SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider 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.

© 2015 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:** 007-013206-001, Rev. D  
**Release Date:** May 2016
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>SAS Authentication API Authentication using SafeNet Authentication Service Cloud</td>
<td>5</td>
</tr>
<tr>
<td>SAS Authentication API using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE</td>
<td>5</td>
</tr>
<tr>
<td>SafeNet Authentication Service Authentication API Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Configuring Office 365 ProPlus and AD FS</td>
<td>6</td>
</tr>
<tr>
<td>Enabling Office 365 Federated Domains</td>
<td>7</td>
</tr>
<tr>
<td>Configuring Gemalto SafeNet Authentication Service AD FS Agent</td>
<td>8</td>
</tr>
<tr>
<td>Configuring the AD FS Authentication Policy</td>
<td>9</td>
</tr>
<tr>
<td>Downloading and Installing Office 365 ProPlus</td>
<td>11</td>
</tr>
<tr>
<td>Enabling Modern Authentication for Office 365 ProPlus</td>
<td>13</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>13</td>
</tr>
<tr>
<td>Creating Users Stores in SafeNet Authentication Service</td>
<td>13</td>
</tr>
<tr>
<td>Assigning an Authenticator in SafeNet Authentication Service</td>
<td>14</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service Auth Node and Downloading the Encryption Key</td>
<td>14</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>17</td>
</tr>
<tr>
<td>Signing In to Outlook 2013</td>
<td>17</td>
</tr>
<tr>
<td>Signing In to OneDrive for Business 2013</td>
<td>20</td>
</tr>
<tr>
<td>Signing in to Skype for Business 2016</td>
<td>23</td>
</tr>
<tr>
<td>Appendix A: Obtaining the Office365 SharePoint URL</td>
<td>26</td>
</tr>
<tr>
<td>Appendix B: MFA Advanced Configuration Using PowerShell Commands</td>
<td>27</td>
</tr>
<tr>
<td>Appendix C: Registering Office 365 Tenant Account for the Public Preview</td>
<td>28</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>29</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet 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

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Office 365 ProPlus is 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 describes how to:

- Configure SAML authentication in Office 365 ProPlus using SafeNet Authentication Service as an identity provider.

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

Office 365 ProPlus can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by service providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization
Environment

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

- **SafeNet Authentication Service**—Version 3.3
- **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 Authentication Service.

SAS Authentication API Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service Cloud provides a service for SAS Authentication API that is already implemented in the SAS Cloud environment and can be used using the Gemalto SafeNet SAS AD FS Agent.

SAS Authentication API using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service (SAS) comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.
- **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with AD FS infrastructure, which uses a special on-premises agent called Gemalto SafeNet SAS AD FS Agent.
SafeNet Authentication Service Authentication API Flow using SAS

AD FS provides extensible multi-factor authentication through the concept of “additional authentication providers” that are invoked during secondary authentication. External providers can be registered in AD FS.

Once a provider is registered with AD FS, it is invoked from the AD FS authentication code via specific interfaces and methods that the provider implements and that AD FS calls. Because it provides a bridge between AD FS and an external authentication provider, the external authentication provider is also called an AD FS MFA “adapter”.

Gemalto SafeNet SAS AD FS Agent is an AD FS MFA adapter that provides users a way to authenticate through AD FS using SAS as a secondary authenticator.

The image below describes the dataflow of a multi-factor authentication transaction for Office 365 ProPlus.

1. A user attempts Sign in to Office 365 ProPlus. The user is redirected to the AD FS proxy server (WAP), then after successful authentication, is forwarded to SafeNet Authentication Service (SAS) for a secondary authentication (AD FS multi-factor authentication).
2. The user uses his SAS token for authenticating. SAS collects and evaluates the user’s credentials.
3. The SAS 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

Office 365 tenant account must be registered for the public preview of Microsoft Office 365 and Office 365 Pro Plus. For more information, refer to “Appendix C: Registering Office 365 Tenant Account for the Public Preview” on page 28.

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 Gemalto SafeNet Authentication Service AD FS Agent, 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.
3. At the command prompt, type Connect-MsolService, and then press Enter.
4. On the Enter Credentials window, enter your Office 365 user name and password, and then click OK.

5. At the command prompt, type Convert-MsolDomainToFederated -DomainName <your domain name>, and then press 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.

![Screen image of AD FS Trust Relationships](image)

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

### Configuring Gemalto SafeNet Authentication Service AD FS Agent

1. Run the Gemalto SafeNet Authentication Service (SAS) Agent for AD FS.
2. On the **SFA MFA Plug-in Manager** window, on the **Policy** tab, ensure that the following are selected:
   - Enable agent
   - Pre-generate challenge
3. Click the **Communications** tab. Then, in the **Primary Server** field, enter the SAS server IP address or name (and the port number if non-causal is used).

   In case your SAS server is not installed on the same machine as AD and AD FS, the encryption key file needs to be loaded (as explained in step 3 of “Configuring SafeNet Authentication Service Auth Node and Downloading the Encryption Key” on page 14).

4. Click **Apply**. Enabling the agent registers the SafeNet MFA (multi-factor authentication) adapter with AD FS and enables it at a global policy level.

5. You can verify your settings by testing authentication from the agent to the authentication server. To do so, under **Authentication Test**, enter your user name and passcode, and then click **Test**. The result of the test will be displayed in the **Authentication Test Result** box.

6. Click **OK** when finished.

**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**.

![Edit Global Primary Authentication](image1)

*(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](image2)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
4. On the **Multi-factor** tab, perform the following steps:
   a. Under **Users/Groups**, add the users and/or groups for which MFA will be required.
   b. Under **Locations**, select **Extranet** and/or **Intranet**, according to your preferred configuration.
   c. Ensure that **SafeNet Multi Factor Authentication (SMFA)** is selected as an additional authentication method.
   d. Click **Apply**
   e. Click **OK**.

   ![Edit Global Authentication Policy](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 console, under **Install Office on more devices**, click **Install**

![Office 365 Install Office on more devices](image1)

*(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.

![Office 365 Install Office on more devices](image2)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
4. After the download is complete, double-click the downloaded file to install Office 365 ProPlus.

(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:

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\EnableADAL</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Version</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
<tr>
<td>HKCU\SOFTWARE\Microsoft\Office\15.0\Common\Identity\Debug\TCOTrace</td>
<td>REG_DWORD</td>
<td>3</td>
</tr>
</tbody>
</table>

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

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Office 365 ProPlus using SAML authentication requires:

- Creating Users Stores in SafeNet Authentication Service, page 13
- Assigning an Authenticator in SafeNet Authentication Service, page 13
- Configuring SafeNet Authentication Service Auth Node and Downloading the Encryption Key, page 14

Creating Users Stores in SafeNet Authentication Service

Before SafeNet Authentication Service (SAS) can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the Create User shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory/LDAP server using the SAS Synchronization Agent

For further details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.
Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Office 365 ProPlus.

The following authenticators are supported:

- eToken PASS
- RB-1 keypad token
- KT-4 token
- SafeNet GOLD
- SMS tokens
- MP-1 software token
- GrIDsure
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the SafeNet Authentication Service Subscriber Account Operator Guide to learn how to provision the different authentication methods to the users in the SAS user store.

http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Ac

Configuring SafeNet Authentication Service Auth Node and Downloading the Encryption Key

In the event that the SafeNet Authentication Service (SAS) server is not installed on the same machine as AD and AD FS, the following steps must be performed:

1. Log in to the SAS console as the account operator.
2. Click **Virtual Servers > Comms > Authentication Processing**.
3. Click the **Authentication Agent Settings** link, and then click **Download** to download the encryption key file. This file will be needed in step 3 in “Configuring Gemalto SafeNet Authentication Service AD FS Agent,” on page 8.

4. Click **Virtual Servers > Comms > Auth Nodes**.

5. Click the **Auth Nodes** link.

6. Under **Auth Nodes**, click **Add**.
7. Under **Add Auth Node**, complete the following fields, and then click **Save**.

- **Auth Node Name**: Enter a host description.
- **Resource Name**: Enter a resource name which will identify in a push notification which authentication node it relates to.
- **Low IP Address In Range**: Enter the lowest IP address that will authenticate with SAS.
- **High IP Address In Range**: Enter the highest IP address that will authenticate with SAS. (The low and high IP addresses may be the same, since the node is referencing a single machine.)
- **Exclude from PIN change requests**: Do not select this option.
- **Configure FreeRADIUS Synchronization**: Do not select this option.

The authentication node is added to the system.
Running the Solution

For this integration, the SafeNet GrIDsure token is configured for authentication with the SAS solution.

Signing In to Outlook 2013

In the following solution, launch Outlook 2013, and then log in to Office 365.

1. Double-click the Outlook 2013 icon.

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

2. 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.

4. On the **Sign in** window, enter your office 365 user name (for example, **Bob@sfntcloud.com**), and then click **Next**.
5. You will be redirected to your organization’s login window. Enter your AD password, and then click **Sign in**.

![Login Window](image1.png)

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

6. After successful authentication, you will be redirected to SAS to enter your one-time password. In the **OTP** field, enter your Personal Identification Pattern (PIP), and then click **Submit**.

![OTP Form](image2.png)
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

In the following solution, launch OneDrive for Business 2013, and then log in to Office 365.

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 26), 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 Office 365 user name (for example, **Bob@sfntcloud.com**), and then click **Next**.

![Sign in window](image)

*(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**.

![Login window](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
5. After successful authentication, you will be redirected to SAS to enter your one-time password. In the **OTP** field, enter your Personal Identification Pattern (PIP), and then click **Submit**.

6. 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, the following message is displayed.

![Image: Microsoft OneDrive for Business]

*(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.

![Image: OneDrive for Business]

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

**Signing in to Skype for Business 2016**

Skype for Business 2016 supports the Modern Authentication (ADAL) and AD FS authentication, and SAS as a secondary authentication.

To work with ADAL, ensure that:

- Your Office 365 tenant account is registered on the public preview ([http://aka.ms/PublicPreview](http://aka.ms/PublicPreview)).
- Your client machine is a part of your registered Azure AD domain.

In the following solution, launch Skype for Business 2016, and then log in to Office 365.

1. Double-click the **Skype for Business 2016** icon.
2. Enter your Office 365 username (for example, bob@sfntdemo.com), and then click **Sign in**.

3. You will be redirected to your organization’s login window. Enter your AD password, and then click **Sign in**.
4. After successful authentication, enter your SAS token passcode.

5. After successful authentication, you will be logged in to your Skype for Business account.
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: MFA Advanced Configuration Using PowerShell Commands

AD FS server 2012 R2 includes new cmdlets for installing the AD FS server role and for initial configuration of the federation server and federation server proxy. One of the cmdlets is used for by-passing the AD FS Management user interface. That stipulate additional authentication is required by use of User/Group, Devices, or Locations.

For example, if an MFA policy is be used by location only (for example, Extranet), then simply select the location as Extranet. All users connecting from outside the corporate network must then use MFA. Conversely, to enforce MFA for a specific subset of users/groups, irrespective of their location (Extranet or Intranet), add them via the Users/Groups option in the UI. Finally, if Unregistered devices or Registered devices (via Workplace Join) need to use MFA, they can be specified through Devices.

The challenge arises when dealing with a combination of policy, for example, when stating an MFA requirement by device and by location.

AD FS will now trigger MFA when an unregistered device (non-workplace joined) connects to AD FS and when users are connecting from the Internet. The policies are evaluated independently, and MFA may be unintentionally enforced for a registered device in a Workplace Join scenario, when the desired outcome was actually to ensure that a single authentication factor (the device certificate paired with the a specific user) was sufficient for access from the outside. This is the logical OR behavior.

Rules are evaluated independently when set through the user interface. Given that requirements through the UI operate this way, if there is a requirement to enforce MFA via policy where:

- it is an unregistered device
  
  AND

- connecting from the Internet

The AD FS Management UI does not support this arrangement. Instead, more refined policies can be handled with PowerShell, using combinations of authentication rules. Two common commands are:

- **Get-AdfsAdditionalAuthenticationRule**—This command will return the current rules of AD FS MFA.

- **Set-AdfsAdditionalAuthenticationRule -AdditionalAuthenticationRules**—This command will set a new rule.

The most common request is to prevent Outlook’s ActiveSync and AutoDiscover from requesting MFA (since a second password request is not available, and thus will continue to fail when MFA is enabled). To configure AD FS to require MFA only to web-based requests (ActiveSync and AutoDiscover are not web-based), use the following command:

```
```

**NOTE:** If copy-paste does not work, then type the command manually.
To configure this rule for a specific user group, use \&\&\&, which will act as “AND” in the following command:


**NOTE:** To locate the user group’s value, you can use Active Directory Explorer, which is available for download here:


The above commands will apply the MFA rules to not only Office 365, but to all the relying parties in your AD FS. To apply MFA rules to Office 365 only, use the following commands:

$rp = Get-AdfsRelyingPartyTrust –Name "Your Office 365 RP name as it appears in AD FS"


**Appendix C: Registering Office 365 Tenant Account for the Public Preview**

Modern authentication includes Active Directory Authentication Library (ADAL)-based login to Microsoft Office 2013 or 2016 clients.

1. Sign up for the public preview (http://aka.ms/publicpreview) using your Office 365 tenant account.

2. After your Office 365 tenant account is enabled, set the appropriate registry keys on your windows machine (refer to the section “Enabling Modern Authentication for Office 365 ProPlus” on page 13).
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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td>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.</td>
</tr>
</tbody>
</table>