SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for IMC with IBM Domino (Notes Traveler)
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 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: 007-013521-001, Rev. A
Release Date: June 2016
# Contents

- Third-Party Software Acknowledgement ................................................................................. 4
- Description ................................................................................................................................. 4
- Applicability ............................................................................................................................... 5
- Environment ................................................................................................................................. 5
- Audience ...................................................................................................................................... 5
- RADIUS-based Authentication using SafeNet Authentication Service Cloud .................................. 6
- RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE .......................................................... 6
- RADIUS Authentication Flow using SafeNet Authentication Service ............................................. 7
- RADIUS Prerequisites .................................................................................................................... 7
- Configuring SafeNet Authentication Service ................................................................................. 8
  - Creating Users Stores in SafeNet Authentication Service .............................................................. 8
  - Assigning an Authenticator in SafeNet Authentication Service ..................................................... 8
  - Adding IMC as an Authentication Node in SafeNet Authentication Service ............................... 9
  - Checking the SafeNet Authentication Service RADIUS Address ............................................. 11
- Configuring the IMC Server ........................................................................................................... 12
  - Adding a RADIUS Authentication Profile on the IMC Server .................................................... 12
  - Adding a New Resource IP Connection Profile on the IMC Server ........................................... 16
- Running the Solution .................................................................................................................. 20
- Appendix A: Creating an IMC Connection .................................................................................... 22
- Appendix B: Trouble Shooting ....................................................................................................... 24
- Support Contacts ......................................................................................................................... 24
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as IMC (IBM Mobile Connect) with IBM Domino (Notes Traveler).

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 (SAS) 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.

IBM Mobile Connect (IMC) provides a full-featured wireless virtual private network (VPN). This software employs end-to-end data encryption to deliver security-rich access to enterprise applications over wireless and wired networks. IBM Mobile Connect enables access to enterprise applications and data from virtually any location, while protecting an organization’s sensitive information.

IBM® Domino® is an advanced platform for hosting social business applications. It delivers scalable, security-rich applications at a low cost, helping you improve productivity, accelerate operations and enhance decision-making.

IBM® Notes® Traveler (formerly IBM Lotus® Notes Traveler) is mobile email software that provides quick access to email, calendar and contacts from a wide range of mobile devices or tablets. This no charge mobile offering is available for IBM Notes and Domino® users. Enhance the productivity of your mobile workforce with this security-rich software.

This document describes how to:

- Deploy multi-factor authentication (MFA) options IMC with Lotus Domino using SafeNet one-time (OTP) authenticators managed by SafeNet Authentication Service.
- Configure IMC to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the IMC with IBM Domino (Notes Traveler) environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service. IMC can be configured to support multi-factor authentication in several modes. The RADIUS protocol 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 (SAS)**—Cloud version 3.5.2912.32855
- **Connection Manager**—Version 6152
- **Gatekeeper**—Version 6152
- **Mobility Client**—Version 6152
- **Domino Server**—Version 9.01
- **Traveler Server**—Version 9.0.1
- **Domino Client (Designer)** —Version 9.01
- **iNotes**—Version 9.0

Audience

This document is targeted to system administrators who are familiar with IMC with IBM Domino (Notes Traveler), and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service (SAS).
RADIUS-based Authentication using SafeNet Authentication Service Cloud

SafeNet Authentication Service (SAS) Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to:

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.

RADIUS-based Authentication using SafeNet Authentication Service-SPE and SafeNet Authentication Service-PCE

For both on-premises versions, SafeNet Authentication Service (SAS) can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS)** or the legacy **Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.
For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:


- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

**RADIUS Authentication Flow using SafeNet Authentication Service**

SafeNet Authentication Service (SAS) communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for IMC with IBM Domino (Notes Traveler).

1. A user attempts to log on to IMC with IBM Domino (Notes Traveler) (through a secure path) using IMC Mobility Client and an OTP token.
2. IMC sends a RADIUS request with the user’s credentials to SafeNet Authentication Service (SAS) for validation.
3. The SAS authentication reply is sent back to IMC.
4. The user is granted or denied access to IMC based on the OTP value calculation results from SAS.
5. The user is able to connect to IBM Domino (IBM Notes Traveler) through a secure connection.

**RADIUS Prerequisites**

To enable SafeNet Authentication Service (SAS) to receive RADIUS requests from IMC to access IBM Domino Traveler, ensure the following:

- End users can authenticate from the IMC environment with a static password before configuring IMC to use the RADIUS authentication.
• Ports 1812/1813 are open to and from IMC
• A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
• IBM Lotus Domino (8.0.1) with IBM Notes Traveler is up and running on another machine.
• Before install the IMC server, SQL and .Net Framework 4.0 must be installed on the same machine.
• All the configured services on IMC server are up and running.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with IMC using RADIUS protocol requires the following:

• Creating Users Stores in , page 8
• Assigning an Authenticator in , page 8
• Adding IMC as an Authentication Node in , page 9
• Checking the SafeNet Authentication Service RADIUS Address, page 11

Creating Users Stores in SafeNet Authentication Service

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

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

For 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 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 IMC.

The following authenticators are supported:

• eToken PASS
• RB-1 Keypad Token
• KT-4 Token
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.


**Adding IMC as an Authentication Node in SafeNet Authentication Service**

Add a RADIUS entry in the SafeNet Authentication Service (SAS) **Auth Nodes** module to prepare it to receive RADIUS authentication requests from IMC. You will need the IP address of IMC and the shared secret to be used by both SAS and IMC.

1. Log in to the SAS console with an Operator account.

![Image of SafeNet console](http://www.safenet-inc.com/resources/integration-guide/data-protection/Safenet_Authentication_Service/Safenet_Authentication_Service__Subscriber_Account_Operator_Guide/)
2. Click the **COMMS** tab, and then select **Auth Nodes**.

3. In the **Auth Nodes** module, click the **Auth Nodes** link.

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>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>
The authentication node is added to the system.

### Checking the SafeNet Authentication Service RADIUS Address

Before adding SafeNet Authentication Service (SAS) as a RADIUS server in IMC, check its IP address. The IP address will then be added to IMC, as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.
2. Click the **COMMS** tab, and then select **Auth Nodes**.
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes Module](image)

### Configuring the IMC Server

Configuring the IMC server requires:

- Adding a RADIUS Authentication Profile on the IMC Server, page 12
- Adding a New Resource IP Connection Profile on the IMC Server, page 16

**NOTE:** Before adding a RADIUS Authentication Profile on the IMC server, Shut down the Connection Manager, and then check and ensure that the status of Connection Manager is stopped.

### Adding a RADIUS Authentication Profile on the IMC Server

1. On the IMC Server machine, click **Start > All Programs > IBM Mobile Connect > Gatekeeper**.
2. On the **Gatekeeper - Login** window, enter the administrator user ID and password, and then click **Log In**.

![Gatekeeper - Login](image)

*(The screen image above is from IBM®. Trademarks are the property of their respective owners.)*
3. On the IMC server administrator console, in the left pane, expand Mobile Connect, right-click the organizational unit (for example, SafeNet-Inc), and then click Add Resource > Authentication Profile > RADIUS Authentication.

![Image of IMC configuration interface](image.png)

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

4. On the Add a New Authentication Profile window, complete the following fields, and then Click Next.

<table>
<thead>
<tr>
<th><strong>Common Name</strong></th>
<th>Enter a name for the authentication profile (for example, SAS RADIUS Authentication Profile).</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Enter a description for the authentication profile.</td>
</tr>
<tr>
<td><strong>Challenge user for user ID and password</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

![Image of RADIUS authentication profile configuration](image.png)

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of RADIUS servers</td>
<td>Enter the IP address of the SAS RADIUS server.</td>
</tr>
<tr>
<td>Port number of RADIUS servers</td>
<td>Enter the port number of the SAS RADIUS server port.</td>
</tr>
<tr>
<td>RADIUS shared Secret</td>
<td>Enter the SAS RADIUS shared secret that you entered earlier in step 2 of</td>
</tr>
<tr>
<td></td>
<td>“Adding IMC as an Authentication Node in SafeNet Authentication Service” on</td>
</tr>
<tr>
<td></td>
<td>page 9.</td>
</tr>
</tbody>
</table>

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

6. Ensure that **Enable LTPA** is not selected. Click **Next**.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
7. Select the organizational unit (for example, **SafeNet-Inc**) in which the newly created RADIUS authentication profile is added, and then click **Finish**.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
Adding a New Resource IP Connection Profile on the IMC Server

1. On the IMC server administrator console, in the left pane, expand Mobile Connect, right-click the organizational unit (for example, SafeNet-Inc), and then click Add Resource > Connection Profile > Connection Profile (IP).

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
2. On the **Add a Connection Profile** window, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Common name</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a name for the connection profile (for example, <em>IP Connection Profile</em>).</td>
<td>Enter a description for the connection profile.</td>
</tr>
</tbody>
</table>

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

3. Click **Next**.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
4. Under **Transport profile(s)**, select the transport profile (for example, **LAN - Transport profile for LAN**) to be assigned to the connection profile, and then click **Next**.

5. Complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Diffie-Hellman</strong></th>
<th>Select this key exchange algorithm.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client validation model</strong></td>
<td>Select <strong>None</strong>.</td>
</tr>
<tr>
<td><strong>Authentication profile</strong></td>
<td>Select the RADIUS authentication profile (for example, <strong>SAS RADIUS Authentication</strong>) that you created earlier in step 4 of &quot;Adding a RADIUS Authentication Profile on the IMC Server&quot; on page 12.</td>
</tr>
</tbody>
</table>
6. Select the primary organizational unit (for example, SafeNet-Inc) in which the newly created connection profile is added, and then click Finish.

7. On the IMC server administrator console, in the left pane, expand Mobile Connect, expand Default Resources, and then double-click Connection Profile.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
8. In the right pane, in the **common name** column, select **IP profile**, and then click **Properties**.

9. On the **Connection Profile (IP)** window, on the **Security tab**, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Diffie-Hellman</strong></th>
<th>Select this key exchange algorithm.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client validation model</strong></td>
<td>Select <strong>None</strong>.</td>
</tr>
<tr>
<td><strong>Authentication profile</strong></td>
<td>Select the RADIUS authentication profile (for example, <strong>SAS RADIUS Authentication Profile</strong>) that you created earlier in step 4 of “Adding a RADIUS Authentication Profile on the IMC Server” on page 12.</td>
</tr>
</tbody>
</table>

![Connection Profile (IP) window](image)

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

**Running the Solution**

For this integration, SafeNet MobilePASS token is configured for authentication with the SafeNet Authentication Service (SAS) solution.

1. On the client machine, double-click the IMC connection icon (for example, **SafeNet-Inc**).

![SafeNet-Inc icon](image)

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
2. On the IMC server connection window, complete the following fields, and then click **Connect**.

<table>
<thead>
<tr>
<th>Organizational unit</th>
<th>Enter the name of the organizational unit (for example, <strong>SafeNet-Inc</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Enter your user name.</td>
</tr>
<tr>
<td>Password</td>
<td>Generate an OTP using the SafeNet MobilePASS token, and then enter that OTP in this field.</td>
</tr>
</tbody>
</table>

![IMC connection window](image)

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

After successful authentication, you will be logged in to the IMC server. In the system tray, the following icon will be displayed indicating that the connection with the IMC server is established.

![System tray icon](image)

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

3. In a web browser, open any of the following URLs to open Domino, iNotes, or Notes Traveler, respectively:
   - `http://<Domain Or IP>/Mail/Admin.nsf` (iNotes)
   - `http://<Domain or IP>/names.nsf` (Domino Server)
   - `http://<Domain or IP>/traveler.nsf` (Traveler)

   **NOTE:** As confirmed by IBM, Domino, iNotes, or Notes Traveler does not support single sign-on (SSO). So, after connecting to IMC using the token password, enter the default user credentials created in the Domino directory.

   Ticket No: PMR 25437,756,000
   IBM Person: Brian C Erle (erlebc@us.ibm.com)
4. On the login window, enter your static username and password created in the Domino directory, and then click **Log in**.

![Server Login](image1)

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

After successful authentication, you will be allowed to access IBM Notes Traveler.

![Lotus Traveler](image2)

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

**Appendix A: Creating an IMC Connection**

1. On the client machine, click **Start > All Programs > IBM Mobility Client > Connections.**

2. On the **Mobility Connections** window, double-click the **Create Connection** icon.

![Mobility Connections](image3)

*(The screen image above is from IBM®. Trademarks are the property of their respective owners.)*
3. On the **Create a Connection** window, enter the name of the mobility connection (for example, **SafeNet-Inc**), and then click **Next**.

4. On the **Network Setup - IP Based** window, enter the IP address of IMC, and then click **Next**.

5. Click **Finish**.
6. The **Start Dialer** confirmation message is displayed. Click **Yes** to start the connection instantly or **No** start the connection later.

![Start Dialer](image)

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

### Appendix B: Trouble Shooting

The following challenges were faced during this integration:

- In this solution, the two IMC interfaces could not be taken as internal and external due to some lab environment snags. So, both the interfaces were taken as internal and internal.

- After connecting to IMC using the token password, the LTPA token does not work every-time to connect to IBM Domino. IBM Domino asks for a new LTPA token every-time. To resolve this challenge, you will need to enter your login credentials twice, one while connecting to IMC and second while connecting to IBM Domino.

### 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&lt;br&gt;4690 Millennium Drive&lt;br&gt;Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td>United States 1-800-545-6608&lt;br&gt;International 1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">Customer Portal</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>