SafeNet Authentication Service
Push OTP Integration Guide

Using SAS as an Identity Provider for Microsoft Dynamics CRM
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: 007-013355-001, Rev. A
Release Date: November 2015
Third-Party Software Acknowledgement

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

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.

Dynamics CRM is the customer relationship management software developed by Microsoft. Out of the box, the product focuses mainly on sales, marketing, and service (helpdesk) sectors.

This document describes how to:

- Configure Microsoft Dynamics CRM to work with AD FS as an authenticator and SafeNet Authentication Service as a secondary authentication method.

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

Microsoft Dynamics CRM can be configured to support multi-factor authentication in several modes. The AD FS MFA will be used for the purpose of working with the SafeNet Authentication Service Push OTP solution.

The primary objective of the Push OTP solution is to reduce the friction around two-factor authentication, and provide users with an improved two-factor authentication experience.

It is likely that most users already own and always carry a device that can be used as a second factor of authentication. Using the mobile phone as an authenticator replaces the need for a user to carry any additional hardware. So, with Push OTP, a user can:

- Receive authentication requests in real-time via push notifications to his or her smart phone.
- Assess the validity of the request with the information displayed on the screen.
- Respond quickly with a one-tap response to approve or deny the authentication.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet's cloud-based authentication service
- **MobilePASS+ application**
- **Gemalto SafeNet SAS Agent for AD FS**—Version 2.0
Environment

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

- SafeNet Authentication Service (SAS)
- Microsoft Dynamics CRM Server 2015
- AD FS—in Windows Server® 2012 R2

Audience

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

SAS Authentication API using SAS Cloud

SAS 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 Agent for AD FS.

SAS Authentication API and Push Protocol 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 Agent for AD FS is an AD FS multi-factor authentication 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 Microsoft Dynamics CRM.

1. A user attempts to log on to Microsoft Dynamics CRM. The user is redirected to the AD FS proxy server (WAP).
2. After successful authentication, the user is forwarded to SafeNet Authentication Service (SAS) for a secondary authentication (AD FS multi-factor authentication).
3. SAS identifies the user or mobile device, and detects that the OTP field is empty. Then:
   - SAS will directly trigger a Push OTP authentication request.
   - The user receives a push notification on the configured mobile device to indicate there is a login request pending.
   - The user taps on the notification to view the login request details, and can respond with a tap to approve or deny the request (approving will require providing the token’s PIN code).
4. The SAS authentication reply is sent back to AD FS, which returns a response to Microsoft Dynamics CRM, accepting or rejecting the user’s authentication request.
5. The user is granted or denied access to Microsoft Dynamics CRM.

**Push OTP Prerequisites**

In order to use SAS OTP, you will need:
- SAS configured to enable OTP
- MobilePASS which is supported on the following OS platforms:
  - MobilePASS+ (Push OTP support)
    - Android 4.x, 5.x
    - iOS 7+
- Gemalto SafeNet SAS Agent for AD FS—Version 2.0
Other Prerequisites

- Ensure that you have a public wildcard certificate matching to your domain name (for example, *.safenetdemos.com).
- Certificate Authority goes to Trusted Root Certification Authorities and the wildcard certificate goes into the Personal store.
- Ensure that the public wildcard certificate *.<domain name.com> (for example, *.safenetdemos.com) is installed in the certificate Personal store, the Trusted Root Authorities store in the AD FS machine, and the Dynamics CRM machine with a private key.
- Ensure that the public wildcard certificate *.<domain name.com> (for example, *.safenetdemos.com) is bound to separate ports in IIS (for example, port 444 for Microsoft Dynamics CRM and port 443 for AD FS).

Configuring Microsoft Dynamics CRM

Configuring Microsoft Dynamics CRM requires the following:

- Configuring Root Domain Web Address in CRM, page 7
- Configuring CRM Server for Claims-based Authentication, page 9
- Configuring Active Directory Security Groups, page 14
- Kernel-mode Authentication, page 22
- Configuring Claims Provider Trusts in AD FS, page 25
- Configuring AD FS Replying Party Trust for Claims-based Authentication, page 28
- Configuring Internet Facing Deployment on the CRM Server, page 38
- Configuring AD FS Relying Party Trust for the Internet Facing Deployment, page 48

Configuring Root Domain Web Address in CRM

Bind the Microsoft Dynamics CRM server to HTTPS, and configure the root domain web address. Also, configure the internal URL for CRM. Users can use this URL, if they want to access CRM within the network without being prompted for credentials.

1. Open the Microsoft Dynamics CRM Deployment Manager.
2. On the Microsoft Dynamics CRM main window, in the left pane, right-click Microsoft Dynamics CRM, and then select Properties.
3. On the Microsoft Dynamics CRM Properties window, on the Web Address tab, complete the following fields, and then click OK.

<table>
<thead>
<tr>
<th>Binding Type</th>
<th>Select HTTPS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Application Server</td>
<td>Enter &lt;Internal URL used to access Microsoft Dynamics CRM&gt;:&lt;Port&gt; (for example, internalcrm.safenetdmeos.com:444).</td>
</tr>
<tr>
<td>Organization Web Service</td>
<td>Enter &lt;Internal URL used to access Microsoft Dynamics CRM&gt;:&lt;Port&gt; (for example, internalcrm.safenetdmeos.com:444).</td>
</tr>
<tr>
<td>Discovery Web Service</td>
<td>Enter &lt;Internal URL used to access Microsoft Dynamics CRM&gt;:&lt;Port&gt; (for example, internalcrm.safenetdmeos.com:444).</td>
</tr>
<tr>
<td>Deployment Web Service</td>
<td>Enter &lt;Internal URL used to access Microsoft Dynamics CRM&gt;:&lt;Port&gt; (for example, internalcrm.safenetdmeos.com:444).</td>
</tr>
</tbody>
</table>

**NOTE:**
- <Internal URL used to access Microsoft Dynamics CRM> refers to the URL that users can use if they want to access CRM within the network without being prompted for credentials.
- <Port> refers to the SSL port bound to the Microsoft Dynamics CRM website (for example, 444).
Configuring CRM Server for Claims-based Authentication

Claims-based authentication is a set of WS-* standards describing the use of a Security Assertion Markup Language (SAML) token. Claims-based authentication requires the availability of a security token service (STS) running on a server. An STS server can be based on Active Directory Federation Services (AD FS) or any platform that provides the official STS protocol.

1. On the Microsoft Dynamics CRM main window, in the left pane, right-click Microsoft Dynamics CRM, and then select Configure Claims-Based Authentication.
2. On the Configure Claims-Based Authentication Wizard window, click Next.

![Configure Claims-Based Authentication Wizard](image)

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

3. In the Federation metadata URL field, enter the federation metadata URL (for example, https://<FQDN of AD FS server>/federationmetadata/2007-06/federationmetadata.xml), and then click Next.

---

**NOTE:** The federation metadata URL is from the AD FS 3.0 federation server, which is configured by default to publish metadata describing itself via HTTPS.

To verify the correct URL, open Internet Explorer in the AD FS 3.0 server and view the federation metadata by using the above URL. Verify that no certificate-related warnings appear.
4. Click Select.

5. On the Windows Security window, select the public wildcard certificate (for example, *.<domain name.com>) as mentioned in the Other Prerequisites section, and then click OK.
6. Click **Next**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
7. Review the results, fix problems if required, and then click **Next**.

![Configure Claims-Based Authentication Wizard](image)

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

8. Review your selections and then click **Apply**.

![Configure Claims-Based Authentication Wizard](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
9. Click the **View the log file** link, scroll to the bottom of the file and copy the **Federation metadata URL**. This URL will be used in “Configuring AD FS Relying Party Trust for Claims-based Authentication” on page 29. Then, click **Finish**.

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

**Configuring Active Directory Security Groups**

While installing Dynamics CRM 2015, the following Active Directory Security Groups also get installed:

- PrivReportingGroup
- SQLAccessGroup
- ReportingGroup
- PrivUserGroup

For all the four AD security groups, you need to grant permissions to the following accounts:

- CRM server account
- Administration account
- Application pool account
Locating the CRMAppPool Account

You can use IIS Manager to determine which account was used during setting up the CRMAppPool account.
1. From the Start menu, open the Internet Information Services (IIS) console.
2. In the left pane, under Connections, expand the organization node (for example, CRMSERVER), and then select Application Pools.

In the right pane, the CRMAppPool application pool is listed. For the CRMAppPool application pool, note down the account name from the Identity column (for example, SAFENETDEMOS\TESTUSER1).

Granting Permissions in the AD Security Groups

To allow access to the internal URL of Dynamics CRM, grant the Read and Write permissions to the following accounts for the four security groups in the active directory:

- CRM server account
- Administration account
- Application pool account

1. From the Start menu, open Active Directory Users and Computers.
2. On the Active Directory Users and Computers window, in the left pane, expand the domain name as per your environment (for example, safenetdemos.com), and then select the organizational account for Dynamics CRM created at the time of CRM installation (for example, CRM 2015).
3. In the right page, right-click PrivReportingGroup, and then select Properties.

4. On the PrivReportingGroup window, click the Security tab, and then click Add.
5. On the **Select Users, Computers, Service Accounts, Or Groups** window, under the **Enter the Object names to select** box, enter the name of the CRMApplPooI user (for example, **testuser1**), click **Check Names**, and then click **OK**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. On the **Security** tab, perform the following steps:
   a. Under **Group or user names**, select the newly added user (for example, **testuser1**).
   b. Under **Permissions for testuser1**, in the **Allow** column, select the box for the **Write** permission.
   c. Click **OK**.

   ![Screen shot](image)

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

7. Repeat steps 3 to 4.

8. On the **Select Users, Computers, Service Accounts, Or Groups** window, click **Object Types**.

   ![Screen shot](image)

   (The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
9. On the **Object Types** window, select the box for **Computers**, and then click **OK**.

(Click image for full view. Trademarks are the property of their respective owners.)

10. Under the **Enter the Object names to select** box, enter the name of your CRM Server (for example, **CRMSERVER**), click **Check Names**, and then click **OK**.

(Click image for full view. Trademarks are the property of their respective owners.)
11. On the **Security** tab, perform the following steps:

   a. Under **Group or user names**, select the newly added computer (for example, **CRMSERVER**).
   
   b. Under **Permissions for CRMSERVER**, in the **Allow** column, select the box for the **Write** permission.
   
   c. Click **OK**.

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

12. Repeat steps 3 to 4.

13. On the **Select Users, Computers, Service Accounts, Or Groups** window, under the **Enter the Object names to select** box, enter the name of the administrator account (for example, **Administrator**), click **Check Names**, and then click **OK**.

   (The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
14. On the **Security** tab, perform the following steps:
   
a. Under **Group or user names**, select the newly added administrator account (for example, **Administrator**).
   
b. Under **Permissions for Administrator**, in the **Allow** column, select the boxes for the **Full Control**, **Read**, and **Write** permissions.
   
c. Click **OK**.

15. Repeat steps 1 to 14 for the remaining security groups:
   
   - SQLAccessGroup
   - ReportingGroup
   - PrivUserGroup
Kernel-mode Authentication

Internet Information Services (IIS) 7.0 enables kernel-mode authentication by default, and this authentication runs under the machine account. However, Microsoft Dynamics CRM can be configured to run under a domain account, so Kerberos service ticket decryption will fail if kernel mode authentication is enabled.

To determine if a Microsoft Dynamics CRM deployment is using kernel-mode authentication, perform the following steps:

1. From the Start menu, open the Internet Information Services (IIS) console.
2. In the left pane, under Connections, expand the organization node (for example, CRMSERVER), and then click Sites > Microsoft Dynamics CRM.
3. In the right pane, under IIS, double-click Authentication.

4. Select Windows Authentication, and then in the right pane, under Actions, click Advanced Settings.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. On the **Advanced Settings** window, if **Enable Kernel-mode authentication** is selected, it means that the deployment is using kernel-mode authentication. Click **Cancel**.

![Advanced Settings Window](image)

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

### Configuring IIS for useAppPoolCredentials

If Kernel-mode authentication is enabled and domain account is used as the CRM application pool identity, configure IIS to useAppPoolCredentials.

1. From the **Start** menu, open the **Internet Information Services (IIS)** console.
2. In the left pane, under **Connections**, expand the organization node (for example, **CRMSERVER**), and then click **Sites > Microsoft Dynamics CRM**.
3. In the right pane, under **Management**, double-click **Configuration Editor**.

![Configuration Editor](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
4. In the **Configuration Editor** page, in the **Section** field, click **system.web.Server > Security > authentication > windowsAuthentication**.

   ![Configuration Editor](image1)

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

5. In the **useAppPoolCredentials** row, select **True**.

   ![Configuration Editor](image2)

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

6. In the right pane, under **Actions**, click **Apply**.

   ![Configuration Editor](image3)

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

7. From the **Start** menu, open **Run**.
8. On the **Run** window, in the **Open** field, enter `iisreset`, and then click **OK**.

   ![Run Window]

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

**Configuring Claims Provider Trusts in AD FS**

Add a claims rule to retrieve the user principal name (UPN) attribute from Active Directory and send it to Microsoft Dynamics CRM as a UPN.

1. From the **Start** menu, open **AD FS Deployment Manager**.
2. In the left pane, expand **AD FS > Trust Relationships**, and then click **Claims Provider Trusts**.
3. In the middle pane, right-click **Active Directory**, and then click **Edit Claim Rules**.

   ![AD FS Deployment Manager]

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
4. On the **Edit Claim Rules for Active Directory** window, click **Add Rule**.

![Edit Claim Rules for Active Directory](image)

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

5. On the **Add Transform Claim Rule Wizard** window, in the **Claim rule template** field, select **Send LDAP Attributes as Claims**, and then click **Next**.

![Add Transform Claim Rule Wizard](image)

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

<table>
<thead>
<tr>
<th>Claim rule name</th>
<th>Enter a name for the claim rule (for example, <strong>UPN Claim Rule</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute store</strong></td>
<td>Select <strong>Active Directory</strong>.</td>
</tr>
<tr>
<td><strong>LDAP Attribute</strong></td>
<td>Select <strong>User Principal Name</strong>.</td>
</tr>
<tr>
<td><strong>Outgoing Claim Type</strong></td>
<td>Select <strong>UPN</strong>.</td>
</tr>
</tbody>
</table>

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

7. On the **Edit Claim Rules for Active Directory** window, click **OK**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
Configuring AD FS Replying Party Trust for Claims-based Authentication

Configure Microsoft Dynamics CRM Server 2015 as a relying party to consume claims from AD FS 3.0 for authenticating internal claims access.

1. From the Start menu, open AD FS Deployment Manager.
2. In the left pane, expand AD FS > Trust Relationships. Then, right-click Relying Party Trusts and select Add Relying Party Trust.

3. On the Welcome window, click Start.
4. On the Select Data Source window, perform the following steps:
   a. Select Import data about the relying party published online or on a local network.
   b. In the Federation metadata address field, enter the federation metadata URL configured for claims-based authentication.
      This is the URL you copied earlier from the log file in “Configuring CRM Server for Claims-based Authentication” on page 9.
   c. Click Next.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. On the **Specify Display Name** window, in the **Display name** field, a name is displayed automatically. Click **Next**.

![Specify Display Name](image)

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

6. On the **Configure Multi-factor Authentication Now** window, click **Next**.

![Configure Multi-factor Authentication Now](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
7. On the **Choose Issuance Authorization Rules** window, select **Permit all users to access this relying party**, and then click **Next**.

8. In the **Ready to Add Trust** window, click **Next**.
9. On the **Finish** window, click **Close**.

![Add Relying Party Trust Wizard](image)

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

10. On the **Edit Claim Rules for internalcrm.safenetdemos.com** window, click **Add Rule**.

![Edit Claim Rules for internalcrm.safenetdemos.com](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
11. On the **Select Rule Template** window, in the **Claim rule template** field, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.

![Select Rule Template](image)

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

12. On the **Configure Rule** window, complete the following fields, and then click **Finish**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim rule name</td>
<td>Enter a name for the claim rule (for example, <strong>Pass Through UPN</strong>).</td>
</tr>
<tr>
<td>Incoming claim type</td>
<td>Select <strong>UPN</strong>.</td>
</tr>
</tbody>
</table>

![Configure Rule](image)

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

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

14. On the Select Rule Template window, in the Claim rule template field, select Pass Through or Filter an Incoming Claim, and then click Next.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
15. On the **Configure Rule** window, complete the following fields, and then click **Finish**:

<table>
<thead>
<tr>
<th>Claim rule name</th>
<th>Enter a name for the claim rule (for example, <strong>Pass Through Primary SID</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming claim type</td>
<td>Select <strong>Primary SID</strong>.</td>
</tr>
</tbody>
</table>

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

16. On the **Edit Claim Rules for internalcrm.safenetdemos.com** window, click **Add Rule**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
17. On the Select Rule Template window, in the Claim rule template field, select Transform an Incoming Claim, and then click Next.

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

18. On the Configure Rule window, complete the following fields, and then click Finish:

<table>
<thead>
<tr>
<th>Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claim rule name</td>
<td>Enter a name for the claim rule (for example, Transform Windows Account Name to Name).</td>
</tr>
<tr>
<td>Incoming claim type</td>
<td>Select Windows Account Name.</td>
</tr>
<tr>
<td>Outgoing claim type</td>
<td>Select *Name.</td>
</tr>
</tbody>
</table>

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

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
Configuring Internet Facing Deployment on the CRM Server

Configuring an IFD enables access to Microsoft Dynamics CRM from the Internet, outside the company firewall, without using a virtual private network (VPN) solution. Microsoft Dynamics CRM configured for Internet access uses claims-based authentication to verify credentials of external users.

1. On the Microsoft Dynamics CRM Deployment Manager main window, in the right pane, click Configure Internet Facing Deployment.

   ![Microsoft Dynamics CRM Deployment Manager](image1)

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

2. On the Internet-Facing Deployment Configuration Wizard window, click Next.

   ![Internet-Facing Deployment Configuration Wizard](image2)

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

<table>
<thead>
<tr>
<th><strong>Web Application Server Domain</strong></th>
<th>Enter &lt;Domain name of the Dynamics CRM server&gt;:&lt;SSL port bound to the Microsoft Dynamics CRM website&gt; (for example, safenetdemos.com:444).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Organization Web Service Domain</strong></td>
<td>Enter &lt;Domain name of the Dynamics CRM server&gt;:&lt;SSL port bound to the Microsoft Dynamics CRM website&gt; (for example, safenetdemos.com:444).</td>
</tr>
<tr>
<td><strong>Discovery Web Service Domain</strong></td>
<td>Enter &lt;External DNS record for the Discovery Web Service Domain&gt;:&lt;SSL port bound to the Microsoft Dynamics CRM website&gt; (for example, dev.safenetdemos.com:444).</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. In the **Enter the external domain where your Internet-facing servers are located** field, the URL `auth.<domain.name>` is displayed automatically. Add the SSL port bound to the Microsoft Dynamics CRM website (for example, `auth.<domain.name>:444`), and then click **Next**.

5. Review the results, fix problems if required, and then click **Next**.
6. Click **Apply**.

![Image](image_url)

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

7. Click the **View the log file** link, scroll to the bottom of the file and copy the **Federation metadata URL**. This URL will be used in “Configuring AD FS Relying Party Trust for the Internet Facing Deployment” on page 48. Then, click **Finish**.

![Image](image_url)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
Configuring a Wildcard Certificate for READ Permission

The wildcard certificate provided for authentication should be trusted by the computer where you are installing Microsoft Dynamics CRM 2015. Hence, the CRMAppPool account of each Microsoft Dynamics CRM Web application must have READ permission to the private key of the encryption certificate.

1. On the Microsoft Dynamics CRM server, open Microsoft Management Console (MMC).

2. On the MMC window, click File > Add/Remove Snap-in.

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

3. On the Add or Remove Snap-ins window, in the Available snap-ins box, select Certificates and then click Add.

   (The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On the Certificates snap-in window, select **Computer account**, and then click **Next**.

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

5. Click **Finish**.

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

7. On the MMC window, in the left pane, click **Console Root > Certificates > Personal > Certificates**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
8. In the middle pane, right-click the wildcard certificate (for example, *.safenetdemos.com), and then click All Tasks > Manage Private Keys.

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

9. Click Add.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
10. On the **Select Users, Computers, Service Accounts, or Groups** window, under the **Enter the object names to select** box, enter the name of the CRMAppPool user (for example, **testuser1**), click **Check Names**, and then click **OK**.

![Select Users, Computers, Service Accounts, or Groups](image)

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

11. On the **Security** tab, perform the following steps:

   a. Under **Group or user names**, select the newly added user (for example, **testuser1**).

   b. Under **Permissions for testuser1**, in the **Allow** column, select the box for the **Full Control** and **Read** permissions.

   c. Click **OK**.

![Permissions for *.saenetdemos.com private ...](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
12. Repeat step 9.

13. On the Select Users, Computers, Service Accounts, or Groups window, under the Enter the object names to select box, enter NETWORK SERVICE, click Check Names, and then click OK.

14. On the Security tab, perform the following steps:
   a. Under Group or user names, select the newly added computer (for example, NETWORK SERVICE).
   b. Under Permissions for NETWORK SERVICE, in the Allow column, select the box for the Full Control and Read permissions.
   c. Click OK.
Configuring AD FS Relying Party Trust for the Internet Facing Deployment

Configure Microsoft Dynamics CRM Server 2015 as a relying party to consume claims from AD FS 3.0 for authenticating Internet access. With CRM configured for Internet-Facing Deployment, your remote/off-site/mobile users will be able to connect to the CRM system with a web client without a VPN.

1. From the Start menu, open AD FS Deployment Manager.
2. In the left pane, expand AD FS > Trust Relationships. Then, right-click Relying Party Trusts and select Add Relying Party Trusts.
3. On the Welcome window, click Start.
4. On the **Select Data Source** window, perform the following steps:

   a. Select **Import data about the relying party published online or on a local network**.

   b. In the **Federation metadata address** field, enter the metadata URL to locate the federation metadata.xml file.

      This is the URL you copied earlier from the log file in “Configuring Internet Facing Deployment on the CRM Server” on page 38.

   c. Click **Next**.

   ![Select Data Source Window](image.png)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
5. On the **Specify Display Name** window, in the **Display Name** field, a name is displayed automatically. Click **Next**.

![Specify Display Name window](image)

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

6. On the **Configure Multi-factor Authentication Now** window, click **Next**.

![Configure Multi-factor Authentication Now window](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
7. On the **Choose Issuance Authorization Rules** window, select **Permit all users to access this relying party**, and then click **Next**.

8. On the **Ready to Add Trust** window, click **Next**.
9. On the **Finish** window, click **Close**.

![Add Relying Party Trust Wizard](image1)

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

10. On the **Edit Claim Rules for auth.safenetdemos.com** window, click **Add Rule**.

![Edit Claim Rules for auth.safenetdemos.com](image2)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
11. On the Select Rule Template window, in the Claim rule template field, select Pass Through or Filter an Incoming Claim, and then click Next.

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

12. On the Configure Rule window, complete the following fields, and then click Finish:

<table>
<thead>
<tr>
<th>Claim Rule Name</th>
<th>Enter a name for the claim rule (for example, Pass Through UPN).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Claim Type</td>
<td>Select UPN.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
13. On the **Edit Claim Rules for auth.safenetdemos.com** window, click **Add Rule**.

![Edit Claim Rules for auth.safenetdemos.com](image)

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

14. On the **Select Rule Template** window, in the **Claim rule template** field, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.

![Select Rule Template](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
15. On the **Configure Rule** window, complete the following fields, and then click **Finish**:

<table>
<thead>
<tr>
<th>Claim rule name</th>
<th>Enter a name for the claim rule (for example, <strong>Pass Through Primary SID</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming claim type</td>
<td>Select <strong>Primary SID</strong>.</td>
</tr>
</tbody>
</table>

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

16. On the **Edit Claim Rules for auth.safenetdemos.com** window, click **Add Rule**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
17. On the Select Rule Template window, in the Claim rule template field, select Transform an Incoming Claim, and then click Next.

![Add Transform Claim Rule Wizard](image)

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

18. On the Configure Rule window, complete the following fields, and then click Finish:

<table>
<thead>
<tr>
<th>Claim rule name</th>
<th>Enter a name for the claim rule (for example, Transform Windows Account Name to Name).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming claim type</td>
<td>Select Windows Account Name.</td>
</tr>
<tr>
<td>Outgoing claim type</td>
<td>Select *Name.</td>
</tr>
</tbody>
</table>

![Add Transform Claim Rule Wizard](image)

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

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

1. Run the Gemalto SafeNet SAS Agent for AD FS application.

2. On the SAS MFA Plug-In Manager window, on the Policy tab, perform the following steps:
   b. Under Default OTP Policy, select Push Challenge.

3. On the Communications tab, in the Primary Server IP field, enter the SAS server’s IP address or name (and port if non-causal is used). Also, ensure that Strip realm from UPN is selected.

   In case the SAS server is not installed on same machine as the AD and AD FS, the key encryption file needs to be loaded (as explained in “Configuring SAS Auth Node and Encryption Key” on page 66).
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 under **Authentication Test Result**.

6. Click **OK**.

**Configuring the AD FS Authentication Policy**

1. On the **AD FS Management Console**, in the left pane, under **AD FS**, select **Authentication Policies**. Then, in the right pane, click **Edit Global Primary Authentication**.

![AD FS Management Console](image)

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

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

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

Web Application Proxy (WAP) is a role service of the Remote Access server role in Windows Server 2012 R2. WAP provides reverse proxy functionality for web applications inside your corporate network to allow users on any device to access your web applications from outside the corporate network. WAP pre-authenticates access to web applications by using Active Directory Federation Services (AD FS), and also functions as an AD FS proxy.

1. Open **Remote Access Management Console**.
2. On the right pane, click **Publish**.

![Remote Access Management Console](image1.png)

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

3. On the **Welcome** window, click **Next**.

![Publish New Application Wizard](image2.png)

*The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.*
4. On the **Preauthentication** window, select **Pass-through**, and then click **Next**.

   ![Preauthentication window](image1.png)

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

5. On the **Publishing Settings** window, complete the following fields, and then click **Next**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name of your choice (for example, <strong>Domain ORG URL</strong>).</td>
</tr>
<tr>
<td><strong>External URL</strong></td>
<td>Enter <code>&lt;Organizational URL used to access Dynamics CRM&gt;:&lt;SSL port bound to the Microsoft Dynamics CRM website&gt;</code> (for example, <strong><a href="https://org1.safenetdemos.com:444">https://org1.safenetdemos.com:444</a></strong>).</td>
</tr>
<tr>
<td><strong>External Certificate</strong></td>
<td>Select the wildcard domain certificate (for example, *<strong>.safenetdemos.com</strong>).</td>
</tr>
</tbody>
</table>

   ![Publishing Settings window](image2.png)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
6. Repeat steps 1 to 5 to publish the following so that WAP is able to translate internal URLs to external URLs. Also, make sure your external DNS records for each of these URLs points to the WAP server now.

- External Org URL
- Auth URL
- Dev URL
- ADFS URL

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

Disabling URL Translation

Disable URL translation because WAP will re-scope the cookies as part of the URL translation, and CRM leverages a domain cookie that can be shared across sub-domains. If URL translation is not disabled, access to CRM will be prevented. Disabling URL translation will allow the WAP role to pass the cookie along that CRM is expecting.

1. From the Start menu, open Windows PowerShell as an administrator.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
2. Run the following command to get the ID of each of the CRM published URLs you have added:

```
Get-WebApplicationProxyApplication | Format-List
```

3. Copy all the IDs listed. For example, copy the ID that is marked in yellow in the image above.

4. Run the following command one-by-one after replacing `GUID` with the IDs you copied in the previous step:

```
Set-WebApplicationProxyApplication -ID <GUID> -DisableTranslateUrlInResponseHeaders
```

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

The deployment of multi-factor authentication using SAS with Microsoft Dynamics CRM using SAML authentication requires:

- Creating Users Stores in SAS, page 65
- Assigning an Authenticator in SAS, page 65
- Configuring SAS Auth Node and Encryption Key, page 66
- Enabling the Software Token Push OTP Setting, page 66
- Enabling the Allowed Targets Policy, page 68

Creating Users Stores in SAS

Before 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 additional 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 SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Microsoft Dynamics CRM.

The following authenticators are supported:

- 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 SAS Auth Node and Encryption Key

In the event that the 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 4 of “Configuring Gemalto SafeNet SAS Agent for AD FS” on page 58.

4. Click Virtual Servers > COMMS > Auth Nodes.
5. Click the Auth Nodes link, and then click Add.
6. Complete the Auth Notes tab as follows:

<table>
<thead>
<tr>
<th>Auth Node Name</th>
<th>Enter a name for the authentication node.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Name</td>
<td>Enter a resource name to identify, in a push notification, the authentication node it relates to.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the low IP address.</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter 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>Exclude from PIN change requests</td>
<td>Do not select this field.</td>
</tr>
</tbody>
</table>

Repeat steps 5 to 6 twice to add two Auth Nodes incorporating two server’s IPs as mentioned below:

- ADFS Server—SAS MFA agent communication with SAS
- WAP Server—Publish the internal URLs to communicate to the outside world with URL translation by WAP
Enabling the Software Token Push OTP Setting

To use Push OTP authentication, the setting must be enabled in the SAS token policy.

1. Log in to the SAS console with an Operator account.
2. Click the **POLICY** tab, and then select **Token Policies**.

![Image of Token Policies](image)

3. In the **Token Policies** module, click the **Software Token Push OTP Setting** link.

![Image of Software Token Push OTP Setting](image)

4. Select **Enable Push OTP communication with MobilePass+**, and then click **Apply**.

**Enabling the Allowed Targets Policy**

For Push OTP to be permitted during authentication the user must have a MobilePASS+ token enrolled and this policy must be enabled.

The settings to enable this policy will determine which OS targets are presented to users during the self-enrollment of MobilePASS tokens. You can restrict the targets on which MobilePASS+ or MobilePASS 8 tokens are allowed to be activated or enrolled.
1. Log in to the SAS console with an Operator account.

2. Click the POLICY tab, and then select **Token Policies**.

3. In the **Token Policies** module, click the **Allowed Targets Settings** link.

4. On the **MobilePASS** tab, select the desired targets to allow for each MobilePASS application, and then click **Apply**.
Running the Solution

1. Browse to your Microsoft Dynamics CRM Server website’s external address (for example, https://org1.safenetdemos.com:444).

2. You are redirected to the AD FS login page. Under Sign in with your organizational account, enter the Active Directory Username and Password, and then click Sign in.

3. After your credentials are authenticated by your organization’s AD FS, you are redirected to SAS to enter your one-time password (OTP). Select Use my mobile to autosend a passcode, and then click Submit.
4. A push notification is received on the configured mobile device. Tap **Approve**.

5. Enter the **Token PIN** and then tap **Continue**.

A successful message is displayed on the configured mobile device.

**Autosend passcode was successful.**
After successful authentication, you can access the Microsoft Dynamics CRM Dashboard.

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

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<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 1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International 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>