Implementing Domino SAML

A guide to SAML authentication in Domino

Graham Farrell – HCL Level 2 Digital Solutions Engineer.

Table of Contents

Introduction

The purpose of this document is to provide a Domino administrator with an overview of how SAML is implemented in Domino and how they can utilise this method of authentication in their environment. The information in this document can also be used as a basic reference when troubleshooting a SAML issue. When both configuring and troubleshooting a SAML issue, a Domino administrator will need to have an understanding of a number of other topics such as ID Vault and HTTPS that are not covered in detail in this document. However, information is widely available on these topics in the administration help, in knowledgebase articles and the Domino Wiki.

The administration help trail in relation to SAML authentication can be found at the following link

https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_10.0.1/admin/secu_using_security_assertion_markup_language_saml_to_configure_federated_identity_authentication_t.html

I've attempted to make the document as complete as possible based on my experience assisting customers with their SAML configurations and as a supplement for the administration help documentation on the subject. However, there may be specific issues not yet know or specific to a customer's environment that may only appear on attempting to implement SAML.

The latest versions of Domino at the time of writing are 10 and 10.0.1. With Domino 10, support for ADFS 4.0 was introduced. I've focused on Active Directory Federation Services (ADFS) as the identity provider, due to the prevalence of ADFS being used by the majority of the customers whom I have worked with in relation to SAML cases.

As some customers are still using Domino 9.0.1.x and ADFS 3.0, I have also highlighted the slight differences between SAML in both Domino 10.0.x and Domino 9.0.1.x. I have not covered ADFS 2.0 since it is used with Windows Server 2008 R2, which is soon to be no longer supported by Microsoft.

As Domino offers three different options for utilising SAML authentication, I have covered each separately as an independent configuration. This is because some customers, may just wish to implement Notes Federated Login, for example in their organisation. This does mean however that some information in the document is duplicated so that important configuration steps are not missed.

Overview Of SAML Authentication In Domino.

Domino can utilise SAML in three distinct ways.

- SAML Single Sign On. (Sometimes referred to as Basic SAML)
- Notes Federated Login.
- Web Federated Login for iNotes.

While each of these will be covered in detail, Notes Federated Login and Web Federated Login for iNotes require the use of the ID Vault, while SAML Single Sign On does not.

In relation to SAML authentication, Domino is what is known as a service provider. A user requests access to a resource on a SAML enabled Domino server or Internet Site and Domino redirects the user to a partnered Identity Provider to be authenticated.

Active Directory Federation Services is Microsoft's Identity Provider. ADFS can utilise either Forms Based Authentication or Windows Authentication (Kerberos) to authenticate the user.

With Kerberos authentication, if the end user's browser or Notes client has been configured to use Integrated Windows Authentication, all authentication steps are invisible to the user. If set up to use Forms Based Authentication, the user is required to enter their Active Directory user name and password.

Once the user is authenticated in Active Directory, ADFS sends a SAML assertion to Domino which contains the user's email address, the assertion is vouching that the user is who they claim to be.

Domino decodes the SAML assertion and uses the email address included in the assertion, to map the user to their person document in the Domino Directory and then uses their Domino user name to determine if they have access to the resource requested.

In some cases, customers, will not wish to have their users' email addresses matching between their Active Directory User Objects and the Domino person documents. In this case the customer can set up directory assistance to map the users via their Notes Distinguished Name which is stored in an attribute in their Active Directory User Object.

This method will work for SAML Single Sign On and Notes Federated Login, but is not supported for Web Federated Login for iNotes. Web Federated Login for iNotes requires the users email address to match between their Domino person document and their Active Directory User Object, as documented in the following article

https://www-01.ibm.com/support/docview.wss?uid=ibm10880583

As the majority of the customers I have worked with, have the email addresses matching and utilise Kerberos authentication, these are the methods focused on in this document. I have however included an appendix which quickly outlines how to set up name mapping through directory assistance.

Supported Identity Providers and SAML versions.

Domino implemented support for SAML in version 9.0. Earlier versions of Domino and Notes cannot utilise SAML.

Domino supports SAML 1.1 and SAML 2.0, however unless specifically required by the identity provider SAML1.1 should not be used.

Currently Domino supports the following on premise identity providers

IBM® Tivoli® Access Manager/Tivoli Federated Identity Manager (TAM/TFIM) which can use SAML 1.1 or 2.0

Microsoft ADFS 2.0, 3.0 and 4.0 which can only use SAML 2.0

ADFS 2.0 is supported by Domino 9.0 and 9.0.1.

ADFS 3.0 support was added to Domino 9.0.1 FP8.

ADFS 4.0 support was implemented in Domino 10.

The use of any other Identity provider is not supported. While it may be possible for some customers to implement Domino SAML with an identity provider, other that TIFM and ADFS, support cannot assist with any issues implementing SAML with these providers.

Unsupported Configurations.

The following list contains Domino and Notes configurations that are unsupported for use with SAML. Some configurations on the list are already unsupported for use with the ID vault, so may appear familiar to some readers, but should not be considered a complete list.

- Smartcard Protected IDs: The ID Vault does not support these ID files so cannot be used for Notes/Web Federated Login.
- Roaming users whose IDs are stored in a roaming personal address book on the server: The ID Vault does not support these ID files so cannot be used for Notes/Web Federated Login.
- Notes on USB: The ID Vault does not support these ID files so cannot be used for Notes Federated Login.
- User IDs with multiple passwords: The ID Vault does not support these ID files so cannot be used for Notes/Web Federated Login.
- Server based password checking for Notes users: This feature should not be enabled for users who are enabled for Notes Federated Login.
- Notes Single Login: The ID Vault does not support this component.
- The Notes Basic client and Administration client: Only the Notes standard client is supported for Notes Federated Login.
- Web Federated Login with Clustered servers accessed via a load balance/IP sprayer. More information can be found in https://www.ibm.com/support/docview.wss?uid=swg21975613

- Traveler connections: SAML is not supported by Traveler as natively it does not support any form of session authentication.

- Once Notes or Web Federated Login is configured against the ID Vault, Domino expects all ID Vault operations to use this method as documented in SPR # GFAL9ZBJVT, http://www-01.ibm.com/support/docview.wss?uid=swg21990021

- The Notes C-API function Secidfget does not work with Federated Login an enhancement request exists under SPR # RGAU9VLHT3, https://www-01.ibm.com/support/docview.wss?uid=swg21882957

It should be noted that in relation to SPR # GFAL9ZBJVT and SPR # RGAU9VLHT3, that the enhancement requests have been implemented in Domino 10.0.1 FP1. The following parameter should be added to the notes.ini of your mail servers, and those mail servers that are also ID Vault servers, and the server restarted to take effect.

DISABLE_SAML_FLAG=1

If running a version of Domino lower than 10.0.1 FP1, it may be possible to request a hotfix to implement the above fix through a case opened with support. However, if opening a case, a business case as to why you cannot upgrade to Domino 10.0.1 FP1 may be required as part of the hotfix request.

ADFS Server Configuration Requirements.

Depending on the size and type of your organisation, your Domino Administrator may not be the ADFS administrator, and you may already have ADFS configured. Given this I've highlighted just the areas specific to Domino which the ADFS and Domino administrator need to be aware of to enable Kerberos authentication.

The steps required for setting up Integrated Windows Authentication for your users' browsers and Notes client, along with the steps on how to create relying party trusts in ADFS for the different forms of Domino SAML authentication will be covered in detail within the relevant sections later in the document. In this section the required ADFS configurations to implement Kerberos authentication are discussed so that they are set in place by your ADFS administrator prior to implementing the different methods[1].

By default, ADFS uses Forms Based Authentication and Windows Authentication (Kerberos). ADFS 4.0 can also utilise multi-factor authentication, but Domino does not currently support MFA.

Creating The Service Principle Name For Your ADFS Server.

The first step is to create two Service Principle Name entries for your ADFS server. This action can be done through the Windows command prompt, or through PowerShell. The following format is through the Windows command prompt.

```
setspn -s SERVICE/dns_name ADFS Service User Account
```

```
setspn -s SERVICE/shortname ADFS Service User Account
```

So as ADFS runs under and is connected to using the HTTP protocol and if the user account for the ADFS service in Windows is the Active Directory administrator, the following SPNs should be created.

```
setspn -s HTTP/samad.gftad.local Administrator
```

```
setspn -s HTTP/samad Administrator
```

Some documentation has the SETSPN command executed using the switch -a. While this will add the service principle name, it does not check for duplicates, which the -s switch does. It is recommended by Microsoft to use the -s switch as duplicate service principle names, will cause Kerberos authentication to fail. It is imperative that the SPN is set under the user account associated with the ADFS service in windows. If the SPN is set under the incorrect account Kerberos authentication will fail.

If the ADFS server has an alias in DNS, you will need to set up an SPN for each alias also, otherwise Kerberos authentication can also fail. You can use nslookup in exhaustive debugging mode to determine if an alias exists for your ADFS server, for example

```
C:\> nslookup

>set d2

>samad.gftad.local
```

[1] The discussed settings are for ADFS 4.0 and 3.0 for ADFS 2.0, if still used in your organisation, follow the steps listed in the following document https://www-10.lotus.com/ldd/dominowiki.nsf/dx/Cookbookcol_Setting_up_ADFS_for_integrated_Windows_authentication_lprIWArpr_

If the output identifies any alias for the hostname, you will have to add an SPN for the alias also under the same account that the ADFS service runs under.

It should be noted that when checking and setting an SPN that the user account you are logged in as must be a member of the Domain Admins, Enterprise Admins groups or they must have been delegated the appropriate authority to create SPNs otherwise the SPN will not be registered correctly.

Disabling Extended Protection In ADFS.

Once the SPNs have been created you need to disable Extended Protection in ADFS. To complete this task run PowerShell as Administrator and issue the following commands.

```
$FormatEnumerationLimit=-1

Get-ADFSProperties
```

The above commands will return the current settings for ADFS and can be used to confirm if Extended Protection is disabled or not.

If Extended Protection is enabled, as is the default in ADFS, the following command should be executed to disable extended protection.

```
Set-ADFSProperties –ExtendedProtectionTokenCheck None
```

Setting The Supported User Agents

ADFS has a list of supported user agents that can access ADFS via Windows Integrated Authentication. ADFS checks the agent string when performing login requests, and if the agent is not listed authentication will fail.

Most modern browsers will be present, however the Notes embedded browser uses the Mozilla 4.0 agent and may not be listed. If this agent is not listed, integrated windows authentication for Notes Federated Login will fail.

You can check the list of currently supported user agents by issuing the following command in PowerShell

```
Get-AdfsProperties | select -ExpandProperty WiaSupportedUserAgents
```

You can add the Mozilla 4.0 to the list of supported user agents in ADFS using the following command in PowerShell.

```
Set-ADFSProperties -WIASupportedUserAgents @("MSIE 6.0", "MSIE 7.0", "MSIE 8.0", "MSIE 9.0", "MSIE 10.0", "Trident/7.0", "MSIPC", "Windows Rights Management Client", "Firefox/25.0", "Firefox/47.0", "Mozilla/4.0", "Mozilla/5.0")
```

Again, it should be noted that you should just add "Mozilla/4.0" to the existing list within your ADFS configuration and your list may differ from the one shown above.

Configuring Integrated Windows Authentication In Your Browsers.

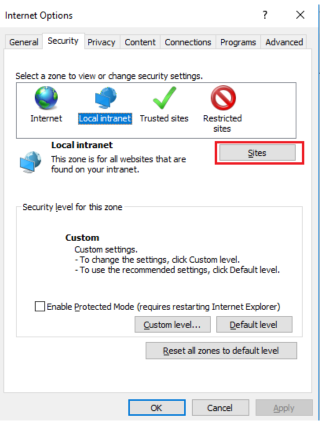
The following setting may be configured through different methods such as a GPO, however for simplicity, how to manually apply the required settings are just listed in this document.

For Internet Explorer

1. Select Tools → Internet Options.

2. Click on the Security tab and the Local Intranet Zone.

3. Click on the Sites button.



Select a zone to view or change security settings.

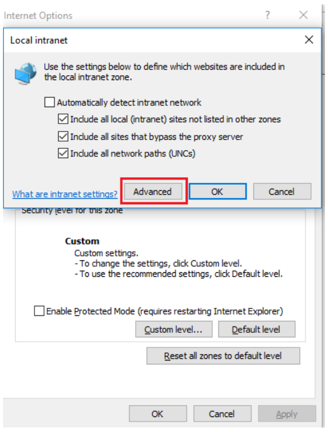
Local intranet
This zone is for all websites that are found on your intranet.

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☐ Enable Protected Mode (requires restarting Internet Explorer)

4. Click on the Advanced Button.



Use the settings below to define which websites are included in the local intranet zone.

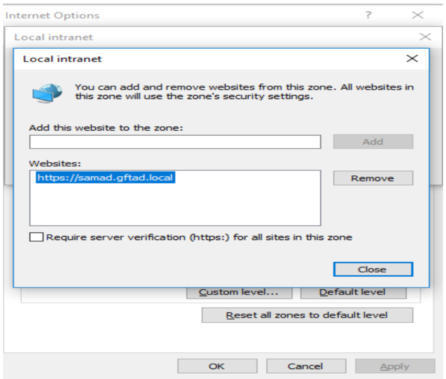
☐ Automatically detect intranet network
☑ Include all local (intranet) sites not listed in other zones
☑ Include all sites that bypass the proxy server
☑ Include all network paths (UNCs)

Security level for this zone

Custom
Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☐ Enable Protected Mode (requires restarting Internet Explorer)

5. Enter the https URL for your ADFS server and click Add and then close.



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:
https://samad.gftad.local

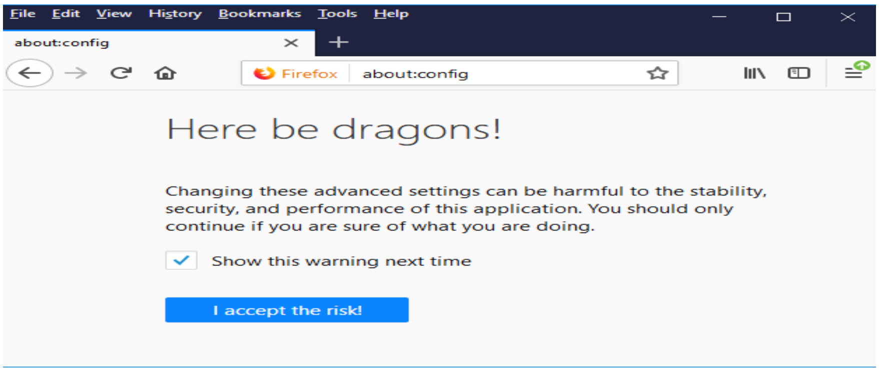
☐ Require server verification (https:) for all sites in this zone

6. Select the Advanced tab, and scroll down to the Security section.
   The setting Enable Integrated Windows Authentication should automatically be enabled/selected. If not select this option. Click Apply and OK to close Internet Options and restart Internet Explorer.

For Firefox.

1. In the address bar type about:config

2. Click on I accept the risk.



Here be dragons!

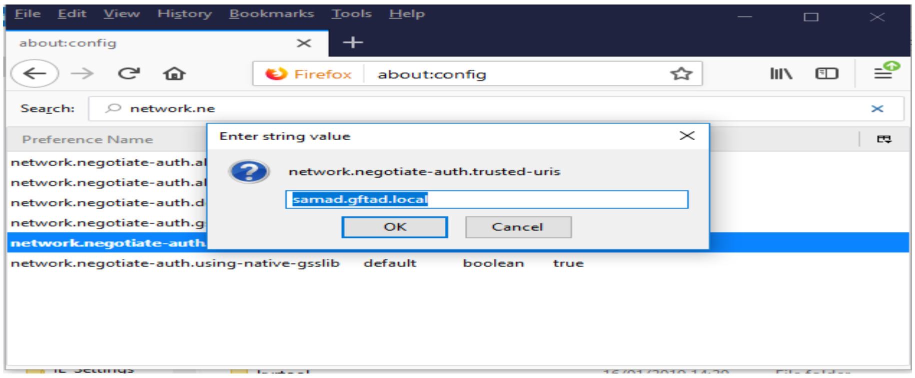
Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.

☑ Show this warning next time

I accept the risk!

3. In the search bar type network.ne

4. Click on network.negotiate-auth.trusted.uris and type the fully qualified host name for your ADFS server



Search: network.ne

network.negotiate-auth.al
network.negotiate-auth.al
network.negotiate-auth.d
network.negotiate-auth.g
network.negotiate-auth
network.negotiate-auth.using-native-gsslib default boolean true

Enter string value

network.negotiate-auth.trusted-uris

samad.gftad.local

5. Click OK and restart Firefox.

SAML Single Sign On For Domino.

The following section will outline the steps to configure your Domino web server(s) to utilise SAML Single Sign On authentication and how to create the required relying party trust in ADFS.

SAML Single Sign On, or Basic SAML as it also known, is the simplest implementation of SAML for Domino and is intended for allowing users to be authenticated via ADFS when accessing web based applications hosted on Domino without need for the ID Vault or policy settings. Some customers use this method for both internal users and when hosting applications that will be accessed by external organisations.

It is assumed that the required configuration settings in ADFS relating to Kerberos and Integrated Windows Authentication for your users' browsers, listed earlier in the document have been completed.

Configuring Your Domino Server

We will cover the steps required to create the IdP Configuration database and relying party trusts within ADFS later, but first it is important that your Domino servers or the Domino servers which host the Internet site(s), that you wish to enable for SAML Single Sign On, are appropriately configured.

1. Make sure you can connect to your Domino server using a web browser over HTTPS. This is a requirement for using ADFS as it expects all communication to be done through HTTPS, and you must have a SHA-2 certificate for your Domino server(s) and/or Internet sites.
   The following documents list the process for creating either a third party or self-signed certificate for your Domino Server, or Internet site.

   https://www-10.lotus.com/ldd/dominowiki.nsf/dx/3rd_Party_SHA-2_with_OpenSSL_and_kyrtool?open

   https://www-10.lotus.com/ldd/dominowiki.nsf/dx/Self-signed_SHA-2_with_OpenSSL_and_kyrtool

2. Password synchronisation between the Notes password and Internet password in the user's security policy must be disabled.

3. Disable the Internet Password Lockout feature if previously enabled.

4. The server ID file cannot be password protected, if using the Create Button to create a certificate in the document within the IdP Catalog database to encrypt the SAML assertions. Most customers in my experience do not have their server ID files password protected and this document follows this situation.
   However, if your organisation requires that a password is set for your Domino server ID files you will need to follow this document in order to create the SP.XML file.
   https://www.ibm.com/support/knowledgecenter/SSKTMJ_10.0.0/admin/secu_creating_a_domino_metadata_file_if_the_server_id_file_is_password_protected_t.html

5. The Domino administrator who creates the IdP Catalog database must be listed in the following fields in the security tab of the server document or be a member of a group listed in these fields.

    a. Full Access Administrators.

    b. Administrators.

    c. Sign or run unrestricted methods or operations.

6. Clock synchronisation between the Domino Server and the ADFS server must be implemented, otherwise authentication will fail. Even with NTP it has been seen that even time differences of a few seconds can cause authentication to fail.
   The following parameters should be added to the noteas.ini file to help deal with time creep. Please note 10 is the maximum value for these parameters
   SAML_NotBeforeSkewInMinutes=10

   SAML_NotOnOrAfterSkewInMinutes=10

Import The ADFS Servers SSL Certificate Into The Domino Directory.

As mentioned previously, ADFS requires all communication to be through HTTPS to facilitate this the root certificate of the ADFS server certificate must be imported into your Domino Directory as an Internet Certifier and an Internet Cross Certificate created from this entry.

Have your ADFS server administrator provide a base 64 encoded .crt file of the ADFS server's root CA certificate. If the ADFS server has a self-signed certificate, it must have the Certificates KeyUsage field values for Certificate Signer and CRL Signer in order to be able to import the certificate correctly into Domino as an Internet Certifier.

Using the Administration client select the Configuration Tab → Security → Certificates view.

Select the Actions menu → Import Internet Certificates option and select the .crt file provided.

On the Import Internet Certificates dialog click Accept All, you should receive a message stating the import was successful.

Create An Internet Cross Certificate For the ADFS Servers SSL Certificate

Select the Configuration Tab → Security → Certificates → Internet Certifiers view and open the document for the ADFS server's Internet Certifier document created earlier.

Select Actions → Create Cross Certificate and confirm that you wish to cross certify the certificate.

On the Issue Cross Certificate dialog, set the Server to your Domino Administration server and the Certifier to your Organisation certifier and click Cross Certify.

Creating And Configuring The IdP Catalog Database.

The IdP Catalog database stores the partnership configuration documents for each of your Domino servers or Internet sites and the identity provider.

When authentication is attempted the corresponding configuration document in the database is accessed to confirm that the received assertion is valid.

Full details on how to create configuration documents are covered later, this section simply details how to create the database and the conventions that must be observed.

1. The database is not created by default when Domino is installed or upgraded to Domino version 9.0 or higher. You must create the database on your server using the idpcat.ntf template with the Notes Administration client.

2. The database must be named idpcat.nsf. If your Domino server is installed on a *nix operating system or a mixed Windows and *nix environment, the filename must be in lowercase.

3. The idpcat.nsf must not be enabled for document locking.

4. There should be only one idpcat.nsf database for your entire Domino domain. Each server that is configured for SAML Single Sign On authentication should contain a replica of the idpcat.nsf.

To create the IdP Catalog database, using your Notes Administration client connect to the first Domino Server that you wish to enable for SAML Single Sign On authentication.

Select File → Application → New and on the New Application dialog

1. In the Server field select the server where you are enabling SAML authentication.

2. In the Title field enter a descriptive title for the database.

3. In the File name field enter idpcat.nsf

4. Click the Advanced templates option and select the server and idP Catalog template.

5. Click OK and the database will be created and opened.

You can now proceed to create a configuration document for your Domino Server or Internet Site hosted on this server and to replicate the database to any other server that you wish to enable SAML Single Sign On, open the database on that server and proceed to create a configuration document on that replica.[2]

[2] A common issue is the certificate for the ADFS server expiring and such a scenario is documented in https://www-01.ibm.com/support/docview.wss?uid=swg21998370

Creating a IdP Configuration Document in Domino 10 or higher.

Domino 10 introduced some improvements to how IdP configuration documents are created along with enabling support for ADFS 4.0. These enhancements have changed the layout of the IdP configuration documents also, when compared to Domino 9.0.x.

In the IdP Catalog database complete the following steps. Again this document assumes that your server’s ID file is not password protected.

1. Click Add IdP Config to open a new IdP configuration document.

2. In the Host names or addresses mapped to this site field the fully qualified host name of your Domino server/Internet site should automatically be entered. If it is not click on the drop-down arrow and select the server/Internet site. You must also the add the IP address of your server/Internet site using a semi-colon to separate the two entries.
For example: domweb.gftad.local; 192.168.56.3

3. Leave the Protocol Version field set to SAML 2.0.

4. Leave the State field set to Enabled.

5. Leave the Federation Product field set to AuthnRequest SAML 2.0 Compatible.

6. Set the Service Provider ID field to HTTPS URL of your Domino Server/Internet site.

7. In the IdP name field enter any text that you wish to describe the partnership.

8. Click on Save and Close. Then select the document and click Edit IdP config.

9. Click on the Certificate Management tab.

10. Click on Create SP Certificate and in the Create Company Certificate dialog enter a name for the certificate for example Domadsrv, and must be unique for each configuration.

11. In the Domino URL field the HTTPS URL for your Domino Server or Internet Site document should be entered.

12. While Domino does not support Single Logout for SAML, the Single Logout URL field should have a correctly formatted HTTPS URL for your ADFS server entered. Note this value is expected by TIFM

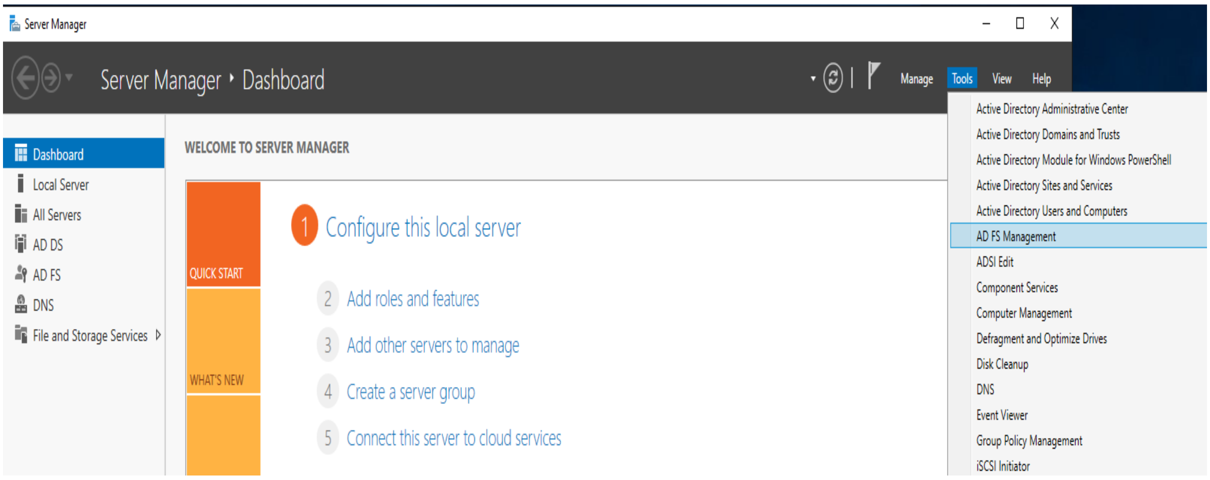
13. Click on Export SP XML. This file will be provided to the ADFS administrator to create the relying party trust in ADFS for your Domino Server/Internet site document.

At this point we will move over to ADFS to create a relying party trust for our Domino Server/Internet site. We can leave the IdP configuration document open or click Save and Close.

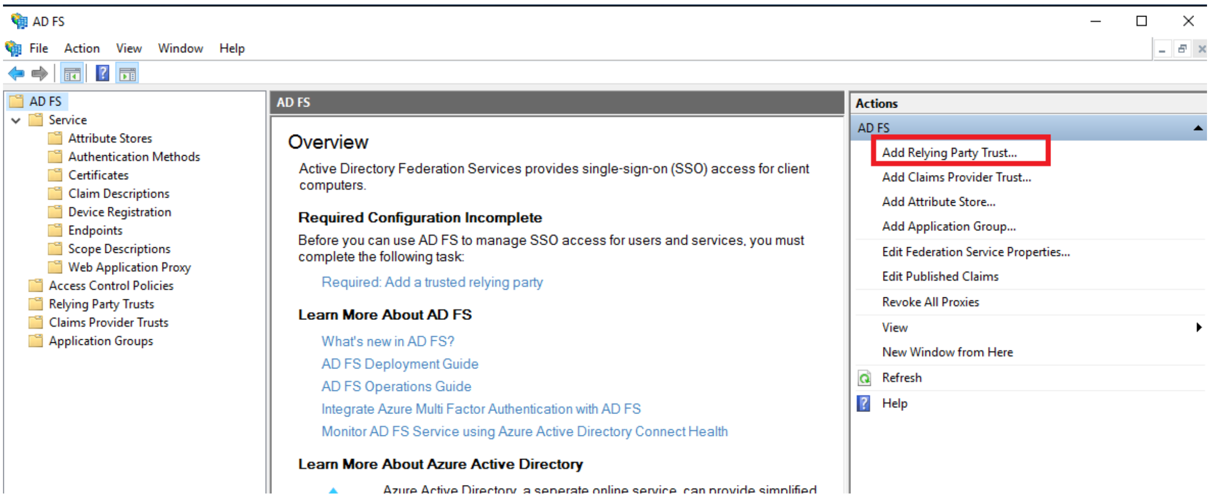
Creating A Relying Party Trust In ADFS

Once you have exported the SP XML file and provided this to your ADFS administrator, they can create a relying party trust for your Domino Server/Internet Site by importing this SP XML file into ADFS by following these steps.

1. On the Server Manager, select Tools → ADFS Management.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

2. Select Add Relying Party Trust.



Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

Learn More About AD FS

What's new in AD FS?

AD FS Deployment Guide

AD FS Operations Guide

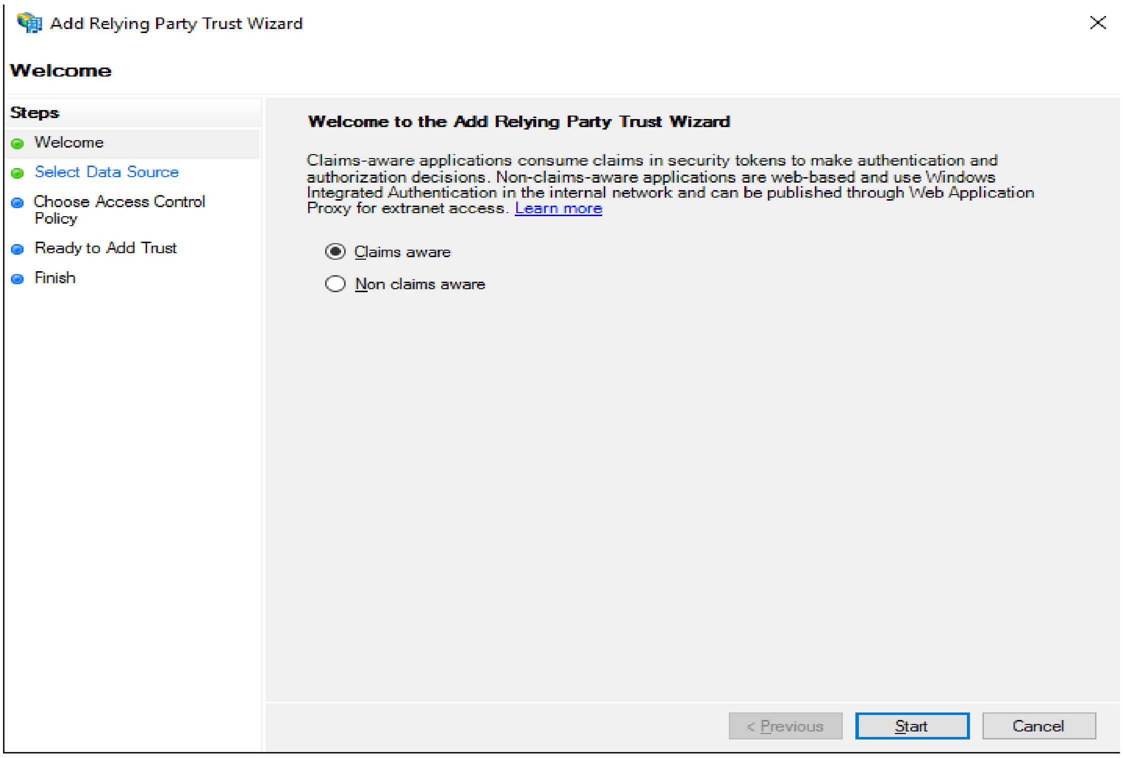
Integrate Azure Multi Factor Authentication with AD FS

Monitor AD FS Service using Azure Active Directory Connect Health

Learn More About Azure Active Directory

Azure Active Directory, a senerate online service, can provide simplified

3. Leave Claims aware selected and click Start.



Add Relying Party Trust Wizard

Welcome

Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

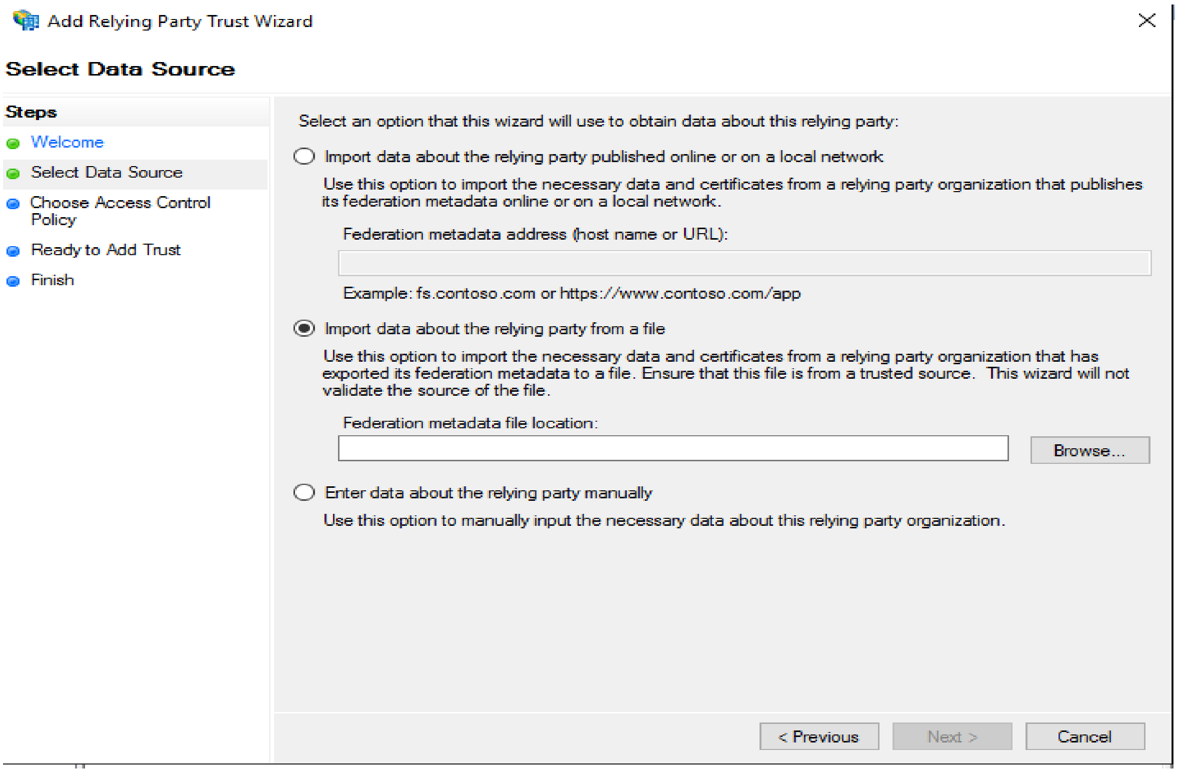
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

4. Select Import data about the relying party trust from a file and click Browse to select the SP XML file exported from your IdP configuration document and click Next.



Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

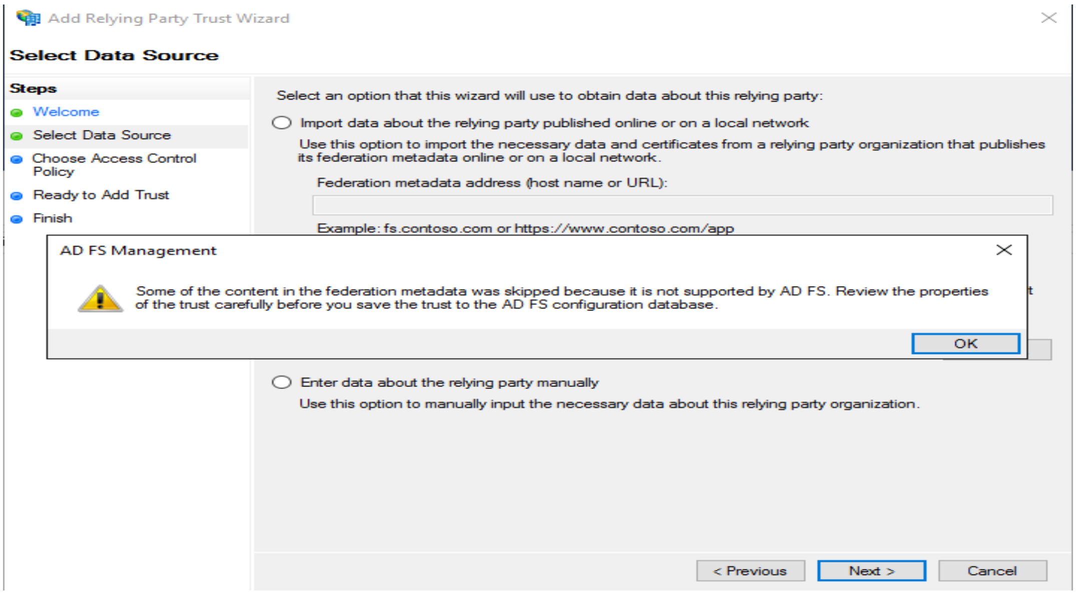
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

5. Click OK on the information message and then click Next. This action imports the Identity Provider, Certificate and Endpoint information for your Domino Server/Internet site into ADFS from the SP XML file automatically.



Add Relying Party Trust Wizard

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

AD FS Management

Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.

○ Enter data about the relying party manually

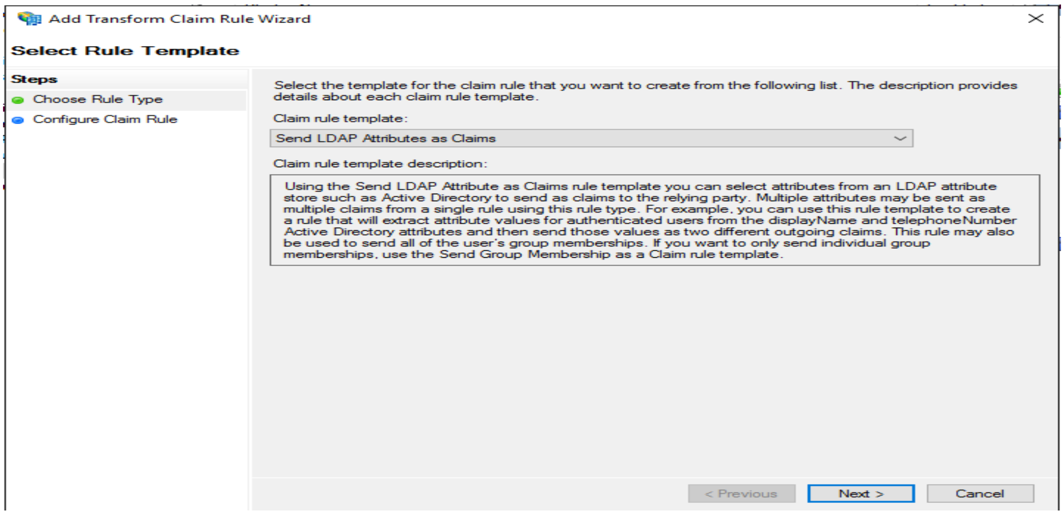
Use this option to manually input the necessary data about this relying party organization.

6. On the Choose Access Control Policy window, leave the default settings as is and click Next.

7. You can now review the settings for the partnership with your Domino Server/Internet site document, there should be no reason to change any of the settings and you can click Next to proceed.

8. Once the relying party trust has been entered successfully, click Close and you will be presented with the Claim Rule Wizard.

9. On the Choose Rule Type window click Next.



Add Transform Claim Rule Wizard

Select Rule Template

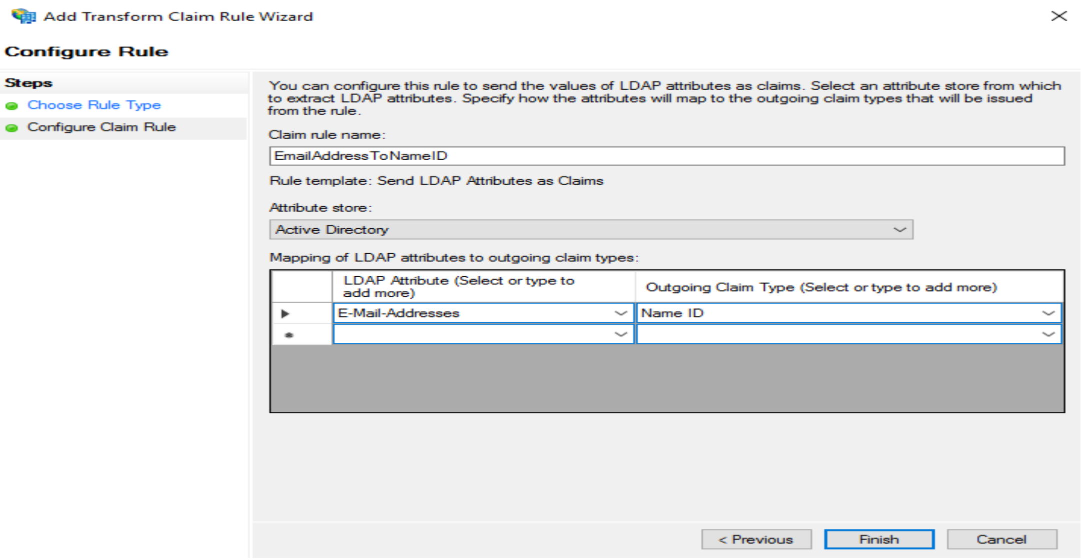
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

10. On the Configure Claim Rule Dialog enter EmailAddressToNameID as the Claim Rule name. Select Active Directory as the Attribute Store. In the LDAP Attribute drop down, select E-Mail-Address In the Outgoing Claim Type drop down, select Name ID.
    Then click Finish



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
EmailAddressToNameID

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	Name ID
*		

The ADFS administrator must now export the FederationMetaData xml file from the ADFS server and provide this to the Domino administrator. The Domino administrator can complete this step using Firefox if they know the URL of the ADFS server by entering the following format URL, replacing ServerName with the fully qualified host name of your ADFS server.

https://ServerName/FederationMetadata/2007-06/FederationMetadata.xml

for example, https://samad.gftad.local/FederationMetadata/2007-06/FederationMetadata.xml

The reason Firefox should be used is that, Internet Explorer will open the file rather than downloading the file. Copying the contents from the screen and saving it as a XML file results in an incorrect format for the file and will cause authentication to fail.

Importing The FederationMetaDate XML File Into Your IdP Configuration Document.

You may wish to create a copy of the federationmetadata.xml file before completing the steps below, as the import action deletes the file. Just make sure to delete the copy once you are sure that the import has been successful.

Bring the IdP Configuration document into edit mode if closed earlier.

On the Basics tab, click on the Import XML File button and navigate to the FederationMetaData.xml file exported earlier and then click OK.

This action populates the following fields with data from the FederationMetaData.xml file and the data should not be edited.

1. The Single sign-on service URL and Artefact resolution service url fields on the Basics tab. The latter field may not be populated, and if so should not affect SAML authentication.

2. The Signing X.509 certificate and Encryption X.509 certificate fields of the Advanced tab.

Once the FederationMetaData.XML file has been imported click Save and Close.

If you wish to enable SAML single Sign On for more than one Domino Server or Internet site, you must repeat the above process for each server/Internet site.

If setting up SAML for another Domino server or Internet site hosted on another server, you must first create a replica of the IdP Catalog database on the other server and create the IdP configuration document on this replica. This is required due to the fact that, when the certificate is created in the IdP configuration document, it is stored in the server's ID file. This certificate is used to decrypt the SAML assertion received from the ADFS server as part of the SAML authentication process. If the certificate is not present, the decryption of the assertion will fail and authentication will then fail.

If you have created the IdP configuration document on the wrong replica, you can delete the IdP configuration document and relying party trust in ADFS and complete the steps again from the correct replica, or you could attempt to export the certificate from the wrong server's ID file and import it into the correct server's ID file by completing steps 1 and 3 in the following document

https://www-01.ibm.com/support/docview.wss?uid=swg22016213

Creating a IdP Configuration Document in Domino 9.0 - 9.0.1.

While you can still export the settings from the IdP configuration document in Domino 9.0 – 9.0.1, some customers have reported issues with the settings not being correctly exported within this file when imported into ADFS 2.0 and 3.0 in that the name of the server was not correctly set in the export.xml file.

Given this, it is often recommended to customers that they create the relying party trust for their Domino Server/Internet site by manually creating the Relying Party Trust document in ADFS as outlined in the next section.

Manually Create A Relying Party Trust In ADFS For Your Domino Server/Internet Site.

1. Open the ADFS manager.
2. Click on Add Relying Party Trust.
3. On the Welcome window click Start.
4. On the Select Data Source window, select the Enter data about the relying party manually option and click Next.
5. On the Specify Display Name pane, enter a descriptive name for your Domino server partnership and click Next.

6. On the Choose Profile pane, the option ADFS profile option should be automatically selected, if not select this option and click next.

7. On the Configure Certificate pane, just click Next

8. On the Configure URL pane, select the Enable support for the SAML 2.0 Web SSO protocol option, and then enter the secure URL for your Domino server's fully qualified host name or Internet Site with the references to the Domino Directory and the SAMLLogin command, for example: https://domweb.gftad.local/names.nsf?SAMLLogin and then click Next.

9. On the Configure Identifiers pane, in the Relying party trust identifier field, enter the secure URL for your Domino server's fully qualified host name, or your Internet site, for example https://domweb.gftad.local, and then click Add and then click Next.

10. On the Choose Issuance Authorisation Rules pane, the option Permit all users to access the relying party, should be selected by default, if not select this option and click Next.

11. On the Ready to Add Trust pane, you can select any of the tabs and change the details if required. But this should not be needed so click Next

12. On the Finish pane, the option Open the Edit Claim Rules dialog for this relying party trust when the wizard closes is selected by default, as this is a required step leave the option selected and click Next.

13. The Edit Claims Rules dialog will now open, click Add Rule.

14. On the Add Transform Claim Rule Wizard Dialog's Choose Rule Type pane leave the default option Send LDAP Attributes as Claims selected and click Next.

15. On the Configure Claim Rule pane, in the Claim rule name field enter the value EmailAddressToNameID or similar as the name.

16. For the Attribute store select Active Directory from the drop-down list.

17. In the Mapping of LDAP attributes for outgoing claim types, select E-Mail-Addresses as the LDAP Attributes and select Name ID as the Outgoing Claim Type and then click Finish.

18. You will now be brought back to the Edit Claims Rule dialog. Click Apply and then OK.

The ADFS side of the partnership is now configured and the ADFS manager can be closed.

Your ADFS administrator will now have to export these details from ADFS into a XML file which needs to be imported into the IdP configuration document in Domino, or the Domino administrator can complete this step if they know the URL of the ADFS server.

Using Firefox to access the ADFS server using the following URL replacing ServerName with the fully qualified host name of your ADFS server.

https://ServerName/FederationMetadata/2007-06/FederationMetadata.xml

for example, https://samad.gftad.local/FederationMetadata/2007-06/FederationMetadata.xml

The reason Firefox should be used is that Internet Explorer will open the file rather than downloading the file. Copying the contents from the screen and saving it as a XML file results in an incorrect format for the file and will cause authentication to fail.

Completing The IdP Configuration Document in Domino 9.0 - 9.0.1.

On your server open the IdP Configuration database and click Add IdP Config and on the Basics Tab

1. In the Host names or addresses mapped to this site field enter the fully qualified host name and IP address of your Domino server/Internet site. You should separate the name and IP address using a semi colon.

2. In the IdP name field enter any text that you wish to describe the partnership.

3. Change the Protocol Version field to SAML 2.0.

4. Leave the Federation Product field set as ADFS.

5. In the Service provider ID field enter the HTTPS URL for your Domino Server/Internet site.

6. You must now import the Federation Metadata file from your ADFS server by clicking Import XML file and browsing to where you have saved the XML file and click open. This will populate the rest of the fields in the Basics tab.

7. Click on the Certificate Management tab.

8. In the Company name field enter a name to identify the Internet certificate that will be imported by the ADFS identity provider. The name must be unique for each configuration.

9. Save and close the document, then reopen the document in edit mode and select the Certificate Management tab again.

10. Click the Create Certificate button, this adds the Internet certificate to the server ID file.

11. In the Domino URL field enter the secure URL to your domino server/Internet site as was entered in the Configure Identifiers pane, in the Relying party trust identifier field of the associated ADFS relying party trust configuration.

12. In the Single Logout URL field enter the link expected by Identify Provider. Note this value is expected by TIFM, but is not actually supported by Domino.

13. Click Export XML to save an IdP XML file as an attachment in the document.

14. Click Save and Close

Completing The Configuration For SAML Single Sign On.

Once you have completed the creation of the IdP configuration document by importing the FederationMetaData.XML file from your ADFS server and saving the changes, you can complete the following steps to finish the configuration of your Domino Server/Internet Site.

Setting SAML As The Authentication Method For Your Domino Server/Internet Site.

It is recommended to set up a simple test application such as a Notes Discussion database and add the users whom you will be testing with to the ACL of the database. This database can then be set as the homepage of your Domino server/Internet site document.

If your Domino server does not host an Internet Site, you must open the server document in edit mode and

1. Select the Internet Protocols → Domino Web Engine tab.

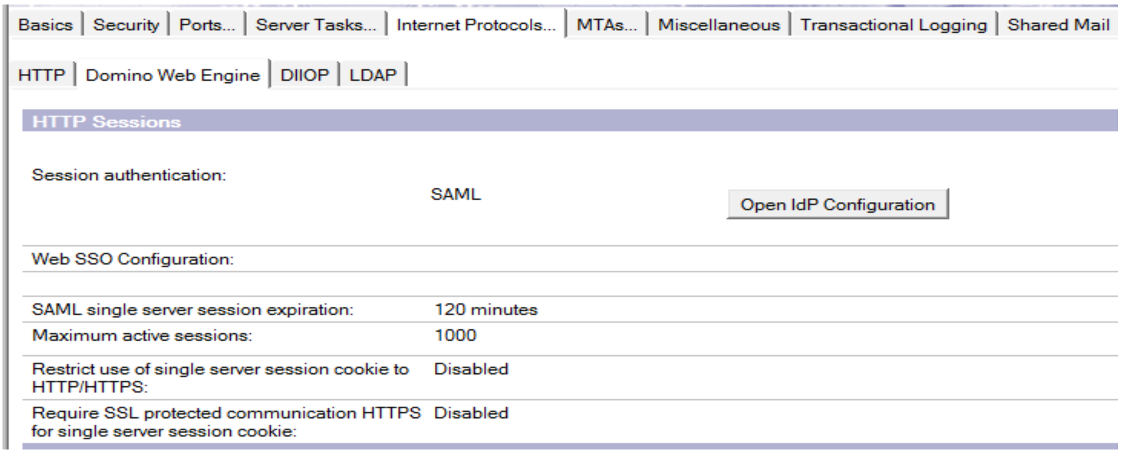
2. Select the Session Authentication field and select SAML.

3. The Open IdP Configuration button should now become active, click on this to ensure that the corresponding configuration document should be opened.

4. If not using an SSO document, leave the SAML single server session expiration field set at 120 minutes[3].

5. Save your changes to the server document and restart Domino.

[3] If using an LTPA token, all servers should be configured for SAML single sign on authentication.


Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared Mail
HTTP | Domino Web Engine | DIIOP | LDAP
Open IdP Configuration

HTTP Sessions

Session authentication:	SAML
Web SSO Configuration:	
SAML single server session expiration:	120 minutes
Maximum active sessions:	1000
Restrict use of single server session cookie to HTTP/HTTPS:	Disabled
Require SSL protected communication HTTPS for single server session cookie:	Disabled

If you are enabling SAML for an Internet site hosted on your Domino server, you must open the Internet site document in edit mode and

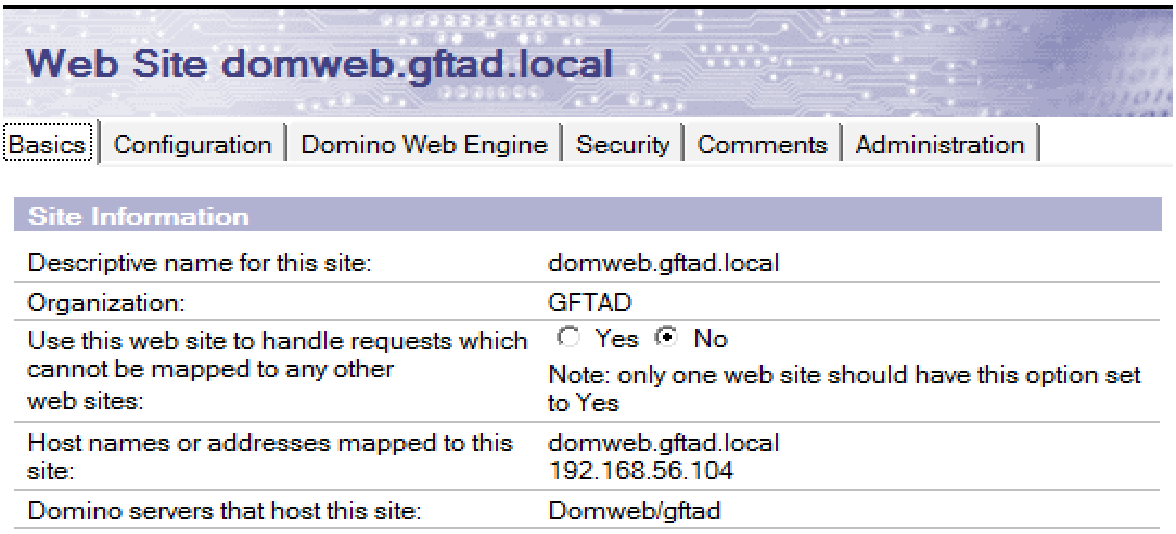
1. Select the Domino Web Engine tab.

2. Select the Session Authentication field and select SAML.

3. The Open IdP Configuration button should now become active, click on this to ensure that the corresponding configuration document should be opened.

4. If not using an SSO document, leave the SAML single server session expiration field set at 120 minutes.

5. Save your changes to the Internet site document and restart Domino.


Web Site domweb.gftad.local
Basics | Configuration | Domino Web Engine | Security | Comments | Administration

Site Information

Descriptive name for this site:	domweb.gftad.local
Organization:	GFTAD
Use this web site to handle requests which cannot be mapped to any other web sites:	○ Yes ● No Note: only one web site should have this option set to Yes
Host names or addresses mapped to this site:	domweb.gftad.local 192.168.56.104
Domino servers that host this site:	Domweb/gftad

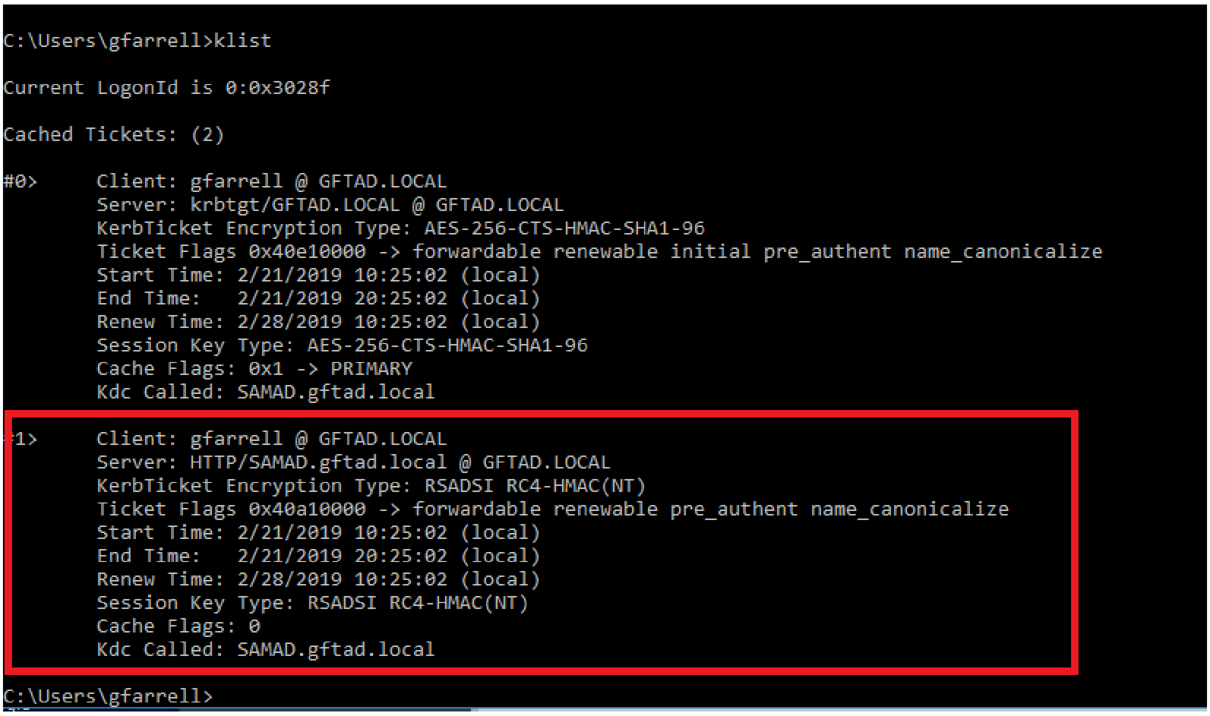
Testing SAML Single Sign On.

Log into a Windows client machine on your Active Directory domain and open your selected browser and enter the HTTPS URL for your Domino Server/Internet site document.

If using Kerberos/Integrated Windows Authentication, you should be automatically logged into the Notes discussion database that you set as the home URL of your server/Internet site.

If you have any errors connecting enable the debug parameters listed below and review the output to see what errors are returned. If you cannot determine the cause of the failure open a case with support for their assistance.

You can confirm if your test user is receiving a Kerberos ticket for the ADFS server by opening the Windows Command Prompt and entering the command klist, which will return the tickets issued to the user. You should see a ticket for your ADFS server listed as shown below.



```
C:\Users\gfarrell>klist

Current LogonId is 0:0x3028f

Cached Tickets: (2)

#0>     Client: gfarrell @ GFTAD.LOCAL
        Server: krbtgt/GFTAD.LOCAL @ GFTAD.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 2/21/2019 10:25:02 (local)
        End Time:   2/21/2019 20:25:02 (local)
        Renew Time: 2/28/2019 10:25:02 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: SAMAD.gftad.local

#1>     Client: gfarrell @ GFTAD.LOCAL
        Server: HTTP/SAMAD.gftad.local @ GFTAD.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 2/21/2019 10:25:02 (local)
        End Time:   2/21/2019 20:25:02 (local)
        Renew Time: 2/28/2019 10:25:02 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called: SAMAD.gftad.local

C:\Users\gfarrell>
```

Debug Parameters.

The following debug parameters may be helpful if you encounter any issues configuring this authentication method.

DEBUG_SAML=31

For issues with TLS you can add.

DEBUG_SSL_ALL=2

For issues with name mapping/resolution the following parameters can also be added

WEBAUTH_VERBOSE_TRACE=1

LOGLEVEL_NAME_MAPPING=1

DEBUG_NAMELOOKUP=1

Notes Federated Login.

Notes Federated Login (NFL) allows an organisation utilise SAML authentication for your Notes client users whose IDs are vaulted in a ID Vault database.

With Notes Federated Login, your ID Vault servers are partnered with ADFS for SAML authentication with either ADFS or TIFM as the identity provider. Your ID Vault servers do not have to have the Domino HTTP task running as it is the Notes client that handles the HTTP portion of the SAML authentication routine. Notes Federated Login can utilise Integrated Windows Authentication or Forms Based Authentication. The focus of this document will be on utilising Integrated Windows Authentication, and assumes that the user agent "Mozilla/4.0" has been added to your ADFS configuration. Please review the section ADFS Server Configuration Requirements if it has not.

The configuration is more complex than SAML Single Sign On and in Domino 10 the enhancements made to support ADFS 4.0 have changed how the IdP configuration document and replying party trust can be created and configured.

With Domino 9.0 – 9.0.1 you could configure the relying party trust in ADFS to use the following URL format as the endpoint https://idvaultserver.com/names.nsf?SAMLLogin, the same format as used for SAML Single Sign On. This meant that customers who enabled the HTTP task on their ID Vault servers could test that the partnership between their Domino server and ADFS was working correctly by following the steps to set up SAML Single Sign On, before moving on to configuring Notes Federated Login.With Domino 10 however, this has changed as Domino sends https://idvaultserver.com/names.nsf? SAMLIDLogin automatically to ADFS 4.0 with AuthnRequst SAML 2.0 compatible set as the Federation Product in the IdP configuration document as can be seen with DEBUG_SAML=31 set on the ID Vault server.

```
[0978:003C-0ABC] 21/02/2019 13:33:48.28 ConfigCacheAdd> Adding config to cache: ContextId=1
hostname=Domadsrv.gftad.local

[0978:003C-0ABC] 21/02/2019 13:33:48.28 SECformatAuthnRequestRedirectURL> samlUrl
https://samad.gftad.local/adfs/ls/, samlProdiverID https://Domadsrv.gftad.local

[0978:003C-0ABC] SECformatAuthnRequestRedirectURL: AssertionConsumerServiceURL
AssertionConsumerServiceURL="https://Domadsrv.gftad.local/names.nsf?SAMLIDLogin"

[0978:003C-0ABC] 21/02/2019 13:33:48.28 SECAuthnRequestSignData> CalcDigest Issuer CN=gftad, error No error

[0978:003C-0ABC] 21/02/2019 13:33:48.28 SECAuthnRequestSignData> CalcDigest Digest Size: 1E6 Data
<samlp:AuthnRequest AssertionConsumerServiceURL="https://Domadsrv.gftad.local/names.nsf?SAMLIDLogin"
Destination="https://samad.gftad.local/adfs/ls/" ID="_B685EEFBE9DDFB2A49
```

Given that Domino 10 – 10.0.1 and ADFS v 4.0 are the latest versions of the products provided by HCL and Microsoft at the time of writing, I will follow their use for the remainder of this document. Just be aware that with Domino 9.0 – 9.0.1 that the replying party trust and IdP configuration document for your ID Vault server can be set up using the same steps as for SAML for Single Sign On authentication, and then the rest of the configuration steps listed in this document can be followed to complete the configuration for Notes Federated Login.

You use a security settings policy to apply Notes Federated Login to your users. The required settings for this document will be covered in full later in the document. It allows the Notes client to communicate over HTTPS to the ADFS server, retrieve the SAML assertion and send this to your ID Vault servers so that the user's ID can be downloaded.

Notes Federation Login Authentication Flow.

When configured correctly the following authentication flow occurs when a user launches their Notes client.

1. The Notes client connects to its mail server. The user's policy is checked and if the user's mail server is not an ID Vault server a referral is returned for the ID Vault server.

2. An NRPC request to download the user's ID is sent to the ID Vault server.

3. The ID Vault server returns the URL of the identity provider (ADFS server).

4. The Notes embedded browser sends a HTTPS request to the identity provider.

5. The user is authenticated with the identity provider.

6. The identity provider returns the SAML assertion to the Notes client.

7. The Notes client sends the assertion to the ID Vault server via NRPC.

8. The ID Vault server returns the unlocked ID file to the Notes client where it is stored in memory.

With Notes Federated Login the user's ID is stored in memory, to allow for offline access to the Notes Client, Notes Shared Login can also be enabled for the users via the security settings policy that also enables Notes Federated Login.

Configuring Your ID Vault Servers.

While some of the information below has been mentioned previously in the document, I'm listing them here again in case the document is not being read in order and you just wish to obtain information on how to implement Notes Federated Login.

We will cover the steps required to create the IdP Configuration database and relying party trusts within ADFS later, but first it is important that your ID Vault Servers are correctly configured

1. Password synchronisation between the Notes password and Internet password in the user's security policy must be disabled.

2. Disable the Internet Password Lockout feature if previously enabled.

3. The server ID file cannot have a password if using the Create Button to create a certificate in the document within the IdP Catalog database to encrypt the SAML assertions.
   Most customers do not have their server ID files password protected and this document follows this scenario. If the customer has password protected their servers' IDs they must follow the steps listed in the Administration help to create the SP.XML file
   https://www.ibm.com/support/knowledgecenter/SSKTMJ_10.0.0/admin/secu_creating_a_domino_metadata_file_if_the_server_id_file_is_password_protected_t.html

4. The Domino administrator who creates the IdP Catalog database must be listed in the following fields in the security tab of the server document or be a member of a group listed in these fields.
   a. Full Access Administrators.

   b. Administrators.

   c. Sign or run unrestricted methods or operations.

5. The Domino Server and the ADFS server must have their clocks synchronised, otherwise authentication will fail. Even with NTP enabled a difference of a couple of seconds can cause authentication to fail.
   The following parameters should be added to the notes.ini file of the ID vault server(s) which you are configuring to help deal with time creep. Please note 10 is the maximum value for these parameters

   ```
   SAML_NotBeforeSkewInMinutes=10

   SAML_NotOnOrAfterSkewInMinutes=10
   ```

Import The ADFS Servers SSL Certificate Into The Domino Directory.

While your ID Vault server does not need to be running the Domino HTTP task, as the Notes client handles the HTTP connection to the ADFS server, you must import the root certificate of your ADFS server's certificate into your Domino Directory as an Internet Certifier, and create an Internet Cross Certificate from this entry. This Internet Cross Certificate is added to your users' local address book, through the security settings policy that you must create for implementing Notes Federated Login.

Have your ADFS server administrator provide a base 64 encoded .crt file of the ADFS server's root CA certificate. If the ADFS server has a self-signed certificate, it must have the Certificates KeyUsage field values for Certificate Signer and CRL Signer in order to be able to import the certificate correctly into Domino as an Internet Certifier.

Using the Administration client select the Configuration Tab → Security → Certificates view.

Select the Actions menu → Import Internet Certificates option and select the .crt file provided.

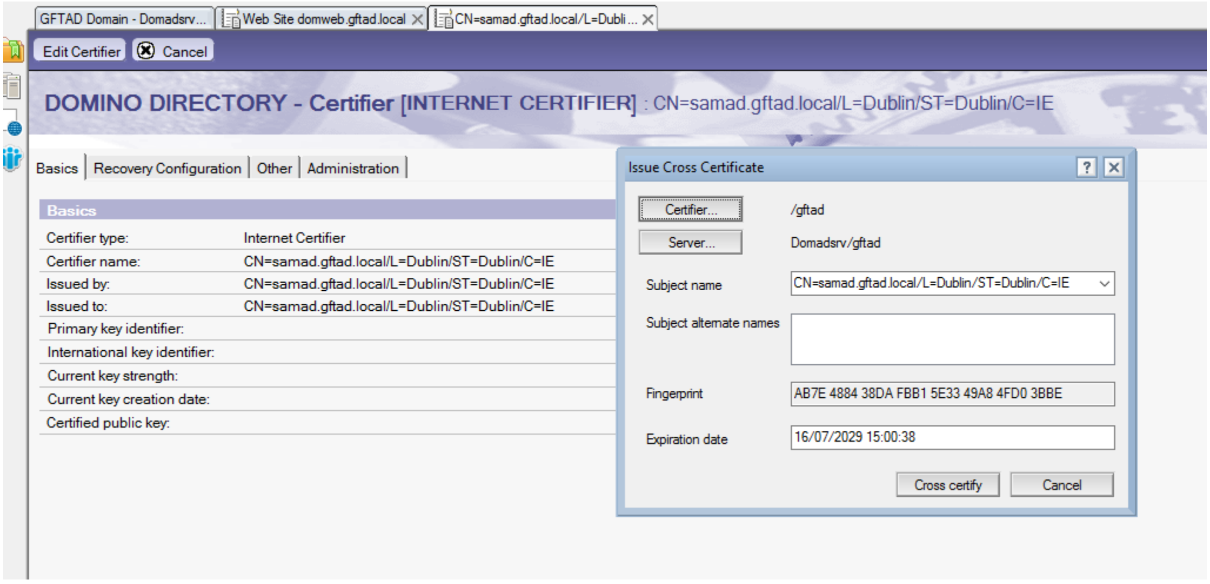
On the Import Internet Certificates dialog click Accept All, you should receive a message stating the import was successful.

Create An Internet Cross Certificate For the ADFS Servers SSL Certificate

Select the Configuration Tab → Security → Certificates → Internet Certifiers view and open the document for the ADFS server's Internet Certifier document created earlier.

Select Actions → Create Cross Certificate and confirm that you wish to cross certify the certificate.

On the Issue Cross Certificate dialog, set the Server to your Domino Administration server and the Certifier to your Organisation certifier and click Cross Certify.



DOMINO DIRECTORY - Certifier [INTERNET CERTIFIER] : CN=samad.gftad.local/L=Dublin/ST=Dublin/C=IE

Basics

Certifier type:	Internet Certifier
Certifier name:	CN=samad.gftad.local/L=Dublin/ST=Dublin/C=IE
Issued by:	CN=samad.gftad.local/L=Dublin/ST=Dublin/C=IE
Issued to:	CN=samad.gftad.local/L=Dublin/ST=Dublin/C=IE
Primary key identifier:	
International key identifier:	
Current key strength:	
Current key creation date:	
Certified public key:	

Issue Cross Certificate

Certifier...	/gftad
Server...	Domadsrv/gftad
Subject name	CN=samad.gftad.local/L=Dublin/ST=Dublin/C=IE
Subject alternate names	
Fingerprint	AB7E 4884 38DA FBB1 5E33 49A8 4FD0 3BBE
Expiration date	16/07/2029 15:00:38

Creating And Configuring The IdP Catalog Database.

The IdP Catalog database stores the partnership configuration documents for each of your ID Vault servers and the identity provider. Full details on how to create these partnership configuration documents are covered later, this section simply details how to create the database and the conventions that must be observed

In relation to the IdP Catalog database the following must be observed.

1. The database is not created by default when Domino is installed or upgraded to Domino version 9.0 or higher.
   You must create the database on your primary ID Vault server using the idpcat.ntf template using the Administration client.

2. The database must be named idpcat.nsf. If your ID Vault server is installed on a *nix operating system, or in a mixed Windows and *nix environment, the filename must be in lowercase.

3. The idpcat.nsf must not be enabled for document locking.

4. There should be only one idpcat.nsf database for your entire domain. The database should be created first on your primary ID Vault server and then replicated to each vault replica server.

To create the IdP Catalog database the following steps must be completed using your Administration client on your primary ID Vault server.

Select File → Application → New and on the New Application dialog

1. In the Server field select the server where you are enabling SAML authentication.

2. In the Title field enter a descriptive title for the database.

3. In the File name field enter idpcat.nsf

4. Click the Advanced templates option and select the server and idP Catalog template.

5. Click OK and the database will be created and opened.

You can now proceed to create a configuration document for your ID Vault server.

It should be noted that in relation to Notes Federated Login and clustered ID Vault servers there are some known issues

1. Failover between ID Vault servers during login results in failed authentication as reported in SPR # NPEI9PF5UH. In this case if the ID Vault server that the Notes client connects to at the start of the SAML authentication process goes down, the Notes client cannot be failed over to a cluster mate of the original ID Vault server and have SAML authentication succeed.

2. During login or set up of a Notes client the incorrect server being selected from the Vault configuration will cause authentication and or set up to fail. This was reported in SPR # SRAOB3EQMB and is fixed in Domino 10.0

Creating a IdP Configuration Document in Domino 10 or higher.

Domino 10 introduced some improvements to how IdP configuration documents are created along with enabling support for ADFS 4.0, which is the focus of this document.

In the IdP Catalog database complete the following steps. The steps are based on not having your server's ID file password protected.

1. Click Add IdP Config to open a new IdP configuration document.

2. In the Host names or addresses mapped to this site field the fully qualified host name of your ID Vault server site should automatically be entered. If it is not click on the drop-down arrow and select the server.

3. Leave the Protocol Version field set to SAML 2.0.

4. Leave the State field set to Enabled.

5. Leave the Federation Product field set to AuthnRequest SAML 2.0 Compatible.

6. Set the Service Provider ID field to HTTPS URL of your ID Vault server. This is required even though the HTTP task is not active on your ID Vault server.

7. In the IdP name field enter any text that you wish to describe the partnership.

8. Click on Save and Close. Then select the document and click Edit IdP config.

9. Click on the Certificate Management tab.

10. Click on Create SP Certificate and in the Create Company Certificate dialog enter a name for the certificate for example Domadsrv, and must be unique for each configuration.

11. In the Domino URL field the HTTPS URL for your ID Vault server should be entered.

14. While Domino does not support Single Logout for SAML, the Single Logout Url field should have a correctly formatted HTTPS URL for your ADFS server. Note this value is expected by TIFM, but is not actually supported by Domino

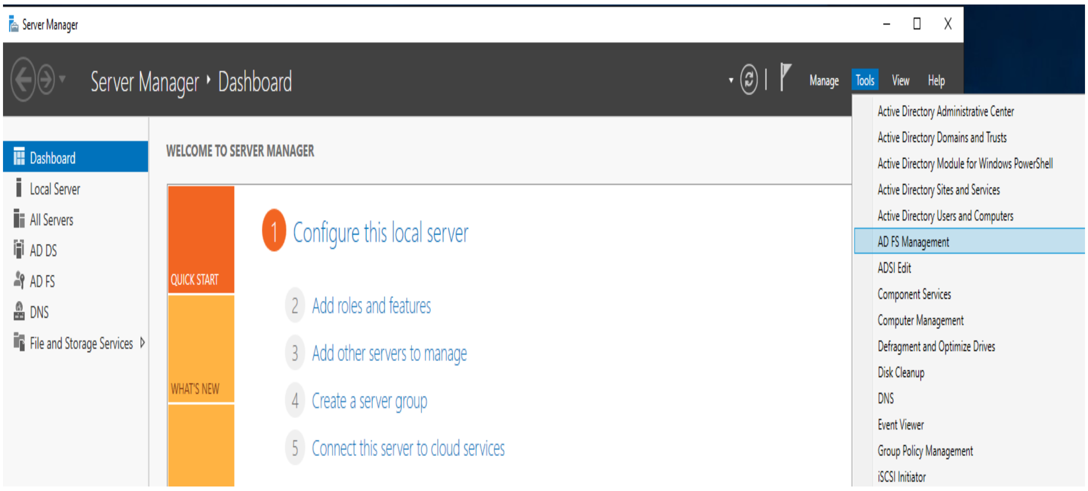
15. Click on Export SP XML. This file will be provided to the ADFS administrator, to create the relying party trust in ADFS for your Domino Server/Internet site document.

At this point the SP.XML file should be provided to the ADFS administrator who will use this file to create a new relying party trust for our ID Vault server. We can leave the IdP configuration document open or click Save and Close.

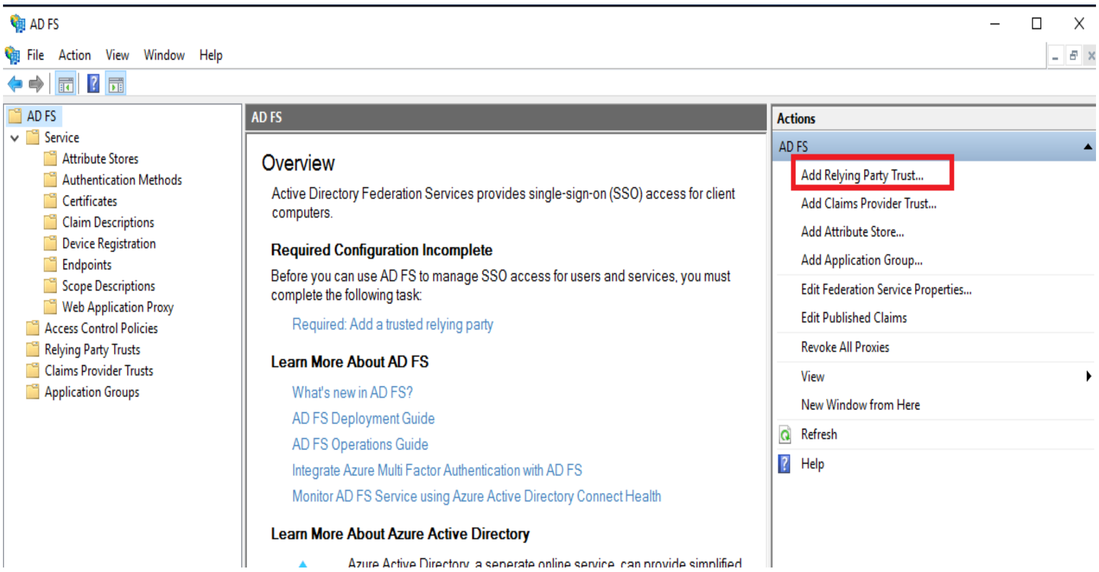
Creating A Relying Party Trust In ADFS

Once you have exported the SP XML file you can create a relying party trust for your Domino Server/Internet Site by importing the SP XML file.

1. On the Server Manager, select Tools → ADFS Management.


Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

2. Select Add Relying Party Trust.



Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

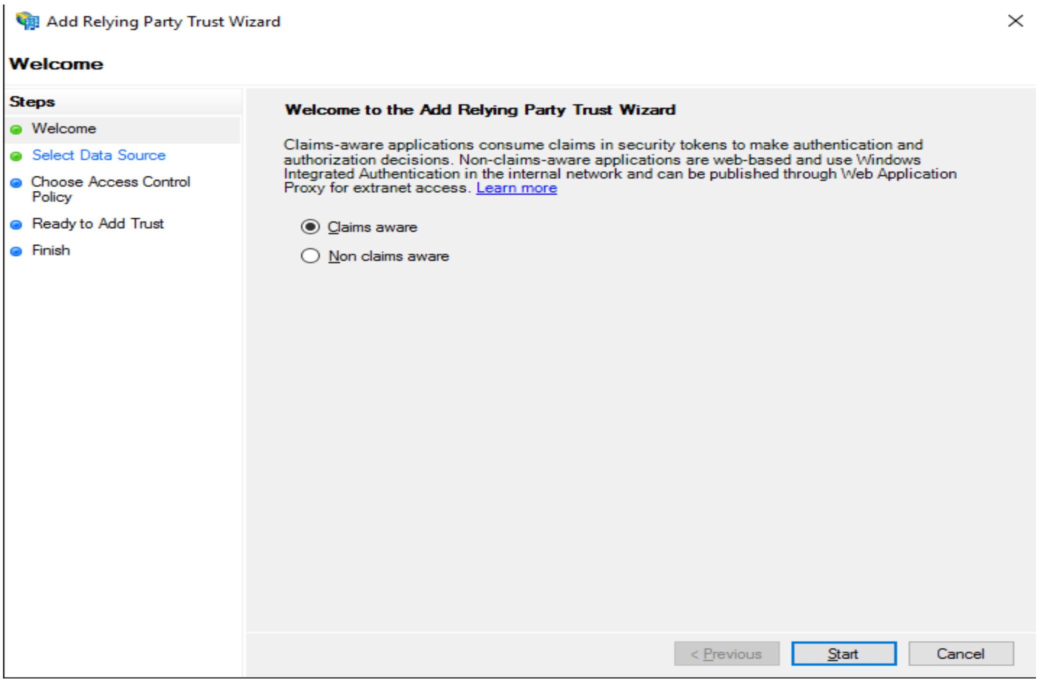
Learn More About AD FS

What's new in AD FS?
AD FS Deployment Guide
AD FS Operations Guide
Integrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health

Learn More About Azure Active Directory

Azure Active Directory, a seperate online service, can provide simplified

3. Leave Claims aware selected and click Start.



Add Relying Party Trust Wizard

Welcome

Steps
- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

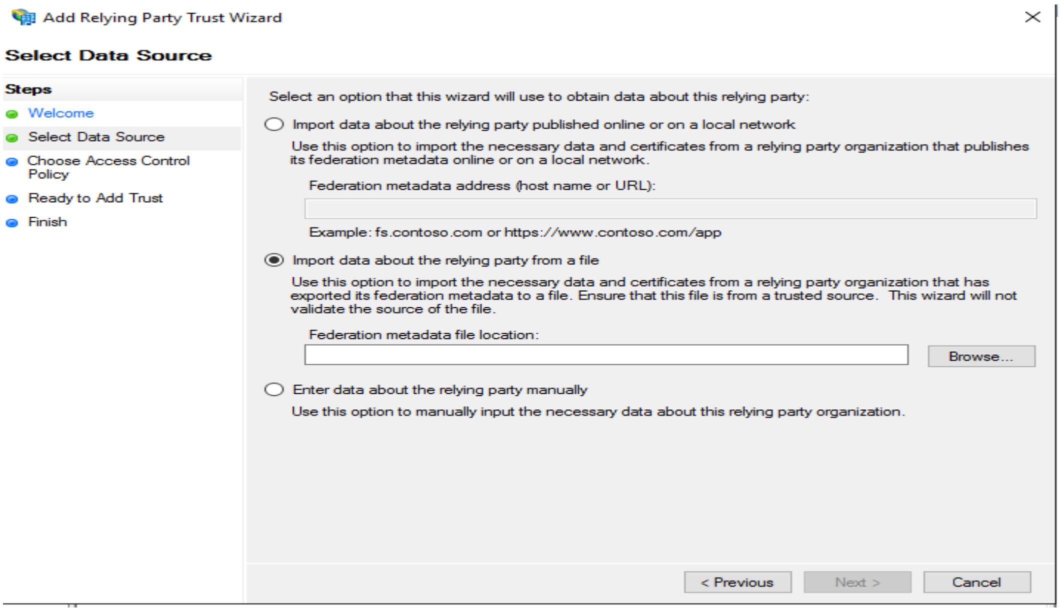
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

4. Select Import data about the relying party trust from a file and click Browse to select the SP XML file exported from your IdP configuration document and click Next.



Add Relying Party Trust Wizard

Select Data Source

Steps
- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

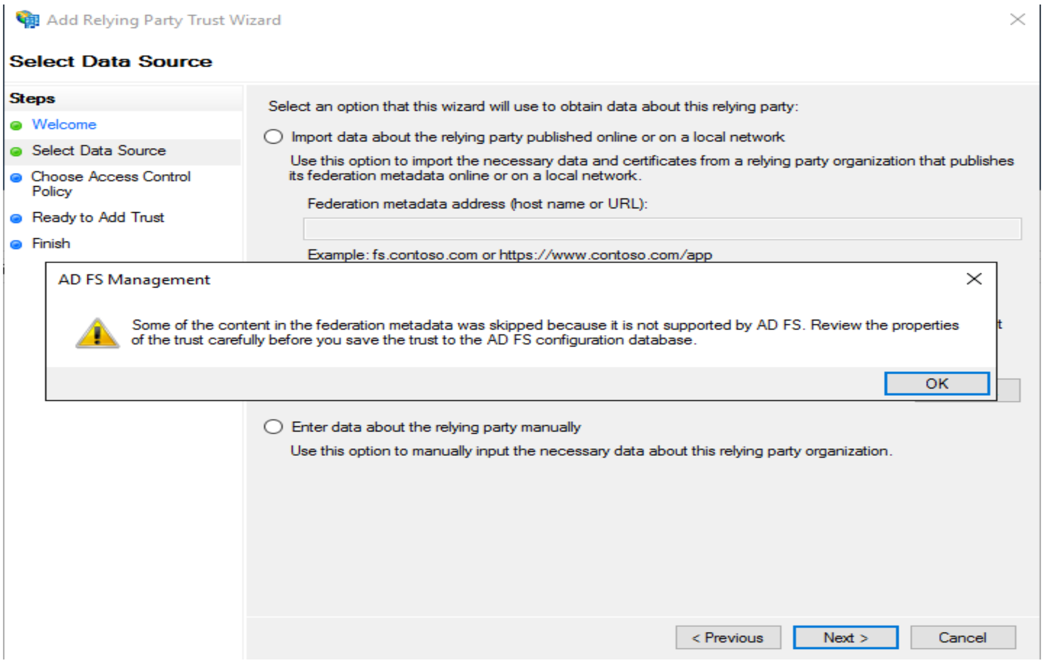
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

5. Click OK on the information message and then click Next. This action imports the Identity Provider, Certificate and Endpoint information for your ID Vault server into ADFS from the SP XML file automatically.



Select Data Source

Steps
- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

AD FS Management

Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.

○ Enter data about the relying party manually

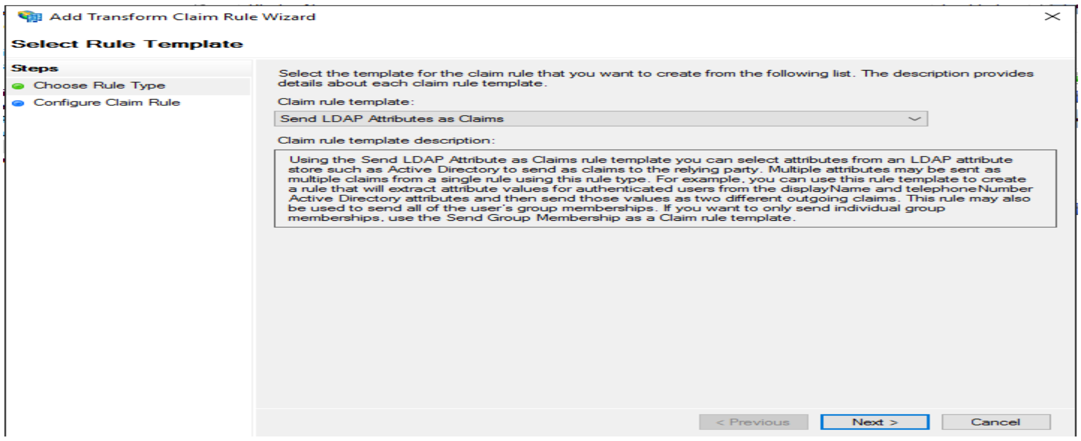
Use this option to manually input the necessary data about this relying party organization.

6. On the Choose Access Control Policy window, leave the default settings as is and click Next.

7. You can now review the settings for the partnership with your Domino Server/Internet site document, there should be no reason to change any of the settings and you can click Next to proceed.

8. Once the relying party trust has been entered successfully, click Close and you will be presented with the Claim Rule Wizard.

9. On the Choose Rule Type window click Next.



Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

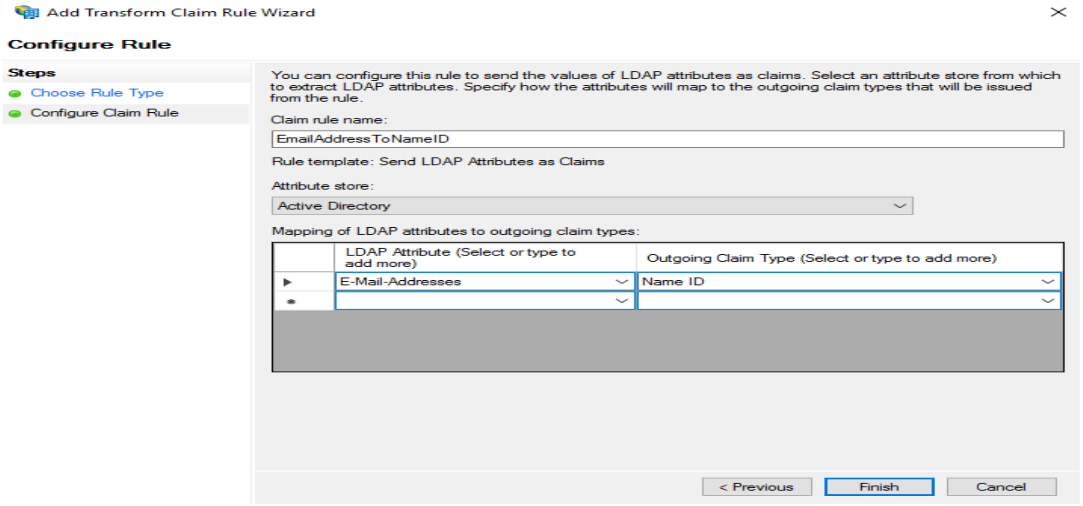
Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

10. On the Configure Claim Rule Dialog enter EmailAddressToNameID as the Claim Rule name. Select Active Directory as the Attribute Store. In the LDAP Attribute drop down, select E-Mail-Address In the Outgoing Claim Type drop down, select Name ID.
Then click Finish



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: EmailAddressToNameID

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
E-Mail-Addresses	Name ID

The ADFS administrator must now export the FederationMetaData xml file from the ADFS server and provide this to the Domino administrator, or if the Domino administrator knows the URL for the ADFS server they can complete this step by using FireFox to access the ADFS servers replacing ServerName with the fully qualified host name of your ADFS server.

https://ServerName/FederationMetadata/2007-06/FederationMetadata.xml

for example, https://samad.gftad.local/FederationMetadata/2007-06/FederationMetadata.xml

The reason Firefox should be used is that Internet Explorer will open the file rather than downloading the file. Copying the contents from the screen and saving it as a XML file results in an incorrect format for the file and will cause authentication to fail.

Importing The FederationMetaDate XML File Into Your IdP Configuration Document.

You may wish to create a copy of the federationmetadata.xml file before completing the steps below, as the import action deletes the file. Just make sure to delete the copy once you are sure that the import has been successful.

Bring the IdP Configuration document into edit mode if closed earlier.

On the Basics tab, click on the Import XML File button and navigate to the FederationMetaData.xml file exported earlier and then click OK.

This action populates the following fields with data from the FederationMetaData.xml file and the data should not be edited.

a) The Single sign-on service URL and Artefact resolution service url fields on the Basics tab. The latter field may not be populated, and if so should not affect SAML authentication.

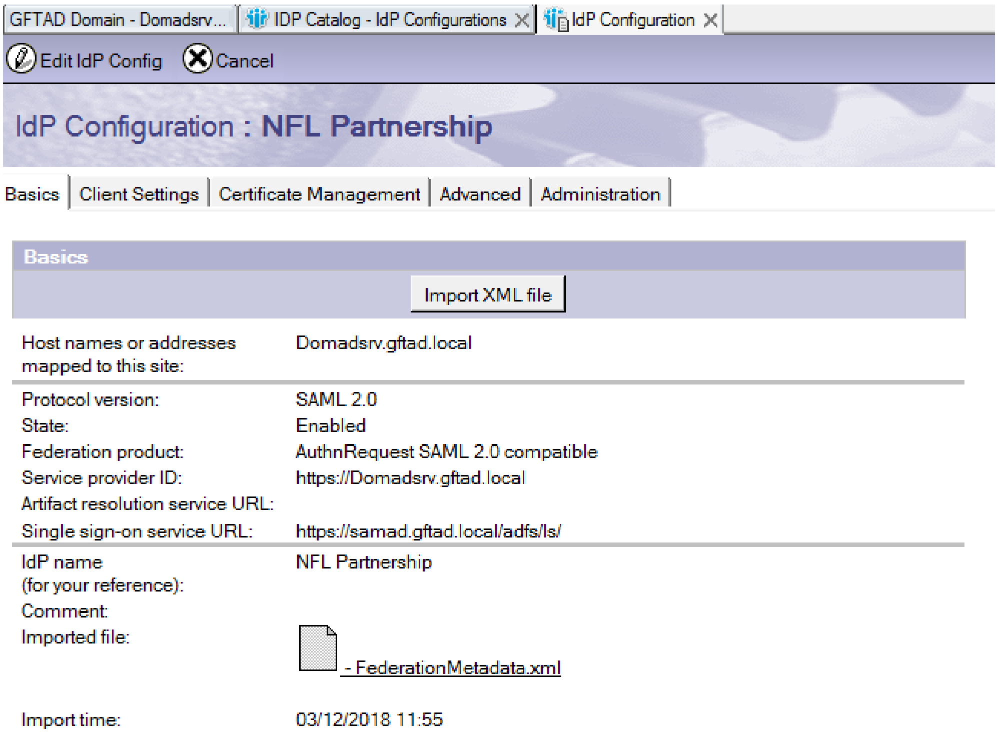
b) The Signing X.509 certificate and Encryption X.509 certificate fields of the Advanced tab.

Once the FederationMetaData.XML file has been imported click Save and Close.

If you have vault replica servers, you must replicate the IdP configuration database to these servers and complete the same process above to partner the vault replica server(s) with ADFS, or you can create the replica of the database and attempt to copy the certificate created and stored in the primary ID vault servers ID file to your vault replica servers ID file, using steps 1 and 3 in the following document

https://www-01.ibm.com/support/docview.wss?uid=swg22016213

This is required due to the fact that, when the certificate is created in the IdP configuration document, it is stored in the server's ID file. This certificate is used to decrypt the SAML assertion received from the ADFS server as part of the SAML authentication process. If the certificate is not present, the decryption of the assertion will fail and authentication will then fail.



IdP Configuration : NFL Partnership

Basics

Host names or addresses mapped to this site:	Domadsrv.gftad.local
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://Domadsrv.gftad.local
Artifact resolution service URL:	
Single sign-on service URL:	https://samad.gftad.local/adfs/ls/
IdP name (for your reference):	NFL Partnership
Comment:	
Imported file:	- FederationMetadata.xml
Import time:	03/12/2018 11:55

Creating a IdP Configuration Document in Domino 9.0 - 9.0.1.

While you can still export the settings from the IdP configuration document in Domino 9.0 – 9.0.1, some customers have reported issues with the settings not being correctly exported within this file when imported into ADFS 2.0 and 3.0 in that the name of the server was not correctly set in the export.xml file.

Given this, it is often recommended to customers that they create the relying party trust for their Domino Server/Internet site by manually creating the Relying Party Trust document in ADFS, as outlined in the next section.

Manually Create A Relying Party Trust In ADFS For Your ID Vault Server.

1. Open the ADFS manager.

2. Click on Add Relying Party Trust.

3. On the Welcome window click Start.

4. On the Select Data Source window, select the Enter data about the relying party manually option and click Next.

5. On the Specify Display Name pane, enter a descriptive name for your Domino server partnership and click Next.

6. On the Choose Profile pane, the option ADFS profile option should be automatically selected, if not select this option and click next.

7. On the Configure Certificate pane, just click Next

8. On the Configure URL pane, select the Enable support for the SAML 2.0 Web SSO protocol option, and then enter the secure URL for your ID Vault server's fully qualified host name with the references to the Domino Directory and the SAMLIDLogin command, for example: https://domadsrv.gftad.local/names.nsf?SAMLIDLogin and then click Next.

   It should be noted that the value here must be the value entered into the Host names or addresses mapped to this site field in the ID vault server IdP configuration document that you create later. You may prefer to use the following format for the ID Vault server, vault.hostname.domain/names.nsf?SAMLIDLogin, as is mentioned in some documentation regarding setting up Notes Federated Login, rather than the format mentioned above.

9. On the Configure Identifiers pane, in the Relying party trust identifier field, enter the secure URL for your ID Vault server, for example https://domadsrv.gftad.local, and then click Add and then click Next. It should be noted that this is an identifier, and not an actual HTTP connection but it is a requirement within ADFS for a HTTPS URL format.

10. On the Choose Issuance Authorisation Rules pane, the option Permit all users to access the relying party, should be selected by default, if not select this option and click Next.

11. On the Ready to Add Trust pane, you can select any of the tabs and change the details if required. But this should not be needed so click Next

12. On the Finish pane, the option Open the Edit Claim Rules dialog for this relying party trust when the wizard closes, is selected by default, as this is a required step leave the option selected and click Next.

13. The Edit Claims Rules dialog will now open, click Add Rule.

14. On the Add Transform Claim Rule Wizard Dialog's Choose Rule Type pane leave the default option Send LDAP Attributes as Claims selected and click Next.

15. On the Configure Claim Rule pane, in the Claim rule name field enter the value EmailAddressToNameID or similar as the name.

16. For the Attribute store select Active Directory from the drop-down list.

17. In the Mapping of LDAP attributes for outgoing claim types, select E-Mail-Addresses as the LDAP Attributes and select Name ID as the Outgoing Claim Type and then click Finish.

18. You will now be brought back to the Edit Claims Rule dialog. Click Apply and then OK.

The ADFS side of the partnership is now configured and the ADFS manager can be closed. Your ADFS administrator will now have to export these details from ADFS into a XML file which needs to be imported into the IdP configuration document in Domino, or the Domino administrator can complete this step if they know the URL of the ADFS server.

Using Firefox to access the ADFS server using the following URL replacing ServerName with the fully qualified host name of your ADFS server.

https://ServerName/FederationMetadata/2007-06/FederationMetadata.xml

for example, https://samad.gftad.local/FederationMetadata/2007-06/FederationMetadata.xml

The reason Firefox should be used is that Internet Explorer will open the file rather than downloading the file. Copying the contents from the screen and saving it as a XML file results in an incorrect format for the file and will cause authentication to fail.

Completing The IdP Configuration Document in Domino 9.0 - 9.0.1.

On your server open the IdP Configuration database and click Add IdP Config and on the Basics Tab

1. In the Host names or addresses mapped to this site field enter the fully qualified host name of your ID Vault server in the same format as it was entered in the Configure URL pane of the corresponding relying party trust in ADFS.

2. In the IdP name field enter any text that you wish to describe the partnership.

3. Change the Protocol Version field to SAML 2.0.

4. Leave the Federation Product field set as ADFS.

5. In the Service provider ID field enter the HTTPS URL for your ID Vault server.

6. You must now import the Federation Metadata file from your ADFS server by clicking Import XML file and browsing to where you have saved the XML file and click open. This will populate the rest of the fields in the Basics tab.

7. Click on the Certificate Management tab.

8. In the Company name field enter a name to identify the Internet certificate that will be imported by the ADFS identity provider. The name must be unique for each configuration.

9. Save and close the document, then reopen the document in edit mode and select the Certificate Management tab again.

10. Click the Create Certificate button, this adds the Internet certificate to the server ID file.

11. In the Domino URL field enter the secure URL to your ID Vault server as was entered in the Configure Identifiers pane, in the Relying party trust identifier field of the associated ADFS relying party trust configuration.

12. In the Single Logout URL field enter the link expected by Identify Provider. Note this value is expected by TIFM, but is not actually supported by Domino.

13. Click Export XML to save an IdP XML file as an attachment in the document, then click Save and Close.

Creating The Security Settings Policy Document For Notes Federated Login.

The ability to use Notes Federated Login for authentication is applied to your users through a security settings policy document.

When creating a policy for Notes Federated Login it is recommended to use an explicit policy as the Domino administrator user should not be enabled for Notes Federated Login as it is only supported for the standard Notes client and not the Administration client.

An item to note is that Notes Federated Login is very sensitive to the ID vault trust chain. Each organisation and organisational unit must trust the ID Vault and their corresponding certificates must exist in the Domino Directory and ID Vault configuration documents. Having missing trust certificates will cause numerous issues for Notes Federated Login in relation to setup and usage of the Notes client, and other actions such as renaming a Notes Federated Login enabled user.

Given this it is important that before you create your security settings policy document for Notes Federated Login, your ID Vault configuration has trusted the organisation and all organisational units and the certificates exist in the Domino directory.

It should also be noted that Notes Federated Login should not be enabled during a key rollover or when the user is in the middle of a rename.

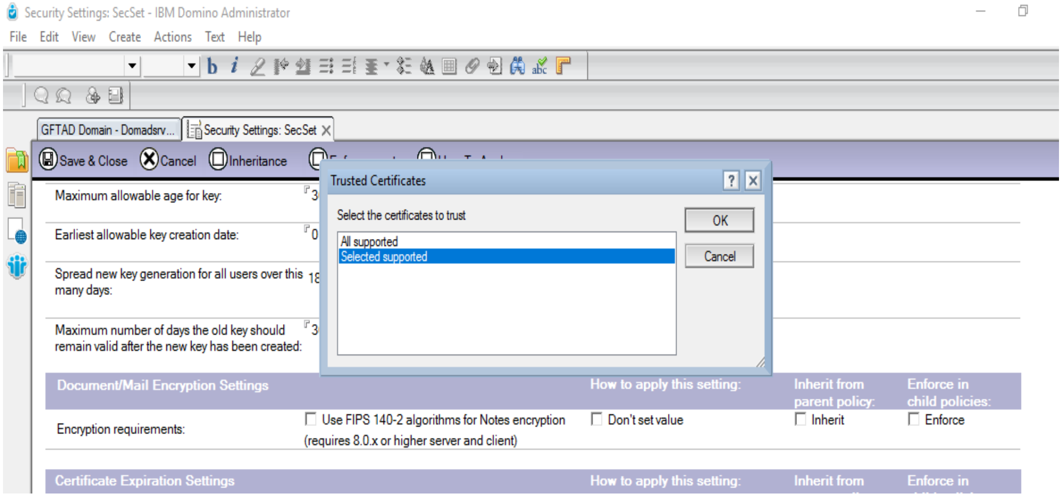
In the security settings document select the Password Management → Federated Login tab.

Set the field, Enable Notes Federated Login with SAML IdP to Yes.

Set the field, Allow password authentication with ID Vault to Yes

Select the Keys & Certificates Tab

Under the Administrative Trust Defaults section click Update Links and then Select supported to open the Select the certificates to trust dialog:


Security Settings: SecSet - IBM Domino Administrator
File
Edit
View
Create
Actions
Text
Help
GFTAD Domain - Domadsrv...
Security Settings: SecSet
Save & Close
Cancel
Inheritance
Trusted Certificates
OK
Cancel

Select the certificates to trust

All supported

Selected supported

Maximum allowable age for key: 3

Earliest allowable key creation date: 0

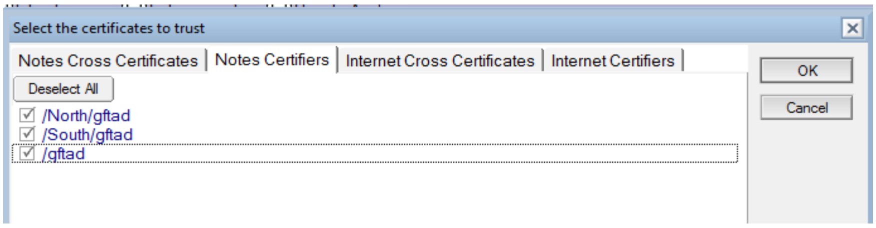
Spread new key generation for all users over this many days: 18

Maximum number of days the old key should remain valid after the new key has been created: 3

Document/Mail Encryption Settings		How to apply this setting:	Inherit from parent policy:	Enforce in child policies:
Encryption requirements:	☐ Use FIPS 140-2 algorithms for Notes encryption (requires 8.0.x or higher server and client)	☐ Don't set value	☐ Inherit	☐ Enforce

Certificate Expiration Settings	How to apply this setting:	Inherit from	Enforce in

1. Click on Click on the Notes Certifiers tab and click Select All.



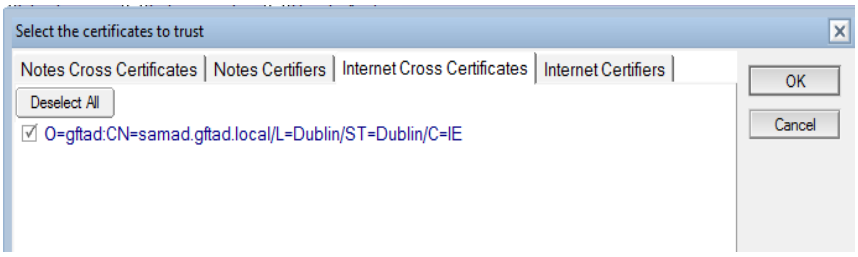
Select the certificates to trust

Notes Cross Certificates | Notes Certifiers | Internet Cross Certificates | Internet Certifiers

Deselect All

☑ /North/gftad
☑ /South/gftad
☑ /gftad

2. Click on the Internet Cross Certificates tab and select the cross certificate for the ADFS server.



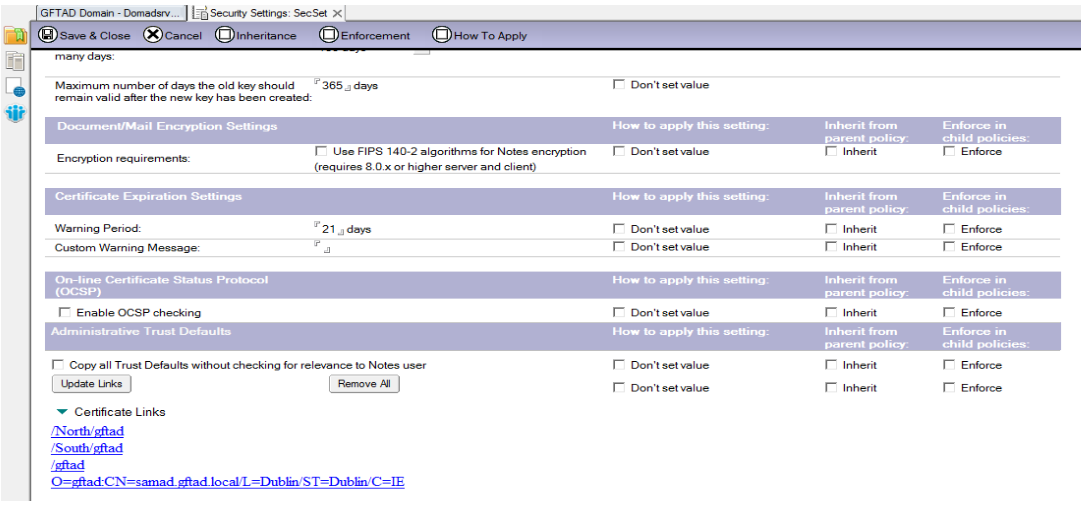
Select the certificates to trust

Notes Cross Certificates | Notes Certifiers | Internet Cross Certificates | Internet Certifiers

Deselect All

☑ O=gftad:CN=samad.gftad.local/L=Dublin/ST=Dublin/C=IE

3. Click OK when done and you will be returned to the security settings document and the selected certificates will be listed.



GFTAD Domain - Domadsrv... | Security Settings: SecSet

many days:

Maximum number of days the old key should remain valid after the new key has been created:	365 days	□ Don't set value		
Document/Mail Encryption Settings		**How to apply this setting:**	**Inherit from parent policy:**	**Enforce in child policies:**
Encryption requirements:	□ Use FIPS 140-2 algorithms for Notes encryption (requires 8.0.x or higher server and client)	□ Don't set value	□ Inherit	□ Enforce
Certificate Expiration Settings		**How to apply this setting:**	**Inherit from parent policy:**	**Enforce in child policies:**
Warning Period:	21 days	□ Don't set value	□ Inherit	□ Enforce
Custom Warning Message:		□ Don't set value	□ Inherit	□ Enforce
On-line Certificate Status Protocol (OCSP)		**How to apply this setting:**	**Inherit from parent policy:**	**Enforce in child policies:**
□ Enable OCSP checking		□ Don't set value	□ Inherit	□ Enforce
Administrative Trust Defaults		**How to apply this setting:**	**Inherit from parent policy:**	**Enforce in child policies:**
□ Copy all Trust Defaults without checking for relevance to Notes user		□ Don't set value	□ Inherit	□ Enforce
Update Links	Remove All	□ Don't set value	□ Inherit	□ Enforce

▼ Certificate Links

/North/gftad
/South/gftad
/gftad
O=gftad:CN=samad.gftad.local/L=Dublin/ST=Dublin/C=IE

Select the ID Vault tab.

In the Assigned Vault field add the ID Vault database name in the format /vault database name

Set the Allow automatic ID downloads field to Yes.

Click Save and Close[4].

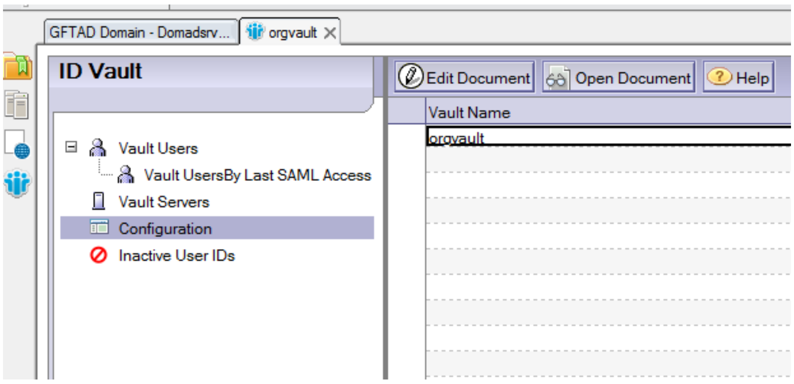
You can now create an explicit policy which uses this security settings document and assign this to your test users.

[4] You can also enable Notes Shared Login in this policy if you so wish for Windows users only, I would suggest having a separate policy and security settings document with NFL and NSL enabled for testing purposes.

Configure The ID Vault Database.

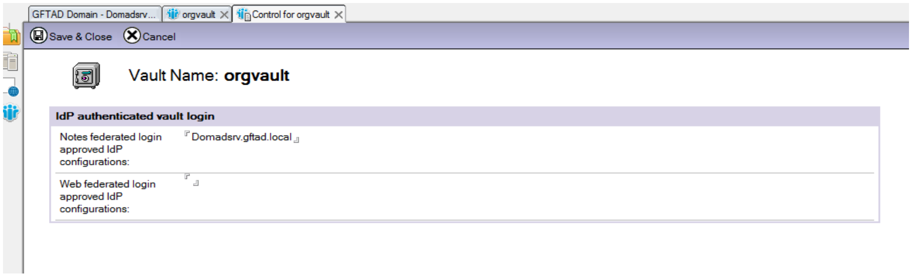
As part of the process for enabling Notes Federated Login, you must edit the ID Vault configuration document within the ID Vault database to add the fully qualified host name of your ID Vault server(s) used to create the partnerships with ADFS to the configuration. To complete this task in the Administration client:

1. Select the Files tab → IBM_ID_VAULT view.
2. Double click on your ID Vault database.
3. Select the Configuration view.



Vault Name
orgvault

4. Click Edit Document.
5. In the Notes federated login approved IdP configurations field enter the fully qualified host name of your ID Vault server. If you have replicas of the ID Vault database, you must create IdP configuration documents for these servers as mentioned above and list their host names in this field also. Each host name should be separated using a semi-colon.



Vault Name: **orgvault**

IdP authenticated vault login

Notes federated login approved IdP configurations: Domadsrv.gftad.local

Web federated login approved IdP configurations:

6. Click Save & Close and then close the database.

Completing The Configuration For Notes Federated Login.

Once you have completed the required configuration steps listed above and your ID Vault servers are not running the HTTP task, the configuration is now complete, and Domino must be restarted to take effect.

If running the HTTP task, you will need to complete the additional steps listed earlier in the SAML Single Sign On section of the document.

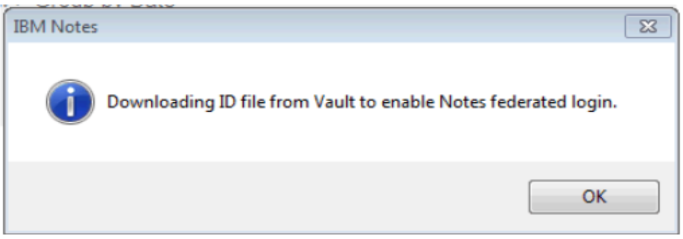
Testing Notes Federated Login.

This test is based on the premise that your user was already assigned the Notes Federated Login test policy when they were registered or was assigned the policy after registration, and the machines that they are logging into a part of the Active Directory domain.

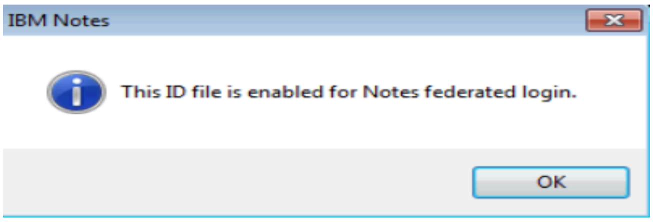
1. Log onto the Windows client.

2. Launch the Notes client set up for the user. As mentioned previously you must use a standard Notes client 9.0 or higher.

3. When the client is configured and the user connects to their server to open their mail file they will be informed that their ID is being downloaded and enabled for Notes Federated Login and once enabled informed that this operation has completed.



Downloading ID file from Vault to enable Notes federated login.



This ID file is enabled for Notes federated login.

4. Once the Notes client has been configured for Notes Federated Login, when the user restarts Notes they should be logged in without being asked to provide a user name or password.

5. When the user selects File → Security → User Security in their Notes client they should see the following message “Your ID is not stored on disk. It was downloaded from ID vault and is in memory”.

If an error occurs review your configuration settings using the pointers below. If your configuration settings are correct enable the debug parameters listed in the next section and if required open a case with support.

1. Verify all the required certificates have been added to the policy and these have been pushed to the user’s local address book.
1. You ID file was synching with the vault before enabling Notes Federated Login.
2. ID Vault database configuration has the correct fully qualified host name.
3. ADFS has been correctly set up for Windows Authentication

Debug Parameters

On your ID Vault Servers enable

```
Debug_SAML=31

Debug_IDV_Connect=1

Debug_IDV_Trace=1

Debug_IDV_TrustCert=1
```

In the notes.ini file of your Notes client set

```
DEBUG_OUTFILE=debugout.txt
DEBUG_CONSOLE=1
CLIENT_CLOCK=32
DEBUGGINGWCTENABLED=4294967295
CONSOLE_LOG_ENABLED=1
DEBUG_DYNCONFIG=1
DEBUG_TRUST_MGMT=1
DEBUG_IDV_TRACE=1
DEBUG_BSAFE_IDFILE_LOCKED=8
```

In the \Notes\Data\workspace\.config\rcpinstall.properties of your Notes client set

```
com.ibm.notes.internal.federated.manager.level=FINEST

com.ibm.notes.java.api.internal.level=FINEST

com.ibm.notes.java.init.level=FINEST

com.ibm.notes.java.init.win32.level=FINEST

com.ibm.rcp.accounts.internal.auth.module.level=FINEST

com.ibm.rcp.core.internal.launcher.level=FINEST

com.ibm.rcp.internal.security.auth.dialog.level=FINEST

com.ibm.rcp.internal.security.auth.samlsso.level=FINEST

com.ibm.rcp.platform.personality.level=FINEST

com.ibm.rcp.roaming.service.internal.level=FINEST

com.ibm.workplace.internal.notes.security.auth.level=FINEST

com.ibm.workplace.internal.notes.security.level=FINEST

com.ibm.workplace.noteswc.level=FINEST
```

Web Federated Login.

Web Federated Login (WFL) allows SAML authentication to be utilised for iNotes users accessing their mail file through their browser.

The configuration for Web Federated Login requires two IdP configuration documents, one for the iNotes web server and one for the ID Vault server, meaning two relying party trusts must also exist in ADFS. The first partnership is required to authenticate the user to gain access to their iNotes server, and the second partnership is required to download the user's ID from the ID Vault to memory on the iNotes server.

Where you create the IdP configuration document for the ID Vault is important. While a replica of the IdP configuration database must exist on the iNotes server and the first configuration document must be created in the database on this server, the iNotes server may not be a vault replica server.

If this is the case, then the second IdP configuration document must be created on the ID Vault server. If the iNotes server is a vault replica server, then both IdP configuration documents should be created in the IdP configuration database on the iNotes server itself. This is due to the authentication flow for Web Federated Login.

Web Federated Login Authentication Flow.

Access to the iNotes web server is done through HTTPS and when accessing their iNotes server the user's browser is redirected to the configured identity provider. The identity provider authenticates the user and sends a SAML assertion is sent to the user's browser which is redirected to their iNotes server to authenticate the user, hence the IdP configuration document must be created on a replica of the IdP configuration database on this server as the certificate to encrypt/decrypt the SAML assertions is stored in the server's ID file.

When the user's ID needs to download from the ID Vault, a NRPC request is sent to the ID Vault server which returns the URL for the identity provider. The identity provider again authenticates the user and sends a SAML assertion to the ID Vault server which is used to extract the ID from the ID Vault and store it in memory on the iNotes server. As the certificates to encrypt/decrypt the assertions are stored within the server's ID file therefore the second IdP configuration document must be created in the IdP configuration database on the ID Vault server.

Configuration Considerations: SSO With The LTPA Token.

In relation to SSO configurations being used with Web Federated Login, you must have an IdP configuration document and relying party trust for each iNotes web server and a corresponding IdP configuration document for accessing the ID Vault for each server.

Web Federated Login is currently not supported with the use of a load balancer or IP sprayer to access clustered Domino servers this is reported in the following documents

https://www-01.ibm.com/support/docview.wss?uid=swg21975613

https://www-01.ibm.com/support/docview.wss?uid=swg21628861

The reason for this is that the assertions must be sticky. Some customers have found that not using a SSO configuration, but rather using SAML single server expiration as the preferred method of session management to deal with failover scenarios, as this will ensure that the required SAML assertions are generated in this scenario, which will not occur if the user has an active LTPA token.

Another scenario where the use of LTPA tokens can be where customers have their users access a portal[5] site that is not enabled for SAML authentication, and then access their iNotes servers which are enabled for Web Federated Login but are included in the LTAP token configuration.

In this scenario, as the user's browser already has the LTPA token, the iNotes servers assume that they have been authenticated via SAML, and when the user attempts to read an encrypted mail they will be prompted to enter their Notes password.

The solution in this scenario is to have the Web Federated Login iNotes servers use SAML single server expiration and not LTPA, so that the required SAML assertions to authenticate the user and download their ID from the vault to the memory of the iNotes server are generated, or to have the Web Federated Login enabled servers to be included in their own LTPA configuration, separate from that used by the portal site.

Configuration Considerations: Name Mapping Is Not Supported

The use of name mapping of a user's Notes distinguished name, through directory assistance is not supported for Web Federated Login. You must math your user's email address between their Active Directory User Object and Domino person document as documented in

https://www-01.ibm.com/support/docview.wss?uid=ibm10880583

Configuration Considerations: iNotes DNS Aliases.

If your iNotes web server has an alias in DNS you must also create a IdP configuration document and relying party trust for the alias as per

http://www-01.ibm.com/support/docview.wss?uid=swg22009126

Configuring Your Domino iNotes Server.

The steps below are similar to enabling SAML Single Sign On and must be completed before creating the IdP Configuration database, or creating a replica of the IdP Configuration database on the server[6].

1. Make sure you can connect to your Domino server using a browser over HTTPS. This is a requirement for using ADFS as it expects all communication to be done through HTTPS, and you must have a SHA-2 certificate for your Domino server(s) and/or Internet sites.
   Please follow the steps in the following documents which list how to create either a third-party SHA-2 or a self-signed SHA-2 certificate for your Domino server(s)/Internet sites.

   https://www-10.lotus.com/ldd/dominowiki.nsf/dx/3rd_Party_SHA-2_with_OpenSSL_and_kyrtool?open

   https://www-10.lotus.com/ldd/dominowiki.nsf/dx/Self-signed_SHA-2_with_OpenSSL_and_kyrtool

[5] The use of the term Portal here refers to an extended homepage site that some customers generate to provide links to various applications and servers, and does not refer to WebSphere Portal

[6] If your iNotes server is not a vault replica server, you must configure your ID vault server by following the steps under the Notes Federated Login section of this document.

2. Password synchronisation between the Notes password and Internet password in the user's security policy must be disabled.

3. Disable the Internet Password Lockout feature if previously enabled.

4. The server ID file cannot have a password if using the Create Button to create a certificate in the document within the IdP Catalog database to encrypt the SAML assertions.
Most customers in my experience do not have their server ID files password protected and this document follows this scenario. However, if your organisation does have your Domino server ID files password protected you will need to follow this document in order to create the SP.XML file.
https://www.ibm.com/support/knowledgecenter/SSKTMJ_10.0.0/admin/secu_creating_a_domino_metadata_file_if_the_server_id_file_is_password_protected_t.html

5. The Domino administrator who creates the IdP Catalog database must be listed in the following fields in the security tab of the server document or be a member of a group listed in these fields.

    a. Full Access Administrators.

    b. Administrators.

    c. Sign or run unrestricted methods or operations.

6. Clock synchronisation between the Domino Server and the ADFS server must be implemented, otherwise authentication will fail. The following parameters should be added to the noteas.ini file to help deal with time creep. Please note 10 is the maximum value for these parameters
SAML_NotBeforeSkewInMinutes=10

    SAML_NotOnOrAfterSkewInMinutes=10

Import The ADFS Servers SSL Certificate Into The Domino Directory.

As mentioned previously, ADFS requires all communication to be through HTTPS to facilitate this the root certificate of the ADFS server certificate must be imported into Domino as an Internet Certifier and an Internet Cross Certificate created from this entry.

Have your ADFS server administrator provide a base 64 encoded .crt file of the ADFS server's root CA certificate. If the ADFS server has a self-signed certificate, it must have the Certificates KeyUsage field values for Certificate Signer and CRL Signer in order to be able to import the certificate correctly into Domino as an Internet Certifier.

Using the Administration client select the Configuration Tab → Security → Certificates view.

Select the Actions menu → Import Internet Certificates option and select the .crt file provided.

On the Import Internet Certificates dialog click Accept All, you should receive a message stating the import was successful.

Create An Internet Cross Certificate For the ADFS Servers SSL Certificate

Select the Configuration Tab → Security → Certificates → Internet Certifiers view and open the document for the ADFS server's Internet Certifier document created earlier.

Select Actions → Create Cross Certificate and confirm that you wish to cross certify the certificate.

On the Issue Cross Certificate dialog, set the Server to your Domino Administration server and the Certifier to your Organisation certifier and click Cross Certify[7].

Creating And Configuring The IdP Catalog Database.

The following steps will allow you to create the IdP Catalog database. The IdP Catalog database stores the partnership details for your iNotes web server(s) and ID Vault server(s) and their identity provider.

As mentioned earlier, If your iNotes server is also a vault replica server, you can create the IdP Catalog database on this server, but if iNotes server is not a vault replica server, the database should be created on your primary ID Vault server and a replica of the database created on your iNotes web servers.

In relation to the IdP Catalog database the following must be observed.

1. The database is not created by default when Domino is installed or upgraded to Domino version 9.0 or higher.
   You must create the database on your primary ID Vault server using the idpcat.ntf template using the Administration client.

2. The database must be named idpcat.nsf. If your ID Vault server is installed on a *nix operating system the filename number in lowercase.

3. The idpcat.nsf must not be enabled for document locking.

4. There should be only one idpcat.nsf database for your entire domain. The database should be created first on your primary ID Vault server and then replicated to each vault replica server and iNotes web server.

To create the IdP Catalog database the following steps must be completed using your Administration client on your primary ID Vault server or iNotes server.

Select File → Application → New and on the New Application dialog

[7] A common issue is the certificate for the ADFS server expiring and such a scenario is document in https://www-01.ibm.com/support/docview.wss?uid=swg21998370

1. In the Server field select the server where you are enabling SAML authentication.

2. In the Title field enter a descriptive title for the database.

3. In the File name field enter idpcat.nsf

4. Click the Advanced templates option and select the server and idP Catalog template.

5. Click OK and the database will be created and opened.

Once created you can now create replicas of the database on the required servers and create configuration documents.

Creating IdP Configuration Documents For iNotes in Domino 10 or higher.

As mentioned previously for Web Federated Login two IdP configuration documents are required, one for user authentication and one to download the user's ID file from the ID Vault.

Depending on whether your iNotes server is a vault replica server or not, will determine where the second IdP configuration document is created. The document follows the scenario where the iNotes server is not a vault replica server, so the IdP Configuration database was created on the ID Vault server and a replica of the database created on the iNotes server, meaning also that the second configuration document is created on the ID Vault server. The document is also following the scenario that your server's ID file is not password protected.

In the IdP Catalog database replica on your iNotes server complete the following steps

1. Click Add IdP Config to open a new IdP configuration document.

2. In the Host names or addresses mapped to this site field, the fully qualified host name of your iNotes server/Internet site should automatically be entered. If it is not click on the drop-down arrow and select the server/Internet site. You must also the add the IP address of your server/Internet site to the field, using a semi colon to separate the two entries.
   For example: domweb.gftad.local; 192.168.56.3

3. Leave the Protocol Version field set to SAML 2.0.

4. Leave the State field set to Enabled.

5. Leave the Federation Product field set to AuthnRequest SAML 2.0 Compatible.

6. Set the Service Provider ID field to HTTPS URL of your iNotes server/Internet site.

7. In the IdP name field enter any text that you wish to describe the partnership.

8. Click on Save and Close. Then select the document and click Edit IdP config.

9. Click on the Certificate Management tab.

10. Click on Create SP Certificate and in the Create Company Certificate dialog enter a name for the certificate for example Domweb, and must be unique for each configuration.

11. In the Domino URL field the HTTPS URL for your iNotes server or Internet site should be entered.

12. While Domino does not support Single Logout for SAML, the Single Logout URL field should have a correctly formatted HTTPS URL for your ADFS server entered. Note this value is expected by TIFM

13. Click on Export SP XML. This file will be provided to the ADFS administrator and used create the relying party trust in ADFS for your Domino Server/Internet site document.

On your ID Vault server open the IdP Catalog database

1. Click Add IdP Config to open a new IdP configuration document.

2. In the Host names or addresses mapped to this site field enter the fully qualified host name of your iNotes server/Internet site prefixed with vault e.g. vault.domweb.gftad.local

3. Leave the Protocol Version field set to SAML 2.0.

4. Leave the State field set to Enabled.

5. Leave the Federation Product field set to AuthnRequest SAML 2.0 Compatible.

6. Set the Service Provider ID field to HTTPS url of your iNotes server/Internet site prefixed with vault e.g. https://vault.domweb.gftad.local. This is required even though the HTTP task is not active on your ID Vault server.

7. In the IdP name field enter any text that you wish to describe the partnership.

8. Click on Save and Close. Then select the document and click Edit IdP config.

9. Click on the Certificate Management tab.

10. Click on Create SP Certificate and in the Create Company Certificate dialog enter a name for the certificate for example Domwebvault, and must be unique for each configuration.

12. In the Domino URL field the HTTPS url for your iNotes server/Internet site should be entered e.g. https://domweb.gftad.local

13. While Domino does not support Single Logout for SAML, the Single Logout Url field should have a correctly formatted HTTPS url for your ADFS server entered. Note this value is expected by TIFM

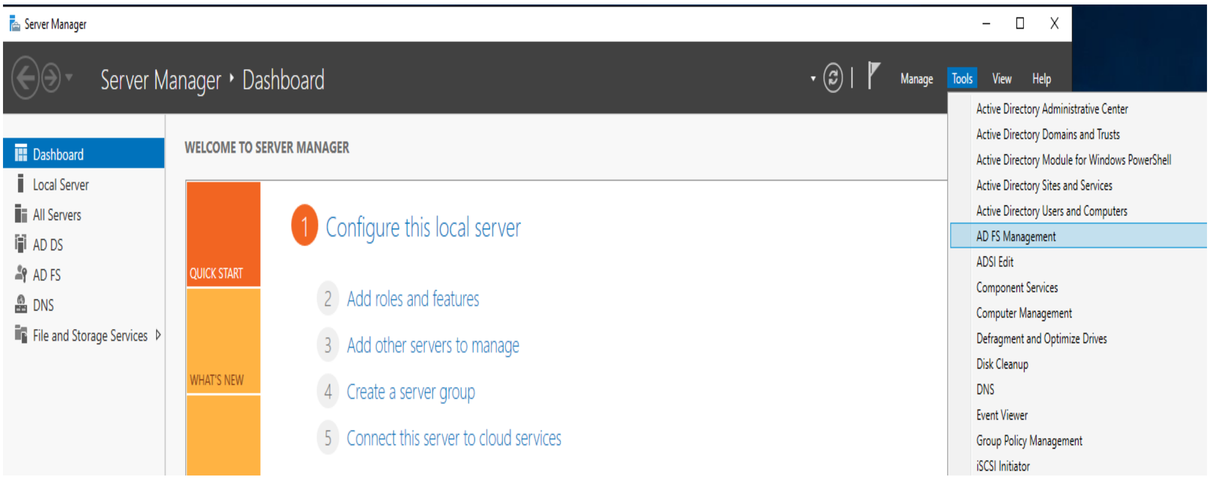
14. Click on Export SP XML. This file will be provided to the ADFS administrator and used to create the relying party trust in ADFS for your Domino Server/Internet site document.

Creating The Relying Party Trusts In ADFS For iNotes

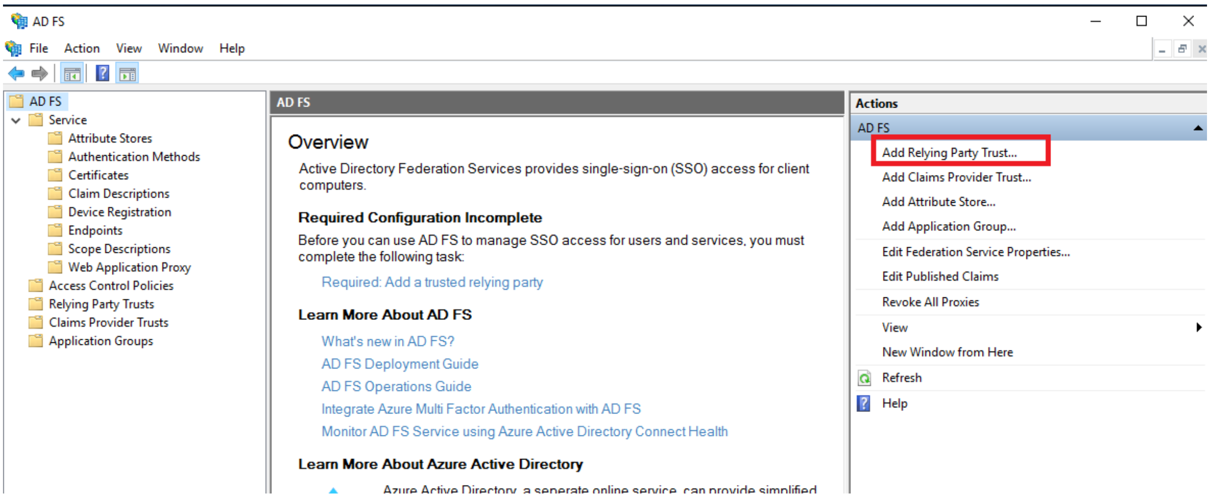
Once you have exported the two SP XML files you or you ADFS administrator, can create the two relying party trusts for your iNotes server/Internet Site by importing the SP XML files.

It is recommended to create the relying party trust for your actual iNotes server/Internet site first, then complete the same steps for the ID Vault configuration for iNotes.

1. On the Server Manager, select Tools → ADFS Management.


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

2. Select Add Relying Party Trust.



AD FS

Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

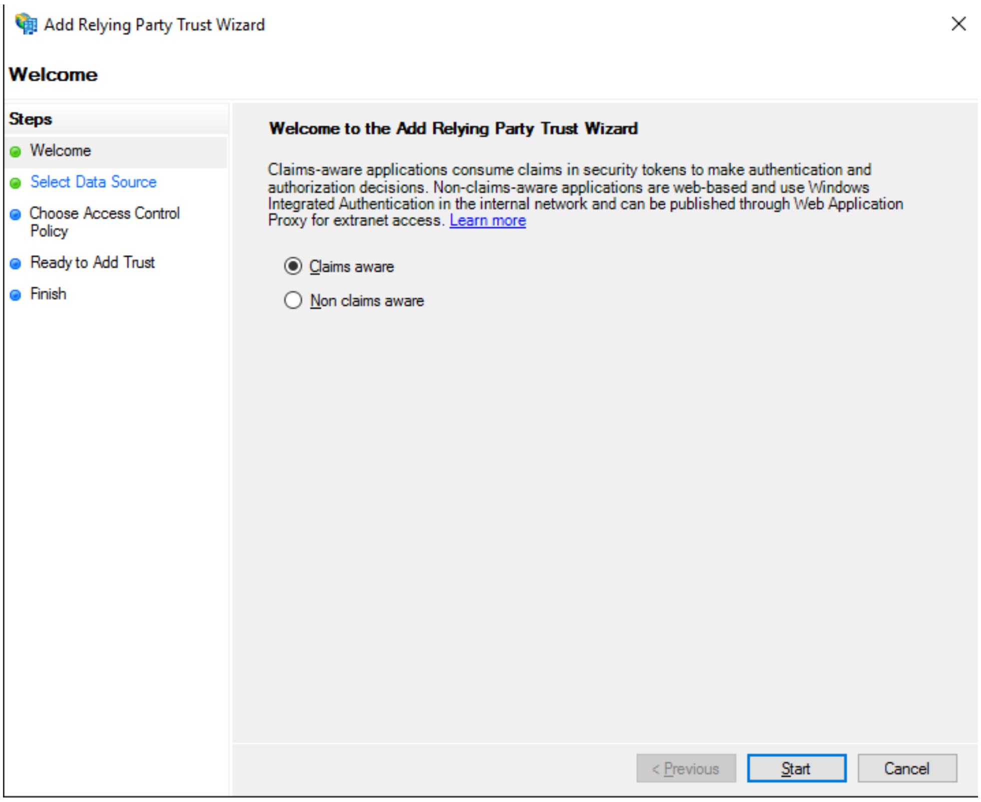
Learn More About AD FS

What's new in AD FS?
AD FS Deployment Guide
AD FS Operations Guide
Integrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health

Learn More About Azure Active Directory

Azure Active Directory, a senerate online service, can provide simplified

3. Leave Claims aware selected and click Start.



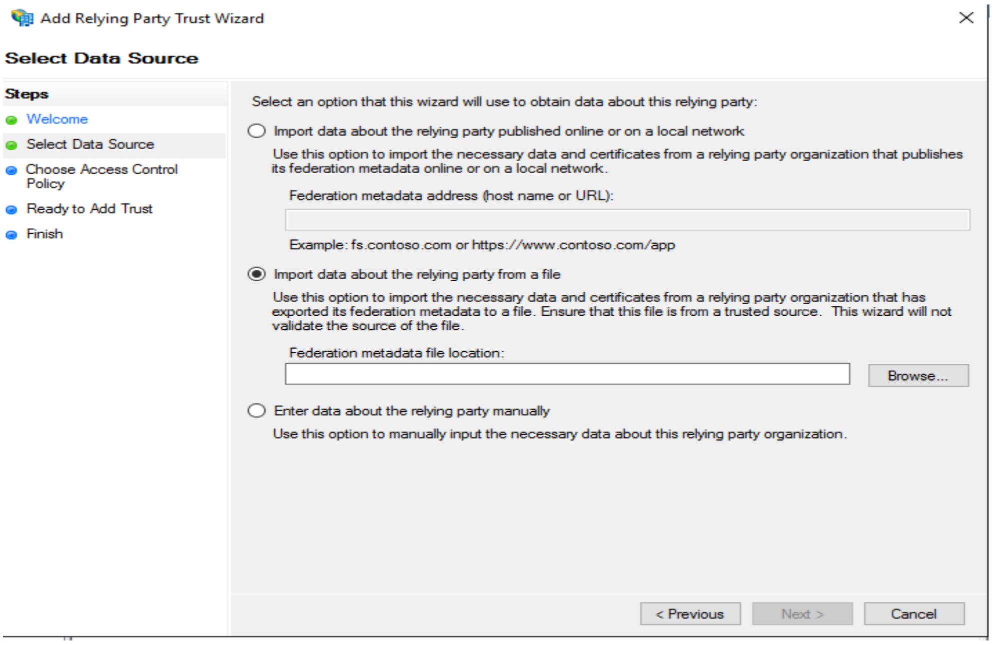
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

4. Select Import data about the relying party trust from a file and click Browse to select the SP XML file exported from your iNotes server/Internet site IdP configuration document and click Next.



Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

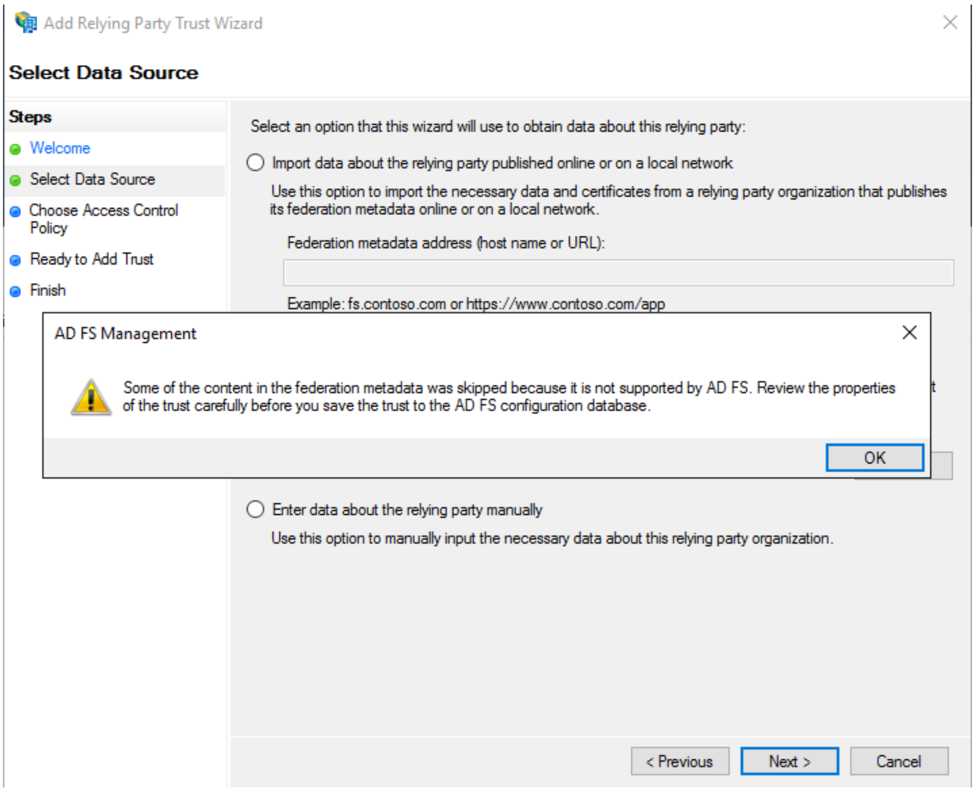
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

5. Click OK on the information message and then click Next. This action imports the Identity Provider, Certificate and Endpoint information for your ID Vault server into ADFS from the SP XML file automatically.



Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

AD FS Management

Some of the content in the federation metadata was skipped because it is not supported by AD FS. Review the properties of the trust carefully before you save the trust to the AD FS configuration database.

○ Enter data about the relying party manually

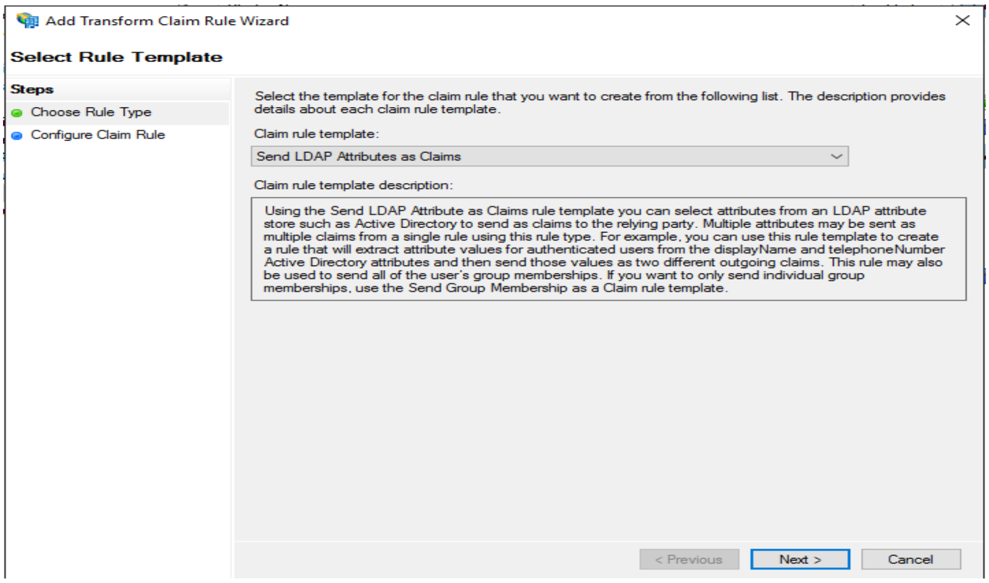
Use this option to manually input the necessary data about this relying party organization.

6. On the Choose Access Control Policy window, leave the default settings as is and click Next.

7. You can now review the settings for the partnership with your Domino Server/Internet site document, there should be no reason to change any of the settings and you can click Next to proceed.

8. Once the relying party trust has been entered successfully, click Close and you will be presented with the Claim Rule Wizard.

9. On the Choose Rule Type window click Next.



Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

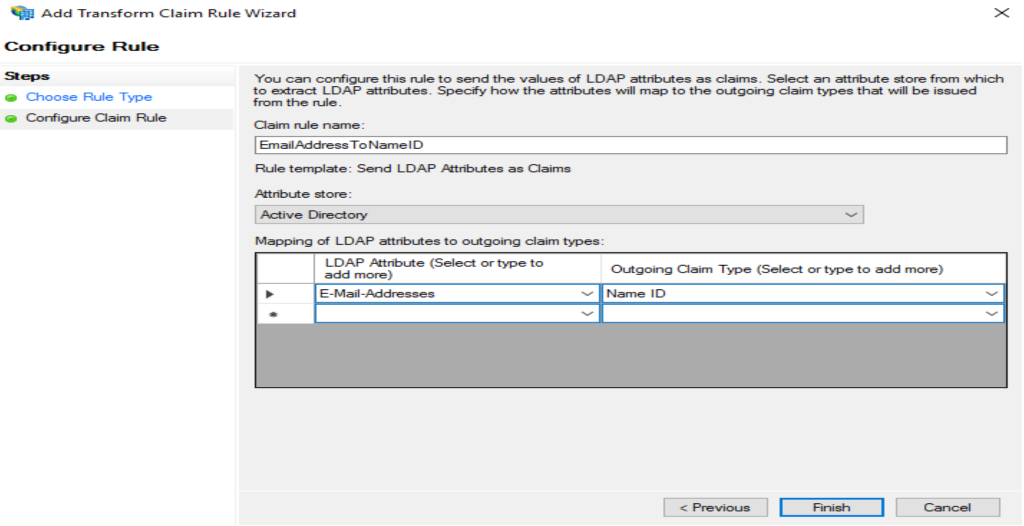
Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

10. On the Configure Claim Rule Dialog enter EmailAddressToNameID as the Claim Rule name. Select Active Directory as the Attribute Store. In the LDAP Attribute drop down, select E-Mail-Address In the Outgoing Claim Type drop down, select Name ID.
    Then click Finish



Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

EmailAddressToNameID

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	E-Mail-Addresses	Name ID
*		

The ADFS administrator can now repeat the above steps for the ID Vault configuration for your iNotes server/Internet site, by importing the SP XML document exported earlier from the corresponding IdP configuration document

The ADFS administrator must now export the FederationMetaData xml file for the iNotes Server and ID Vault configuration, from the ADFS server and provide this to the Domino administrator.

To complete this step, use Firefox to access the following URL replacing ServerName with the fully qualified host name of your ADFS server.

https://ServerName/FederationMetadata/2007-06/FederationMetadata.xml

for example, https://samad.gftad.local/FederationMetadata/2007-06/FederationMetadata.xml

The reason Firefox should be used is that Internet Explorer will open the file on screen rather than downloading the file. Copying the contents from the screen and saving it as a XML file results in an incorrect format for the file and will cause authentication to fail.

Importing The FederationMetaDate XML File Into Your IdP Configuration Documents.

You will need to create a copy of the federationmetadata.xml file before completing the steps below, as the import action deletes the file and you must add the file to your two IdP configuration documents. If creating multiple copies make sure to delete the unused copies later.

On your iNotes server bring the IdP Configuration document into edit mode if closed earlier.

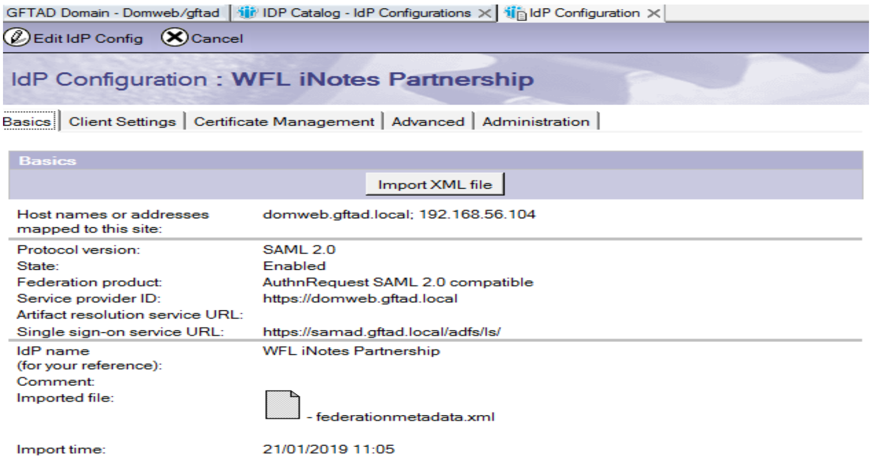
On the Basics tab, click on the Import XML File button and navigate to the FederationMetaData.xml file exported earlier and then click OK.

This action populates the following fields with data from the FederationMetaData.xml file and the data should not be edited.

a) The Single sign-on service URL and Artefact resolution service url fields on the Basics tab. The latter field may not be populated, and if so should not affect SAML authentication.

b) The Signing X.509 certificate and Encryption X.509 certificate fields of the Advanced tab.

Once the FederationMetaData.XML file has been imported click Save and Close.

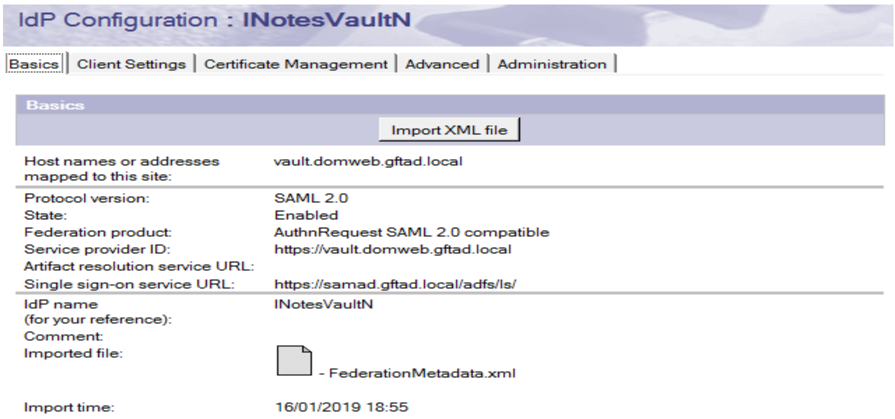


IdP Configuration : WFL iNotes Partnership

Basics

Host names or addresses mapped to this site:	domweb.gftad.local; 192.168.56.104
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://domweb.gftad.local
Artifact resolution service URL:	
Single sign-on service URL:	https://samad.gftad.local/adfs/ls/
IdP name (for your reference):	WFL iNotes Partnership
Comment:	
Imported file:	- federationmetadata.xml
Import time:	21/01/2019 11:05

On your ID Vault server repeat the above steps to import the FederatedMetaData.XML file for the second IdP configuration document for the ID Vault configuration.



IdP Configuration : INotesVaultN

Basics

Host names or addresses mapped to this site:	vault.domweb.gftad.local
Protocol version:	SAML 2.0
State:	Enabled
Federation product:	AuthnRequest SAML 2.0 compatible
Service provider ID:	https://vault.domweb.gftad.local
Artifact resolution service URL:	
Single sign-on service URL:	https://samad.gftad.local/adfs/ls/
IdP name (for your reference):	INotesVaultN
Comment:	
Imported file:	- FederationMetadata.xml
Import time:	16/01/2019 18:55

Creating a IdP Configuration Documents For iNotes in Domino 9.0 - 9.0.1.

As mentioned earlier there are difference in the IdP configuration documents between Domino 9.0-9.0.1 and Domino 10. The difference will be listed in this section as there is more than a difference than the layout of the documents.

While you can still export the settings from the IdP configuration document in 9.0 – 9.0.1, some customers had reported issues with this file when imported into ADFS 2.0 and 3.0.

Given this, customers under advice from support, normally create the relying party trusts by manually adding the settings relating to their iNotes server/Internet site document and ID Vault configuration to ADFS. The FederationMetaData.XML file is then exported from ADFS and then used to create the two new IdP configuration document. The steps in this section will follow this scenario.

Create A Relying Party Trust Manually In ADFS For Your iNotes Server/Internet Site.

1. Open the ADFS manager.
2. Click on Add Relying Party Trust.
3. On the Welcome window click Start.
4. On the Select Data Source window, select the Enter data about the relying party manually option and click Next.
5. On the Specify Display Name pane, enter a descriptive name for your iNotes server and click Next.
6. On the Choose Profile pane, the option ADFS profile option should be automatically selected, if not select this option and click next.
7. On the Configure Certificate pane, just click Next
8. On the Configure URL pane, select the Enable support for the SAML 2.0 Web SSO protocol option, and then enter the secure URL for your Domino server's fully qualified host name or Internet Site with the references to the Domino Directory and the SAMLLogin command, for example: https://domweb.gftad.local/names.nsf?SAMLLogin and then click Next.
9. On the Configure Identifiers pane, in the Relying party trust identifier field, enter the secure URL for your Domino server's fully qualified host name, or your Internet site, for example https://domweb.gftad.local, and then click Add and then click Next.

10. On the Choose Issuance Authorisation Rules pane, the option Permit all users to access the relying party, should be selected by default, if not select this option and click Next.

11. On the Ready to Add Trust pane, you can select any of the tabs and change the details if required. But this should not be needed so click Next

12. On the Finish pane, the option Open the Edit Claim Rules dialog for this relying party trust when the wizard closes is selected by default, as this is a required step leave the option selected and click Next.

13. The Edit Claims Rules dialog will now open, click Add Rule.

14. On the Add Transform Claim Rule Wizard Dialog's Choose Rule Type pane leave the default option Send LDAP Attributes as Claims selected and click Next.

15. On the Configure Claim Rule pane, in the Claim rule name field enter the value EmailAddressToNameID or similar as the name.

16. For the Attribute store select Active Directory from the drop-down list.

17. In the Mapping of LDAP attributes for outgoing claim types, select E-Mail-Addresses as the LDAP Attributes and select Name ID as the Outgoing Claim Type and then click Finish.

18. You will now be brought back to the Edit Claims Rule dialog. Click Apply and then OK.

Create A Relying Party Trust Manually In ADFS For Your iNotes Server ID Vault Configuration.

1. Open the ADFS manager.

2. Click on Add Relying Party Trust.

3. On the Welcome window click Start.

4. On the Select Data Source window, select the Enter data about the relying party manually option and click Next.

5. On the Specify Display Name pane, enter a descriptive name for your iNotes vault configuration and click Next.
6. On the Choose Profile pane, the option ADFS profile option should be automatically selected, if not select this option and click next.

7. On the Configure Certificate pane, just click Next

8. On the Configure URL pane, select the Enable support for the SAML 2.0 Web SSO protocol option, and then enter the secure URL for your Domino server's fully qualified host name or Internet Site with the references to the Domino Directory and the SAMLIDLogin command, for example: https://domweb.gftad.local/names.nsf?SAMLIDLogin and then click Next.

9. On the Configure Identifiers pane, in the Relying party trust identifier field, enter the secure URL for your Domino server's fully qualified host name, or your Internet site, prefixed by vault for example https://vault.domweb.gftad.local, and then click Add and then click Next.

10. On the Choose Issuance Authorisation Rules pane, the option Permit all users to access the relying party, should be selected by default, if not select this option and click Next.

11. On the Ready to Add Trust pane, you can select any of the tabs and change the details if required. But this should not be needed so click Next

12. On the Finish pane, the option Open the Edit Claim Rules dialog for this relying party trust when the wizard closes is selected by default, as this is a required step leave the option selected and click Next.

13. The Edit Claims Rules dialog will now open, click Add Rule.

14. On the Add Transform Claim Rule Wizard Dialog's Choose Rule Type pane leave the default option Send LDAP Attributes as Claims selected and click Next.

15. On the Configure Claim Rule pane, in the Claim rule name field enter the value VaultEmailAddressToNameID or similar as the name.

16. For the Attribute store select Active Directory from the drop-down list.

17. In the Mapping of LDAP attributes for outgoing claim types, select E-Mail-Addresses as the LDAP Attributes and select Name ID as the Outgoing Claim Type and then click Finish.

18. You will now be brought back to the Edit Claims Rule dialog. Click Apply and then OK.

The ADFS side of the partnership is now configured and the ADFS manager can be closed.

Your ADFS administrator will now have to export these details from ADFS into a XML file, and provide them to the Domino administrator.

To complete this step, use Firefox to access the following URL replacing ServerName with the fully qualified host name of your ADFS server.

https://ServerName/FederationMetadata/2007-06/FederationMetadata.xml

for example, https://samad.gftad.local/FederationMetadata/2007-06/FederationMetadata.xml

The reason Firefox should be used is that Internet Explorer will open the file on screen rather than downloading the file. Copying the contents from the screen and saving it as a XML file results in an incorrect format for the file and will cause authentication to fail.

Make sure to make two copies of the XML file as you will need to import it twice, once for your iNotes Idp configuration document and once for your ID Vault configuration document. If making multiple copies delete the unused copies when not required.

Creating The IdP Configuration Documents.

On your iNotes server open the IdP Configuration database and click Add IdP Config and on the Basics Tab

1. In the Host names or addresses mapped to this site field enter the fully qualified host name and IP address of your iNotes server/Internet site. You should separate the name and IP address using a semi colon. For example domweb.gftad.local;192.168.56.104

2. In the IdP name field enter any text that you wish to describe the partnership.

3. Change the Protocol Version field to SAML 2.0.

4. Leave the Federation Product field set as ADFS.

5. In the Service provider ID field enter the HTTPS URL for your iNotes Server/Internet site.

6. You must now import the Federation Metadata file by clicking Import XML file and selecting one of the XML files and click open. This will populate the rest of the fields in the Basics tab.

7. Click on the Certificate Management tab.

8. In the Company name field enter a name to identify the Internet certificate that will be imported by the ADFS identity provider. The name must be unique for each configuration.

9. Save and close the document, then reopen the document in edit mode and select the Certificate Management tab again.

10. Click the Create Certificate button, this adds the Internet certificate to the server ID file.

11. In the Domino URL field enter the secure URL to your iNotes server/Internet site.

12. In the Single Logout URL field enter the link expected by Identify Provider. Note this value is expected by TIFM, but is not actually supported by Domino.

13. Click Export XML to save an IdP XML file as an attachment in the document.

14. Click Save and Close.

On your ID Vault server open the IdP Configuration database and click Add IdP Config and on the Basics Tab

1. In the Host names or addresses mapped to this site field enter the fully qualified host name your iNotes server/Internet site prefixed by vault. For example vault.domweb.gftad.local

2. In the IdP name field enter any text that you wish to describe the partnership.

3. Change the Protocol Version field to SAML 2.0.

4. Leave the Federation Product field set as ADFS.

5. In the Service provider ID field enter the HTTPS URL for your iNotes Server/Internet site prefixed by vault for example https://vault.domweb.gftad.local. This should be the same URL that was entered as the relying party trust identifier earlier in ADFS.

6. You must now import the Federation Metadata file by clicking Import XML file and selecting the second XML file and click open. This will populate the rest of the fields in the Basics tab.

7. Click on the Certificate Management tab.

8. In the Company name field enter a name to identify the Internet certificate that will be imported by the ADFS identity provider. The name must be unique for each configuration.

9. Save and close the document, then reopen the document in edit mode and select the Certificate Management tab again.

10. Click the Create Certificate button, this adds the Internet certificate to the server ID file.

11. In the Domino URL field enter the secure URL to your iNotes server/Internet site.

12. In the Single Logout URL field enter the link expected by Identify Provider. Note this value is expected by TIFM, but is not actually supported by Domino.

13. Click Export XML to save an IdP XML file as an attachment in the document.

14. Click Save and Close.

Create The Security Settings Policy Document For Web Federated Login.

When creating a policy for Web Federated Login it is recommended to use an explicit policy as the Domino administrator user should not be enabled for Web Federated Login. Note if you already have Notes Federated Login enabled, you can edit the existing security settings policy to enable Web Federated Login also.

An item to note is that Web Federated Login, like Notes Federated Login is very sensitive to the ID vault trust chain. While most customers may have only listed the organisation as trusting the ID Vault, Notes Federated Login and Web Federated Login require that each organisation and all organisational units trust the ID Vault and the corresponding certificates exist in the Domino Directory and ID Vault configuration documents. Having missing trust certificates can have numerous effects on Web Federated Login such as those reported in

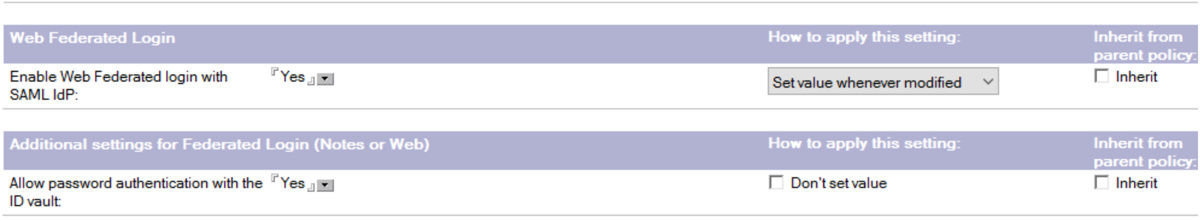
https://www-01.ibm.com/support/docview.wss?uid=swg22012970

Given this, it is important that before you create your security settings policy document for Web Federated Login, your ID Vault configuration has trusted the organisation and organisational units and the certificates exist in the Domino directory.

It should also be noted that Web Federated Login should not be enabled during a key rollover or when the user is in the middle of a rename.

In the security settings document select the Password Management → Federated Login tab.

Set the field, Enable Web Federated Login with SAML IdP to Yes, and How to apply this setting to Set value whenever modified.



Web Federated Login		How to apply this setting:	Inherit from parent policy:
Enable Web Federated login with SAML IdP:	Yes	Set value whenever modified	□ Inherit

Additional settings for Federated Login (Notes or Web)		How to apply this setting:	Inherit from parent policy:
Allow password authentication with the ID vault:	Yes	□ Don't set value	□ Inherit

Set the field, Allow password authentication with ID Vault to Yes

Select the ID Vault tab.

In the Assigned Vault field add the ID Vault database name in the format /vaultname

Set the Allow automatic ID downloads field to Yes.

Set the Allow Notes-based programs to use the Notes ID Vault field to Yes

Click Save and Close. You can now create an explicit policy which uses this security settings document and assign this to your users.

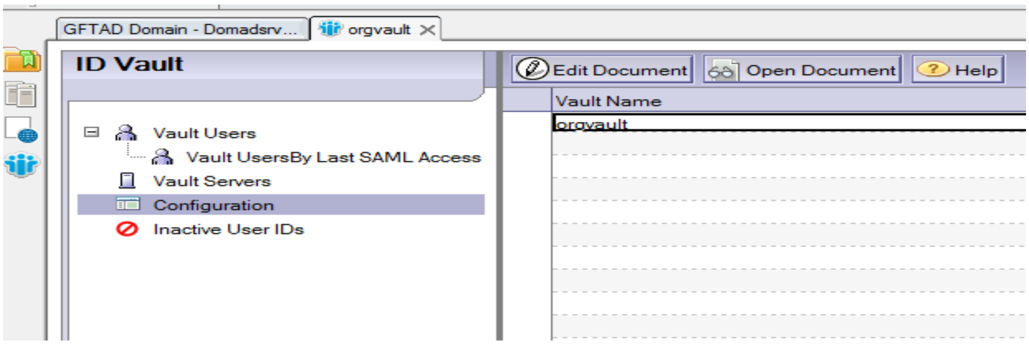
Configure The ID Vault For Web Federated Login.

As part of the process for enabling Web Federated Login, you must edit the ID Vault configuration document within the ID Vault database to add the iNotes servers/Internet sites ID Vault host names. To complete this task in the Administration client:

1. Select the Files tab → IBM_ID_VAULT view.

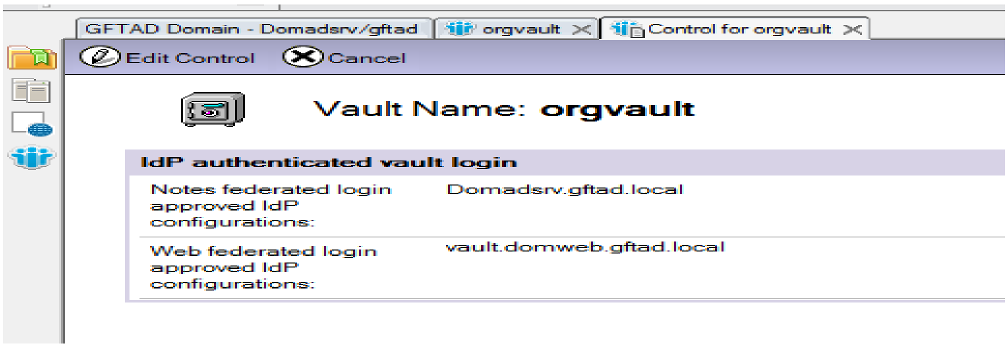
2. Double click on your ID Vault database.

3. Select the Configuration view.



4. Click Edit Document.

5. In the Web federated login approved IdP configurations field enter the ID vault iNotes host name matching the ID Vault configuration document created for your iNotes server/Internet site e.g. vault.domweb.gftad.local; If you have more than one iNotes ID Vault configuration you must list each one field also, with each host name separated by a semi-colon.



Vault Name: orgvault

IdP authenticated vault login

Notes federated login approved IdP configurations: Domadsrv.gftad.local

Web federated login approved IdP configurations: vault.domweb.gftad.local

6. Click Save & Close and then close the database.

Completing The Configuration For Web Federated Login.

Once you have completed the required configuration steps listed above you can complete the following steps to finish the configuration of your iNotes server/Internet site.

Setting SAML As The Authentication Method For Your iNotes Server/Internet Site.

If your iNotes server does not host an Internet Site, you must open the server document in edit mode and

1. Select the Internet Protocols → Domino Web Engine tab.

2. Select the Session Authentication field and select SAML.

3. The Open IdP Configuration button should now become active, click on this to ensure that the corresponding configuration document should be opened. This should be the document created for your iNotes server/Internet site, not the corresponding ID Vault configuration document.

4. If not using an SSO document, leave the SAML single server session expiration field set at 120 minutes[8].

5. Save your changes to the server document and restart Domino.

If you are enabling SAML for an Internet site hosted on your iNotes server, you must open the Internet site document in edit mode and

1. Select the Domino Web Engine tab.

2. Select the Session Authentication field and select SAML.

3. The Open IdP Configuration button should now become active, click on this to ensure that the corresponding configuration document should be opened. This should be the document created for your iNotes server/Internet site, not the corresponding ID Vault configuration document.

4. If not using an SSO document, leave the SAML single server session expiration field set at 120 minutes.

5. Save your changes to the Internet site document and restart Domino.

[8] If using an LTPA token, all servers should be configured for Web Federated Login.

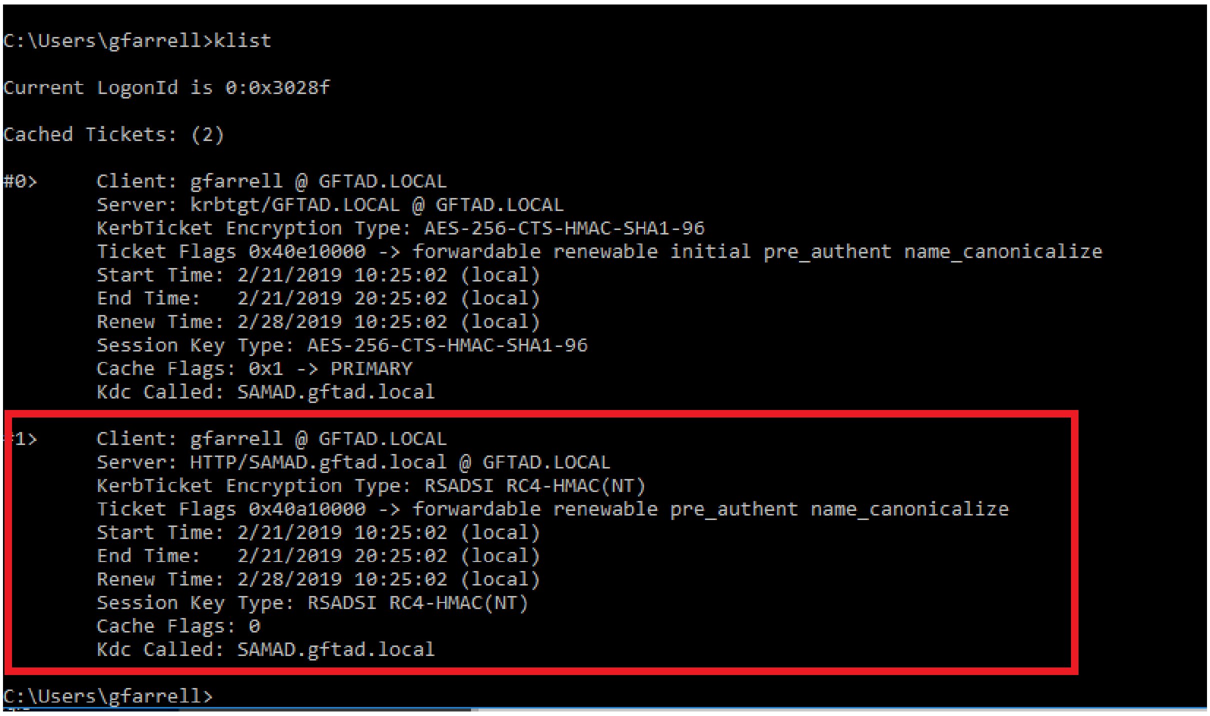
Testing Web Federated Login.

This test is based on the premise that your user was already assigned the Web Federated Login test policy when they were registered or was assigned the policy after registration, and the user was registered with iNotes as their mail system.

1. Send the user an encrypted email.
2. Log onto the Windows 7/10 client using the users AD user name and password.
3. Launch the web browser set up for Integrated Windows Authentication.
4. Enter the HTTPS url for your iNotes server/Internet site.
5. You should be automatically logged into your iNotes mail file.
6. Click on the encrypted mail sent to you in step 1. The user should be able to open this mail without being prompted to provide your Notes password.

If you are prompted to enter your Notes password when reading an encrypted mail or another error occurs enabled the debug parameters listed in the following section, and if required open a case with support.

You can confirm if your test user is receiving a Kerberos ticket for the ADFS server by opening the Windows Command Prompt and entering the command klist, which will return the tickets issued to the user. You should see a ticket for your ADFS server listed as shown below.



```
C:\Users\gfarrell>klist

Current LogonId is 0:0x3028f

Cached Tickets: (2)

#0>     Client: gfarrell @ GFTAD.LOCAL
        Server: krbtgt/GFTAD.LOCAL @ GFTAD.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 2/21/2019 10:25:02 (local)
        End Time:   2/21/2019 20:25:02 (local)
        Renew Time: 2/28/2019 10:25:02 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called: SAMAD.gftad.local

#1>     Client: gfarrell @ GFTAD.LOCAL
        Server: HTTP/SAMAD.gftad.local @ GFTAD.LOCAL
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
        Start Time: 2/21/2019 10:25:02 (local)
        End Time:   2/21/2019 20:25:02 (local)
        Renew Time: 2/28/2019 10:25:02 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0
        Kdc Called: SAMAD.gftad.local

C:\Users\gfarrell>
```

Debug Parameters

The following parameters can be set to debug Web Federated Login issues.

On your iNotes web server(s)

Debug_SAML=31

DEBUG_SSL_ALL=2

On your ID Vault Server(s)

Debug_SAML=31

Debug_IDV_Connect=1

Debug_IDV_Trace=1

Debug_IDV_TrustCert=1

For issues with name mapping/resolution the following parameters can also be added

WEBAUTH_VERBOSE_TRACE=1

LOGLEVEL_NAME_MAPPING=1

DEBUG_NAMELOOKUP=1

Appendix – Configuring Name Mapping Via Directory Assistance.

Throughout the document, the scenario where the user's email address matches between Active Directory and Domino has been used. This is based on the cases I have worked with customers who for the majority do not have name mapping through directory assistance enabled, and the fact that it is not supported for Web Federated Login.

As some customers, will just be enabling SAML For Single Sign On and may wish to enable name mapping through directory assistance, this appendix lists the additional steps required to enable this configuration.

1. Create a directory assistance database on your Domino server(s) that are to be enabled for SAML Single Sign On.

2. Once created and opened, click Add Directory Assistance to create a new document.

3. on the basics tab

    a. Set the Domain type to LDAP

    b. Set the Domain name

    c. Set the search order

    d. Make the domain accessible to all client types.

4. On the Name Context Rules Tab, set Trusted For Credentials to Yes.

5. On the LDAP tab

    a. Enter the fully qualified host name for your PDC server.

    b. Set the LDAP Vendor to Active Directory.

    c. Enter the name and password for the user who has permission to bind to Active Directory in the Optional authentication credential for search field.

    d. Enter your Base DN.

    e. Set the Channel encryption to SSL and the port to 636, if not already set and if required.

    f. Select the option Enable Name Mapping.

    g. In the Attribute to be used as Notes Distinguished Name, enter the name of the attribute in the users' Active Directory User Object that will hold the users' Notes Distinguished Name.

6. Click Save and Close. Repeat the above steps for each server and directory assistance database required.

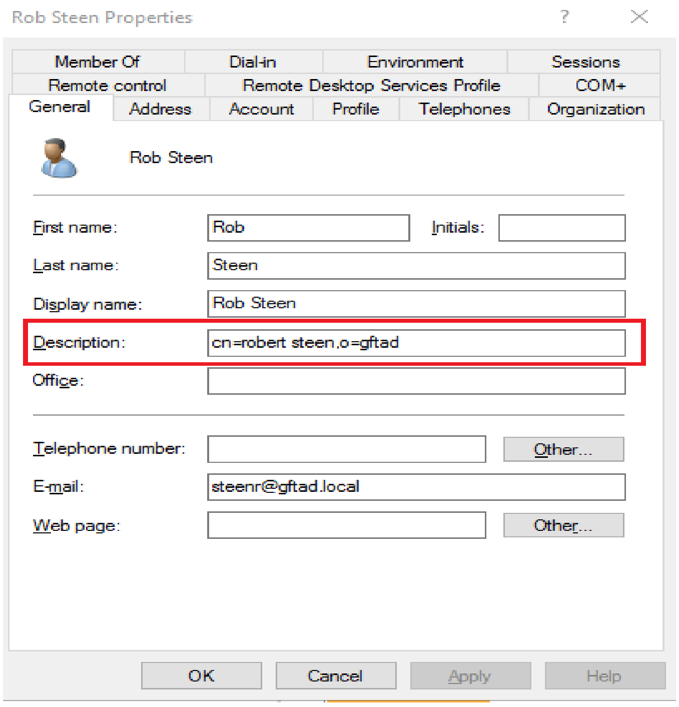
7. Complete the rest of the configuration steps required to set up SAML Single Sign On.

To test complete the following steps

1. Register a test user in Domino and apply either your Web or Notes Federated Login policy.

2. Register the same user in Active Directory, make sure the email address does not match the user's Domino Internet email address.

3. Open their User object and in the Description field enter their Notes Distinguished Name in the format cn=user name, ou= ou name, o=organisation name. Note the ou name is dependent on if you registered the user under an organisational unit in Domino or not.



Rob Steen Properties

Rob Steen

First name: Rob

Initials:

Last name: Steen

Display name: Rob Steen

Description: cn=robert steen,o=gftad

Office:

Telephone number:

E-mail: steenr@gftad.local

Web page:

4. Add the test user to the ACL of the database that you wish to access through SAML.

5. On the machine of the test user, attempt to access the URL for your Domino server/Internet site and the user should automatically be authenticated, if using Integrated Windows Authentication, or by providing their Active Directory user name and password if using Forms Based authentication.