SafeNet Authentication Service
Integration Guide

Using SafeNet Authentication Service as an Identity Provider for IBM Domino
Third-Party Software Acknowledgement

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

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.

IBM Notes and IBM Domino are the client and server, respectively, of a collaborative client-server software platform marketed by IBM. The IBM Notes software client simplifies today’s complex world by integrating messaging, business applications, and social collaboration into one easy-to-use workspace. IBM Notes goes wherever you go, helping you work smarter and faster to provide better business results.

This document describes how to:

- Configure SAML authentication in IBM Domino using SafeNet Authentication Service as an identity provider.

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

IBM Domino 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**—SafeNet’s cloud-based authentication service
- **IBM Domino 9.0.1**
- **AD FS Proxy Server 2.0**
• AD FS Server 2.0
• Notes Client 9.0.1
• Domino Administrator Client 9.0.1

**Audience**

This document is targeted to system administrators who are familiar with IBM Domino, 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 IBM Domino.

1. A user attempts to log on to IBM Domino through the IBM Domino URL.
2. The user is redirected to the AD FS proxy server, which in turn redirects to the AD FS page where the user selects the SAS claim provider.
3. The user is redirected to the SAS Logon page. The user enters the credentials, which are forwarded to the SAS server. SAS collects and evaluates the user's credentials.
4. SAS returns a response to IBM Domino via AD FS, accepting or rejecting the user's authentication request.
SAML Prerequisites

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

Configuring IBM Domino

The federations compatible with IBM Domino are:

- Microsoft Active Directory Federation Services (AD FS) 2.0 integrated with Active Directory
- IBM Tivoli Federated Identity Manager (TFIM, IBM Security Identity Manager)

In this integration guide, we are using AD FS 2.0 as an identity provider for IBM Domino.

Setting up Web Federated Login with IBM iNotes

Web federated login requires the following four components:

- A web browser client for all iNotes users
- A Domino web server running iNotes and functioning as the home (mail) server for iNotes client users
- A Domino ID vault server
- SAML identity provider

To set up web federated login, the iNotes server and the Vault server can be on the two different servers. However, in this integration guide, it is assumed that the iNotes server and the Vault server are on the same server.

For any iNotes server supporting web federated login, you must have two identity provider configuration documents—one document for the iNotes server with SAML authentication (this document must reside in the identity provider Catalog application on the iNotes server) and the other document for the iNotes server interface with the ID vault (this document must reside in the identity provider Catalog application on the ID vault server).

Prerequisites

- The IBM Domino administrator must have deployed ID Vault, and users are able to access their ID for encrypting and decrypting emails.

  **NOTE:** To verify the ID vault deployment, log in to the Notes client as the test user. The user’s ID file will be uploaded to the vault automatically when Notes starts. It is assumed that the Notes client has connectivity to the user’s home server. On the **User Security** window, a user can see the ID file uploaded to the vault.

- The users have email addresses, which are known to the identity provider.
Creating a Configuration Document in the idpcat.nsf Database

The **idpcat.nsf** database is not created by default. It can be created using the **idpcat.ntf** template.

**Downloading the Metadata File**

The identity provider configuration document includes several fields for which the values are supplied automatically when you import the metadata file (**FederationMetadata.xml**) from the identity provider. The AD FS metadata file can be downloaded from the following URL:

```
https://{AD FS server>/FederationMetadata/2007-06/FederationMetadata.xml
```

**Creating an Identity Provider Configuration Document for iNotes Server with SAML Authentication**

1. Open the **Domino Administrator** client.
2. On the **Files** tab, in the right pane, double-click the row containing the **idpcat.nsf** file.

   ![Screen Image](image1.png)
   (The screen image above is from IBM®. Trademarks are the property of their respective owners.)

3. Click **Add IdP Config**.

   ![Screen Image](image2.png)
   (The screen image above is from IBM®. Trademarks are the property of their respective owners.)
4. On the **IdP Configuration** window, on the **Basics** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host names or addresses mapped to this site</strong></td>
<td>Enter either an IP address or web address (DNS host name or Internet site name) representing the Domino ID vault server (Notes server interface to vault server), or both. If you enter both, separate the IP from the web address using a semicolon; for example, <em>Domino.sfnt.com</em>.</td>
</tr>
<tr>
<td><strong>IdP name</strong></td>
<td>Enter a name to identify the web site of the identity provider. The name does not have to be exact, and is only for your administrative convenience. For example, <em>idpSASCloud</em>.</td>
</tr>
<tr>
<td><strong>Protocol version</strong></td>
<td>Select the SAML version; for example, <em>SAML 2.0</em>.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Select <strong>Enabled</strong>.</td>
</tr>
<tr>
<td><strong>Federation product</strong></td>
<td>Select <strong>ADFS</strong>.</td>
</tr>
<tr>
<td><strong>Service provider ID</strong></td>
<td>Enter a string that identifies Domino as a service provider with the identity provider (IdP). This string is usually the same as the URL for the Domino HTTP server; for example, <em><a href="https://domino.sfnt.com">https://domino.sfnt.com</a></em>.</td>
</tr>
</tbody>
</table>

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

5. Click **Import XML file** and specify the metadata file you downloaded earlier. Some of the fields on the **Basics** tab are populated with the information supplied from the imported metadata file. It is recommended to leave intact the information supplied from the imported metadata file.
6. On the **Client Settings** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Windows single sign-on</strong></td>
<td>If this IdP document corresponds to an IdP that uses Windows single sign-on (SPNEGO/Kerberos) user authentication, select <em>Yes</em>. This field is required by the Notes client federated login so that Domino knows how to set up the Notes client embedded browser.</td>
</tr>
<tr>
<td><strong>Sites that are trusted</strong></td>
<td>[Optional] Enter the trusted identity provider (IdP) web host names that differ from the host name configured in the <strong>Basics</strong> tab. Separate the entries with a semicolon or a return character.</td>
</tr>
<tr>
<td><strong>Enforce SSL</strong></td>
<td>If the Notes client embedded browser requires that the URL accessed at the IdP during the login sequence be protected with SSL, select <em>Yes</em>.</td>
</tr>
</tbody>
</table>

![Screen image](image.png)

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

7. On the **Certificate Management** tab, perform the following steps:

   a. Enter the **Company name**, which identifies the certificate in the Domino metadata file (*idp.xml*) to be exported.). Use any string convenient to your administrators.

   b. Click **Create Certificate**. If prompted, save the document, return to the tab, and click **Create Certificate** again.

   When creating the certificate, Domino prepends \texttt{CN=} to the string in the **Company name** field and uses this name as the certificate subject. The name may be visible in the IdP configuration after the metadata file is imported.
c. Two new fields, **Domino URL** and **Single logout URL**, appear.

In the **Domino URL** field, enter a string to identify the fully qualified DNS name in a URL of the Domino server; for example, enter `https://domino.sfnt.com`. The string in this field is used by IdP as the initial part of the URL for sending the user's SAML assertion back to Domino.

In the **Single logout URL** field, enter a URL, if IdP requires.

d. Click **Export XML** to save the created `idp.xml` file as an attachment to the document.

    Export XML is visible only when the previously created `idp.xml` file is not already attached.

8. Click **Save & Close**.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
Creating an Identity Provider Configuration Document for iNotes Server Interface with ID Vault


![Image of idpcat window with Add IdP Config button highlighted]

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

10. On the IdP Configuration window, on the Basics tab, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host names or addresses</td>
<td>Enter a virtual name for the iNotes interface to the vault; for example, vault.domino.sfnt.com.</td>
</tr>
<tr>
<td>mapped to this site</td>
<td></td>
</tr>
<tr>
<td>IdP name</td>
<td>Enter a name to identify the web site of the identity provider. The name does not have to be exact, and is only for your administrative convenience. For example, VaultIdPSASCloud.</td>
</tr>
<tr>
<td>Protocol version</td>
<td>Select the SAML version; for example, SAML 2.0.</td>
</tr>
<tr>
<td>State</td>
<td>Select Enabled.</td>
</tr>
<tr>
<td>Federation product</td>
<td>Select ADFS.</td>
</tr>
<tr>
<td>Service provider ID</td>
<td>Enter the syntactically correct URL, as the virtual hostname would be featured in a URL; for example, <a href="https://vault.domino.sfnt.com">https://vault.domino.sfnt.com</a>. This string is usually the same as the URL for the Domino HTTP server; for example, <a href="https://domino.sfnt.com">https://domino.sfnt.com</a>.</td>
</tr>
</tbody>
</table>
11. Click **Import XML file**, and specify the `metadata.xml` file exported from the IdP. Some of the fields on the **Basics** tab are populated with the information supplied from the imported metadata file. It is recommended to leave intact the information supplied from the imported metadata file.

12. On the **Client Settings** tab, complete the following fields:

<table>
<thead>
<tr>
<th><strong>Enable Windows single sign-on</strong></th>
<th>If this IdP document corresponds to an IdP that uses Windows single sign-on (SPNEGO/Kerberos) user authentication, select <strong>Yes</strong>. This field is required by Notes client federated login so that Domino knows how to set up the Notes client embedded browser.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sites that are trusted</strong></td>
<td>[Optional] Enter the trusted identity provider (IdP) web host names that differ from the host name configured in the <strong>Basics</strong> tab. Separate the entries with a semicolon or a return character.</td>
</tr>
<tr>
<td><strong>Enforce SSL</strong></td>
<td>If the Notes client embedded browser requires that the URL accessed at the IdP during the login sequence be protected with SSL, select <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>
13. On the Certificate Management tab, perform the following steps:

a. Enter the Company name, which identifies the certificate in the Domino metadata file (idp.xml) to be exported. Use any string convenient to your administrators.

b. Click Create Certificate. If prompted, save the document, return to the tab, and click Create Certificate again.

When creating the certificate, Domino prepends CN= to the string in the Company name field and uses this name as the certificate subject. The name may be visible in the IdP configuration after the metadata file is imported.
c. Two new fields, **Domino URL** and **Single logout URL**, appear.

   In the **Domino URL** field, enter a string to identify the fully qualified DNS name in a URL of the Domino server; for example, enter **https://domino.sfnt.com**. The string in this field is used by IdP as the initial part of the URL for sending the user's SAML assertion back to Domino.

   In the **Single logout URL** field, enter a URL, if IdP requires.

   ![IdP Configuration: VaultIdPSASCloud](image)

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

   d. Click **Export XML** to save the created **idp.xml** file as an attachment to the document.

      **Export XML** is visible only when the previously created **idp.xml** file is not already attached.

14. Click **Save & Close**.
Configuring the ID Vault for Web Federated Login

The ID vault administrator must approve the use of an IdP that will provide SAML credentials. The ID vault administrator decides which IdP is trustworthy. Only credentials from a trusted IdP can be used for downloading an ID file stored in this ID vault. The administrator supplies host names for IdP partnerships to the ID vault in a vault document. The vault server uses the host names to look up IdP information from the IdP Catalog application (idpcat.nsf).

1. Open the Domino Administrator client.
2. On the Files tab, in the left pane, click the IBM_ID_VAULT directory. Then, in the right pane, open the ID vault application (for example, IDVaultTest).

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

3. In the left pane, click Vault Users > Configuration. In the right pane, select the ID vault application (for example, IDVaultTest), and then click Edit Document.

   (The screen image above is from IBM®. Trademarks are the property of their respective owners.)
4. In the **Web federated login approved IdP configurations** field, enter the virtual host name; for example, vault.domino.sfnt.com.

5. Click **Save & Close**.

### Configuring the Security Policy Settings Document

After configuring the ID vault for web federated login, you need to edit the security policy. To do so, export a copy of the Internet SSL certificate from your federation (ADFS), import that certificate into your Domino Directory, and cross-certify. For more details, refer to the following URL:


1. Open the **Domino Administrator** client.
2. On the **People & Groups** tab, perform the following steps:
   a. In the left pane, in **Domino Directories**, click **Policies >Settings**.
   b. In the right pane, select the existing security policy settings document.
   c. Click **Edit Settings**.

(See the screen image above is from IBM®. Trademarks are the property of their respective owners.)
3. In Security Settings of your ID Vault, on the **Password Management > Federated Login** tab, select **Yes** for **Enable Web Federated login with SAML IdP**.

![Password Management Basics](image)

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

4. On the **Keys and Certificates** tab, under **Administrative Trust Defaults**, click **Update Links** to add the Notes certifier to the policy.

![Keys and Certificates](image)

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

5. On the **Trusted Certificates** window, click **Selected supported**, and then click **OK**.

![Trusted Certificates](image)

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
6. On the **Select the certificates to trust** window, on the **Notes Certifiers** tab, select the certificate.

![Select the certificates to trust window](image)

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

7. On the **Internet Cross Certificates** tab, select the SSL certificate exported from ADFS, and then click OK.

![Select the certificates to trust window](image)

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

---

**NOTE:** In this guide the ADFS server FQDN is `sam.sam.safenetdemos.com`.

---

8. Save and close the security policy.
Configuring Microsoft AD FS 2.0

To add SAS as an identity provider for IBM Domino through AD FS, perform the following:

- Adding SAS as a Claim Provider Trust in AD FS, page 20
- Adding a Relying Party Trust in AD FS for IBM Domino, page 29

Adding SAS as a Claim Provider Trust in AD FS

1. To open the AD FS 2.0 Management Console, click Start > Administrative Tools > AD FS 2.0 Management.
2. On the AD FS 2.0 window, expand AD FS 2.0 > Trust Relationships.
3. Right-click Claims Provider Trusts, and then click Add Claims Provider Trust.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
4. On the **Welcome** window, click **Start**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
5. On the Select Data Source window, perform the following steps:
   a. Select Import data about the claims provider from a file.
   b. Click Browse and select the path where the SAS metadata (SafeNet-Idp-Metadata.xml) is downloaded.

   **NOTE:** The SAS metadata can be downloaded from: https://idp1.cryptocard.com/idp/shibboleth

   c. Click Next.

6. If a warning message such as the one shown below is displayed, ignore it and click OK.

   (The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
7. On the **Specify Display Name** window, in the **Display name** field, enter the claims provider name to display (for example, SAS) and then click **Next**.

![Specify Display Name](image)

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

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

![Ready to Add Trust](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
9. On the **Finish** window, ensure that **Open the Edit Claim Rules dialog**... is selected, and then click **Close**.

![Finish window](image)

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

10. On the **Edit Claim Rules for SAS** window, click **Add Rule**.

In the window name, **SAS** is the claims provider name you specified previously.

![Edit Claim Rules for SAS window](image)

(The screen image above is from Microsoft®. 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®. Trademarks are the property of their respective owners.)
12. On the **Configure Rule** window, perform the following steps:

   d. In the **Claim rule name** field, enter the rule name to display (for example, **Pass_Through_NameId**).
   
   e. In the **Incoming claim type** field, select **Name ID**.
   
   f. Click **Finish**.

   Ignore any warning messages that are shown.

   (The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
13. On the **Edit Claim Rules for SAS** window, click **OK**.

14. On the **AD FS 2.0** window, click **AD FS 2.0 > Trust Relationships > Claims Provider Trusts**.

15. In the list of claims provider trusts, right-click on the claims provider trust that you created (for example, **SAS**), and then click **Properties**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
16. On the **SAS Properties** window, on the **Advanced** tab, in the **Secure hash algorithm** field, select **SHA-1**, and then click **OK**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
Adding a Relying Party Trust in AD FS for IBM Domino

The relying party trust is the object in AD FS that tells it how to work with a service provider like Domino.

For Notes Federated Login

1. On the AD FS 2.0 window, expand AD FS 2.0 > Trust Relationships. Right-click Relying Party Trusts, and then click Add Relying Party Trust.

![Adding Relying Party Trust in AD FS](image)

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

2. On the Welcome window, click Start.

![Add Relying Party Trust Wizard](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
3. On the **Select Data Source** window, select **Enter data about the relying party manually**, and then click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
4. On the **Specify Display Name** window, in the **Display name** field, enter a name for display for Notes Federated Login (for example, **IBMDominoNFL**), and then click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
5. On the **Choose Profile** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
6. On the **Configure Certificate** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
7. On the **Configure URL** window, perform the following steps:
   a. Select **Enable support for the SAML 2.0 WebSSO protocol**.
   b. In the **Relying party SAML 2.0 SSO service URL** field, enter the following URL:
      
      https://<DominoSrvHostName>/names.nsf?SAMLLogin
      
      where, `<DominoSrvHostName>` is the URL for accessing your Notes server.
   c. Click **Next**.

![Configure URL Wizard](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
8. On the **Configure Identifiers** window, perform the following steps:

   a. In the **Relying party trust identifier** field, enter the URL for Notes Federated Login; for example, `https://<DominoSrvHostName>`.  
      where, `<DominoSrvHostName>` is the host name of the Domino server

      **NOTE:** The value entered in the **Relying party trust identifier** field must match with the value in the **Service Provider ID** field in the Domino idpcat configuration document for iNotes Server with SAML Authentication

   b. Click **Add**.

   c. Click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
9. On the **Choose Issuance Authorization Rules** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
10. On the **Ready to Add Trust** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
11. On the Finish window, select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes**, and then click Close.

![Finish window](image)

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

12. The **Edit Claim Rules** window for the relying party trust you have created should open when the wizard closes. If it does not open, in the Relying Party Trusts list, right-click on the relying party trust you have created, and then click **Edit Claim Rules**.
13. On the **Edit Claim Rules for IBMDominoNFL** window, click **Add Rule**. **IBMDominoNFL** is the relying party trust you have created.

(The screen image above is from Microsoft®. 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®. Trademarks are the property of their respective owners.)
15. On the **Configure Rule** window, perform the following steps:
   a. In the **Claim rule name** field, enter the rule name to display (for example, **Pass_Through_NameId**).
   b. In the **Incoming claim type** field, select **Name ID**.
   c. Click **Finish**.

![Add Transform Claim Rule Wizard](image_url)

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

16. On the **Edit Claim Rules for IBMDominoNFL** window, click **OK**.
For Web Federated Login

1. On the AD FS 2.0 window, expand AD FS 2.0 > Trust Relationships. Right-click Relying Party Trusts, and then click Add Relying Party Trust.

   ![AD FS 2.0 window](image1)

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

2. On the Welcome window, click Start.

   ![Add Relying Party Trust Wizard](image2)

   (The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
3. On the **Select Data Source** window, select **Enter data about the relying party manually**, and then click **Next**.
4. On the **Specify Display Name** window, in the **Display name** field, enter a name for display for Web Federated Login (for example, **IBMDominoWFL**), and then click **Next**.

![Specify Display Name window](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
5. On the **Choose Profile** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
6. On the **Configure Certificate** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
7. On the Configure URL window, perform the following steps:
   a. Select **Enable support for the SAML 2.0 WebSSO protocol**.
   b. In the **Relying party SAML 2.0 SSO service URL** field, enter the following URL:
      
      https://<DominoSrvHostName>/names.nsf?SAMLIDLogin
      
      where, `<DominoSrvHostName>` is the URL for accessing your Notes server
   c. Click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
8. On the Configure Identifiers window, perform the following steps:
   a. In the Relying party trust identifier field, enter a virtual name for Web Federated Login; for example, https://Vault. <DominoSrvHostName>.
       where, <DominoSrvHostName> is the host name of the Domino server

       NOTE: The value entered in the Relying party trust identifier field must match with the value in the Service Provider ID field in the Domino idpcat configuration document for iNotes Server Interface with ID Vault.

   b. Click Add.

   c. Click Next.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
9. On the **Choose Issuance Authorization Rules** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
10. On the **Ready to Add Trust** window, click **Next**.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
11. On the Finish window, select Open the Edit Claim Rules dialog for this relying party trust when the wizard closes, and then click Close.

![Finish window screenshot](image)

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

12. The Edit Claim Rules window for the relying party trust you have created should open when the wizard closes. If it does not open, in the Relying Party Trusts list, right-click on the relying party trust you have created, and then click Edit Claim Rules.

13. Repeat steps 13 onwards from the section "For Notes Federated Login" on page 29.
Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SafeNet Authentication Service (SAS) with IBM Domino using SAML authentication requires:

- Synchronizing Users Stores to SafeNet Authentication Service, page 52
- Assigning an Authenticator in SafeNet Authentication Service, page 52
- Adding IBM Domino as a Service Provider (SP) in SafeNet Authentication Service, page 53
- Enabling SAML Services in SafeNet Authentication Service, page 56

Synchronizing Users Stores to SafeNet Authentication Service

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

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

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


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning an Authenticator in SafeNet Authentication Service

SafeNet Authentication Service (SAS) supports a number of authentication methods that can be used as a second authentication factor for users authenticating through IBM Domino.

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” 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 IBM Domino as a Service Provider (SP) in SafeNet Authentication Service**

Add a service provider entry in the SafeNet Authentication Service (SAS) **SAML Service Providers** module to prepare it to receive SAML authentication requests from IBM Domino. You will need the Entity ID and assertion consumer URL location of AD FS.

**To add IBM Domino as a Service Provider in SafeNet Authentication Service:**

1. Log in to the SafeNet Authentication Service console with an Operator account.
2. Click the COMMS tab, and then click SAML Service Providers.

3. In the SAML Service Providers module, click the SAML 2.0 Settings link.

4. Click Add.
5. Under **Add SAML 2.0 Settings**, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly Name</td>
<td>Enter AD FS server name.</td>
</tr>
<tr>
<td>SAML 2.0 Metadata</td>
<td>Select <strong>Create New Metadata File</strong>.</td>
</tr>
<tr>
<td>Entity ID</td>
<td>Enter the service provider IssuerID or EntityID (for example, http://&lt;AD FS Server hostname&gt;/adfs/services/trust)</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the Assertion Consumer URL (for example, http://&lt;AD FS Server hostname&gt;/adfs/ls/)</td>
</tr>
</tbody>
</table>

**NOTE:** The remaining options are used to customize the appearance of the logon page presented to the user. For more information on logon page customization, refer “Configure SAML Service” in the SAML Configuration Guide: http://www2.safenet-inc.com/sas/implementation-guides/sas-on-prem/SAS-QS-SAML.pdf

Under **Return Attributes**, add the following attributes, and then click **Apply**:

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/claims/EmailAddress">http://schemas.xmlsoap.org/claims/EmailAddress</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
<tr>
<td><a href="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</a></td>
<td>According to ThirdParty Product Requirements</td>
</tr>
</tbody>
</table>
IBM Domino is added as a service provider in the system.

Enabling SAML Services in SafeNet Authentication Service

After IBM Domino has been added to SafeNet Authentication Service (SAS) as a service provider, the users should be granted permission to use this service provider with SAML authentication.

There are two methods to enable the user to use the service provider:

- Manually, one user at a time, using SAML Services module
- Automatically, by defining groups of users, using SAML Provisioning Rules
Using the SAML Services Module

Manually enable a single user to authenticate against one or more configured SAML Service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the ASSIGNMENT tab, and then search for the required user.

3. Click the appropriate user in the User ID column.
4. Click **SAML Services**.

![Image of SAML Services](image)

5. Click **Add**.

![Image of Add SAML Service](image)

6. Under **Add SAML Service**, do the following:
   a. From the **Service** menu, select the IBM Domino service provider.
   b. In **SAML Login ID** field, select the type of login ID (Email) to be sent as a UserID to IBM Domino in the response.
   c. Click **Add**.

![Image of Add SAML Service Form](image)
The user can now authenticate to IBM Domino via AD FS using SAML authentication.

Using SAML Provisioning Rules

Use this module to enable groups of users to authenticate to SAML service providers.

1. Log in to the SafeNet Authentication Service console with an Operator account.

2. Click the POLICY tab, and then click Automation Policies.
3. Click the **SAML Provisioning Rules** link.

4. Click **New Rule**.

5. Configure the following fields, and then click **Add**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rule Name</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>User is in container</strong></td>
<td>Users affected by this rule must be in the selected container.</td>
</tr>
<tr>
<td><strong>Groups</strong></td>
<td>The <strong>Virtual Server groups</strong> box lists all groups. Click the user groups that will be affected by the rule, and then click the right arrow to move it to the <strong>Used by rule</strong> box.</td>
</tr>
<tr>
<td><strong>Parties</strong></td>
<td>The <strong>Relying Parties</strong> box lists all service providers. Click the service providers that the groups of users will authenticate to, and then click the right arrow to move it to <strong>Rule Parties</strong> box.</td>
</tr>
<tr>
<td><strong>SAML Login ID</strong></td>
<td>Select Email. The Email will be returned to the service provider in the SAML assertion.</td>
</tr>
</tbody>
</table>
Running the Solution

You can verify if the iNotes user can access emails over the web once the SAML authentication succeeds.

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

1. In a web browser, open the Domino URL for email; for example, https://<Domino Server Host Name>/mail/<Username>.nsf. You are redirected to the AD FS Sign In page.

2. Select the claim provider trust you configured for SAS, and then click Continue to Sign In. You are redirected to the SAS Login page.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
3. In **User Name** field, enter your user name (for example, **Bob**), and then click **Login**.

4. In the **Password** field, enter your Personal Identification Pattern (PIP), and then click **Login**.

If authentication is successful, you will be allowed to access email through the web browser client.

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

You may receive the following error message in the Domino server logs:

**SECCheckAndParseSAMLResponse**: Exiting: Single Sign-On token has a creation time in the future. Single Sign-On servers may need to have clocks synchronized.

To resolve this issue, update the following parameters in the `note.ini` file to increase the tolerance of the SSO token creation timestamp check:

- **SAML_NotOnOrAfterSkewInMinutes = value**
  

- **SAML_NotBeforeSkewInMinutes = value**
  
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><strong>United States</strong></td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td><strong>International</strong></td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></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>