SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for Microsoft Azure RemoteApp
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:** 007-013410-001, Rev. A

**Release Date:** February 2016
## Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description ............................................................................................................................................................. 4
Applicability ........................................................................................................................................................ 4
Environment ......................................................................................................................................................... 5
Audience ............................................................................................................................................................... 5
SAML Authentication using SafeNet Authentication Service Cloud ................................................................. 5
SAML Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE .......... 5
SAML Authentication Flow using SafeNet Authentication Service ................................................................. 6
SAML Prerequisites ........................................................................................................................................... 6
Configuring Microsoft Azure RemoteApp and AD FS .......................................................................................... 6
  Adding a Domain to Azure .................................................................................................................................. 7
  Syncing the Domain to Azure ........................................................................................................................... 9
  Verifying the AD Connect Installation ........................................................................................................... 9
  Enabling Azure AD Federated Domains ......................................................................................................... 14
  Configuring Gemalto SafeNet Authentication Service Agent for AD FS ...................................................... 16
  Configuring the AD FS Authentication Policy .............................................................................................. 17
  Creating a Microsoft Azure RemoteApp Collection ........................................................................................ 18
Configuring SafeNet Authentication Service .................................................................................................... 22
  Creating Users Stores in SafeNet Authentication Service ............................................................................ 22
  Assigning an Authenticator in SafeNet Authentication Service ................................................................. 23
  Configuring SafeNet Authentication Service Auth Node and Downloading Encryption Key .................... 23
Running the Solution ......................................................................................................................................... 26
  Windows Machine .......................................................................................................................................... 26
  iOS Device ...................................................................................................................................................... 28
Appendix: Connecting to Office 365 on Windows Machine Using Office ProPlus RemoteApp ......................... 32
  Creating a Remote Desktop Service Machine .............................................................................................. 33
  Creating an Azure RemoteApp Template Image ........................................................................................... 38
  Importing the Azure RemoteApp Template Image ....................................................................................... 39
  Creating a Microsoft Azure RemoteApp Collection ..................................................................................... 42
  Connecting to Office 365 on Windows Machine .......................................................................................... 44
Support Contacts ................................................................................................................................................. 47
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft Azure RemoteApp.

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.

Microsoft Azure RemoteApp helps employees stay productive anywhere, and on a variety of devices—Windows, Mac OS X, iOS, or Android. Your company’s applications run on Windows Server in the Azure cloud, where they’re easier to scale and update. Employees install Microsoft Remote Desktop clients on their Internet-connected laptop, tablet, or phone and then can access applications as if they are running locally.

This document describes how to:

- Configure SAML authentication in Microsoft Azure RemoteApp using SafeNet Authentication Service as an identity provider.

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

Microsoft Azure RemoteApp 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
- **Microsoft Azure RemoteApp**—Web Environment (a part of MS Azure Portal)

Audience

This document is targeted to system administrators who are familiar with Microsoft Azure RemoteApp, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

SAML Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides a service for SAML authentication that is already implemented in the SAS Cloud environment and can be used without any installation.

SAML Authentication 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 the Shibboleth infrastructure, which uses a special on-premises agent called SafeNet Authentication Service Agent for Shibboleth.

For more information on how to install and configure the SafeNet Authentication Service Agent for Shibboleth, refer to the SafeNet Support Portal.
SAML Authentication Flow using SafeNet Authentication Service

SafeNet Authentication Service (SAS) communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Microsoft Azure RemoteApp.

1. A user attempts to log on to Microsoft Azure RemoteApp. The user is redirected to AD FS proxy server (WAP), then after successful authentication, is forwarded to SafeNet Authentication Service 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 Microsoft Azure RemoteApp, accepting or rejecting the user’s authentication request.
4. The user is granted or denied access to Microsoft Azure RemoteApp.

SAML Prerequisites

To enable SafeNet Authentication Service (SAS) to receive SAML authentication requests from Microsoft Azure RemoteApp, ensure that the end users can authenticate from the Microsoft Azure RemoteApp environment with a static password.

Configuring Microsoft Azure RemoteApp and AD FS

Configuring Microsoft Azure RemoteApp and AD FS requires the following:

- Adding a Domain to Azure, page 7
- Syncing the Domain to Azure, page 9
- Verifying the AD Connect Installation, page 13
- Enabling Azure AD Federated Domains, page 14
- Configuring Gemalto SafeNet Authentication Service Agent for AD FS, page 16
- Configuring the AD FS Authentication Policy, page 17
- Creating a Microsoft Azure RemoteApp Collection, page 18
Adding a Domain to Azure

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

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

![Image](image1.png)

*(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**.

![Image](image2.png)

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

![Express Settings](image1)

*(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**.

![Connect to Azure AD](image2)

*(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**.

![Configuration complete](image)

(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 AD Connect Installation**

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

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

![Microsoft Azure](image)

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

![DIRECTORY INTEGRATION tab](image)

*(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.

<table>
<thead>
<tr>
<th>Integration with local active directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOMAINS VERIFIED FOR DIRECTORY SYNC</td>
</tr>
<tr>
<td>DOMAINS PLANNED FOR SINGLE SIGN-ON</td>
</tr>
<tr>
<td>DIRECTORY SYNC</td>
</tr>
<tr>
<td>LAST SYNC</td>
</tr>
</tbody>
</table>

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

**Enabling Azure AD Federated Domains**

You need to set the Azure’s domain to a federated domain to use AD FS authentication and AD FS MFA.

1. Log in to the AD FS server machine as the domain administrator.
3. At the command prompt, type **Connect-MsolService**, and then press **Enter**.
4. On the **Enter Credentials** window, enter your Azure AD administrator user name and password, and then click **OK**.

![Enter Credentials window](image)

*(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**.

![Command Prompt](image)

*(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.

![AD FS Management Console](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
Configuring Gemalto SafeNet Authentication Service Agent for AD FS

1. Run the Gemalto SafeNet Authentication Service (SAS) Agent for AD FS.

2. 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 “Configuring SafeNet Authentication Service Auth Node and Downloading Encryption Key” on page 23).
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**.

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.)
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. 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 **OK**.

![Multi-factor tab screenshot](image)

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

**Creating a Microsoft Azure RemoteApp Collection**

1. On the **Microsoft Azure** window, in the left pane, click **REMOTEAPP**, and then in the right pane, on the **REMOTEAPP COLLECTIONS** tab, click **CREATE A REMOTEAPP COLLECTION**.

![RemoteApp creation screenshot](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
2. On the **New** window, perform the following steps:
   a. Click **APP SERVICES > REMOTEAPP > QUICK CREATE**.
   b. Complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the Azure RemoteApp collection (for example, myremoteapp).</td>
</tr>
<tr>
<td><strong>REGION</strong></td>
<td>Select a region.</td>
</tr>
<tr>
<td><strong>PLAN</strong></td>
<td>Select a plan.</td>
</tr>
<tr>
<td><strong>TEMPLATE IMAGE</strong></td>
<td>Select the template image (for example, Office 365 ProPlus).</td>
</tr>
</tbody>
</table>
   c. Click the ✔️ icon.

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

On the **Microsoft Azure** window, in the right pane, the newly created Azure RemoteApp collection is listed with the **STATUS** as **Provisioning**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. After the provisioning process is complete, the status of the Azure RemoteApp collection is changed to **Active**. In the **NAME** column, click the newly created Azure RemoteApp collection (for example, **myremoteapp**).

![Screen Image of Azure RemoteApp](image1.png)

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

4. Click **publish remoteapp programs**.

![Screen Image of Azure RemoteApp](image2.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
5. On the **PUBLISH REMOTEAPP PROGRAMS** window, perform the following steps:
   a. Select or clear the boxes for the remote application programs you want to publish or remove.
   b. Click the [ ] icon.

   ![PUBLISH REMOTEAPP PROGRAMS](image)

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

6. On the **Microsoft Azure** window, in the right pane, click **configure user access**.

   ![Microsoft Azure](image)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
7. On the **USER ACCESS** tab, under **USERS**, in the box, enter the user principal name (UPN) of the user to whom you want to give access to the Microsoft Azure RemoteApp collection, and then click **Save**.

![Image](image.png)

**NOTE:** You can click the icon to add UPNs of more than one user at a time.

(Images above are from Microsoft® software. Trademarks are the property of their respective owners.)

### Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with Microsoft Azure RemoteApp using SAML authentication requires:

- Creating Users Stores in, page 22
- Assigning an Authenticator in, page 23
- Configuring SafeNet Authentication Service Auth Node and Downloading Encryption Key, page 23

### 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 or LDAP server using the SAS Synchronization Agent
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 Microsoft Azure RemoteApp.

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.

Configuring SafeNet Authentication Service Auth Node and Downloading 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.
8. Click the **Authentication Agent Settings** link, and then select **Download** to download the encryption key file. This file will be needed in step 4 of “Configuring Gemalto SafeNet Authentication Service Agent for AD FS” on page 16.

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

4. Under **Auth Nodes**, click **Add**.
5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Description</strong></td>
<td>Type a description for this node (for example, <strong>DC</strong>).</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Type a host name.</td>
</tr>
<tr>
<td><strong>Low IP Address In Range</strong></td>
<td>Type the low IP address.</td>
</tr>
<tr>
<td><strong>High IP Address In Range</strong></td>
<td>Type the high IP address. (The low and high IP addresses may be the same since the node is referencing a single machine.)</td>
</tr>
<tr>
<td><strong>Exclude from PIN change requests</strong></td>
<td>Do not select this check box.</td>
</tr>
</tbody>
</table>

![Auth Nodes screenshot](image)

Using the RADIUS protocol over the Internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, refer to the recommendations included in the SafeNet Authentication Service Administrator Guide.
Running the Solution

You need to install the Microsoft Azure RemoteApp client application on the client machine or device (for example, Windows or iOS).

Windows Machine

1. After installing Microsoft Azure RemoteApp client application on the client machine, double-click the following icon present on the machine’s desktop.

![Azure RemoteApp icon](image1)

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


![Azure RemoteApp window](image2)

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

3. On the Microsoft Azure RemoteApp login window, enter your AD user name (for example, bob@sfntdemo.com), and then click Continue.

![Azure RemoteApp login window](image3)

(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](image1)

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

5. After your credentials are authenticated by your organization’s AD FS, you are redirected to the SAS login window. In the **OTP** field, enter the generated OTP. Then, click **Submit**.

![Login Window](image2)
6. After successful authentication, you can access the Microsoft Azure RemoteApp collection. Click on the icon of any of the published applications to launch it.

![Microsoft Azure RemoteApp](image)

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

**iOS Device**

1. After installing Microsoft Azure RemoteApp client application on the device, double-tap the **RD Client** icon.

![RD Client](image)

*(The screen image above is from iOS software. Trademarks are the property of their respective owners.)*
2. On the **Microsoft Remote Desktop** window, tap the icon.

![Microsoft Remote Desktop window](image)

*It’s lonely here.*

To get started, add the remote desktop that you want to connect to using this device. You can also add remote resources to work with apps and desktops your administrator has set up for you.

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

3. Tap **Add Azure RemoteApp**.

![Add Azure RemoteApp](image)

*(The screen image above is from iOS software. Trademarks are the property of their respective owners.)*
4. Tap **Continue**.

![Azure RemoteApp](image)

**Azure RemoteApp**

Azure RemoteApp helps you use work apps from your phone, tablet or computer.

5. Enter your AD user name (for example, **bob@sfntdemo.com**) and then tap **Continue**.

![Microsoft Azure Sign In](image)

*(The screen image above is from iOS software. Trademarks are the property of their respective owners.)*
6. You are redirected to the AD FS login window. Enter your AD password and then tap **Sign in**.

![AD FS login window](image1)

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

7. After your credentials are authenticated by your organization's AD FS, you are redirected to the SAS login window. In the **OTP** field, enter the generated OTP, scroll down, and then tap **Continue**.

![SAS login window](image2)

*(The screen image above is from iOS software. Trademarks are the property of their respective owners.)*
8. After successful authentication, you can access the Microsoft Azure RemoteApp collection. Tap on the icon of any of the published applications to launch it.

![Microsoft Remote Desktop](image)

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

**Appendix: Connecting to Office 365 on Windows Machine Using Office ProPlus RemoteApp**

Users can connect to Office 365 accounts using Office ProPlus RemoteApp. In this scenario, you will need to create your own remote desktop machine that will be converted into a template image. On the remote desktop machine, you will need to configure the Azure AD Authentication Library (ADAL) feature that enables you to authenticate your Office 365 account from Office ProPlus RemoteApp using AD FS MFA and SafeNet Authentication Service (SAS) as the secondary authentication. So, users connecting to Office ProPlus RemoteApp will be able to login to their Office 365 account using AD FS MFA and SAS a secondary authentication.

Connecting to Office 365 using Office ProPlus RemoteApp requires:

- Creating a Remote Desktop Service Machine, page 33
- Creating an Azure RemoteApp Template Image, page 38
- Importing the Azure RemoteApp Template Image, page 39
- Creating a Microsoft Azure RemoteApp Collection, page 42
- Connecting to Office 365 on Windows Machine, page 44
Creating a Remote Desktop Service Machine

1. Log in to the Microsoft Azure Management portal.
2. On the **Microsoft Azure** window, click **New**.

3. On the **New** window, click **COMPUTE > VIRTUAL MACHINE > FROM GALLERY**.

(Images of the Microsoft Azure portal and New window are shown.)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On the CREATE A VIRTUAL MACHINE window, click Windows Server RDSHwO365P.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. Complete the following fields, and then click the ✨ icon.

<table>
<thead>
<tr>
<th><strong>VIRTUAL MACHINE NAME</strong></th>
<th>Enter a name for the remote desktop service machine (for example, RDS-RemoteApp).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TIER</strong></td>
<td>Select <strong>BASIC</strong> or <strong>STANDARD</strong> as per your preferred configuration.</td>
</tr>
<tr>
<td><strong>SIZE</strong></td>
<td>Select a size for the virtual machine as per your preferred configuration.</td>
</tr>
<tr>
<td><strong>NEW USER NAME</strong></td>
<td>Enter the administrator user name.</td>
</tr>
<tr>
<td><strong>NEW PASSWORD</strong></td>
<td>Enter the administrator password.</td>
</tr>
<tr>
<td><strong>CONFIRM</strong></td>
<td>Re-enter the administrator password.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. The configuration of the machine is verified. Click the icon.

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

7. Click the icon.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
8. The machine will restart automatically. Log in to the remote desktop service machine as an administrator and make the following changes to the registry keys:

<table>
<thead>
<tr>
<th>Registry Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\User Settings\ADAL</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\15.0\User Settings\ADAL\Create\Software\Microsoft\Office\15.0\CommonIdentity</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\15.0\User Settings\ADAL</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Office\15.0\User Settings\ADAL\Create\Software\Microsoft\Office\15.0\CommonIdentity</td>
<td>REG_DWORD</td>
<td>1</td>
</tr>
</tbody>
</table>

The registry keys changes will enable ADAL abilities for users connecting to the remote desktop service machine.

9. Restart the machine and then log in to the machine as an administrator.

   **NOTE:** Log in to one of the Office ProPlus software to verify if the ADAL feature is enabled and working.

10. On the machine’s desktop, double-click the following icon to run the PowerShell command.

    ![ValidateAzureRemoteApp Image](image_url)  

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

![Administrator: ValidateAzureRemoteAppImage window](image)

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

The PowerShell command validates the machine before converting it to an image and then runs the System Preparation (Sysprep) tool.

12. The machine will restart automatically. Shut down the machine.

Creating an Azure RemoteApp Template Image

1. Log in to the Microsoft Azure Management portal.

2. On the Microsoft Azure window, in the left pane, click VIRTUAL MACHINES, and then in the right pane, on the INSTANCES tab, select the virtual machine (for example, RDS-RemoteApp) that you created earlier in step 5 of “Creating a Remote Desktop Service Machine” on page 33, and then click CAPTURE.

![Microsoft Azure window](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the **Capture the virtual machine** window, complete the following fields, and then click the check icon.

<table>
<thead>
<tr>
<th>IMAGE NAME</th>
<th>Enter a name for the template image or use the default name (for example, RemoteDesktopPC-202508-775869).</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMAGE DESCRIPTION (LABEL)</td>
<td>Enter a description for the template image.</td>
</tr>
<tr>
<td>I have run Sysprep on the virtual machine</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

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

On the **Microsoft Azure** window, in the right pane, on the **IMAGES** tab, the new template image is listed.

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

**Importing the Azure RemoteApp Template Image**

Import the newly created Azure RemoteApp template image into the Azure RemoteApp image library.

1. Log in to the Microsoft Azure Management portal.
2. On the Microsoft Azure window, in the left pane, click REMOTEAPP, and then in the right pane, on the TEMPLATE IMAGES tab, click IMPORT OR UPLOAD A TEMPLATEG IMAGE.

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

NOTE: On the TEMPLATE IMAGES tab, click the icon to add a new image if a template image is already listed.

3. On the Add REMOTEAPP TEMPLATE IMAGE window, click Import an image from your Virtual Machines library.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On the IMPORT A TEMPLATE IMAGE window, perform the following steps:
   a. In the VIRTUAL MACHINE IMAGE field, select the template image (for example, RemoteDesktopPC-202508-775869) that you created previously in step 3 of “Creating an Azure RemoteApp Template Image” on page 38.
   b. Select I CONFIRM THAT I FOLLOWED THESE STEPS TO CREATE MY IMAGE.
   c. Click the icon.

5. Complete the following fields and then click the icon.

<table>
<thead>
<tr>
<th>NAME</th>
<th>Enter a name for the RemoteApp template image (for example, RDSmachineforRemoteApp).</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCATION</td>
<td>Select a location.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. On the Microsoft Azure window, in the right pane, the newly created RemoteApp template image is listed.

![Image of Microsoft Azure window with RemoteApp collection]

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

Creating a Microsoft Azure RemoteApp Collection

1. On the Microsoft Azure window, in the left pane, click REMOTEAPP, and then in the right pane, on the REMOTEAPP COLLECTIONS tab, click CREATE A REMOTEAPP COLLECTION.

![Image of Microsoft Azure window with CREATE A REMOTEAPP COLLECTION option]

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
2. On the **New** window, perform the following steps:
   a. Click **APP SERVICES > REMOTEAPP > QUICK CREATE.**
   b. Complete the following fields:
      | Name         | Enter a name for the Azure RemoteApp collection (for example, myremoteapp). |
      | REGION       | Select a region.                                                          |
      | PLAN         | Select a plan.                                                            |
      | TEMPLATE IMAGE | Select the template image for the Azure RemoteApp collection (for example, RDSmachineforRemoteApp) that you created earlier in step 5 of “Importing the Azure RemoteApp Template Image” on page 39. |
   c. Click the **✓** icon.

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

   On the **Microsoft Azure** window, in the right pane, the newly created Azure RemoteApp collection is listed with the **STATUS** as **Provisioning.**

   (The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
Connecting to Office 365 on Windows Machine

1. After installing Microsoft Azure RemoteApp client application on the client’s machine, double-click the following icon present on the machine’s desktop.

   ![Azure RemoteApp](image)

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

2. On the **Azure RemoteApp** window, click **Get Started**.

   ![Azure RemoteApp](image)

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

3. On the Microsoft Azure RemoteApp login window, enter your AD user name (for example, `bob@sfntdemo.com`), and then click **Continue**.

   ![Microsoft Azure](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**.

5. After your credentials are authenticated by your organization’s AD FS, you are redirected to the SAS login window. In the **OTP** field, enter the generated OTP. Then, click **Submit**.
6. After successful authentication, you can access the Microsoft Azure RemoteApp collection. Click on the icon of any of the published applications to launch it.

7. The Office ProPlus application is launched. In the right pane, click **Sign In**.
8. In the **OTP** field, enter your Personal Identification Pattern (PIP), and then click **Login**.

![Screen capture of SafeNet Authentication Service login page](image)

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

After successful authentication, you will be able to access the launched application.

## 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><strong>Address</strong></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><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></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>