

SafeNet Authentication Client Integration Guide

Using SafeNet Authentication Client CBA for Office 365 ProPlus

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: 007-013447-001, 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 Office 365 ProPlus and AD FS.....	7
Enabling Office 365 Federated Domains	7
Configuring the AD FS Authentication Policy.....	8
Downloading and Installing Office 365 ProPlus	10
Enabling Modern Authentication for Office 365 ProPlus	11
Running the Solution	11
Signing In to Outlook 2013.....	11
Signing In to OneDrive for Business 2013	14
Appendix A: Obtaining the Office365 SharePoint URL	17
Appendix B: Configuring AD FS with CBA for Single Authentication	18
Support Contacts	19

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Office 365 ProPlus.

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*.

Office 365 ProPlus is a productivity software (including Word, PowerPoint, Excel, Outlook, OneNote, Publisher, Access, and Lync) that is installed on your desktop or laptop computer. It is a user-based service that allows users to access Office experiences on up to five PCs or Macs, and on their mobile devices. Traditional Office installations were tied to the computers they were installed on. Office 365 ProPlus enables flexible new deployment options that IT and/or individual users can choose from to install Office.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Office 365 ProPlus using SafeNet tokens.

It is assumed that the Office 365 ProPlus environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Office 365 ProPlus 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
- **Office 365 ProPlus**—Including the Office 365 account
- **AD FS**—On Windows Server® 2012 R2

Audience

This document is targeted to system administrators who are familiar with Office 365 ProPlus, 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 Office 365 ProPlus. 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 Office 365 ProPlus, accepting or rejecting the user's authentication request.
4. The user is granted or denied access to Office 365 ProPlus.

Prerequisites

Before implementing certificate-based authentication for Office 365 ProPlus 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 Office 365 ProPlus.

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 Office 365 ProPlus and AD FS

Configuring Office 365 ProPlus and AD FS requires the following:

- Enabling Office 365 Federated Domains, page 7
- Configuring the AD FS Authentication Policy, page 8
- Downloading and Installing Office 365 ProPlus, page 10
- Enabling Modern Authentication for Office 365 ProPlus, page 11

Enabling Office 365 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, enter 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.)

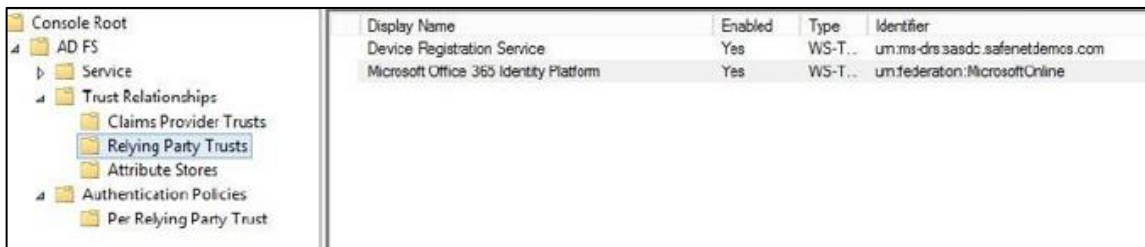
5. At the command prompt, perform the following steps:
 - a. Type **Set-MsolADFSContext –Computer <AD FS machine name>**, and then press **Enter**.
 - b. Type **Convert-MsolDomainToFederated –DomainName <your domain name>**, and then press **Enter**.

```

Administrator: Windows Azure Active Directory Module for Windows PowerShell
PS C:\Users\administrator.SFNTDEMO\Desktop> Connect-MsolService
PS C:\Users\administrator.SFNTDEMO\Desktop> Set-MsolADFSContext -Computer ad.sfn
tdemo.com
PS C:\Users\administrator.SFNTDEMO\Desktop> Convert-MsolDomainToFederated -Domain
Name sfntdemo.com
Successfully updated 'sfntdemo.com' domain.
PS C:\Users\administrator.SFNTDEMO\Desktop> _
  
```

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

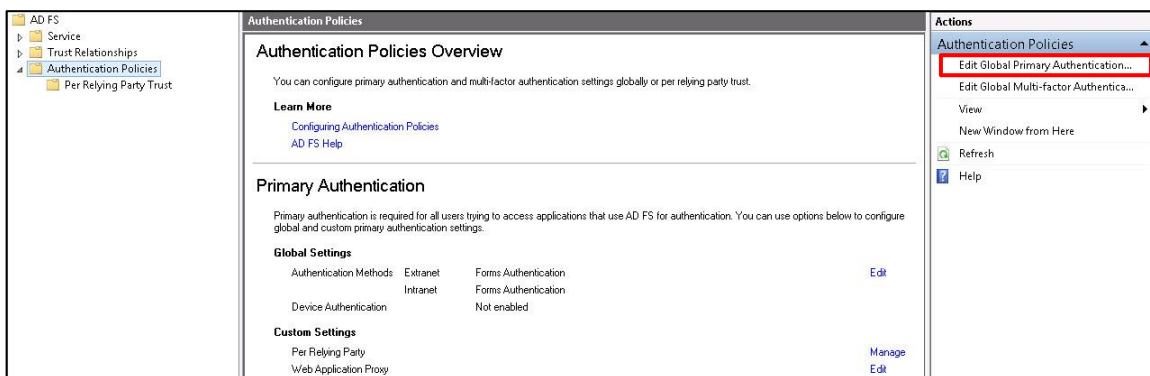
6. Open the ADFS Management console.
7. In the left pane, under **Console Root**, click **AD FS > Trust Relationships > Relying Party Trusts**.
In the right pane, **Microsoft Office 365 Identity Platform** should be listed as a trust.



(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**.

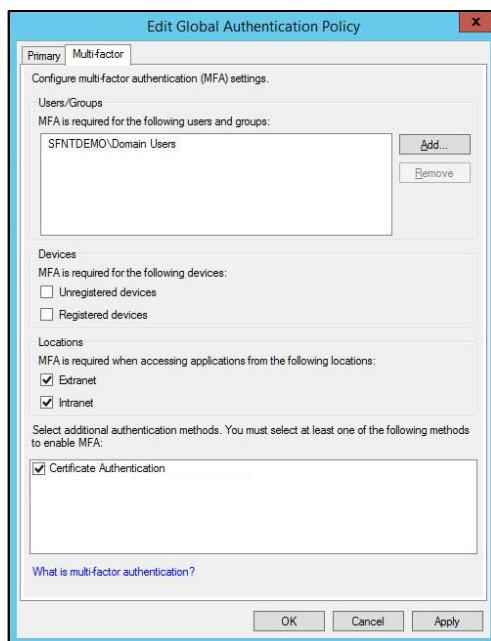


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)



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 B: Configuring AD FS with CBA for Single Authentication” on page 18.

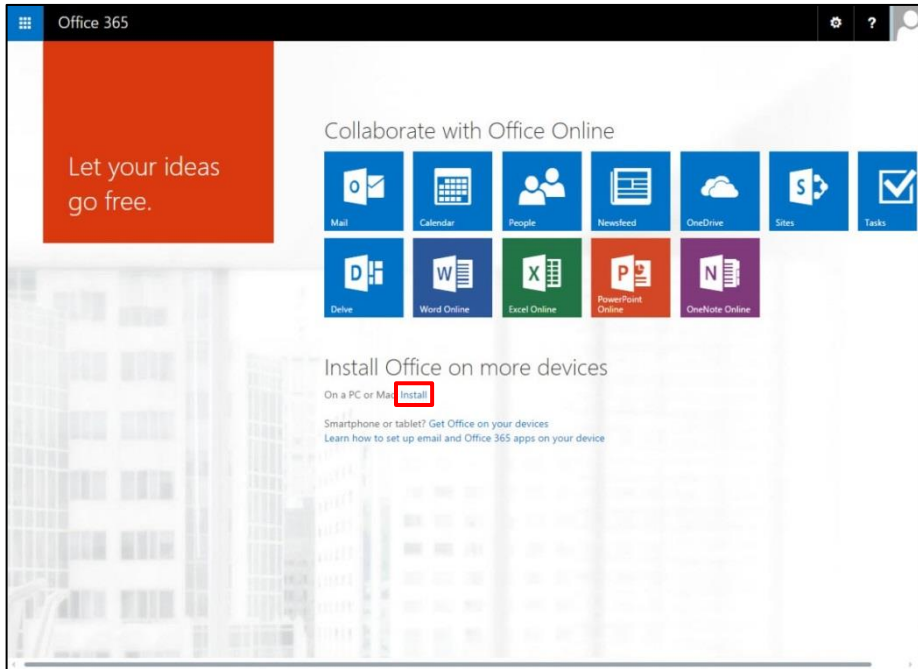
4. On the **Multi-factor** tab, perform the following steps:
 - a. Under **Users/Groups**, add users and/or groups for which MFA will be required.
 - b. Under **Locations**, select **Extranet** and/or **Intranet**, according to your preferred configuration.
 - c. Select **Certificate Authentication**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



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

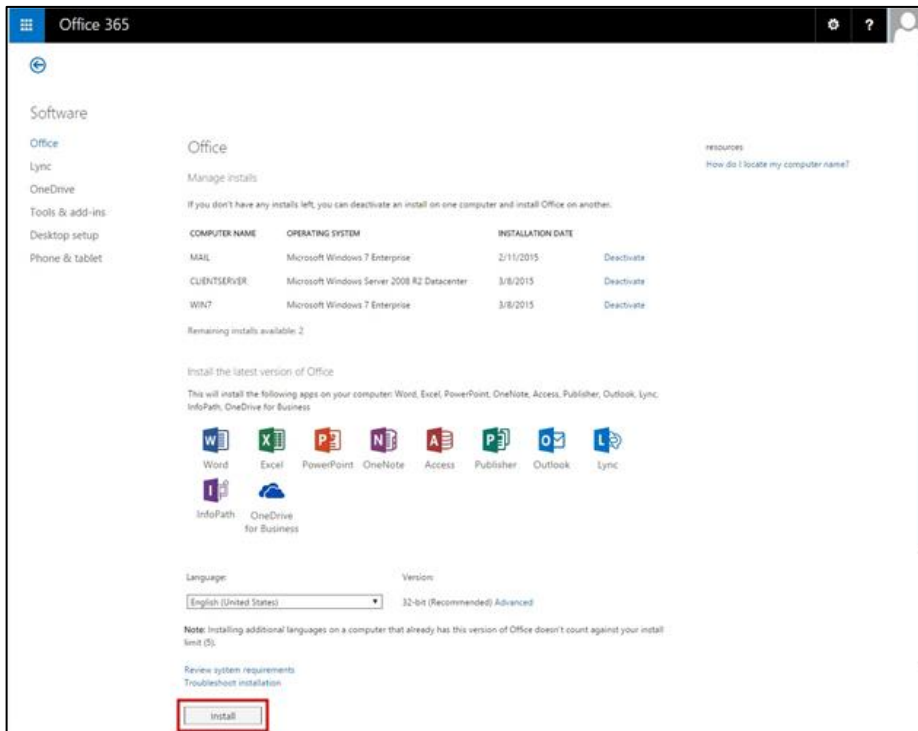
Downloading and Installing Office 365 ProPlus

1. Log in to your Office 365 account.
2. On the Office 365 account console, under **Install Office on more devices**, click **Install**.



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

3. Click **Install** to download the installation file of Office 365 ProPlus.



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

- Double-click the downloaded file to start the installation process.



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

Enabling Modern Authentication for Office 365 ProPlus

To enable modern authentication on a Windows machine that has Office ProPlus installed on it, set the following registry keys:

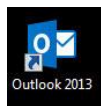
Registry Key	Type	Value
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL	REG_DWORD	1
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Version	REG_DWORD	1
HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Debug\TCOTrace	REG_DWORD	3

After you have set the registry keys, you can set Office 2013 devices apps to use MFA with Office 365.

Running the Solution

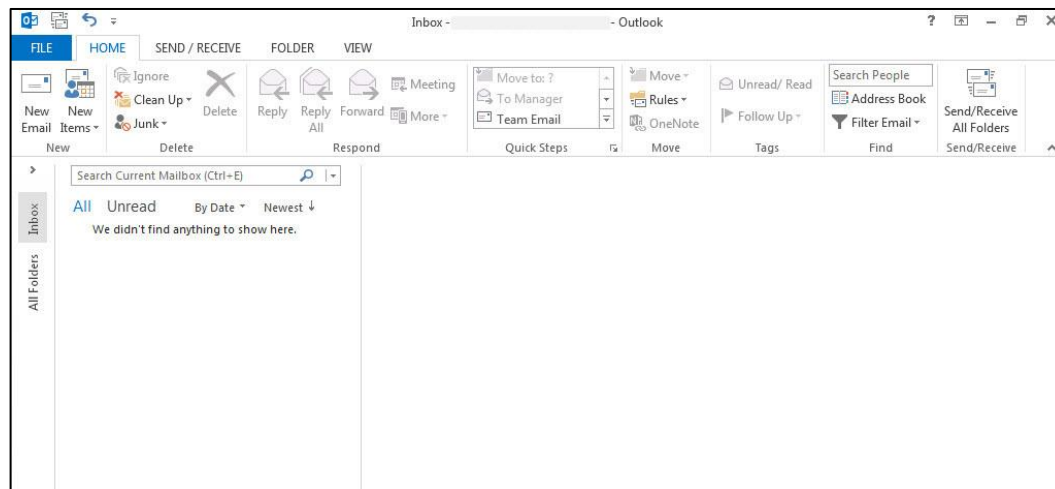
Signing In to Outlook 2013

- Double-click the **Outlook 2013** icon.



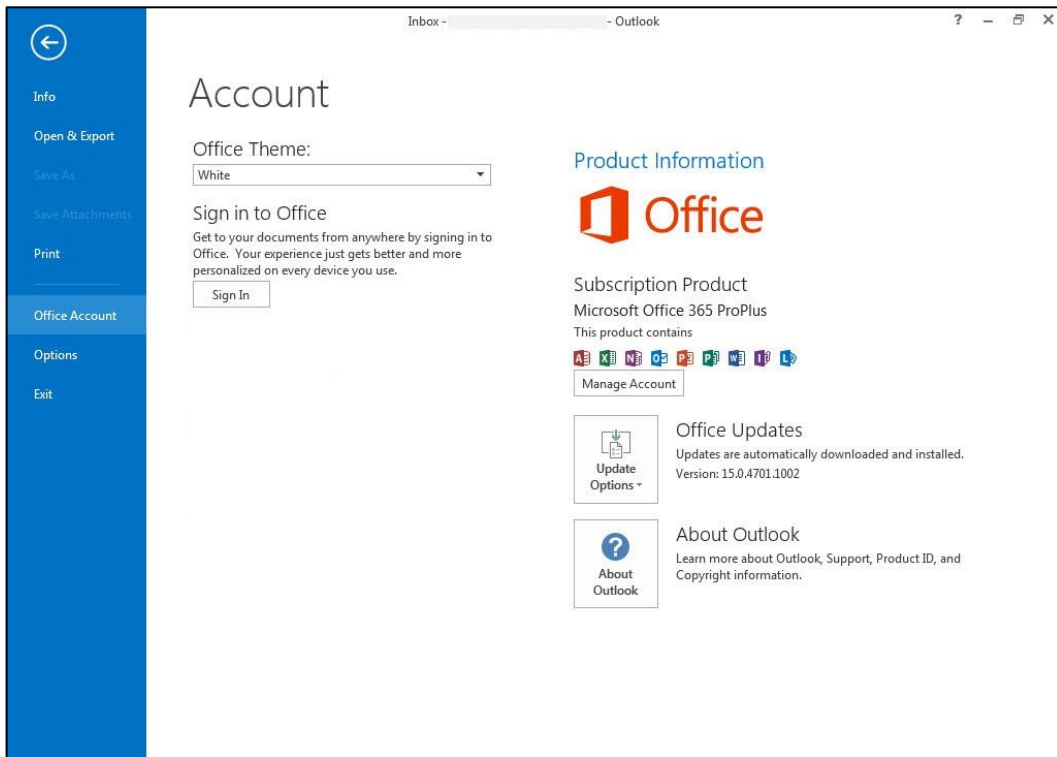
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

- Outlook 2013 is launched. Click the **File** tab.



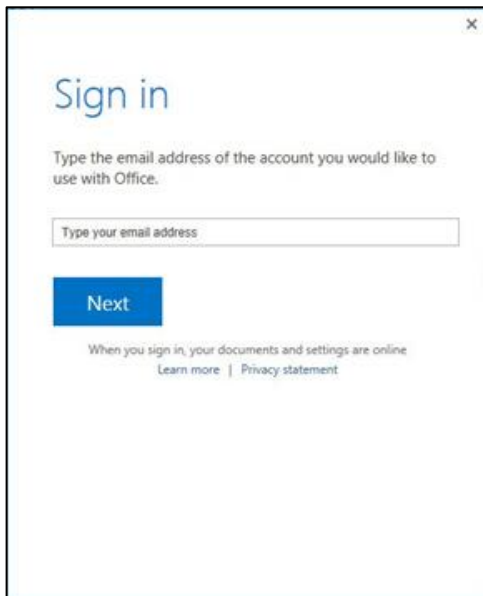
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. In the left pane, click **Office Account**. Then, in the right pane, click **Sign In** to sign in to your Office 365 account.



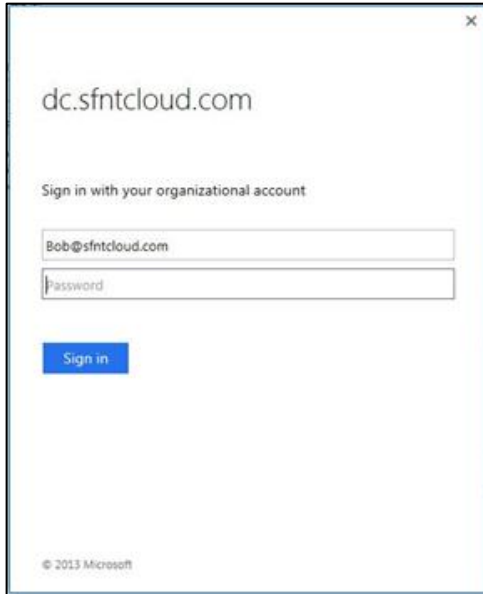
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. On the **Sign in** window, enter your AD user name (for example, **Bob@sfntcloud.com**), and then click **Next**.



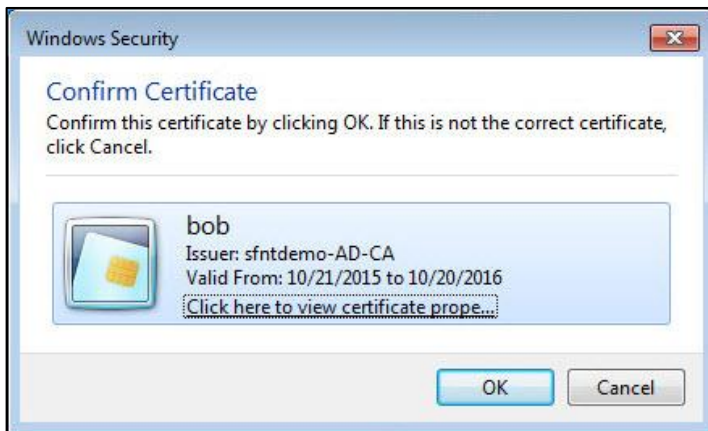
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

5. You will be redirected to your organization's login window. 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.)

6. After successful login, the browser displays all the certificates available on the machine. Select the end user certificate that is added on the SafeNet USB token.
7. You will be redirected to the **Confirm Certificate** window. Click **OK**.

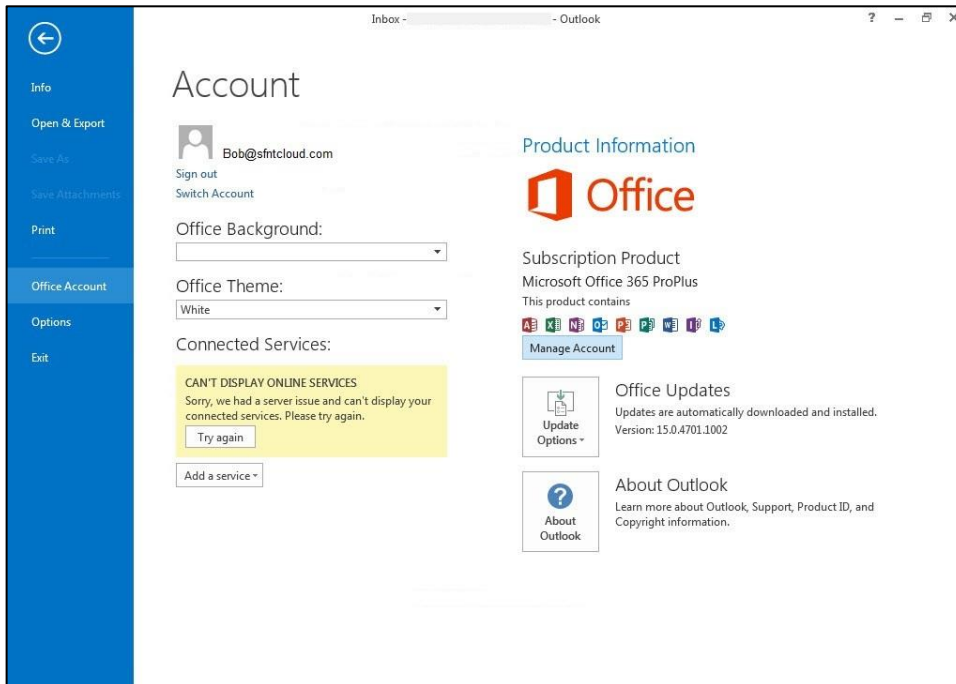


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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



After successful authentication, you will be logged in to your Outlook 2013 account.



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

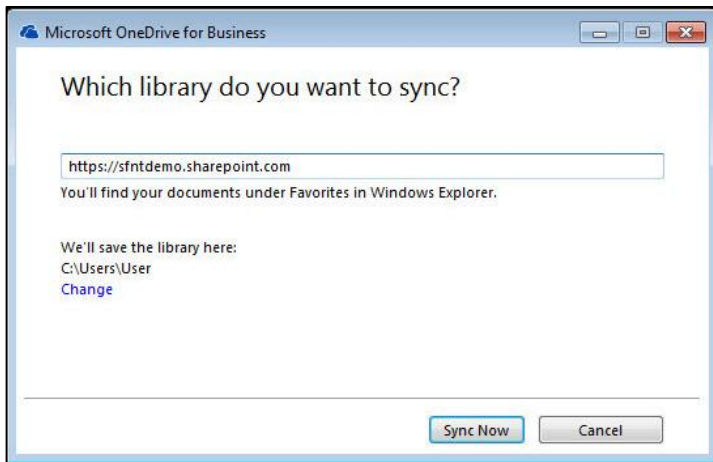
Signing In to OneDrive for Business 2013

1. Double-click the **OneDrive for Business 2013** icon.



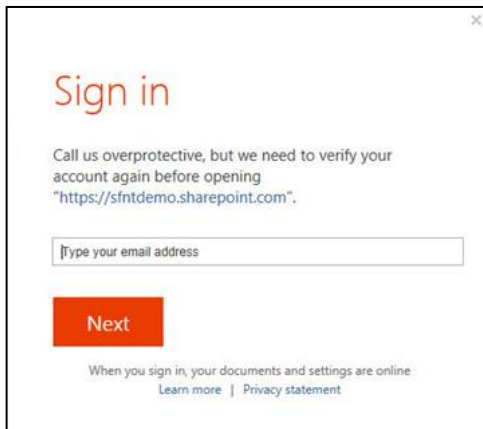
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

2. On the **Microsoft OneDrive for Business** window, enter the SharePoint URL provided by the administrator (refer to “Appendix A: Obtaining the Office365 SharePoint URL” on page 17 for details on how to obtain this URL), and then click **Sync Now**.



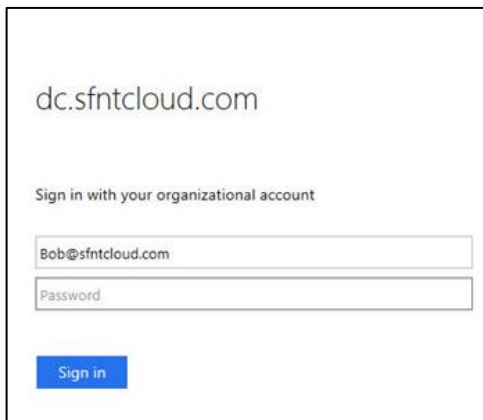
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. On the **Sign in** window, enter your AD user name (for example, **Bob@sfntcloud.com**), and then click **Next**.



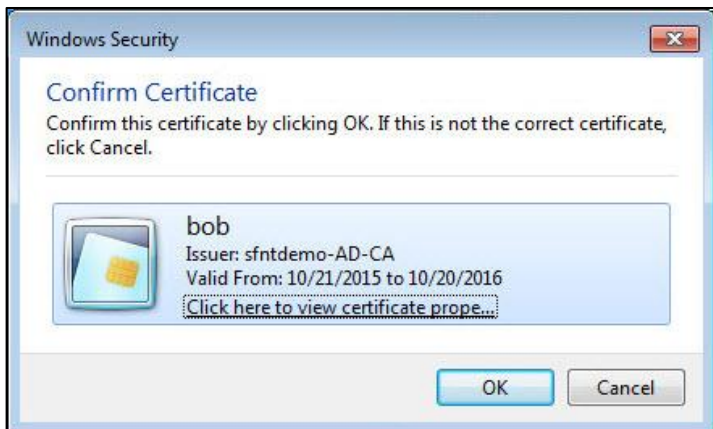
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. You will be redirected to your organization’s login window. Enter your AD password, and then click **Sign in**.



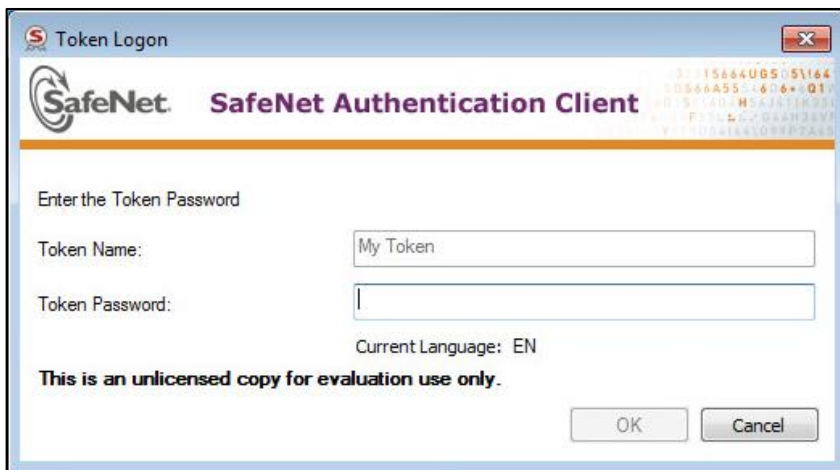
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

5. After successful login, the browser displays all the certificates available on the machine. Select the end user certificate that is added on the SafeNet USB token.
6. You will be redirected to the **Confirm Certificate** window. Click **OK**.

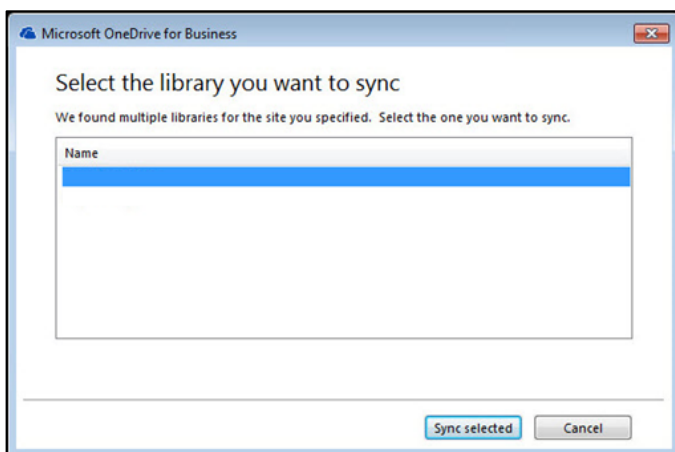


(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

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

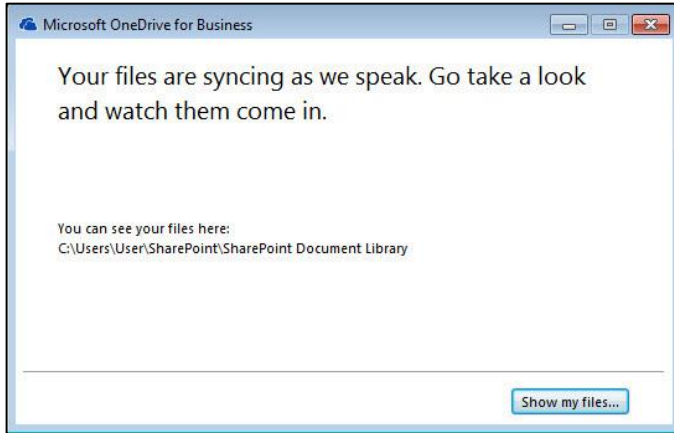


8. After successful authentication, you will be logged in to the **OneDrive for Business 2013**. Select the folder you want to sync, and then click **Sync selected**.



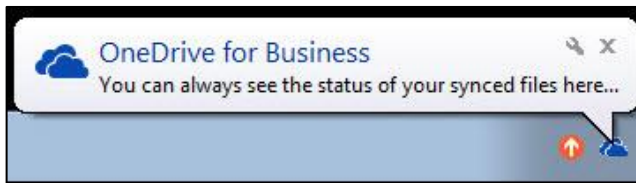
(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

After the synchronization process is started, a message is displayed.



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

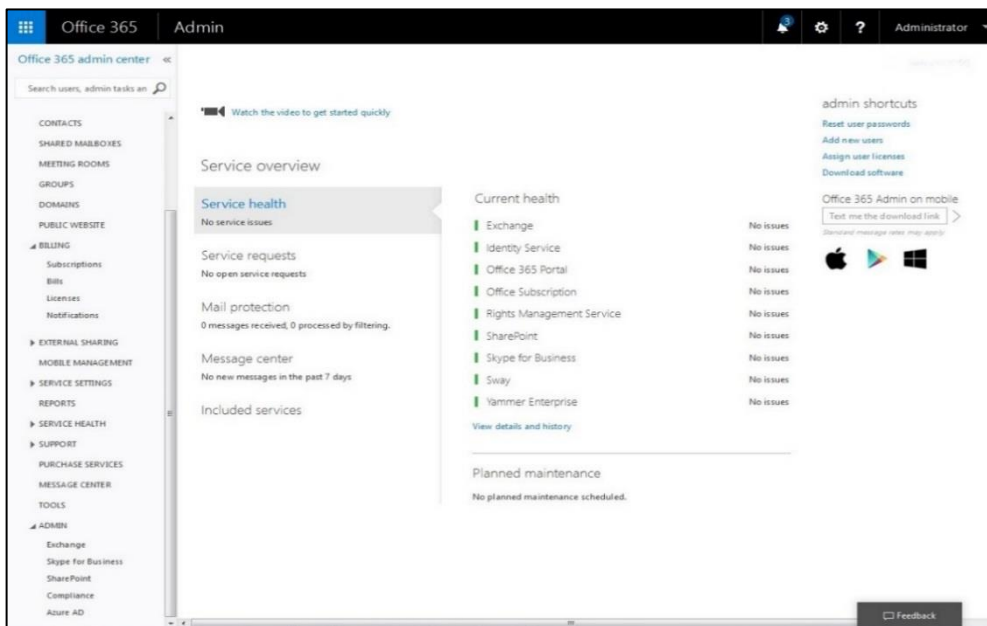
A message is displayed adjacent to the **OneDrive for Business 2013** icon in the system tray to indicate that the synchronization process is running.



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

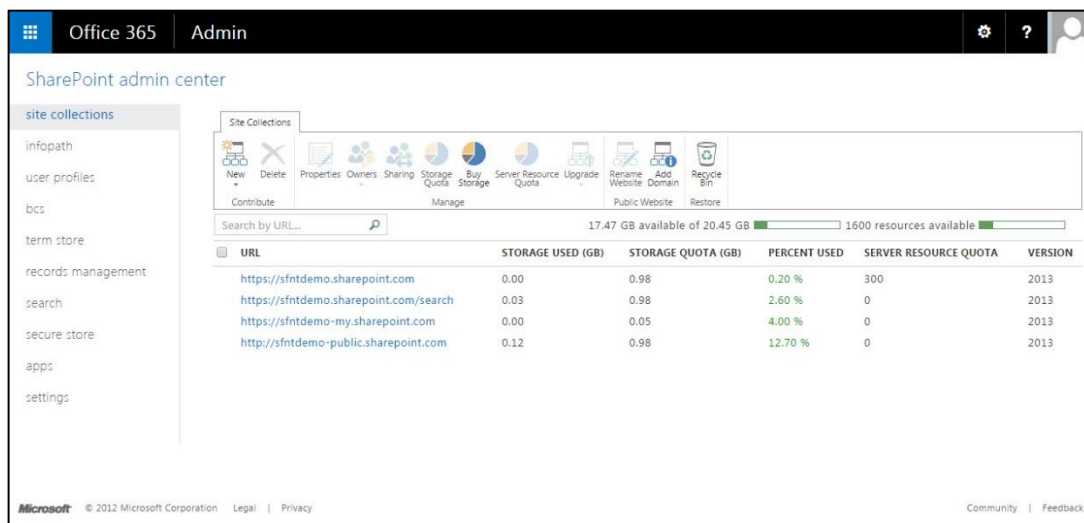
Appendix A: Obtaining the Office365 SharePoint URL

1. Log in to Office365 as an administrator.
2. On the Office365 console, in the left pane, click **Admin > SharePoint**.



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

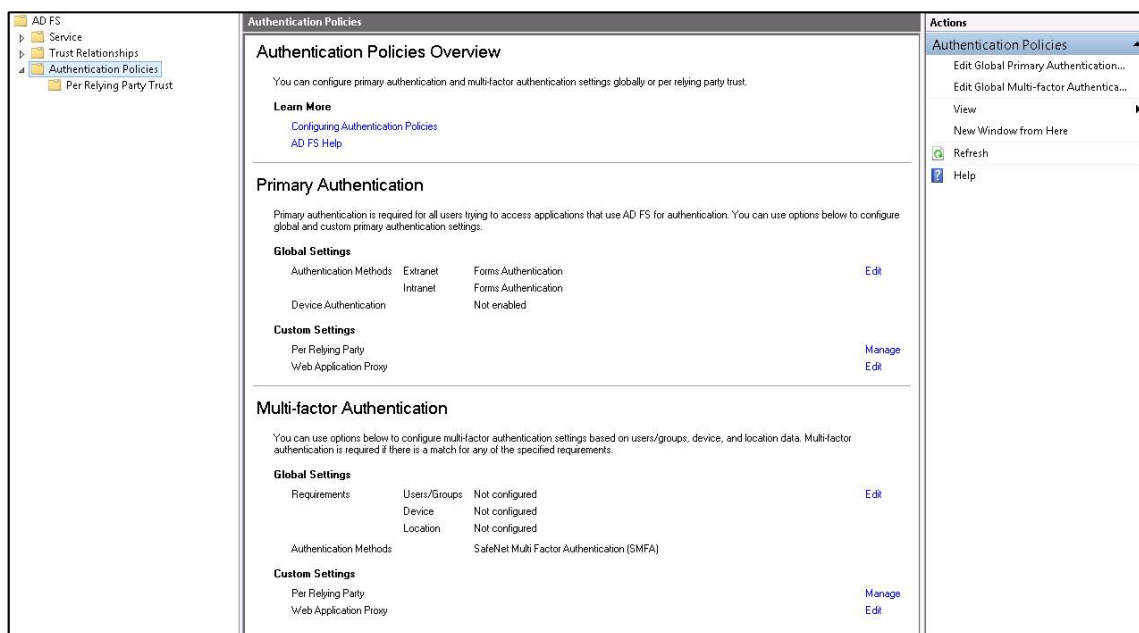
In the right pane, the Office 365 SharePoint URLs are listed.



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

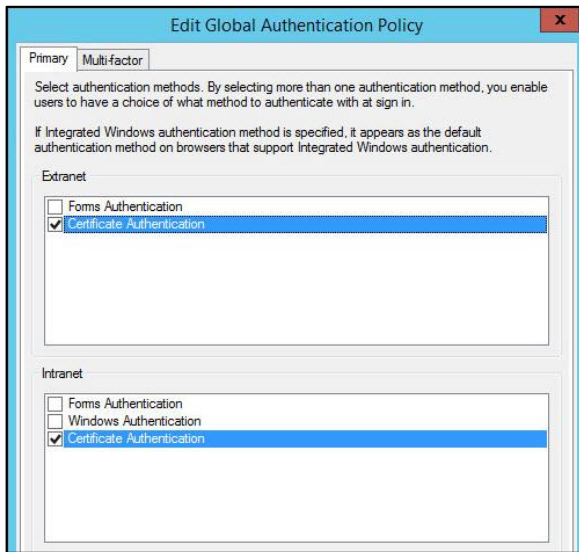
Appendix B: Configuring AD FS with CBA for Single Authentication

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.)

- 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.	