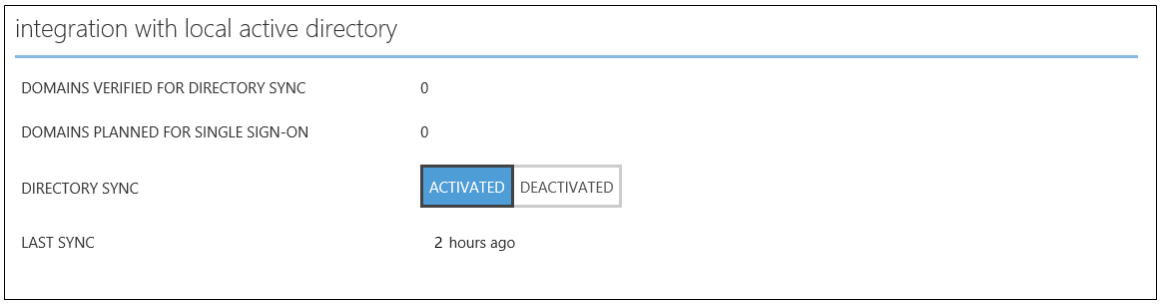
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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.



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

Enabling Azure AD Federated Domains

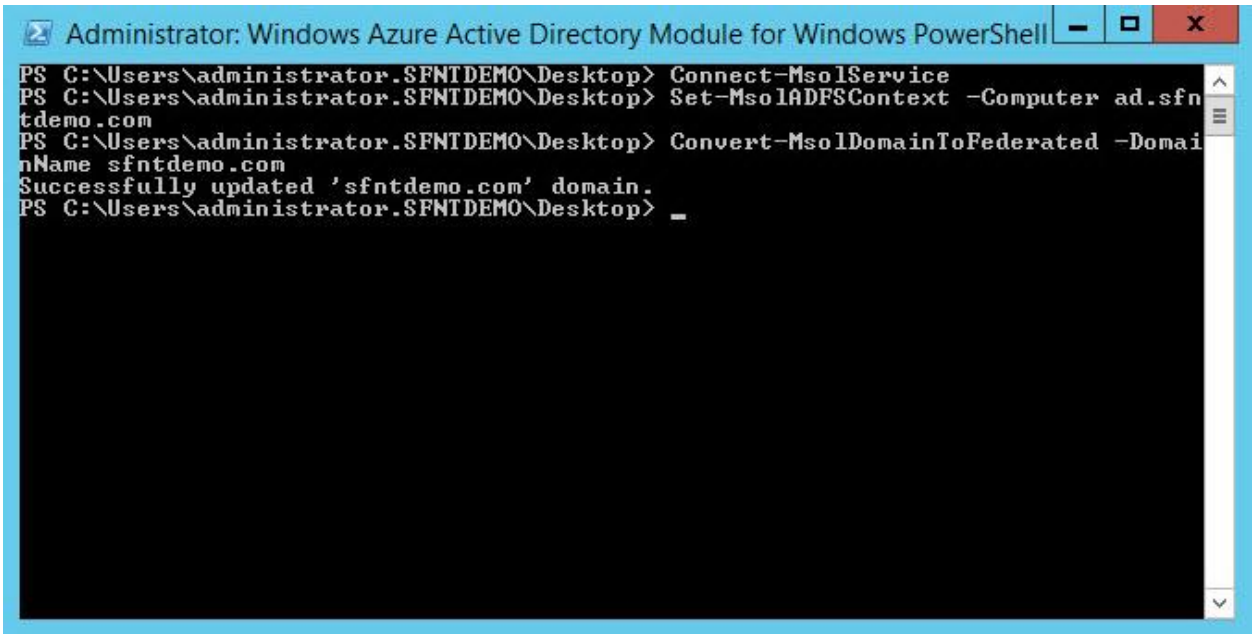
1. Log in to the AD FS server machine as a domain administrator.
2. Open Windows Azure AD Module for Windows PowerShell.
3. At the command prompt, type **Connect-MsolService**, and then press **Enter**.
4. On the **Enter Credentials** window, type your Azure AD administrator username and password, and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

(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–MsolADFSContext –Computer <AD FS machine name>** command and then press **Enter**.

   b. Type the **Convert–MsolDomainToFederated –DomainName <your domain name>** command and then press **Enter**.

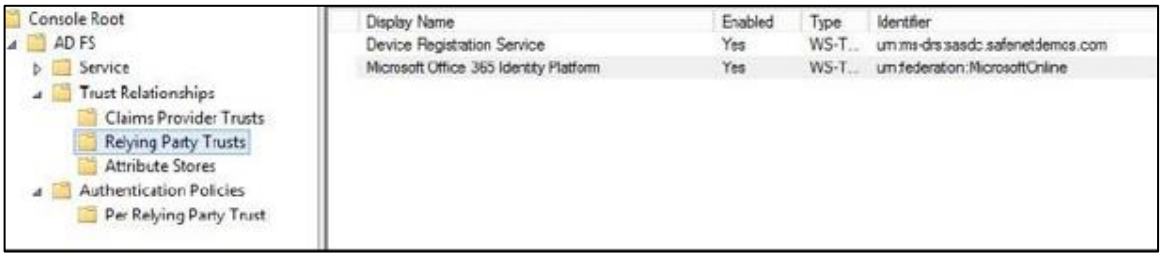


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

6. Open the AD FS Management console.

7. In the left pane, under **Console Root**, click **AD FS > Trust Relationships > Relying Party Trusts**.

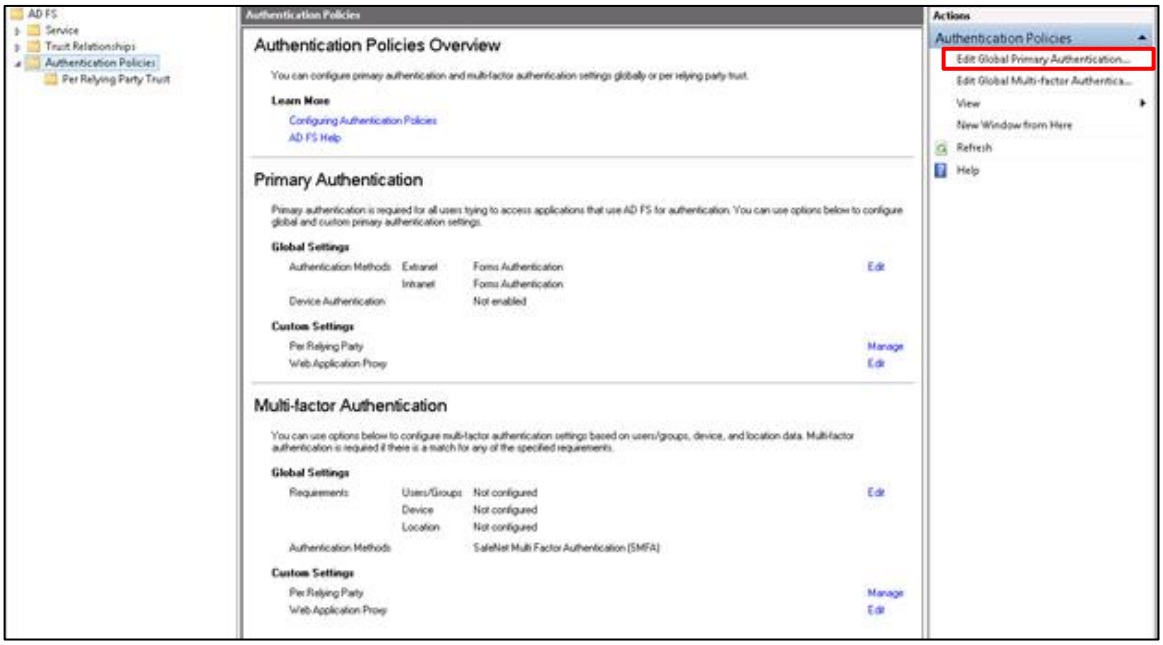
   In the right pane, **Microsoft Office 365 Identity Platform** (currently, this is the Azure Relying Party's display name) should be listed as a trust.



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

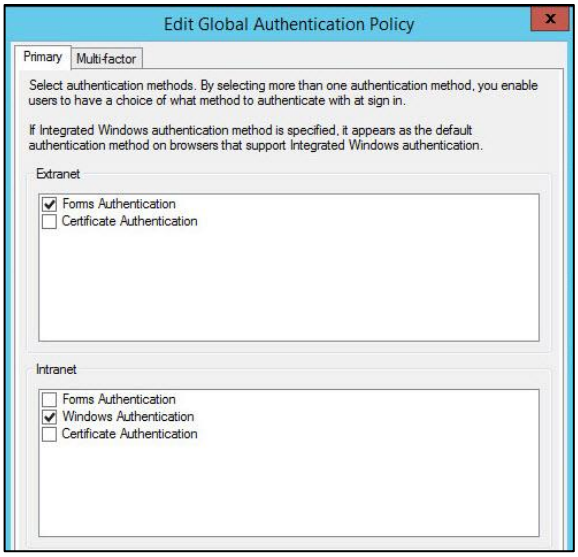
Configuring the AD FS Authentication Policy

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**.



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

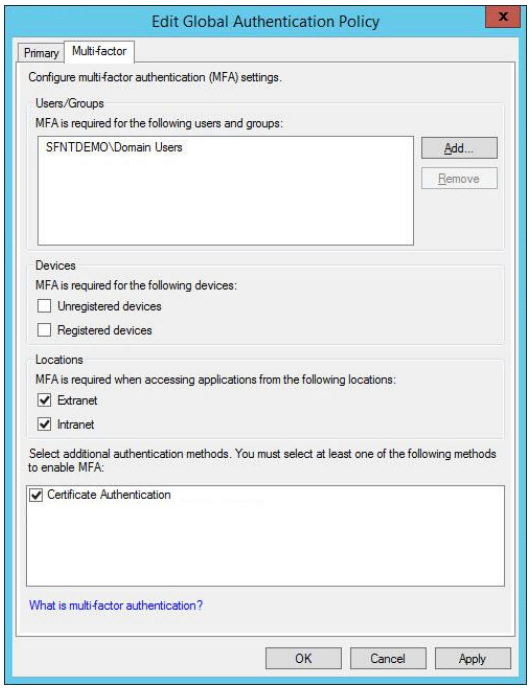
3. On the **Edit Global Authentication Policy** window, on the **Primary** tab, ensure that **Forms Authentication** is selected for both **Extranet** and **Intranet**.



(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**.



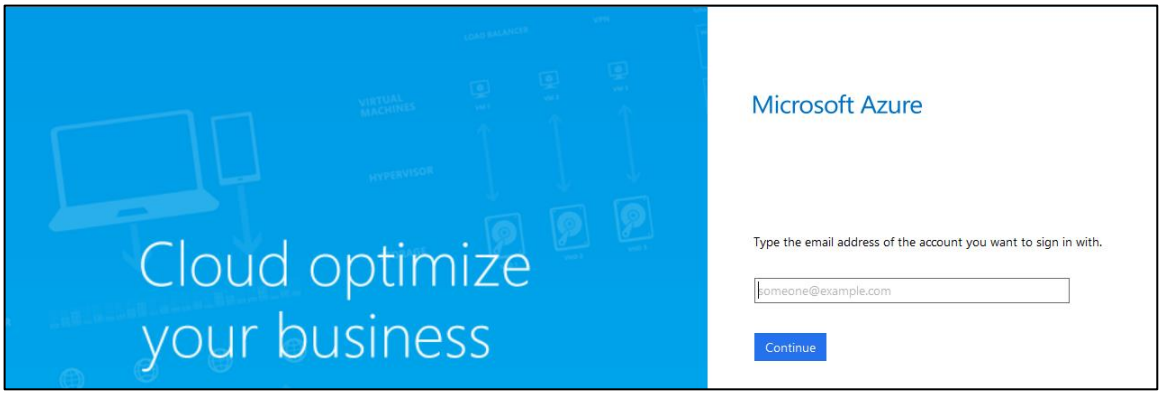
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

Running the Solution

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

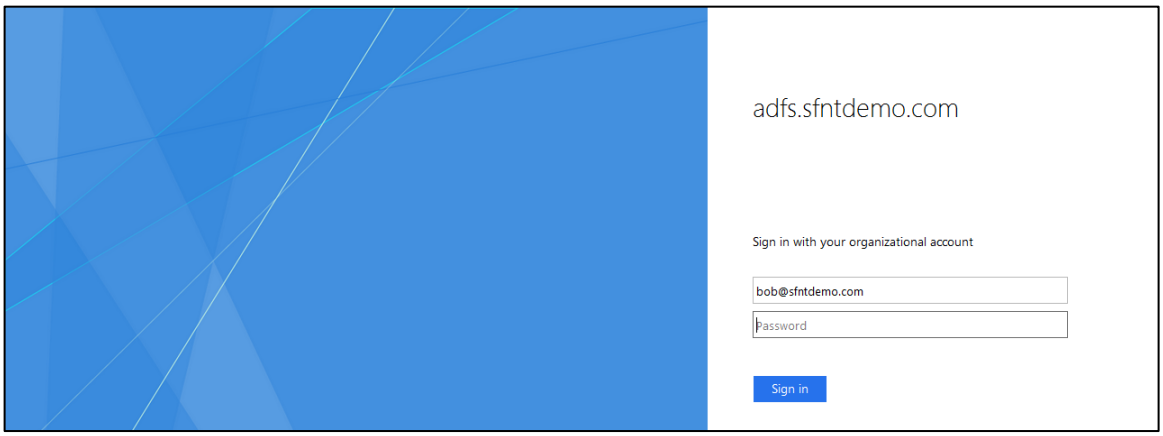
   https://account.activedirectory.windowsazure.com

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



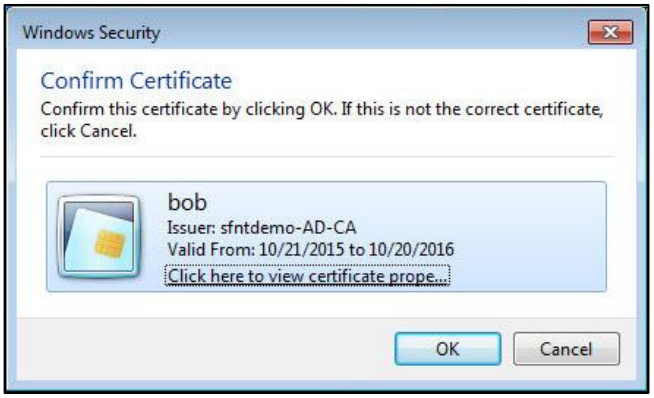
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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



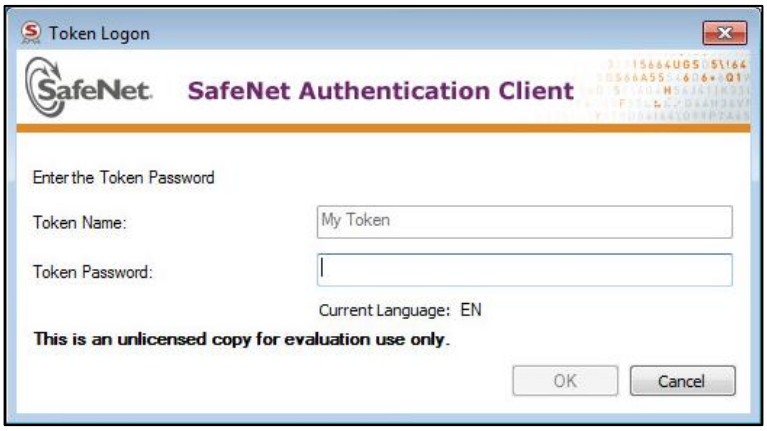
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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**.



(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**.



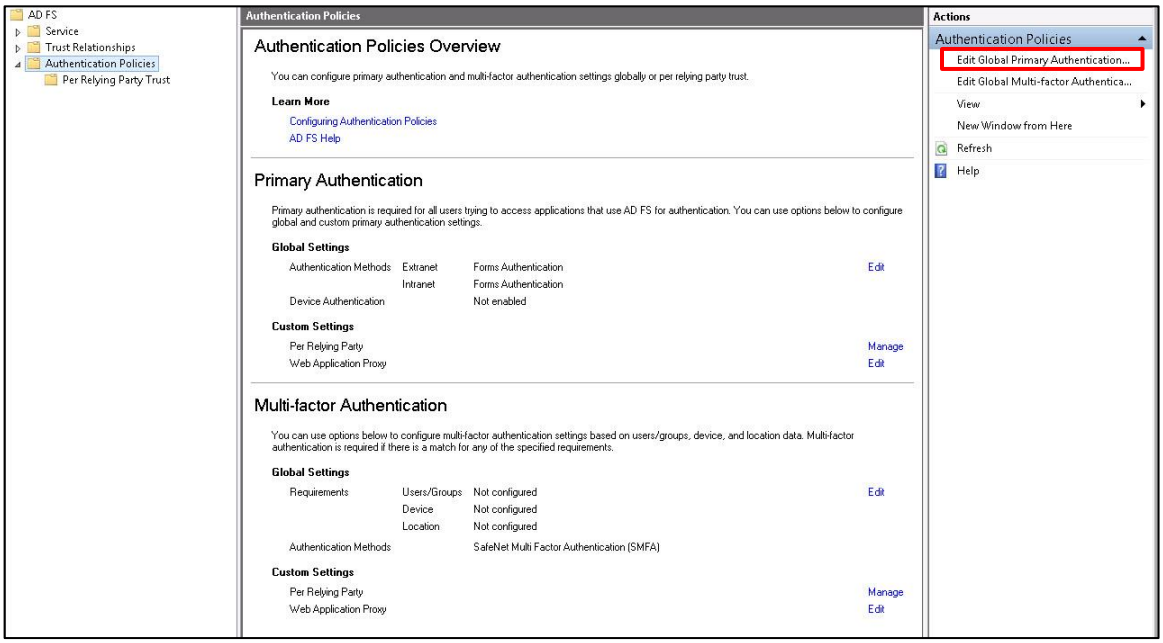
After successful authentication, you are redirected to access the Azure Access Panel.

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

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

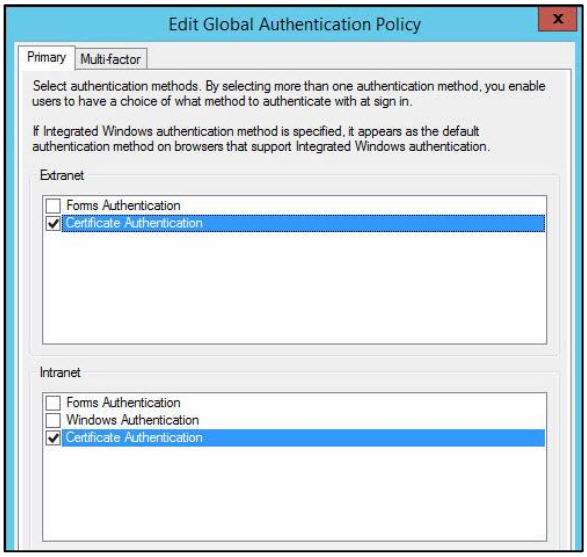
Appendix: Configuring AD FS with CBA for Single Authentication

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**.



(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**.



(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 manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	