SafeNet Authentication Client

Integration Guide

Using SafeNet Authentication Client CBA for Office 365

gemalto
security to be free

Document Number: 007-013412-002, Rev. B

Release Date: May 2018

Contents

Third-Party Software Acknowledgement

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

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.

Office 365 from Microsoft is a cloud-based service that is designed to help meet your organization's needs for robust security, reliability, and user productivity.

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

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

Office 365 can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Office 365 using Gemalto's tokens and smart cards.

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

Office 365 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—** IDGo800 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, refer to the Customization section in *SafeNet Authentication Client Administrator Guide.*
- **Office 365**

Environment

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

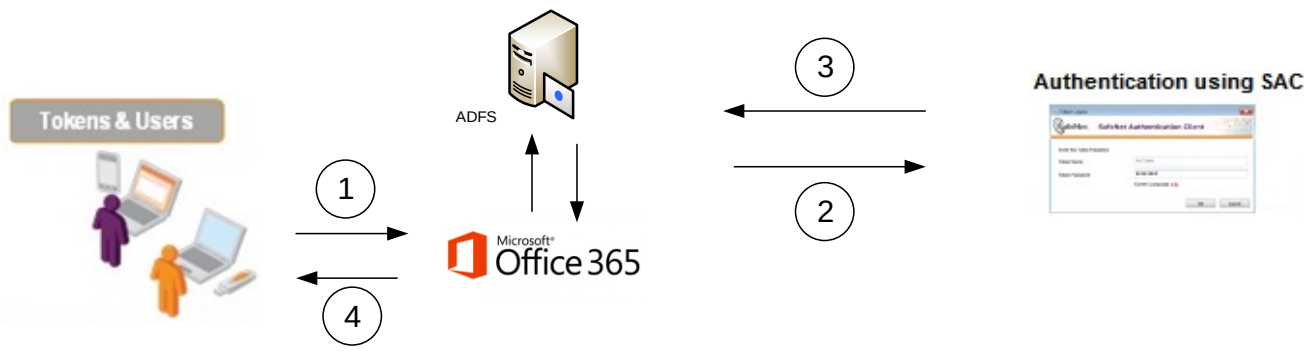
- **SafeNet Authentication Client (SAC)** - Version 10.5
- **Office 365 -** On Cloud
- **AD FS -** On Windows Server® 2012 R2

Audience

This document is targeted to system administrators who are familiar with Office 365, and are interested in adding certificate based 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 connect to Office 365.The user is redirected to AD FS proxy server (WAP) for authentication.
2. After successful authentication, the 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, accepting or rejecting the user's authentication request.
4. The user is granted or denied access to Office 365.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Office 365 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. 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 Gemalto token or smart card enrolled with an appropriate certificate.
- SafeNet Authentication Client (10.5) should be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.5) 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 B
- Gemalto IDPrime MD 840 B
- Gemalto IDCore 30B eToken

For all supported devices please refer to *SafeNet Authentication Client Customer Release Notes*.

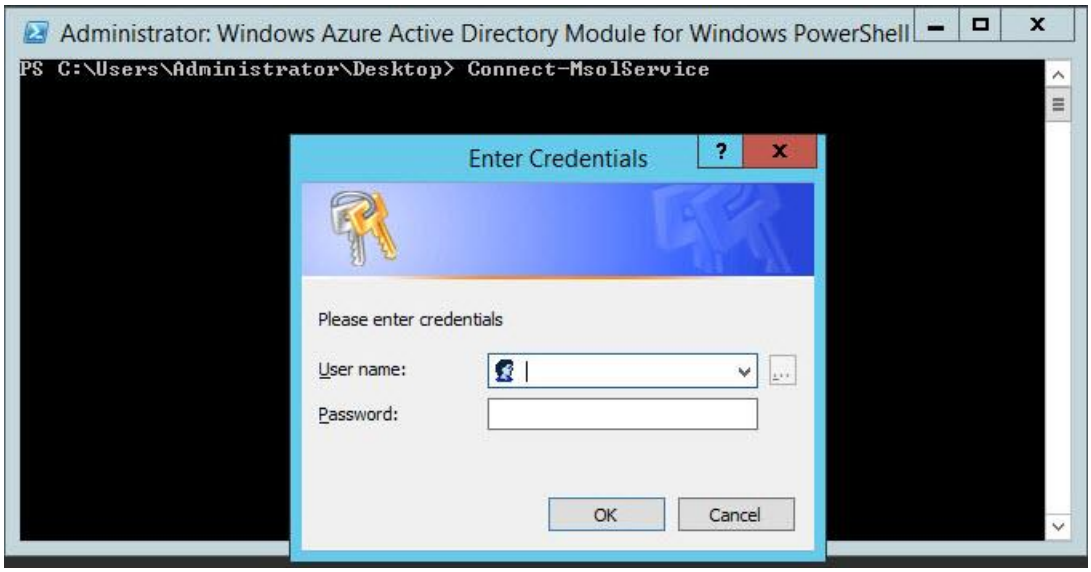
Configuring Office 365 and AD FS

Configuring Office 365 and AD FS requires the following:

- Enabling Office 365 Federated Domains, page 8.
- Configuring the AD FS Authentication Policy, page 9.

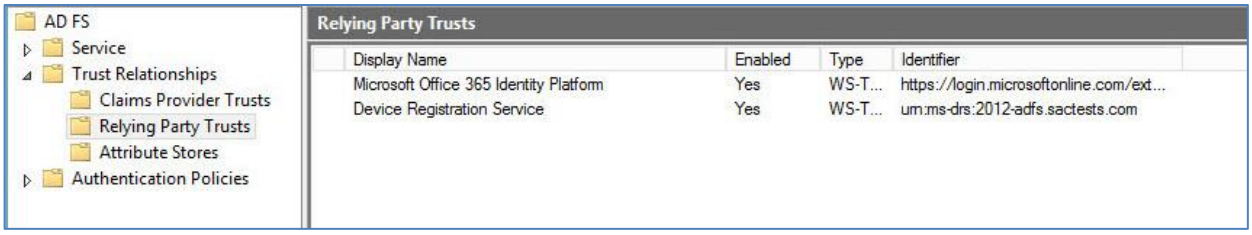
Enabling Office 365 Federated Domains

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 click **Enter**.
4. In the **Enter Credentials** window, enter your Azure AD administrator username and password, and then click **OK**.



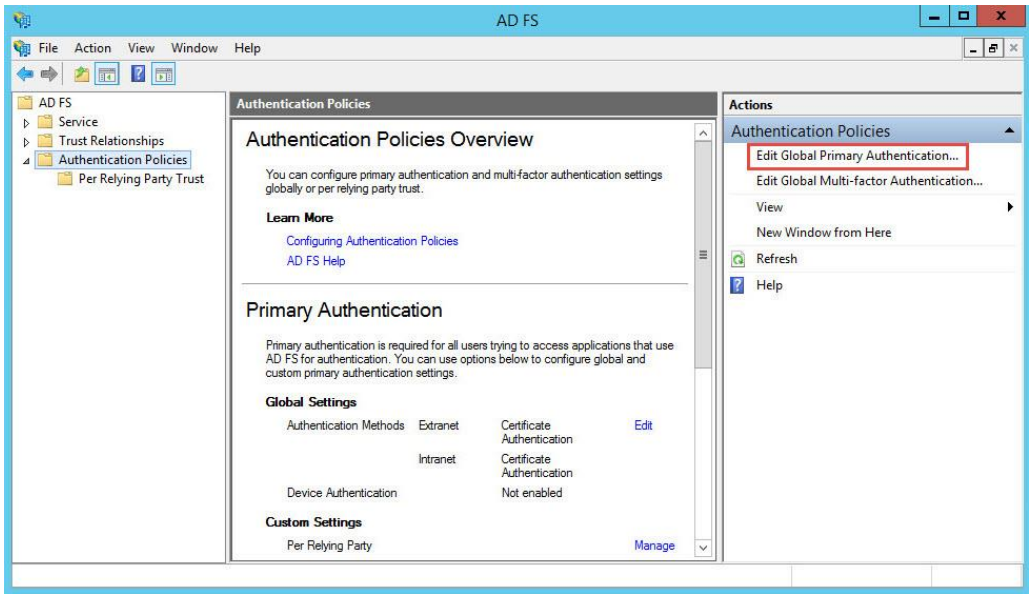
5. At the command prompt, perform the following steps:
   a. Type **Set-MsolADFSContext –Computer <AD FS machine name>**, and then click **Enter**.
   b. Type **Convert-MsolDomainToFederated –DomainName <your domain name>,** and then click **Enter**.

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 should be listed as a trust.

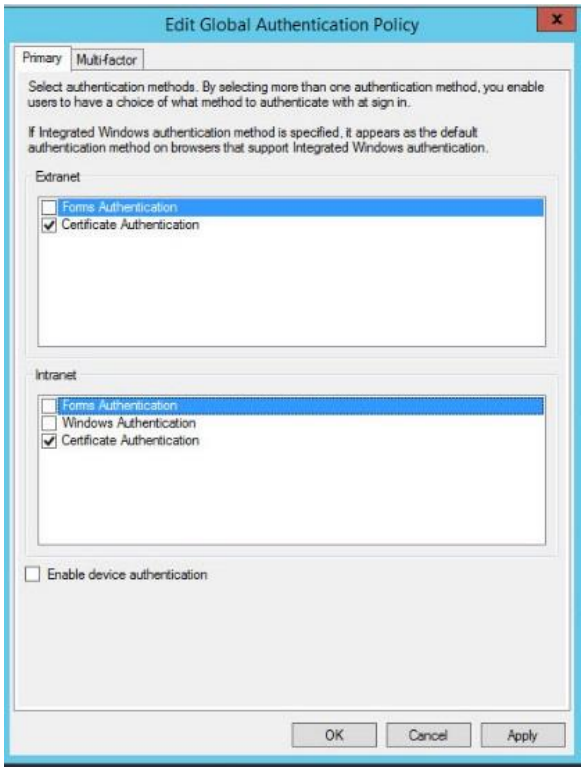


Configuring the AD FS Certificate Based Authentication Policy

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.



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

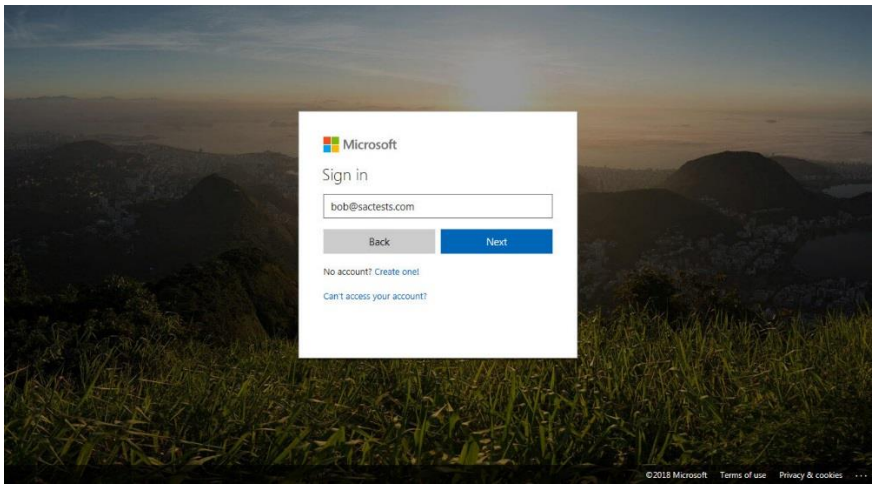


4. Click **OK.**

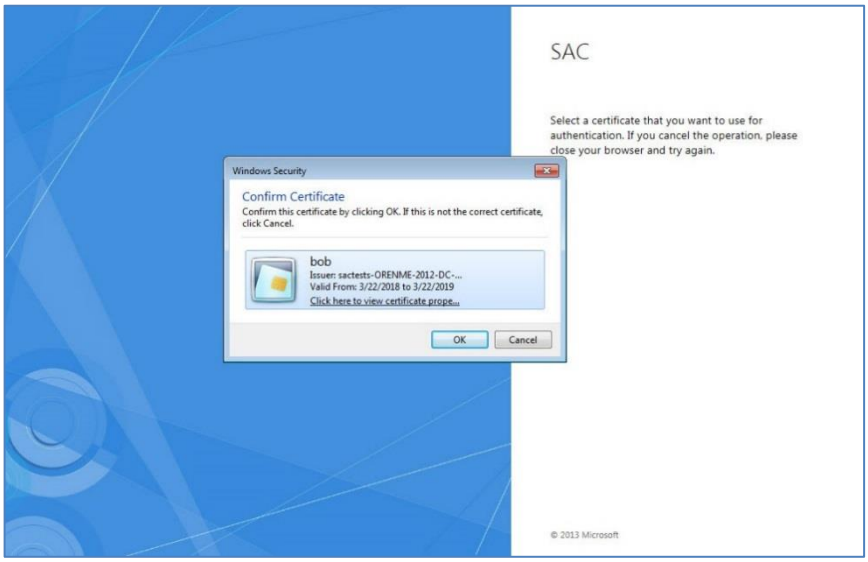
Running the Solution

Connecting to Office 365

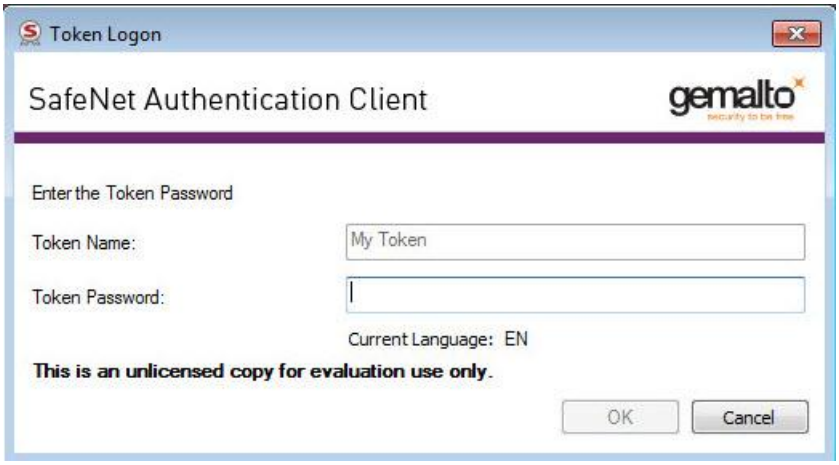
1. Open the following URL in a web browser:
   https://login.microsoftonline.com
2. On the **Office 365** login window, enter your AD user name (for example, **Bob@sactests.com**), and then click **Next**.



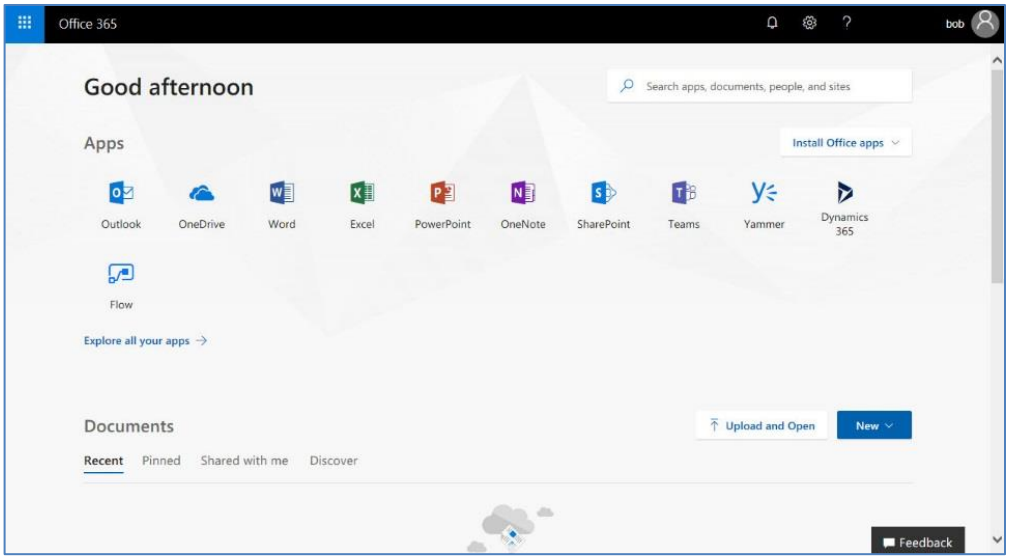
3. You will be redirected to your organization's login page. Select the user certificate and click **OK**.



4. On the **SafeNet Authentication Client Token Logon** window, enter the token password, and then click **OK**.



5. After successful authentication, you are granted access to the **Office 365** dashboard.



Appendix: Connecting to SharePoint in Office 365

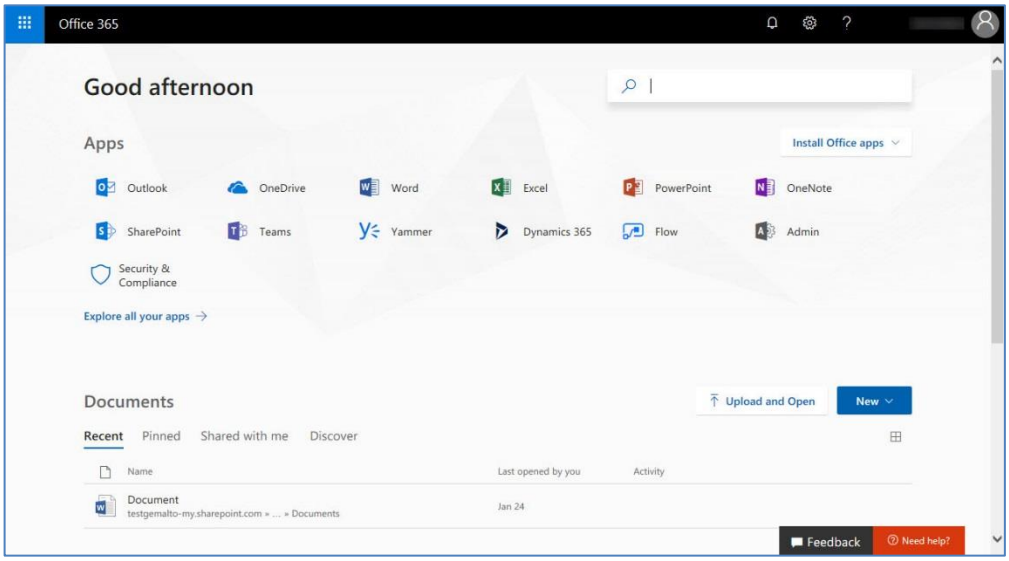
Users can connect to SharePoint in Office 365 using their AD credentials and smartcards. Administrator will provide SharePoint URLs to users.

Connecting to SharePoint in Office 365 requires:

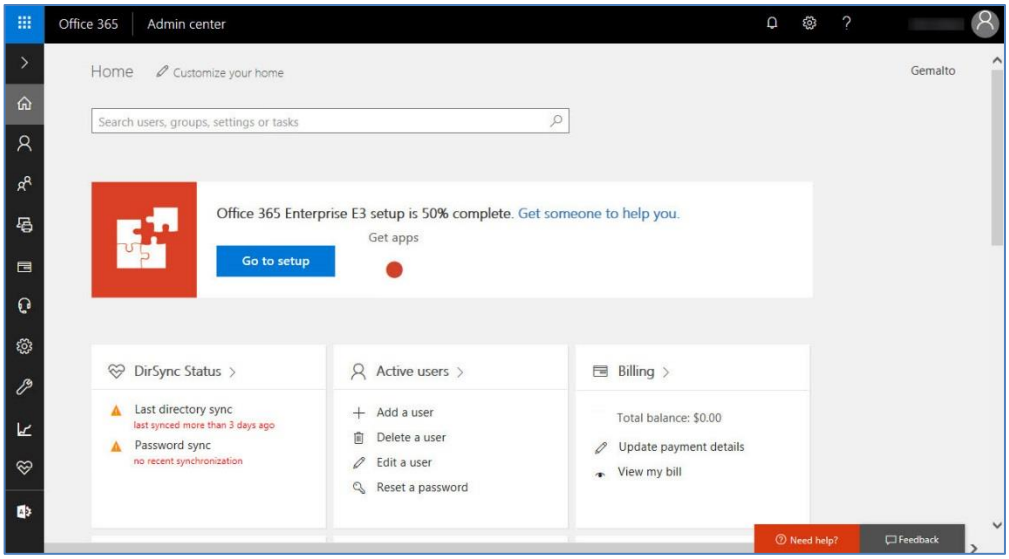
- Getting SharePoint URLs, Page 13
- Connecting to SharePoint, Page 15

Getting SharePoint URLs

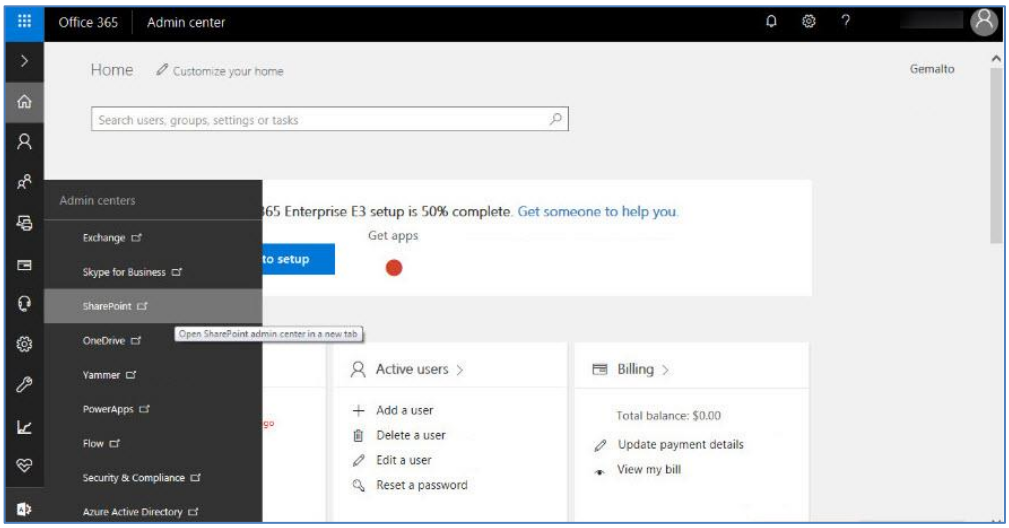
1. Log in to **Office 365 admin center** as an administrator.



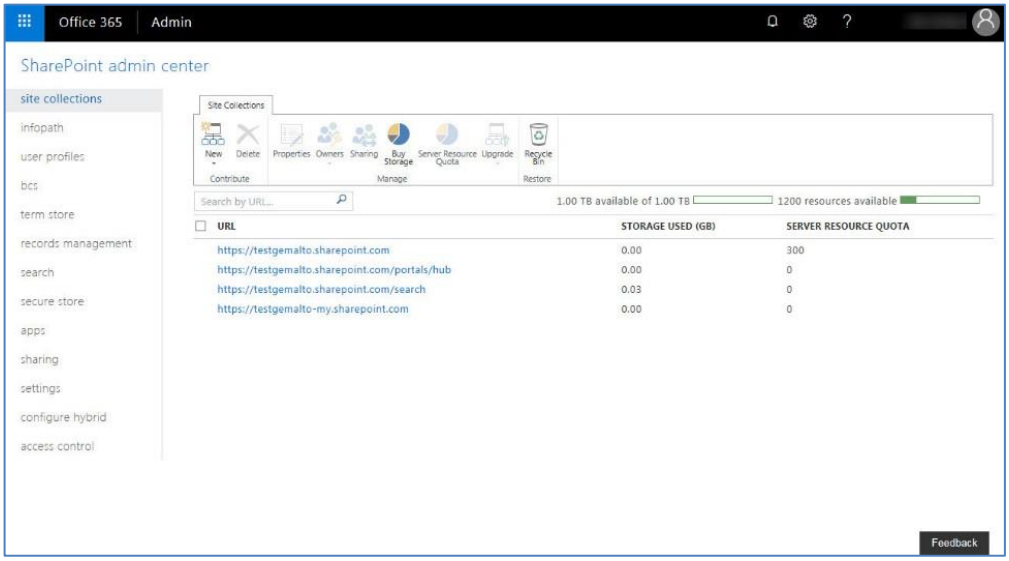
2. Click **Admin**. You will be redirected to the **Admin Center** page.



3. In the left pane select **Admin centers > SharePoint.**



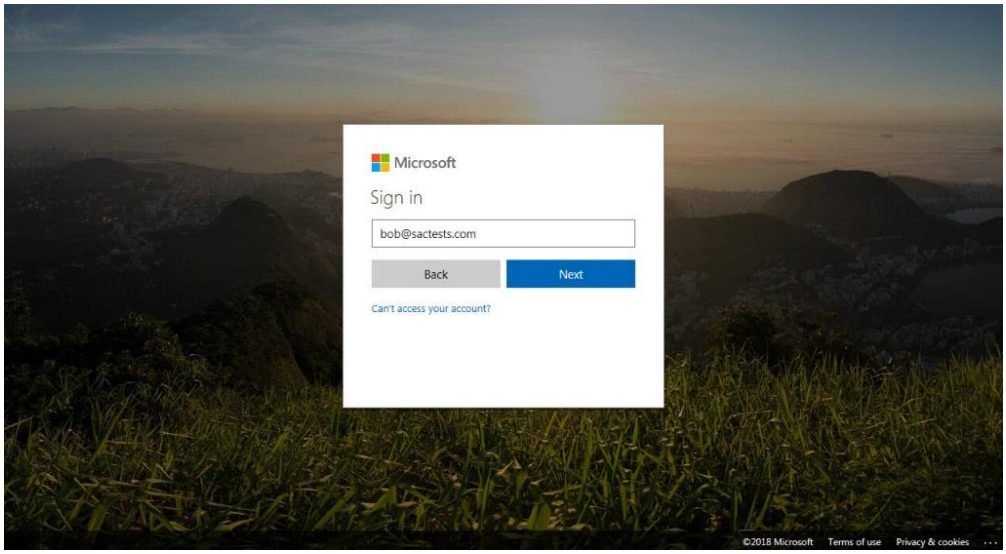
In the right pane, the Office 365 SharePoint URLs are listed.



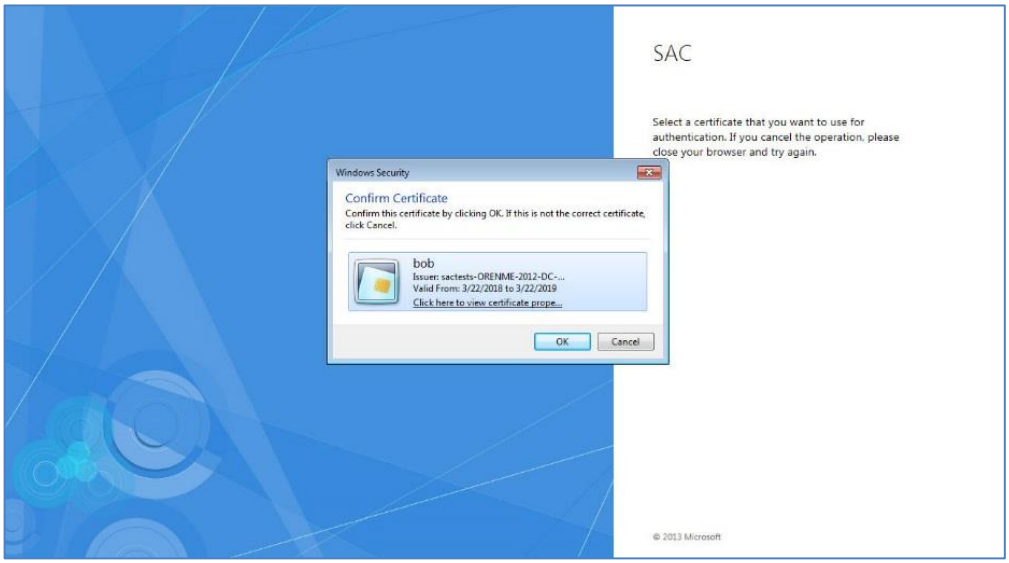
4. Share any or all of the SharePoint URLs with other users.

Connecting to SharePoint

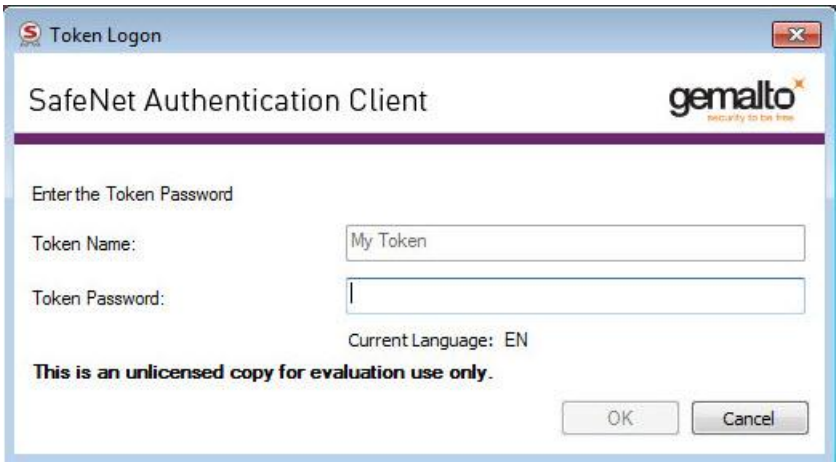
1. In a web browser, open any of the Office 365 SharePoint URLs received from the administrator.
2. On the **Office 365** login window, enter your AD user name (for example, **Bob@sactests.com**), and then click **Next**.



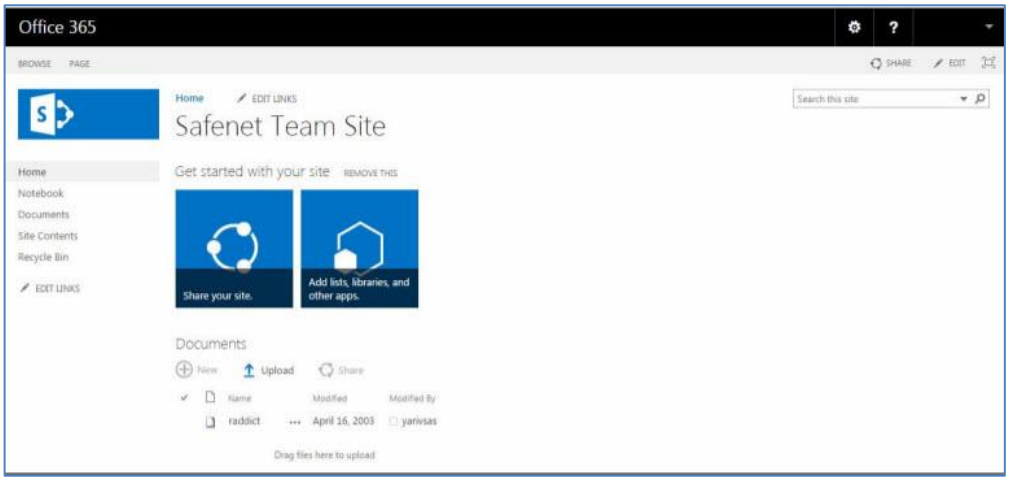
3. You will be redirected to your organization's login page. Confirm the certificate and click **OK**.



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



After successful authentication, the Office 365 SharePoint console is displayed.



Appendix: Secure/Multipurpose Internet Mail Extensions (S/MIME) Configuration

Office 365 uses encryption in two ways: in the service and as customer control. S/MIME allows the user to encrypt email messages.

S/MIME protects your emails from unwanted access.

In order to configure S/MIME with Office 365 the user needs an Enterprise E3 license, in order to upload the certificate via the outlook email client.

Prerequisites:

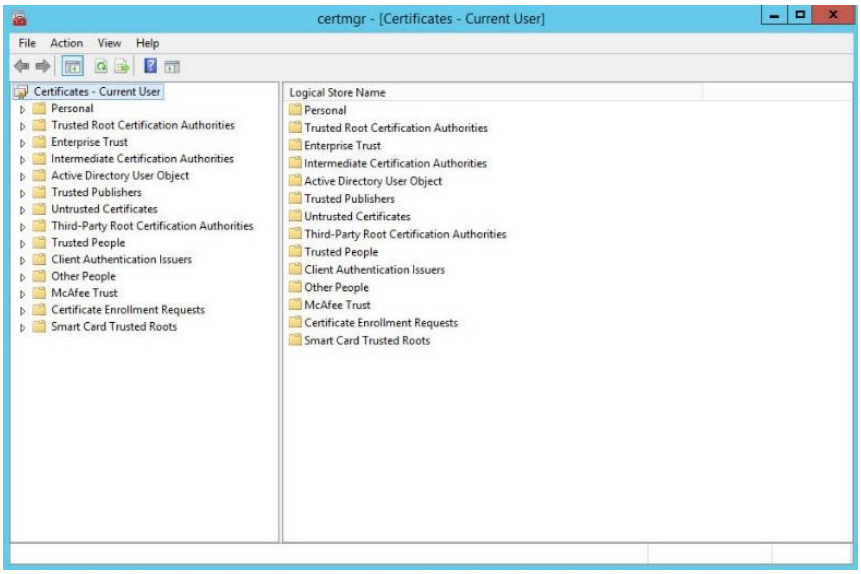
1. Login as Windows Administrator.
2. Install MS KB as follows:

   X86: Windows6.1-KB2819745-x86.msu

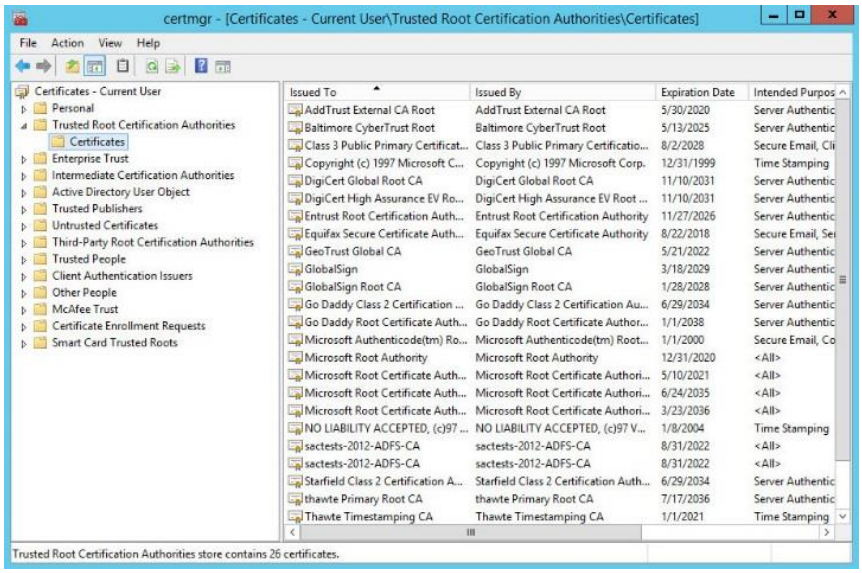
   x64: Windows6.1-KB2819745-x64-MultiPkg.msu

Export to SST file from the trusted Root CA

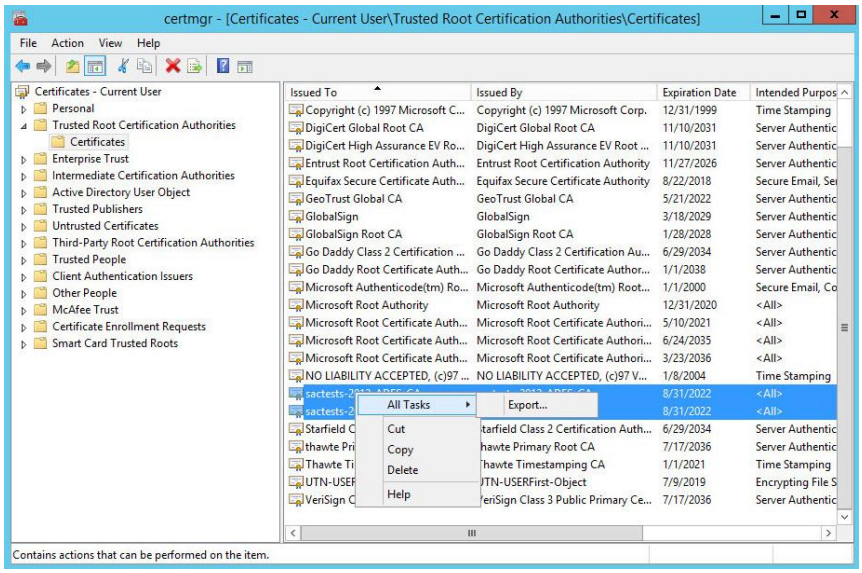
1. On the CA computer, open the certificate manager, and select **Run > certmgr.msc.**



2. Expand **Trusted Root Certification Authorities > Certificates.**

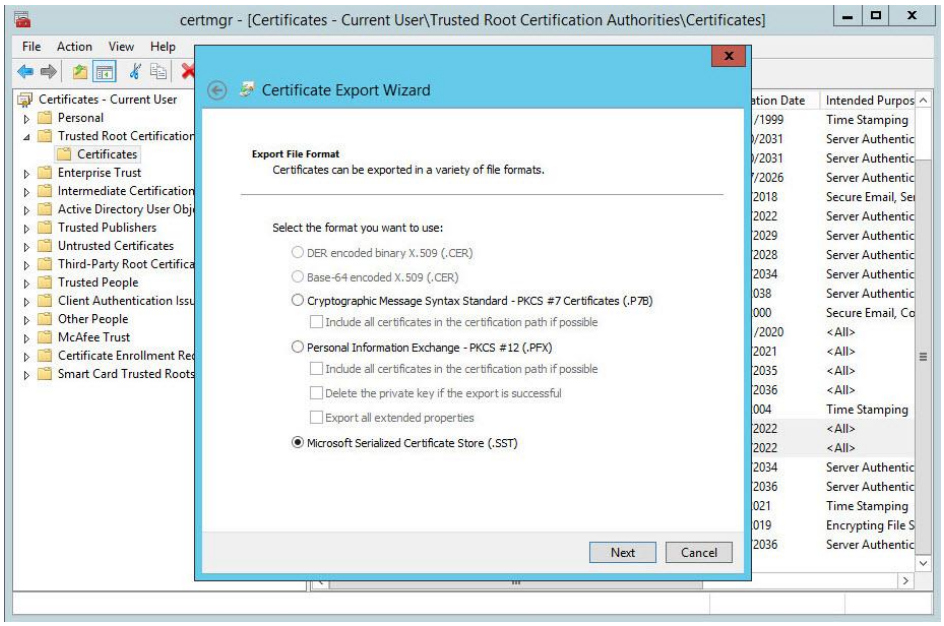


3. Right click on the certificate which you bought for your business email (in our lab we used a self-signed CA, therefore we will use the Root CA certificate), then select **All Tasks > Export.**



NOTE: If you select one certificate, the export .sst option is greyed out, so you must select at least 2 certificates (For example, personal and intermediate certificates).

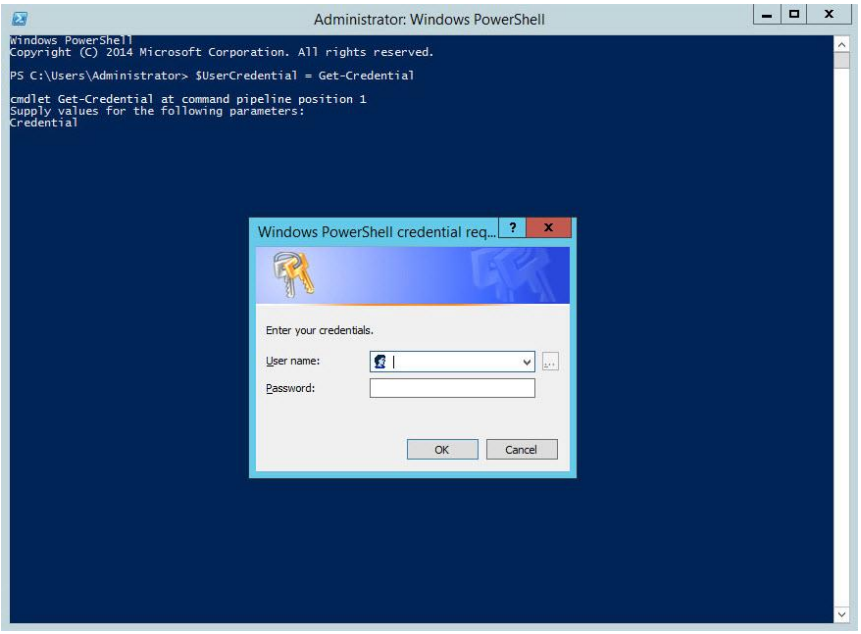
4. Click Next on the first **Certificate Export Wizard** screen, then select Microsoft Serialized Certificate Store (.sst)



5. Click **Next**, then click **Browse** and select the location and file name where the .sst file will be saved.
6. Click Next, Save and then Finish.

Upload .sst file to Exchange Online

1. Open windows **PowerShell** (run as administrator).
2. Connect to the Office 365 admin account by running the command: $**UserCredential = Get-Credential.**
3. The Windows PowerShell credential request window opens. Enter the admin user name and password. Click **OK**.



4. Enter the following command in order to open a session with Exchange online:
   $Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic –AllowRedirection

5. Enter the following command to remove restrictions for uploading the .sst file:
   Set-ExecutionPolicy Unrestricted –force

6. Import the session:
   Import-PSSession $Session

7. Change the path to where the .sst file was saved (for example, cd c:\)

8. Upload the .sst file to Office 365:
   $sst = Get-Content <SST file> -Encoding Byte

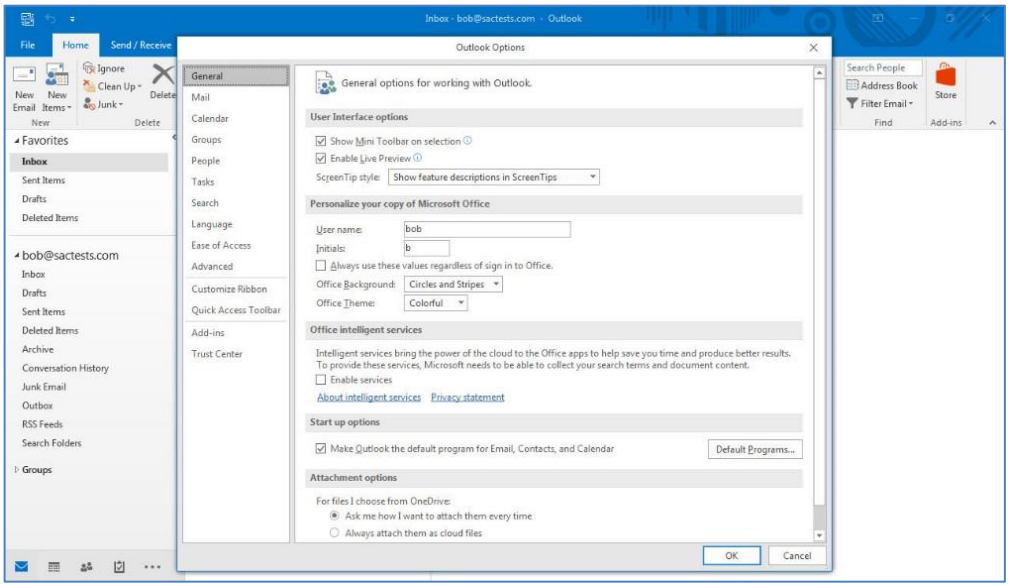
9. Configure the sst file to be used for S/MIME:
   Set-SmimeConfig -SMIMECertificateIssuingCA $sst

10. Close the session:
    Remove-PSSession $Session

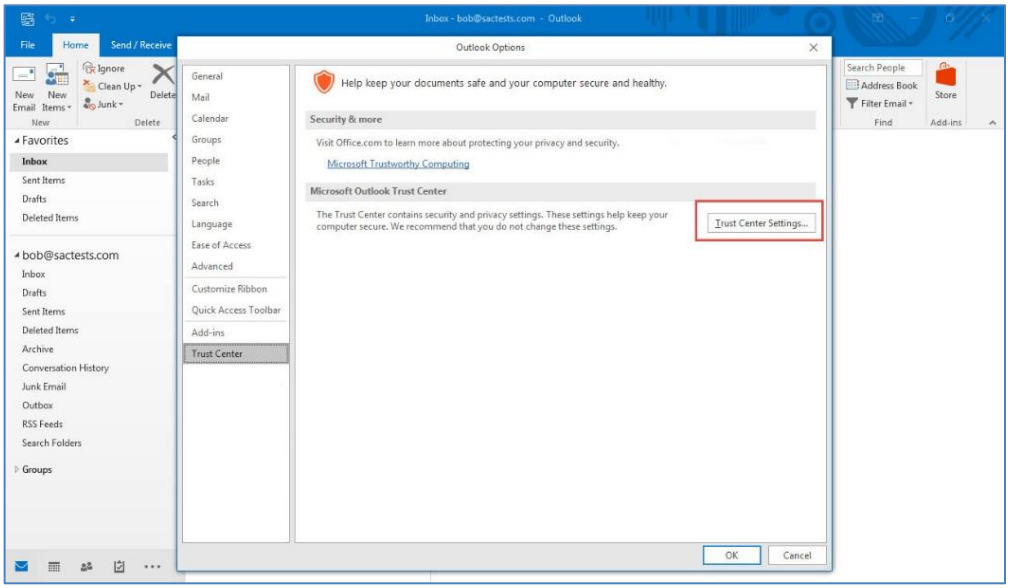
Publish Certificate to GAL (Global Address List)

To encrypt emails with S/MIME we need to upload the user certificate to the GAL.

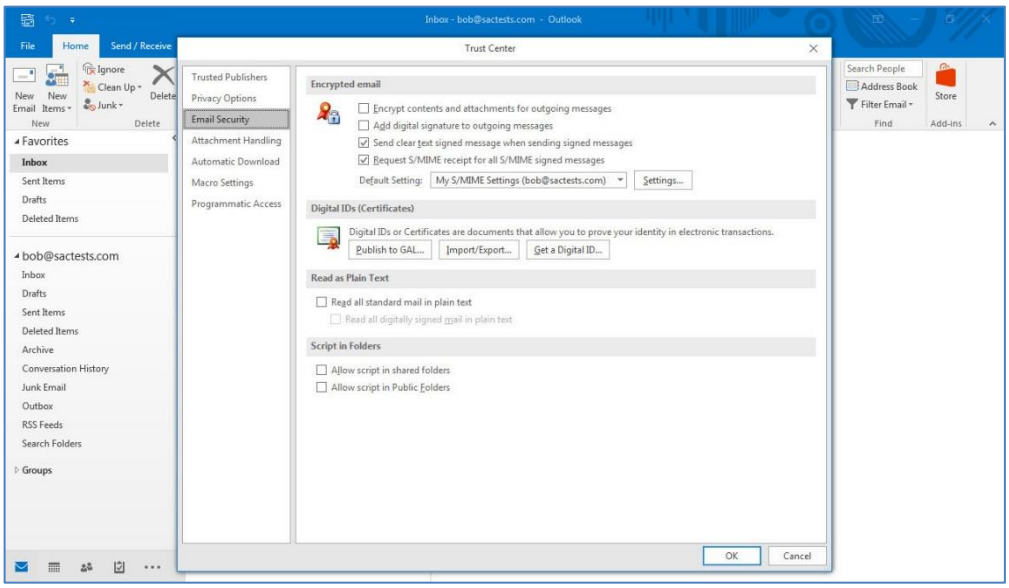
1. Open **Outlook**.
2. Select **File > Options.**



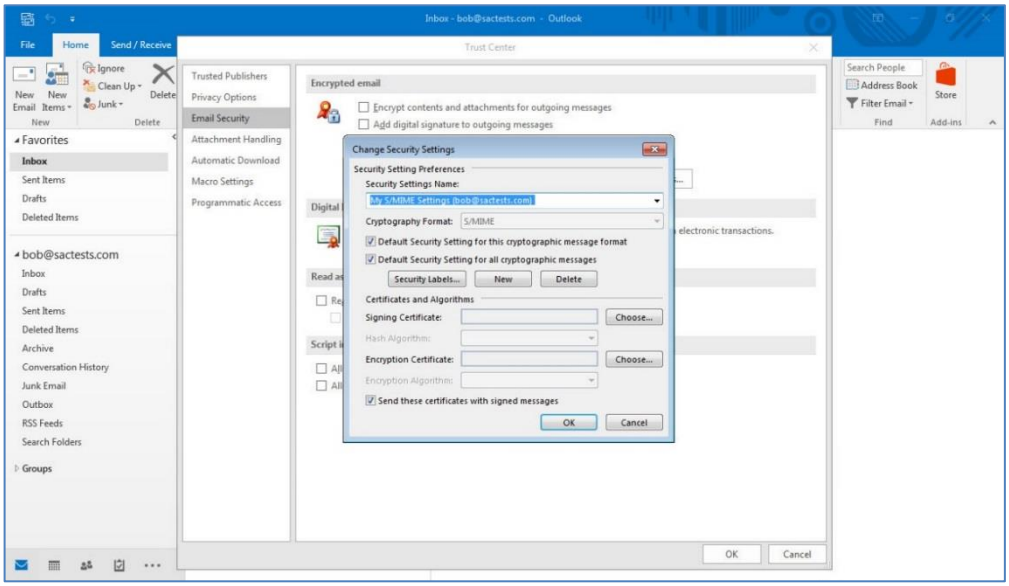
3. On the left pane select **Trust Center** and then on the right pane click **Trust Center Settings**



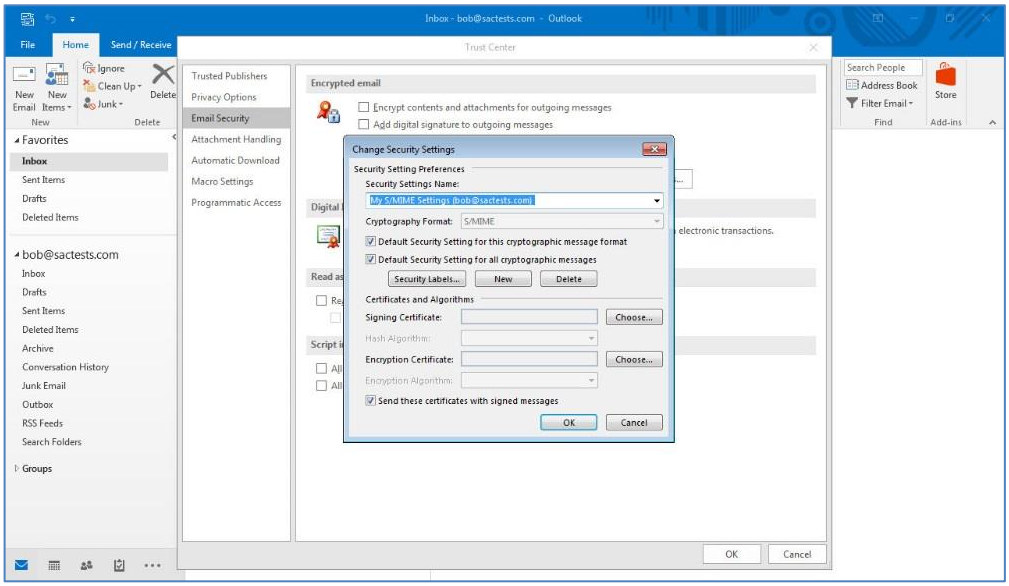
4. On the left pane select **Email Security.**



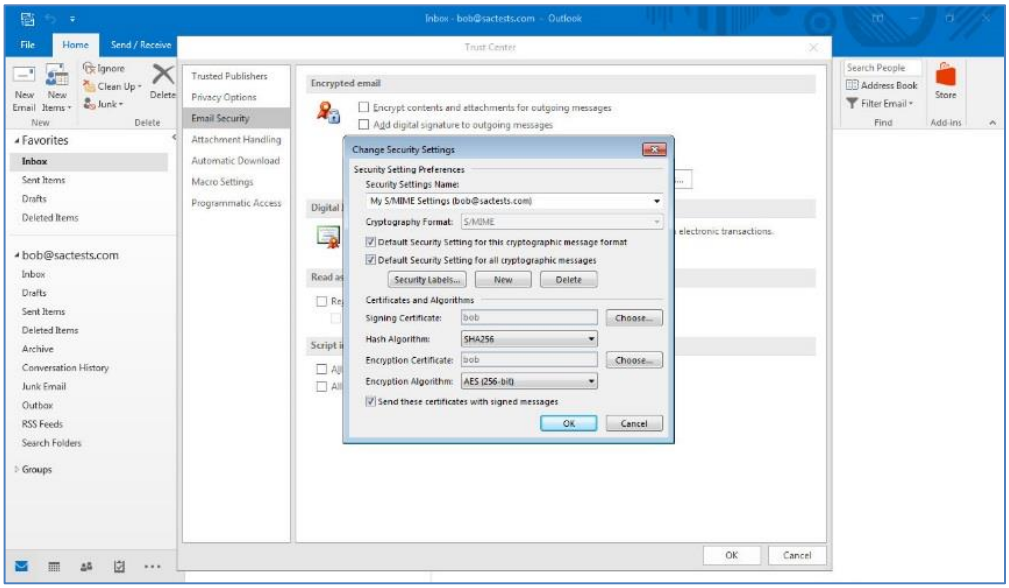
5. In the Trust Center window click **Settings.** The **Change Security Setting** window opens.



6. On the Change Security Settings window, choose Security Setting Name and then click Choose, (to the right of the Signing Certificate field).

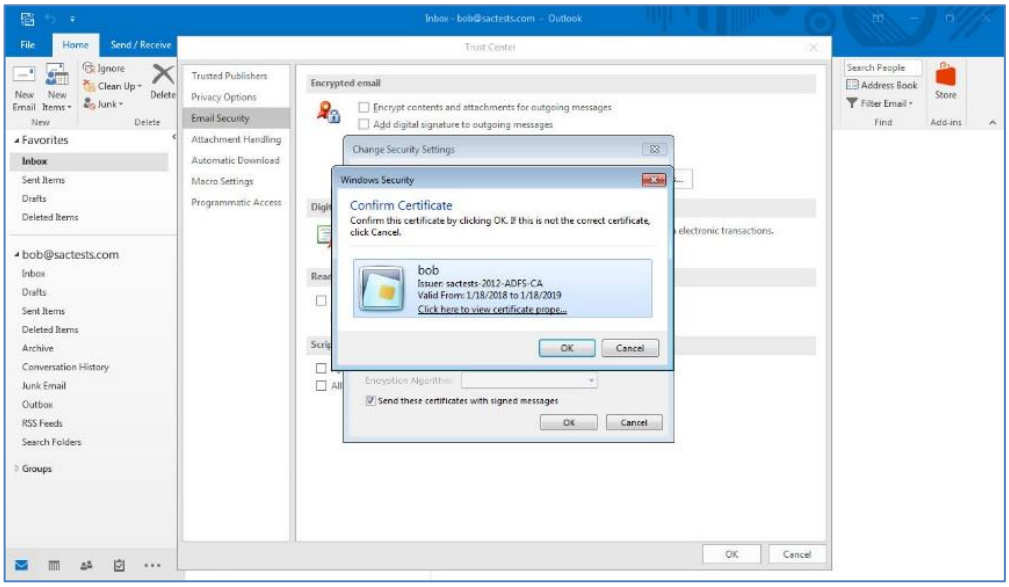


7. The **Confirm Certificate** window opens. Select the certificate issued by the CA you are going to use for S/MIME.
8. After choosing the certificate, click **OK**.



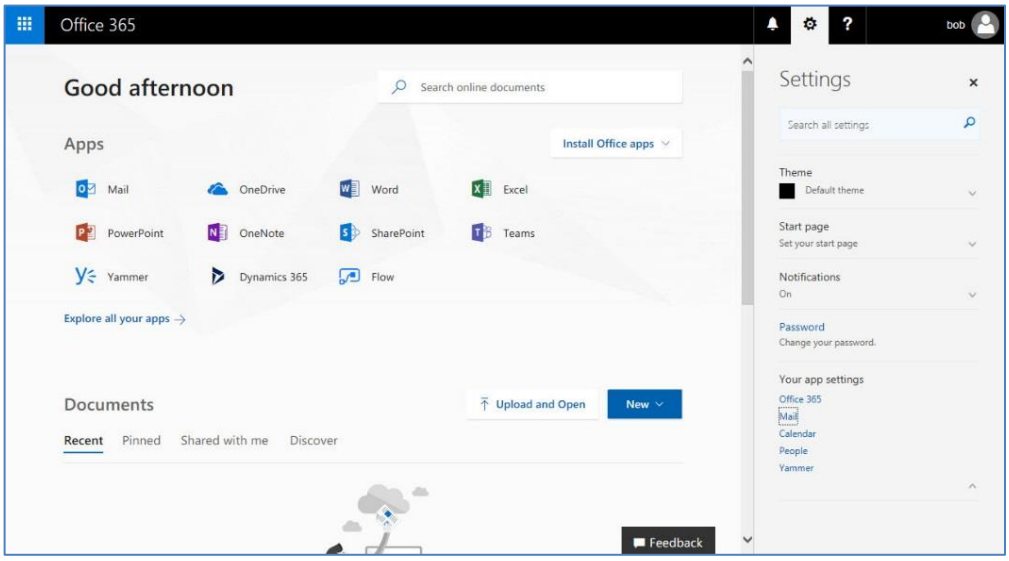
9. !n the **Trust Center** window, click **Publish to GAL** in order to publish your certificate to Office 365.

Once the certificate is uploaded to GAL, you will receive a confirmation message.

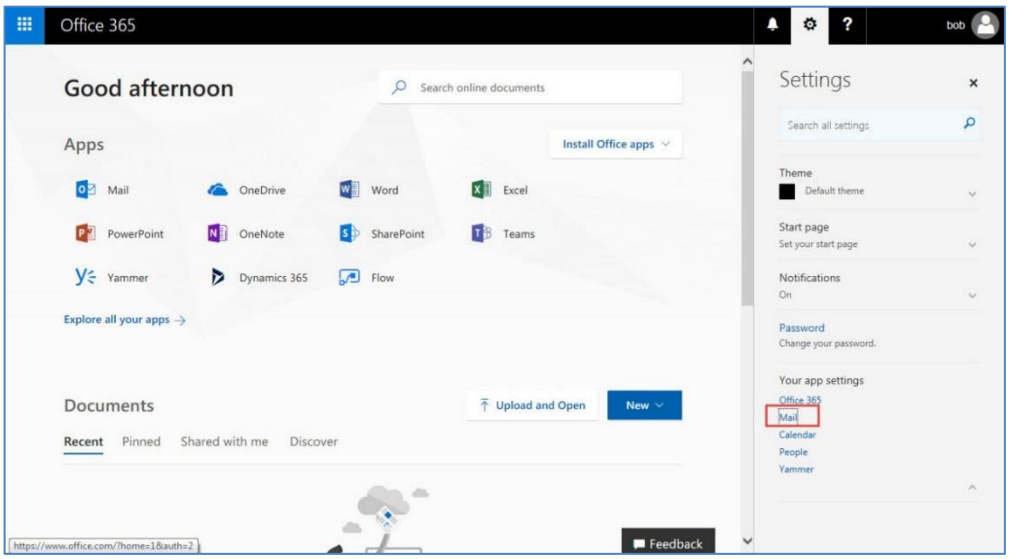


Enable S/MIME in Office 365 OWA

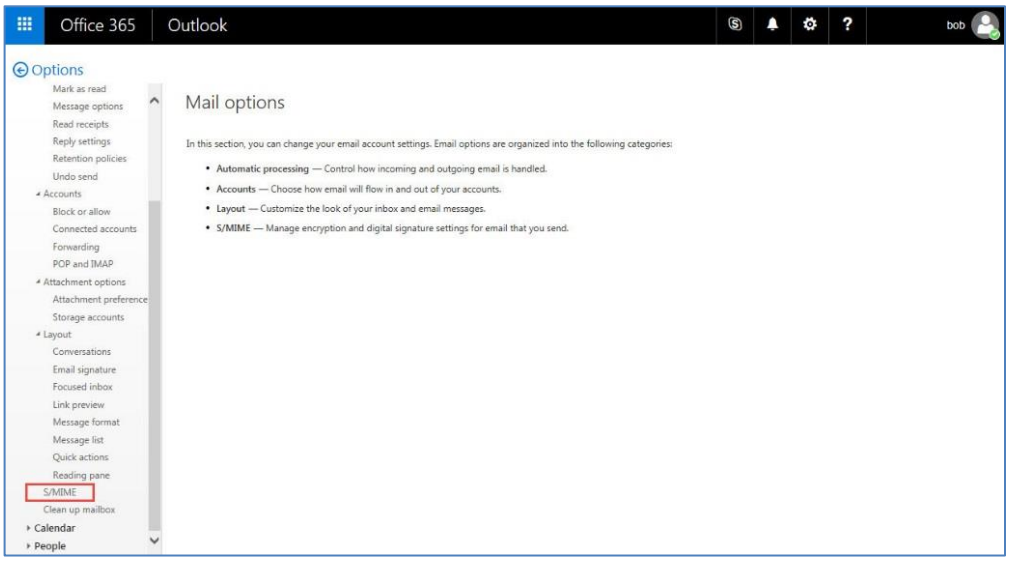
1. Login to Office 365 with the user credentials and click **Office 365**.



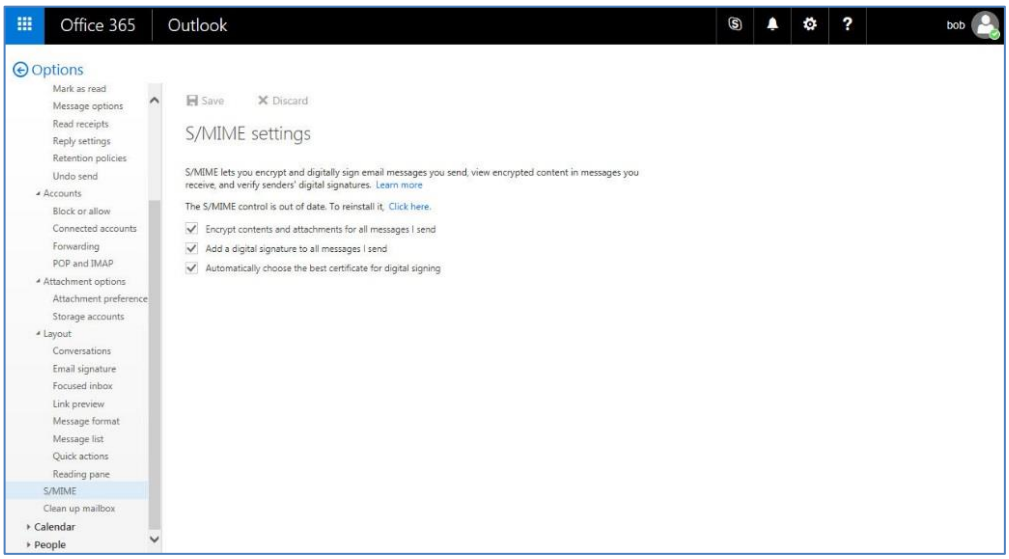
2. On the right pane select **Mail**



3. The user's mail settings window opens. On the left pane select **S/MIME**



4. Check the checkboxes to support S/MIME and click **Save.**



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 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.	