SafeNet Authentication Manager
Integration Guide

Using SAM as an Identity Provider for IBM Domino
# Contents

Third-Party Software Acknowledgement........................................................................................................... 4
Description.............................................................................................................................................................. 4
Applicability............................................................................................................................................................. 4
Environment ............................................................................................................................................................ 4
Audience.................................................................................................................................................................... 5
SAML Authentication using SAM .......................................................................................................................... 5
Authentication Flow using SAM ............................................................................................................................ 6
SAML Prerequisites.................................................................................................................................................. 7
Configuring SafeNet Authentication Manager..................................................................................................... 7
  Synchronizing User Stores to SAM ....................................................................................................................... 7
  Assigning Tokens in SAM ..................................................................................................................................... 7
  Configuring SAM as an Identity Provider ........................................................................................................... 9
  Exporting the SAM Certificate ........................................................................................................................... 12
  Configuring SAM for SAML-based User Federation ....................................................................................... 13
Configuring IBM Domino ....................................................................................................................................... 16
  Setting Up Web Federated Login with IBM iNotes ........................................................................................... 16
  Configuring the ID Vault for Web Federated Login .......................................................................................... 24
  Configuring the Security Policy Settings Document .................................................................................... 25
Configuring Microsoft AD FS 2.0 .......................................................................................................................... 27
  Adding SAM as a Claim Provider Trust in AD FS ............................................................................................ 27
  Adding Relying Party Trust in AD FS for IBM Domino ................................................................................... 34
Running the Solution ............................................................................................................................................... 49
Support Contacts...................................................................................................................................................... 51
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

IBM Notes and IBM Domino are the client and server, respectively, of a collaborative client-server software platform marketed by IBM. The IBM Notes 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:

- Deploy multi-factor authentication (MFA) options in IBM Domino using SafeNet tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in IBM Domino using SafeNet Authentication Manager as an identity provider.

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

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 Manager.

Applicability

The information in this document applies to SafeNet Authentication Manager—a server version of SAM 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 Manager 8.2.158.654
- IBM Domino 9.0.1
- 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 Manager.

SAML Authentication using SAM

SAM provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.
Authentication Flow using SAM

SafeNet Authentication Manager 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 ADFS page where the user selects the SAM claim provider.
3. The user is redirected to SAM. SAM collects and evaluates the user’s credentials.
4. SAM returns a response to IBM Domino via AD FS, accepting or rejecting the user’s authentication request.
SAML Prerequisites

To enable SafeNet Authentication Manager 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 SafeNet Authentication Manager

Using SAM as an Identity Provider for IBM Domino requires the following:

- Synchronizing User Stores to SAM, page 7
- Assigning Tokens in SAM, page 7
- Configuring SAM as an Identity Provider, page 9
- Exporting the SAM Certificate, page 12
- Configuring SAM for SAML-based User Federation, page 13

Synchronizing User Stores to SAM

SAM manages and maintains token information in its data store, including the token status and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Assigning Tokens in SAM

SAM supports a number of tokens methods that can be used as a second authentication factor for users authenticating through IBM Domino.

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)

Tokens can be assigned to users as follows:

- **SAM Management Center**: Management site used by SAM administrators and help desk for token enrollment and lifecycle management.
- **SAM Self-Service Center**: Self-service site used by end users for managing their tokens.
- **SAM Remote Service**: Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
Configuring SAM as an Identity Provider

In order to use IBM Domino as a service provider and SAM as an Identity Provider, SAM has to be set as an Identity Provider.

1. From the Windows Start menu, click Start > Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

2. Click Action > Cloud Configuration.
3. Click the **Info for Service Provider** tab.

![Image of Cloud Settings with Info for Service Provider tab]

4. Fill in the web address of the SAM portals server in the **Domain URL** field.

![Image of Cloud Settings with Domain URL field highlighted]

Enter your company's domain URL in the format `http://my_company.com`

- **Domain URL:**

Copy the following information to the service provider's 'Single Sign-On' settings page:

- **Sign-in page URL:** `<Domain URL>/sancloud/default.aspx`
- **Sign-out page URL:** `<Domain URL>/sancloud/logout.aspx`
- **Change password URL:** `<Domain URL>/sancloud/changePIN.aspx`
5. The rest of the fields are generated according to the Domain URL that was entered.

6. Click **OK**.
Exporting the SAM Certificate

The SAM certificate is shared between SAM and ADFS. The certificate will be used to sign the authentication requests.

1. From the Windows Start menu, click All Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager.

2. On the SafeNet Authentication Manager – Configuration Manager window, click Action > Cloud Configuration.
3. On the **Cloud Settings** window, on the **Info for Service Provider** tab, click **Export Certificate** and save the certificate file. This certificate file will be imported into AD FS in a later step.

![Cloud Settings window]

### Configuring SAM for SAML-based User Federation

SAM’s Token Policy Object (TPO) policies include **Application Authentication Settings** for SAML service providers. These settings are used by SAM’s portal to communicate with service providers.

For general portal configuration, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**To edit the Token Policy Object for SAM’s portal configuration:**

1. Open the Token Policy Object Editor for the appropriate group. See the *SafeNet Authentication Manager 8.2 Administrator’s Guide* for more information.

2. On the **Token Policy Object Editor** window, in the left pane, click **Protected Application Settings > User Authentication**.

![Token Policy Object Editor]

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

3. In the right pane, double-click **Application Authentication Settings**.
4. On the Application Authentication Settings Properties window, perform the following steps:
   a. Select Define this policy setting.
   b. Select Enabled.
   c. Click Definitions.

5. On the Application Authentication Settings window, right-click Application Authentication Settings, and then select Create a new profile.

6. Right-click the new profile and rename it to a friendly name (for example, ADFS for IBM Domino).
7. Click the new profile.

8. Double-click on each of the following policies, and then enter the appropriate information:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Issuer</td>
<td>Enter the Entity ID of ADFS; for example, <code>http://&lt;asdfsServer&gt;/adfs/services/trust</code></td>
</tr>
<tr>
<td>SAM issuer</td>
<td>Enter a unique SAM ID to be identified in SAML authentication. The same value needs to be entered as claims provider identifier in ADFS Claims Provider Trust.</td>
</tr>
<tr>
<td>Application's login URL</td>
<td>Enter the ACS URL of ADFS; for example: <code>https://&lt;asdfsServer&gt;/adfs/ls/</code></td>
</tr>
<tr>
<td>Audience URI</td>
<td>Enter same as Application's login URL above.</td>
</tr>
<tr>
<td>User mapping</td>
<td>Select <code>eMail</code>.</td>
</tr>
</tbody>
</table>

9. Enable the appropriate authentication methods for your organization. See the *SafeNet Authentication Manager Version 8.2 Administrator’s Guide* for detailed information about authentication methods.

The following is an example of completed fields in the Application Authentication Settings window:

10. Click OK until all of the Token Policy Object Editor windows are closed.
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 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 a web federated login, the iNotes server and the Vault server can be on two different servers. However, in this integration guide, it is assumed that the iNotes server and the Vault server are on the same servers.

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).

Prerequisite

- The IBM Domino administrator must have deployed the 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.
- Make sure that SSL is properly enabled at IIS as per the below document: http://www-10.lotus.com/ldd/dominowiki.nsf(dx/Cookbookcol_Setting_up_ADFS_for_integrated_ Windows_authentication_lprlWARpr_

  * Make sure you have created the AD FS Kerberos identity by using SETSPN commands on the AD FS machine.
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 (FederationMeatadata.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.

3. Click Add IdP Config.

(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, Domino.sfnt.com.</td>
</tr>
<tr>
<td><strong>IdP name</strong></td>
<td>Enter a name to identify the website of the identity provider. The name does not have to be exact, and is only for your administrative convenience. For example, idpSAMCloud.</td>
</tr>
<tr>
<td><strong>Protocol version</strong></td>
<td>Select the SAML version; for example, SAML 2.0.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Select Enabled.</td>
</tr>
<tr>
<td><strong>Federation product</strong></td>
<td>Select ADFS.</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, <a href="https://domino.sfnt.com">https://domino.sfnt.com</a>.</td>
</tr>
</tbody>
</table>

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 <strong>Yes</strong>. 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 <strong>Yes</strong>.</td>
</tr>
</tbody>
</table>

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 **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**, are displayed.
   - 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 required by the IdP.

   ![IdP Configuration: idpSAMCloud](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.

8. Click **Save & Close**.

Creating an Identity Provider Configuration Document for iNotes Server Interface with the ID Vault

1. On the **idpca** – IBM Domino Administrator window, click **Add IdP Config**.

   ![idpca - IBM Domino Administrator](image)

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host names or addresses mapped to this site</td>
<td>Enter a virtual name for the iNotes interface to the vault; for example, <code>vault.domino.sfnt.com</code>.</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, <code>VaultIdPSAMCloud</code>.</td>
</tr>
<tr>
<td>Protocol version</td>
<td>Select the SAML version; for example, <code>SAML 2.0</code>.</td>
</tr>
<tr>
<td>State</td>
<td>Select <code>Enabled</code>.</td>
</tr>
</tbody>
</table>
Federation product | Select ADFS.
---|---
Service provider ID | Enter the syntactically correct URL, as the virtual hostname would be featured in a URL; for example, `https://vault.domino.sfnt.com`. This string is usually the same as the URL for the Domino HTTP server; for example, `https://domino.sfnt.com`.

3. 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.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Windows single sign-on</td>
<td>If this IdP document corresponds to an IdP that uses Windows single sign-on (SPNEGO/Kerberos) user authentication, select Yes. This field is required by Notes client federated login so that Domino knows how to set up the Notes client embedded browser.</td>
</tr>
<tr>
<td>Sites that are trusted</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>Enforce SSL</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 Yes.</td>
</tr>
</tbody>
</table>
5. 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**, are displayed.

      - 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 required by the IdP.
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.

6. 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.

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

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 (AD FS), import that certifier 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.

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.

(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 tab](image1)

   *(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 window](image2)

   *(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](image3)

   *(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 AD FS, and then click **OK**.

   ![Internet Cross Certificates tab](image4)

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

   **NOTE:** In this guide the AD FS server FQDN is **sam.sam.safenetdemos.com**.

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

To add SAM as an identity provider for IBM Domino through ADFS, perform the following:

- Adding SAM as a Claim Provider Trust in AD FS, page 27
- Adding Relying Party Trust in AD FS for IBM Domino, page 34

Adding SAM 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.
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 SAM metadata (**SAM-IDP-Metadata.xml**) is downloaded.
      For downloading the metadata file, see the section “Exporting the SAM Certificate” on page 12.
   c. Click **Next**.

   ![Select Data Source Window](image)

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

6. If the warning message as shown in the image below is displayed, ignore it and click **OK**.

   ![Warning Message](image)

   *(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, **SAMasIdP**), and then click **Next**.

8. On the **Ready to Add Trust** window, click **Next**.
9. On the **Finish** window, ensure that **Open the Edit Claim Rules dialog**... is selected, and then click **Close**.

![Finish window]

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

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

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

![Edit Claim Rules for SAMasIDP window]

(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 **Transform an Incoming Claim**, and then click **Next**.

![Select Rule Template](image)

(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:
   a. In the **Claim rule name** field, enter the rule name to display (for example, **Transform_NameId**).
   b. In the **Incoming claim type** field, select **Name ID**. The **Incoming name ID format** field will become available.
   c. In **Incoming name ID format** field, select **Email**.
   d. In **Outgoing claim type** field, select **Name ID**.
   e. Leave the **Outgoing name ID format** as **Unspecified**.
   f. Click **Finish**.

Ignore any warning messages that are shown.
13. On the **Edit Claim Rules for SAMasIDP** 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, **SAMasIDP**), and then click **Properties**.

![AD FS 2.0 window](image1)

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

16. On the **SAMasIDP Properties** window, on the **Advanced** tab, in the **Secure hash algorithm** field, select **SHA-1**, and then click **OK**.

![SAMasIDP Properties window](image2)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
Adding 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, click AD FS 2.0 > Trust Relationships. Right-click Relying Party Trusts and then click Add Relying Party Trust.

![Image](image1.png)

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

2. On the Welcome window, click Start.

![Image](image2.png)

(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 Notes Federated Login (for example, IBMDominoNFL), and then click Next.
5. On the **Choose Profile** window, click **Next**.

6. On the **Configure Certificate** window, click **Next**.
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:  
   ```plaintext
   https://<DominoSrvHostName>/names.nsf?SAMLLogin
   ```
   where, `<DominoSrvHostName>` is the URL for accessing your Notes server.

c. Click **Next**.

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,  
   ```plaintext
   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.
   
   b. Click **Add**.
   
   c. Click **Next**.
9. On the **Choose Issuance Authorization Rules** window, click **Next**.
10. On the **Ready to Add Trust** window, click **Next**.

![Add Relying Party Trust Wizard](image)

(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**.

![Add Relying Party Trust Wizard](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 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, 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 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**.

![Select Rule Template](image.png)

*(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**.

   ![Configure Rule Wizard](image)

   *(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.

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

2. On the Welcome window, click Start.

   (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**.

   ![Select Data Source Window]

   *(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 Web Federated Login (for example, **IBMDominoWFL**), and then click **Next**.

   ![Specify Display Name Window]

   *(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**.

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 the value in the **Service Provider ID** field in the Domino idpcat configuration document.

   b. Click **Add**.
   c. Click **Next**.
9. On the **Choose Issuance Authorization Rules** window, click **Next**.
10. On the **Ready to Add Trust** window, click **Next**.

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**.
12. The **Edit Claim Rules** window for the relying party trust you 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, and then click **Edit Claim Rules**.

13. Repeat steps 13 onwards from the section "For Notes Federated Login" on page 34.

### 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 eToken PASS token is configured for authentication with the SAM 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 SAM (for example: **SAMasIDP**), and then click **Continue to Sign In**. You are redirected to the SAM **Login** page.

3. In the **Username** field, enter your user name, and then click **OK**.
4. In the **OTP Authentication Code** field, enter the OTP generated on the assigned token, and then click **OK**.

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

*(The screen image above is from IBM®. 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 SafeNet Customer Support. SafeNet 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 SafeNet 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>SafeNet, 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></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td></td>
</tr>
</tbody>
</table>
|                              | Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.