



Single Sign-On

Technical Reference Guide

Version 1.3

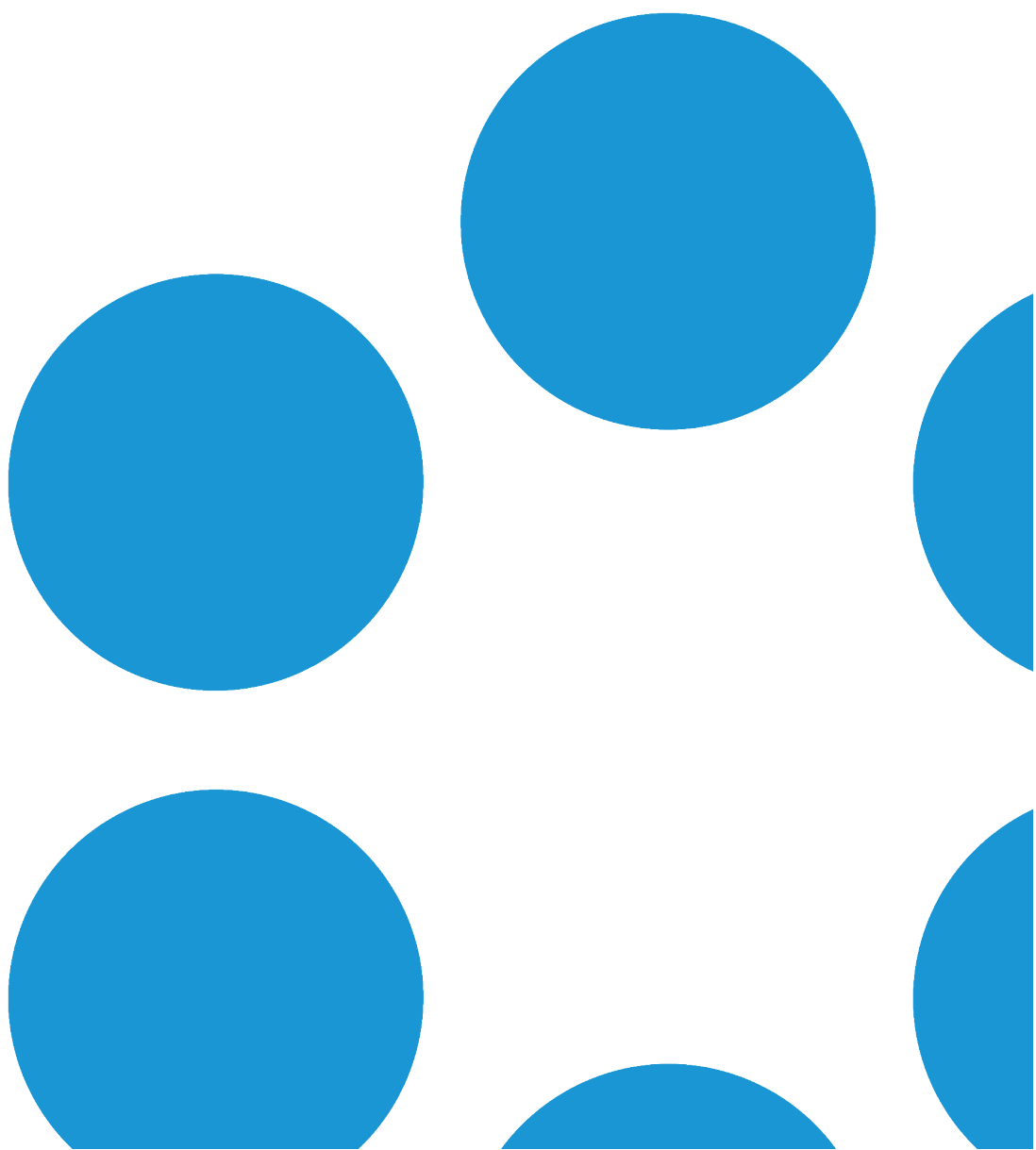




Table of Contents

Version Details	4
Online Support	4
Comments and Feedback	4
Copyright	4
About this Document	6
Intended Audience	6
Standards and Conventions	6
About Single Sign-On using the SAML based Connector	7
The SAML Transaction Steps for vFire	7
Glossary of Terms	8
Technical and Access Requirements	9
Supported Interfaces	10
Configuring vFire for Single Sign-On	11
Importing Identity Provider Metadata	13
Adding an Identity Provider	13
Deleting an Identity Provider	14
Installing a Service Provider Signing Certificate	15
Adding a Signing Certificate	15
Configuring the Service Provider	19
Adding a Service Provider	19



Deleting a Service Provider	23
Exporting Service Provider Metadata	24
Importing Service Provider metadata into the Identity Provider	26
Claim Rules	29
Note on Claim Rules	31
Person Import and Resource Mapping	32
SSO Troubleshooting	35
SSL Binding	42
Creating a Self Signed Certificate	44
Extending the Single Sign-On Connector	48
Adding New Claims to the ICNF File	50
Azure Multi-factor Authentication	52
Multi-factor Authentication User Transaction Steps for vFire	53
Multi-Factor Authentication Technical Transaction Steps for vFire	55
Configuring Azure Active Directory discovery	56
Configuring vFire Core	56
Configuring Azure Active Directory.	57
Further Information	59
Product Information and Online Support	59
Technical Support	59
Comments and Feedback	59



Version Details

This document supports the version of the product listed, and supports all subsequent versions until the document is replaced by a new edition. The table below contains version details for the guide.

Version Number	Date	Details
1.0	September 2016	This is the initial version of this document
1.1	12 September 2016	Addition of the Azure Multi Factor Authentication documentation
1.2	7 October 2016	Addition of topic on Configuring Azure Active Directory discovery through Secure Lightweight Directory Access Protocol (TLS 1.2)
1.3	17 May 2017	Update to the list of SSO supported products

Online Support

For information about Alemba products, or licensing and services, visit www.alemba.com.

For software updates, documentation, release notes and support using the system, visit www.alemba.help/help



You may need to register to access some of these details.

Comments and Feedback

If you have any comments or feedback on this documentation, submit it to info@alembagroup.com.

Copyright

Copyright © Alemba Limited (or its licensors, including ©2010 - 2017 VMware, Inc). All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at: <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. VMware Service



Manager™ is also trademark of VMware, Inc. Alemba™, vFire™ and vFireCore™ are trademarks of Alemba Limited (vFire Core™ is developed by Alemba Limited from VMware, Inc's product "VMware Service Manager", under licence from VMware, Inc). All other marks and names mentioned herein may be trademarks of their respective companies.



About this Document




This guide contains instruction and information on how to configure Single Sign On for your vFire systems.

Intended Audience

This document is written for system administrators, responsible for the configuration of the organization's vFire systems.

Standards and Conventions

The following standards and conventions are used throughout the document:

	Prerequisites, including security rights and access you may need prior to completing the task. Prerequisites are also highlighted in a shaded box.
	Information related to the current topic that may be of particular interest/significance. Notes are also highlighted in a shaded box.
	Warnings. These are also highlighted in a shaded box.
Field name	Fields are highlighted in bold text.



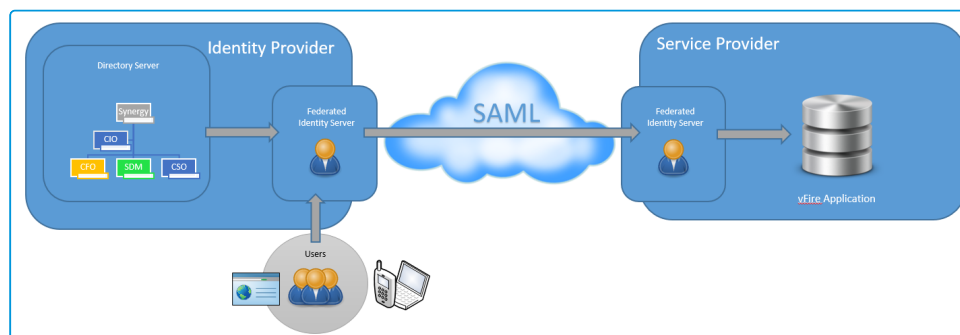
About Single Sign-On using the SAML based Connector

 This feature is only available on SQL systems.

This topic provides an introduction to how vFire Core can be configured for Single Sign-On (SSO) using Security Assertion Markup Language (SAML) and the technical requirements to use this functionality.

vFire Core Analysts and Users will typically need access to a large number of internally and externally hosted (Cloud) applications each requiring usernames and passwords. Identity federation helps to solve this issue by providing a secure mechanism for sharing identities and therefore removing the need to maintain a separate user profile for vFire Core.

SAML is an identity federation standard language that enables SSO without the need to remember passwords and is a convenient way to access web applications due to enhanced security. It limits potential risks by eliminating the need for extra web application passwords by establishing a trust between the vFire Application and the Organization's Federated Identity system(s).

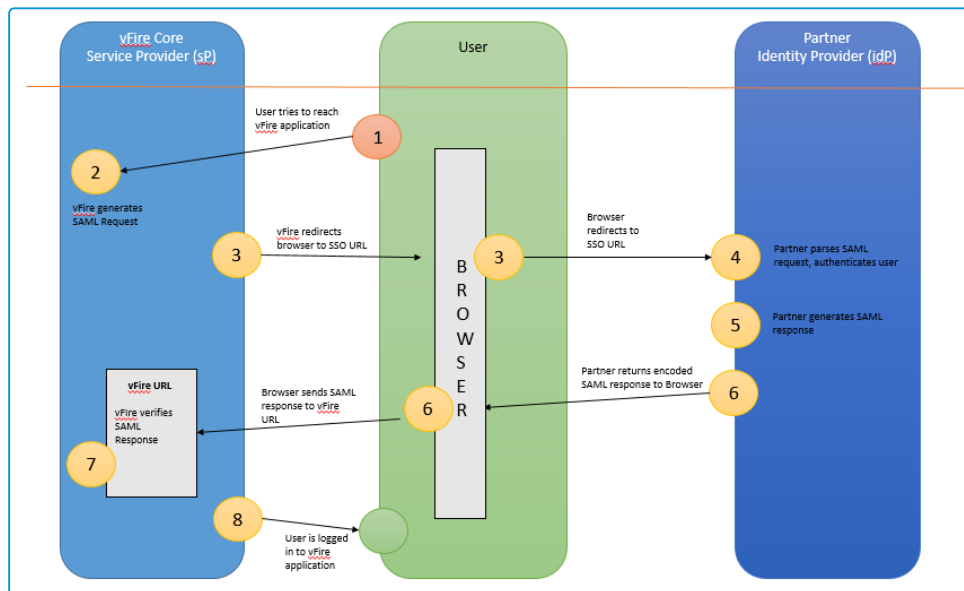


The SAML Transaction Steps for vFire

1. The vFire User or Analyst makes a request to access the application by loading an appropriate vFire URL in a Browser.
2. The vFire application will detect this request and generate a SAML request.
3. This is redirected back to the User/Analyst's browser with the SSO URL.
4. The Identity Provider, MS ADFS or other Partner, checks the request and then authenticates the User/Analyst.



5. The SAML Response is generated.
6. It is then passed back to the User/Analyst's Browser which is then sent to the vFire URL.
7. vFire verifies this response.
8. The User is logged into the vFire application.



Glossary of Terms

Federated Identity is the means of linking a person's electronic identity across multiple distinct identity management systems.

Single Sign-On is a property of access control of multiple related but independent software systems allowing a user to log in to vFire Core with a single ID and password.

SAML is an XML based open standard for exchanging authentication and authorization data between for instance, an application with a user's own organizational log in credentials.

Service Provider (sP) in this case is the application for which Users are attempting to access and log in to i.e. the vFire Application.

Identity Provider (IdP) is the source of the SAML service (e.g. ADFS, Shibboleth) which provides the Service Provider (vFire Application) with the authorization for users to log on and use the application.




Technical and Access Requirements

The Single Sign-On Connector has been developed using SAML 2.0 Standards.

In vFire 9.4.4, 5.1.2 and 6.0 onwards, the Single Sign-On Connector is installed by default and does not require a separate license.

Before you start

Before you configure the Single Sign-On Connector it is recommended that you highlight the Single Sign-On Connector and press the  button in the toolbar to ensure the connector is installed correctly. See [Testing Connectors](#) for details on how to do this.

We advise you to disable **IIS Windows Authentication** and **vFire Integrated Security** to ensure a consistent user experience.



The examples use Microsoft Active Directory Federation Services (ADFS). However, other Federated Identity Providers are supported as long as they adhere to SAML 2.0 standards.

The following Identity Providers have been certified by Alemba:

- Active Directory Federation Services
- ADFS Proxy
- Azure ADFS



Azure Premium is recommended if you want to be able to modify the Identity Provider Claim Rules.


- Ping Federate

When a web request is received using a URL which has a configured Service Provider, that request will be authenticated using SSO, irrespective of other authentication settings.



Supported Interfaces

Single Sign-On is supported for the following vFire Interfaces:

vFire Interface	SSO Supported
vFire Core	✓
vFire Core Portal	✓
vFire Officer & Portal  Also supported for vFire Wallboard and vFire Admin	✓
vFire Officer app	✗
vFire app	✗

The Single Sign-On Connector supports Azure Multi-Factor authentication, further details can be found in the topic on [page 52](#).



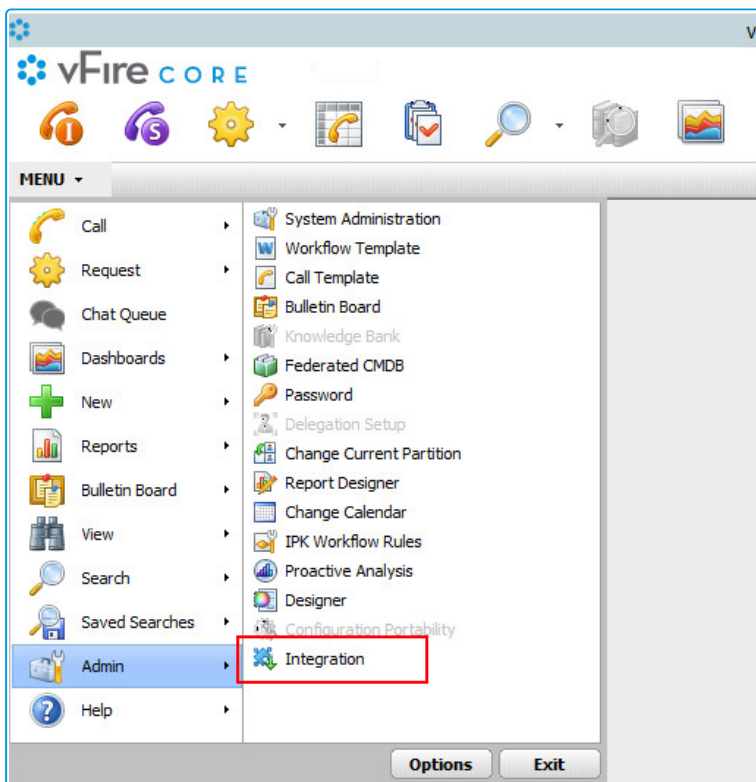
Configuring vFire for Single Sign-On

Before you start

You must have **Integration Setup** selected in the **Admin** tab of your **General Access security role**.

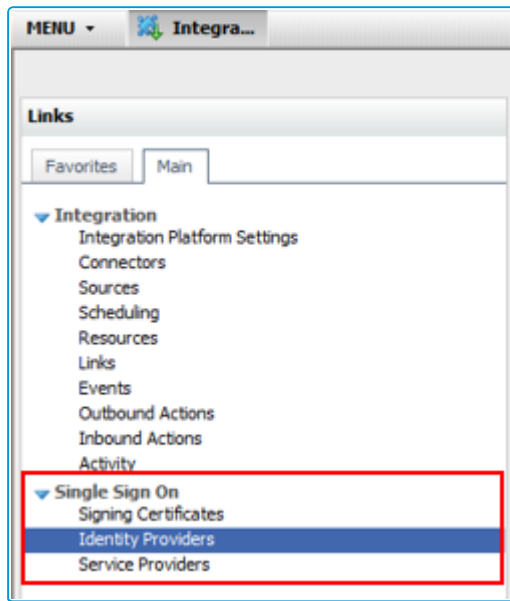
vFire provides a common platform to set up integration with a variety of external applications. The Integration Platform is enabled and configured through the **Integration Platform Settings** window.

Select **Menu** and then **Admin**. From the submenu, select **Integration**.





The **Integration Platform** menu is displayed, with Single Sign-On menu options.



The Single Sign-On Explorer Menu options enable you to configure the Single Sign-On components:

- Signing Certificates – enables you to configure Signing Certificates for use by the connector.
- Identity Providers – enables you to add the metadata from the Identity Provider.
- Service Providers – enables you to configure Service Providers for vFire.

There are 6 steps required to configure vFire as your Service Provider and successfully connect to your chosen Identity Provider:

1. **Export Identity Provider Metadata (XML)** to create a federated trust between the Identity Provider and the Service Provider (vFire). The Microsoft ADFS metadata can be downloaded from <https://<adfs-server-name>/federationmetadata/2007-06/federationmetadata.xml>.
2. [page 13](#).
3. [page 15](#).
4. [page 19](#).
5. [page 24](#).
6. [page 13](#).



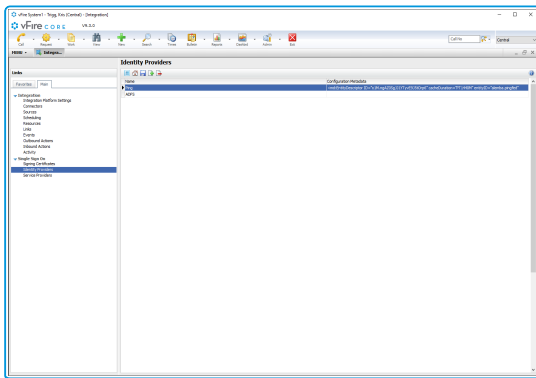
Importing Identity Provider Metadata

When creating a Service Provider for vFire you will need to specify which Identity Provider to use.

Adding an Identity Provider

To add a new identity provider:

1. Select **Menu > Admin > Integration > Identity Providers**.



2. Select . The Details window is displayed.

3. Complete the details.

Name Add a Display Name for the Identity Provider.

**Secure Hash Algorithm**

Choose SHA-1 or SHA-256 from the dropdown list.



The Hash Algorithm here must be the same as the one selected for the Relying Party when importing service provider metadata.

Metadata

Copy and Paste the metadata XML from your Identity Provider into this field.



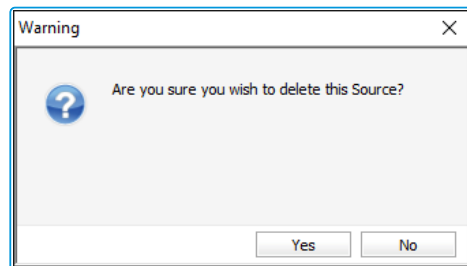
The metadata must include the public key for the IdP Signing Certificate (this is included by default in ADFS metadata).

4. Select  to save the details.

Deleting an Identity Provider

1. Select an Identity Provider in the Identity Providers browse table.

2. Select  .



3. A warning is displayed. Click **Yes** to delete the Identity Provider or **No** to cancel.

Click **Yes** to delete the

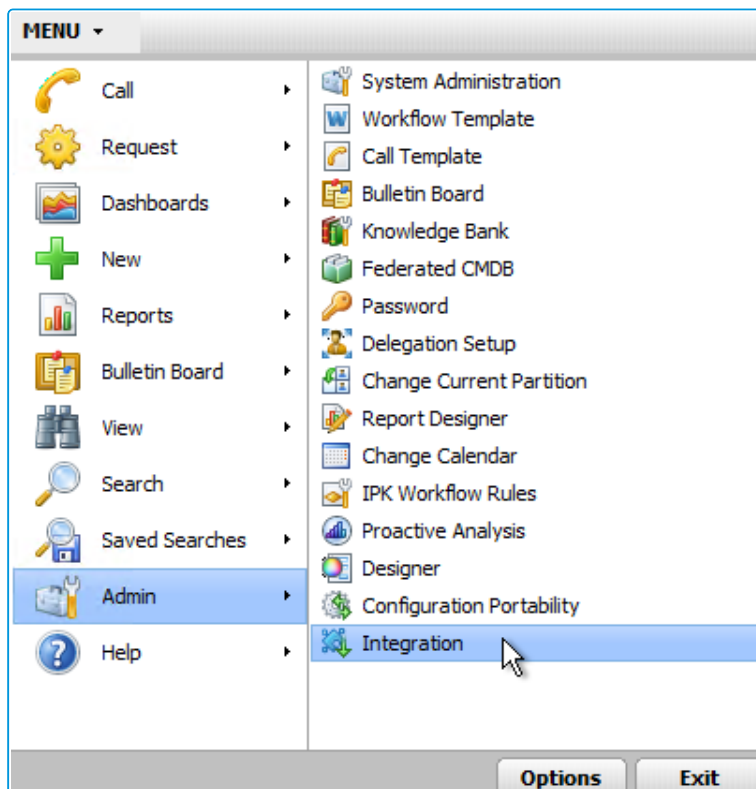


Installing a Service Provider Signing Certificate

Service Provider (vFire Application) initiated sign on requires SSL Signing. This is configured in vFire by defining a unique vFire Identifier for the SSL Certificate. You may wish to create a resource mapping (if used) prior to carrying out this step, although this information can be added at a later date.

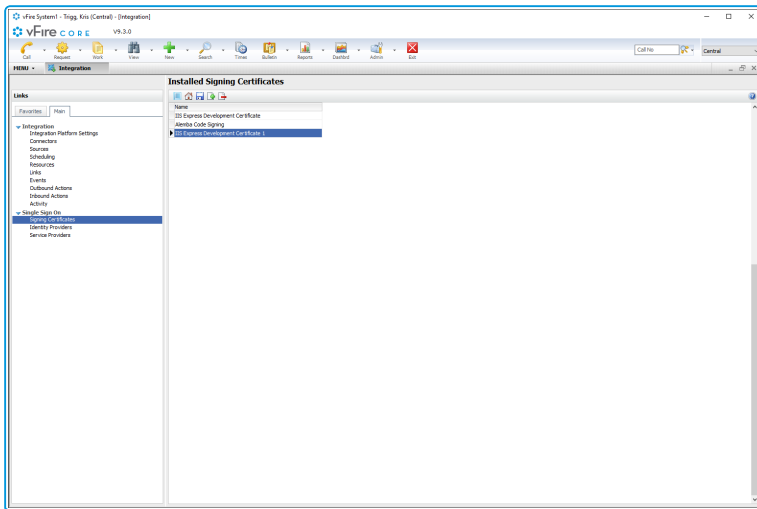
Adding a Signing Certificate

1. Select **Menu** and then **Admin**. From the submenu, select **Integration**



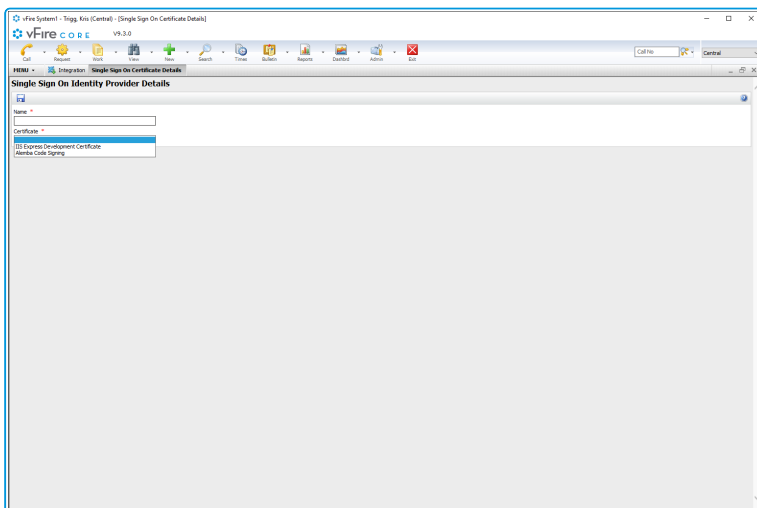


2. Then select Signing Certificates.



3. Select .


4. The Single Sign On Identity Provider Details window is displayed.



Complete the details.

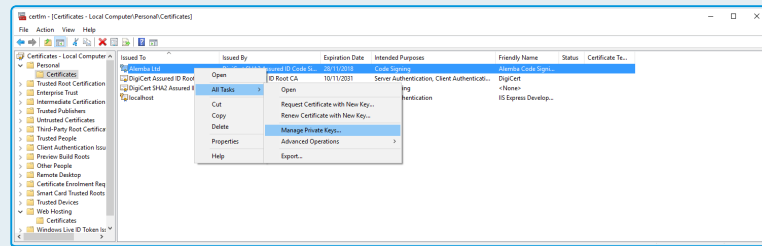
- Name** Add a Display Name for the Signing Certificate
- Certificate** Choose a Certificate to make this available to your Service Provider (The Certificate dropdown field shows all certificates installed in the Local Machine store of the vFire web server)

5. Select  to save the details.


 Certificates must have a private key and the IIS Application Pool must have full control



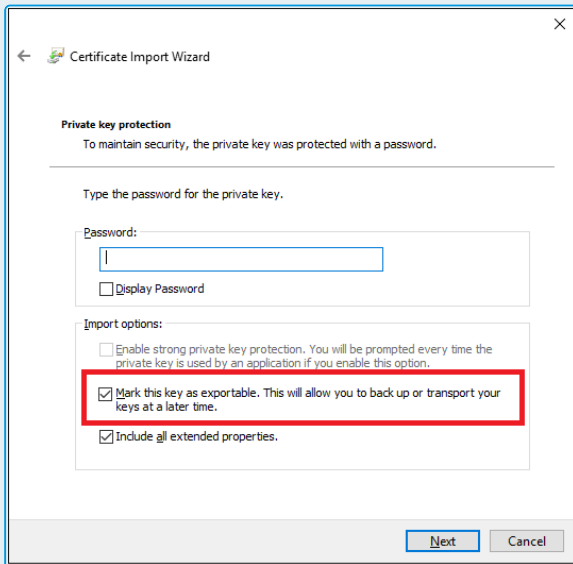
of the certificate. Permissions for the certificate can be changed using **Manage**



Private Keys.

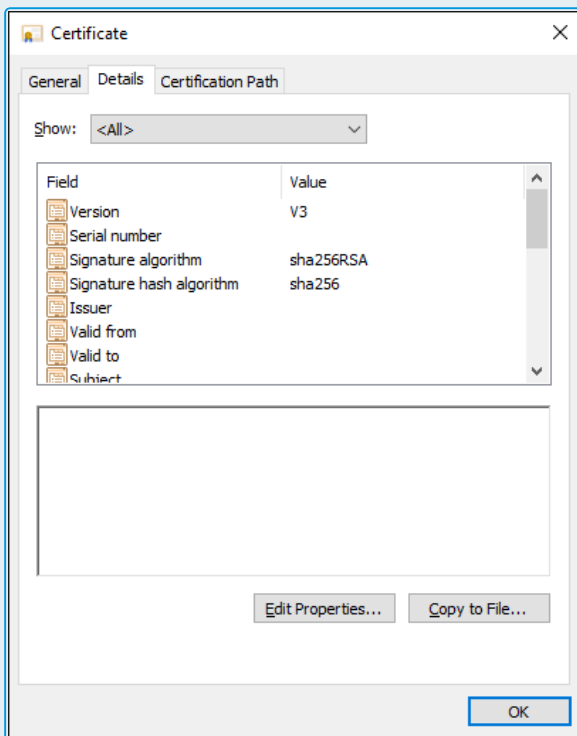
 If you are using the SHA-256 Secure Hash Algorithm (a Requirement for Azure AFDS for example), ensure that :

- the certificate has been marked as exportable when it is installed





- the certificate contains the SHA-256 Signature Algorithm. You can find this information by viewing the certificate properties



An SHA256 certificate can be used to create SHA1 and SHA256 signatures. A SHA1 certificate cannot be used to create SHA256 signatures.



Configuring the Service Provider

You must configure Service Providers for each vFire resource vFire Core, vFire Self Service Portal, vFire Officer or vFire Portal.

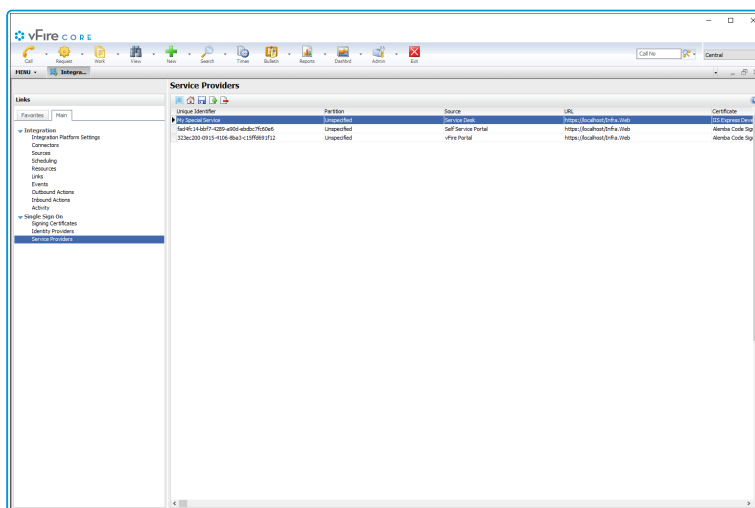


When a web request is received using a URL which has a configured Service Provider, that request will be authenticated using SSO, irrespective of other authentication settings.

Adding a Service Provider

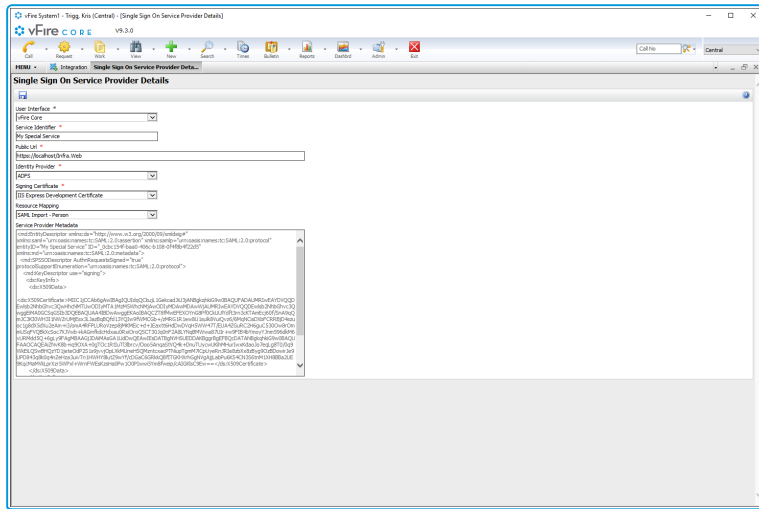
Adding a new Service Provider will enable SSO for the URL configured.

1. Select **Menu** and then **Admin**. From the submenu, select **Integration**.
2. From the **Single Sign On** group in the explorer pane, select the **Service Providers** option.





3. Select . The Single Sign-On Service Provider Details window is displayed.




4. Complete the details.

User Interface Choose a User Interface from the dropdown

Service Identifier A Service Identifier will be automatically generated. This Identifier must be unique to the vFire system and must be unique to the Identity Provider. Therefore this value is editable, and can be changed at any time to meet these requirements.


Public URL The Public URL for the service will be generated based upon the URL of the current session but this URL is editable to allow for flexible configuration. This URL will be used to specify the redirect URL used by the Identity Provider. It does not need to be Internet facing, but must be resolvable by all users of the service.

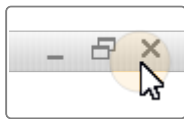
This URL is used to select an Identity Provider when a web request is received. It does not include the specific interface e.g. core.aspx or core.aspx?lite

 Multiple Service Providers can be configured for a single service using different URLs and service identifiers. This allows for flexible configuration of SSO in a variety of environments. However, in this version you are unable to configure the Public URL to direct to a specific Portal System.



Identity Provider	Select the Identity Provider from the drop-down field
Signing Certificate	Select the Signing Certificate from the drop-down field
Resource Mapping	Select the Resource Mapping from the drop-down field. (This information can be updated later if the required resource mapping has not been configured.) Resource Mapping defaults to disabled, if this is set on the Service Provider configuration then the SSO Connector will not attempt to update User Records.
Service Provider Metadata	This field will display any changes made by changing the values in the Service Provider details.

5. Select  to save the details. This will update the metadata. Then select



to close the window.

Partitioning

If Users are partitioned, SSO for the Self Service Portal can be configured per partition. If you choose vFire Self Service Portal in the User Interface dropdown field and Users are partitioned then an additional Partition dropdown field will be displayed allowing for you to set the User Partition parameter for the Service Provider.

Users of the self service portal must then access the service using a partitioned URL:

 <http://server/system/core.aspx?lite&PARTITION=1> where 1 = the Ref value of the Partition.

This does not affect the partitions the User has access to within vFire, it is used by the Identity Provider for logins to the Self Service portal.

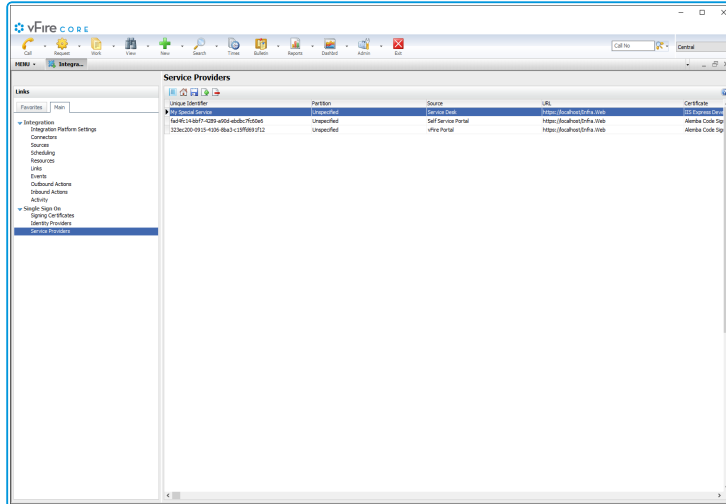


Changes to the settings on the Service Provider Details screen has the ability to break the communications between the Identity Provider and the Service Provider. If the Signing Certificate, Service Identifier or Public URL changes, the details must be updated on the Identity Provider (by using the updated metadata xml).




Deleting a Service Provider

1. Select **Menu** and then **Admin**. From the submenu, select **Integration**.
2. From the **Single Sign On** group in the explorer pane, select the **Service Providers**



option.

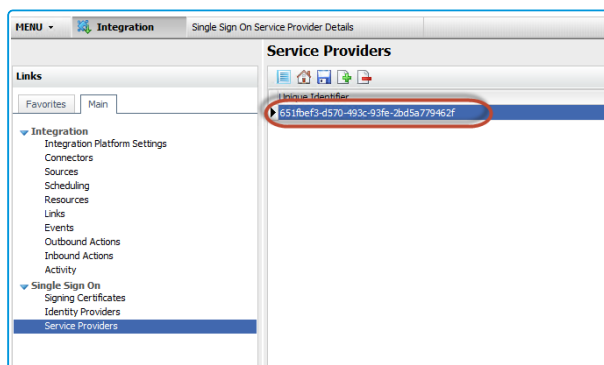
3. Select the Service Provider in the Service Provider browse table, and select .
4. When the Warning message is displayed, select Yes to confirm the deletion.



Exporting Service Provider Metadata

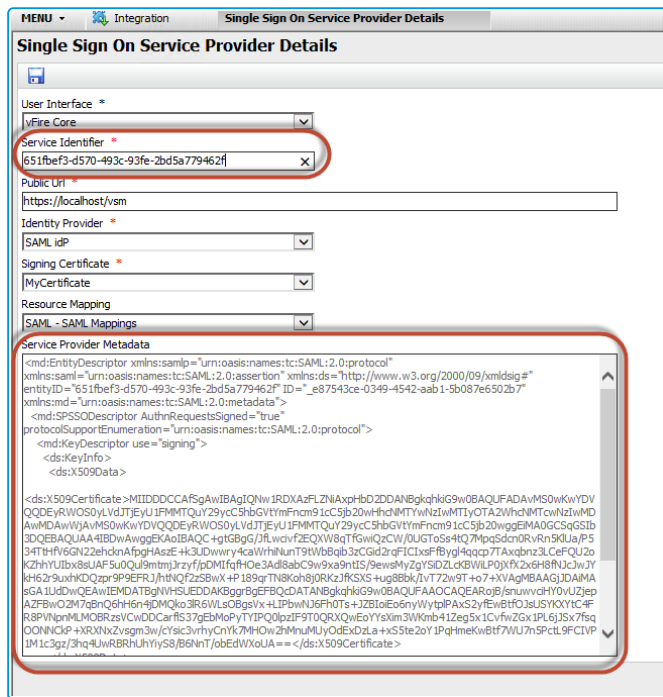
The Service Provider metadata is required to be imported into the Identity Provider to complete the trust relationship between the Identity Provider and the vFire Application. Prior to this, you must export the metadata. To export the Service Provider metadata, follow these steps:

1. Select **Menu, Admin** and then **Integration**.
2. From the **Single Sign On** group of options in the explorer pane, select **Service Providers**.
3. Select the Service Provider from the list.





4. Make note of the string listed in the **Service Identifier** field.
5. Copy the XML data in the **Service Provider Metadata** field



and store it in a text file. You

will be referencing this file as part of the export, so it is advisable to store it in an appropriate location, and name it accordingly.

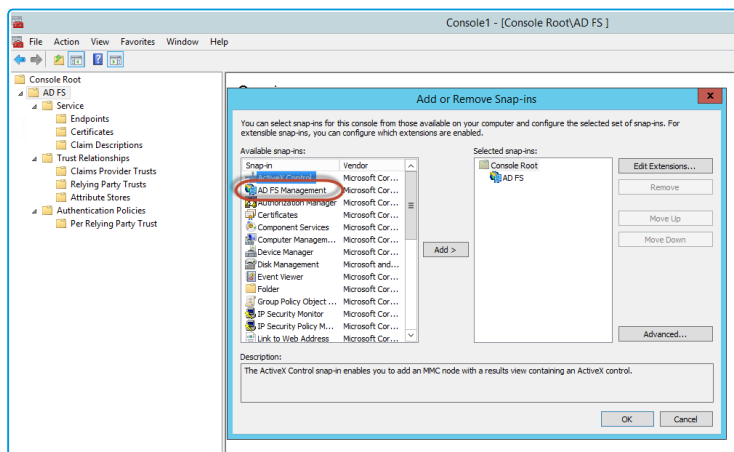


Importing Service Provider metadata into the Identity Provider

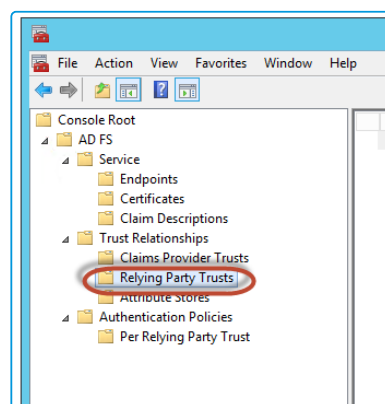
The Service Provider metadata must be imported into the Identity Provider to complete the trust relationship between the Identity Provider and the vFire Application. To Import the Service Provider metadata, follow these steps:

On the Identity Provider Server (Server hosting your domain's ADFS Server):

1. Open the **Microsoft Management Centre (MMC)**
2. Add the **AD FS Management** snap-in.
3. Click **File > Add/Remove Snap-in** .
4. Select **AD FS Management** from the list.



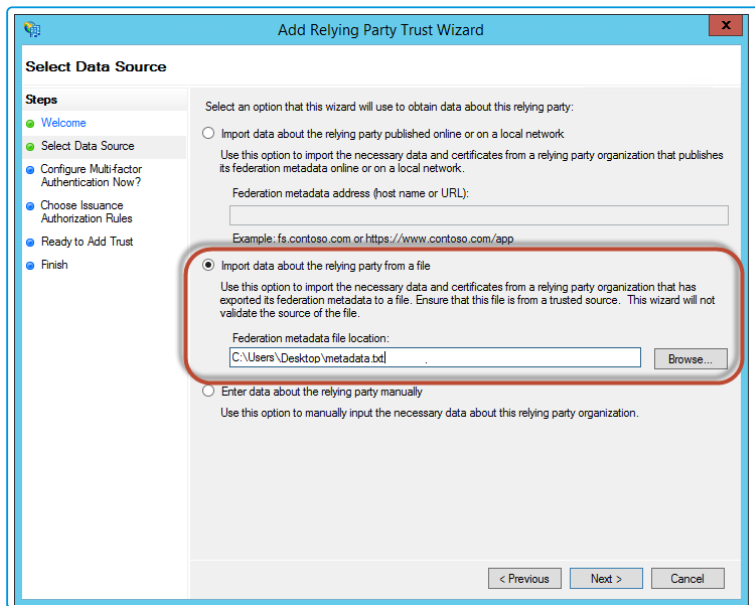
5. Click **OK**.
6. Expand the **AD FS** tree in the new snap-in.



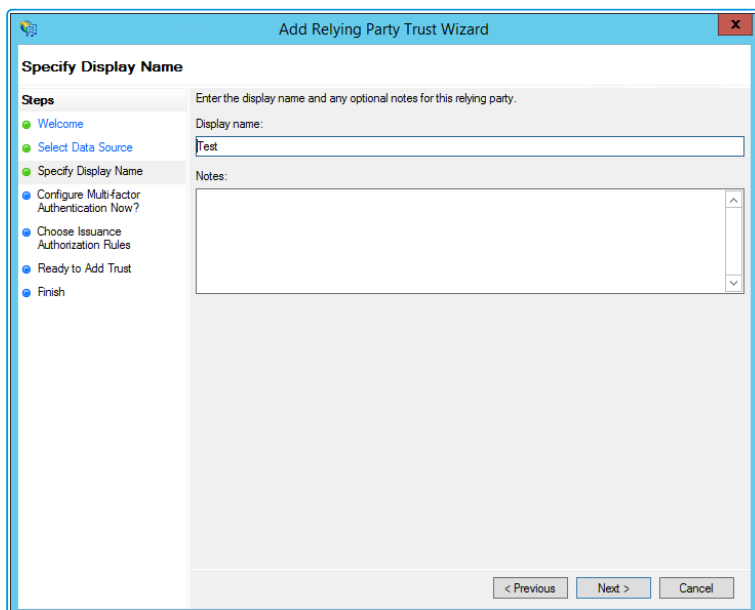
7. Select **Relying Party Trusts**.



8. Right click the folder and select **Add Relying Party Trust**. The Add Relying Party Trust wizard will open.
9. Click **Start**.
10. Select the **Import data about the relying party from a file** radio button.
11. Click **Browse**.
12. Select the text file with the metadata you saved earlier.



13. Click **Next**
14. Enter a **Display Name** for the party trust.





15. Click **Next**
16. Select the **I Do not want to configure multi-factor authentication settings for this relying party trust at this time** radio button.

Add Relying Party Trust Wizard

Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.

Multi-factor Authentication		Global Settings
Requirements	Users/Groups	Not configured
	Device	Not configured
	Location	Not configured

I do not want to configure multi-factor authentication settings for this relying party trust at this time.
 Configure multi-factor authentication settings for this relying party trust.

You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see [Configuring Authentication Policies](#).

< Previous Next > Cancel

17. Click **Next**.
18. Select **Permit all users to access this relying party** radio button.

Add Relying Party Trust Wizard

Choose Issuance Authorization Rules

Issuance authorization rules determine whether a user is permitted to receive claims for the relying party. Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.

Permit all users to access this relying party
 The issuance authorization rules will be configured to permit all users to access this relying party. The relying party service or application may still deny the user access.

Deny all users access to this relying party
 The issuance authorization rules will be configured to deny all users access to this relying party. You must later add issuance authorization rules to enable any users to access this relying party.

You can change the issuance authorization rules for this relying party trust by selecting the relying party trust and clicking Edit Claim Rules in the Actions pane.

< Previous Next > Cancel

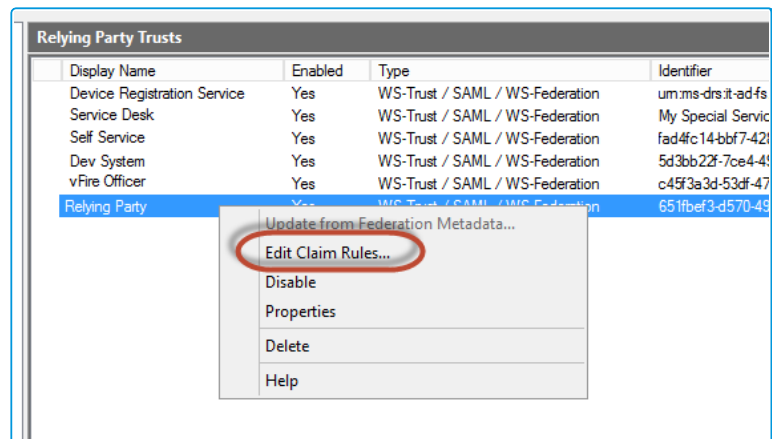
19. Click **Next**, and **Next** again on the **Ready to Add Trust** screen.
20. Click **Finish**



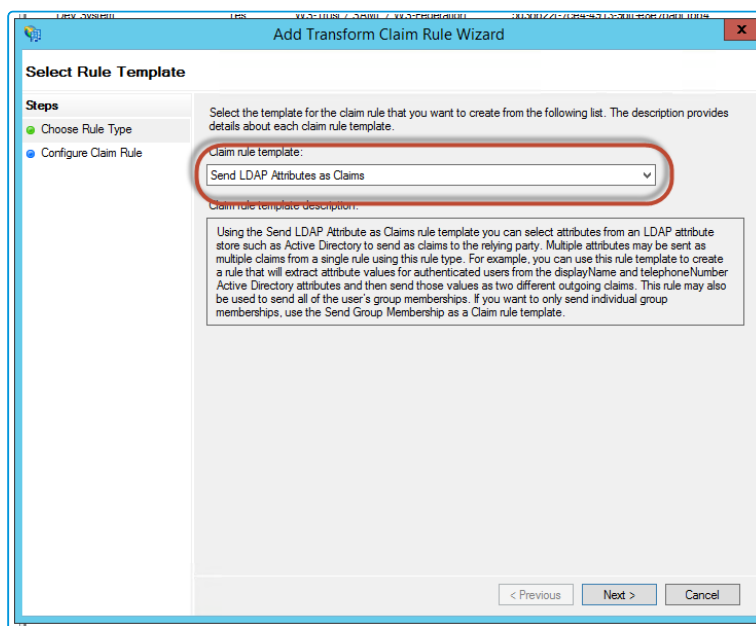
Claim Rules

Once you have completed the **Add Relying Party Trust Wizard** you will need to configure the rules for the relying party. To configure this:

1. Right Click on the **Relying Party Trust** you just created.



2. Select **Edit Claim Rules**.
3. Click **Add Rule**. The **Add Transform Claim Rule Wizard** will open.
4. Select **Send LDAP Attributes as Claims** as the Claim Rule Template.



5. Click **Next**.
6. Enter a relevant **Claim Rule Name** for the rule.
7. Select **Active Directory** under **Attribute Store** drop-down field.



8. Map the LDAP Attributes to Outgoing Claim Values.

Edit Rule - test 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: test Rule

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)
User-Principal-Name	Name ID
Given-Name	first name
Surname	Surname
E-Mail-Addresses	E-Mail Address
▶▶	

View Rule Language... OK Cancel

9. Click **OK**, **Apply** and **OK** to complete the rule.

10. Right click on the Relying Party trust from the MMC snap-in and select **Properties**.

Relying Party Properties

Organization Endpoints Proxy Endpoints Notes Advanced

Monitoring Identifiers Encryption Signature Accepted Claims

Specify the display name and identifiers for this relying party trust.

Display name: Relying Party

Relying party identifier: Add

Example: https://fs.contoso.com/adfs/services/trust

Relying party identifiers: 651fbef3-d570-493c-93fe-2bd5e779462f Remove

OK Cancel Apply

11. Select the Identifiers tab.

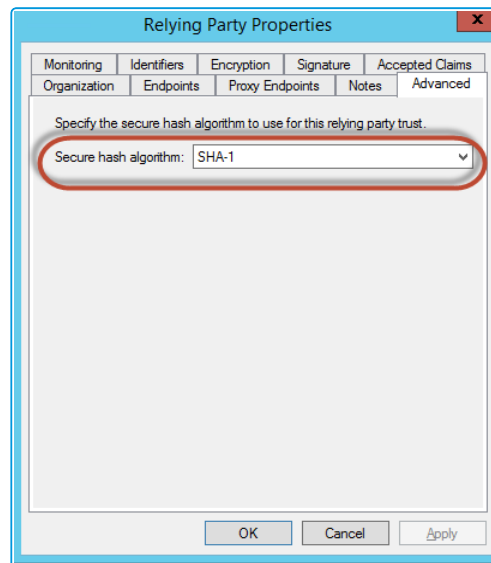
12. In the **Relying Party Identifier** field, enter/paste the Service Identifier string extracted from the vFire Service Provider Record.

13. Click **Add**.

14. Click **Advanced** tab.



- Set the **Secure Hash Algorithm** to **SHA-1** or **SHA-256**; whichever is selected in the



Identity Provider details.

- Click OK

Note on Claim Rules

The Single Sign On Connector does not read the LDAP Attributes directly, instead it reads the attributes received in the Inbound SAML Assertion. **Name ID** is a special SAML Assertion attribute which represents the User Name.

The Single Sign On Connector currently ships with mappings for User Name, First Name, Surname and Email Address by default. It is recommended that the Identity Provider Claims be configured for these vFire Single Sign On connector mappings



In ADFS, some special cases of the Inbound Claims are translated to similar looking Display Names. However, if you select the names using the drop-down then the actual Outbound Claim is displayed in the URL format, which can cause confusion, the Single Sign On Connector therefore translates this back to a value that more closely resembles the display name:



Connector receives Email Address and not
<http://schemas.xmlsoap.org/claims/EmailAddress>



SAML	ADFS LDAP Attribute Display	ADFS Outbound Claim Display *	ADFS Outbound Claim Actual	Converted To	vFire ICNF
Name ID	Name ID	Name ID	Name ID	User Name	User Name
First Name	Given-Name	Given Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	First Name	First Name
Surname	Surname	Surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Surname	Surname
Email Address	E-Mail-Addresses	E-Mail Address	http://schemas.xmlsoap.org/claims/EmailAddress	Email Address	Email Address
First Name	Given-Name	First Name	First Name		First Name

*ADFS Outbound Claim Display is free text



For Azure, you must use the connector and set the matching rules to ensure that users do not have multiple usernames. This is configurable in the Premium version.

Person Import and Resource Mapping

The Single Sign-On Connector, in the same way as other vFire Directory Services connectors, can allow Person Records to be imported directly into vFire from the Identity Provider. The Person Records in vFire will then be kept up to date.



In order to use the Single Sign-On Connector an Integration Resource Mapping needs to be **configured**.

Recommended Field Mappings for Single Sign-On Connector Person Import

vFire	Connector Mapping	Identity Provider
First Name	First Name	First Name
Surname	Surname	Surname
User Qualified Name	User Name	User Name
NT Account Name	User Name	User Name (<i>must be same as User Qualified Name</i>)
Login ID	User Name	User Name (<i>must be unique</i>)
NT Domain Name	<i>Must be blank</i>	<i>Must be blank</i>

All of the SAML based Identity Providers can be configured to send a variety of attributes with the SAML Security assertions, however it may not always be easily configurable through the respective user interfaces. For example the Active Directory Manager attribute is not exposed through the Microsoft ADFS User Interface.

Once the attributes have all been exposed by the Identity Provider the vFire Integration Platform and SSO Connector can easily consume these attributes and import/update Person Records as per other LDAP Connectors, however as this is time consuming and/or requires specific skills to configure the Identity Provider Claims then it may be a consideration to pre populate Users and Analysts using another method such as directly synchronising to an Active Directory Source, bulk import using a CSV file and the CSV Connector or by manual population initially.

It is also possible to configure SSO for a brand new system as long as the Username is mapped as above, however the accounts will only be created upon the initial login to vFire,



therefore it is again recommended to pre populate the vFire System with Users and Analysts using another method such as directly synchronising to an Active Directory Source, bulk import using a CSV file and the CSV Connector or by manual population in order to have a useable system.

Once the Users and Analysts have been pre populated you can then use Resource Matching rules to match to and update the seeded database records with the Identify Provider using the SSO Connector.



SSO Troubleshooting

Issue:	Page cannot be displayed on Sso.aspx
Resolution	<p>Make sure there is an SSL binding for the website. SSL is required.</p> <p>Check that there is an spid in the query string</p> <p>404 indicates non spid or an invalid spid. This must be the Service Provider Identifier and can be Url encoded.</p>

Issue:	Error processing login request. Invalid Login ID or Password Please Verify and re-enter your login information
Resolution	Using the recommended configuration, where SAML Name ID is mapped to User Principal Name by the IdP, the user name will be compared to User Qualified Name (USER_QUALIFIED) and NT Account Name (USER_SAM). Both must equal the User Principal Name, which should be in the form name@domain

Issue:	User Import doesn't seem to work
Resolution	User import may fail if the update would result in a duplicate Login ID (USER_ID), User Qualified Name or NT Account Name/Domain

Issue:	Could not load file or assembly 'Newtonsoft.Json, Version=4.5.0.0, Culture=neutral, PublicKeyToken=30ad4fe6b2a6aeed' or one of its dependencies
---------------	---



Resolution	<p>Add the following to the configuration section of the web.config</p> <pre><runtime> <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1"> <dependentAssembly> <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral"/> <bindingRedirect oldVersion="0.0.0.0-8.0.0.0" newVersion="8.0.0.0"/> </dependentAssembly> </assemblyBinding> </runtime></pre>
------------	--

Issue:	SignatureDescription could not be created for the signature algorithm supplied.
Resolution	<p>The secure hash algorithm used for the Relying Party trust is not set to SHA1. ADFS defaults to SHA256, but this is not supported.</p> <p>Change the hash algorithm to SHA1 on the advanced tab of the Relying Party Trust</p>

Issue:	Assertion Subject does not define a NameID
--------	--



Resolution	User Principal Name should be mapped to Name ID in the IdP claims configuration
-------------------	---

Issue:	I can't see my signing certificate
Resolution	<p>Digital certificates must</p> <ul style="list-style-type: none">• have a private key• must be installed in the local machine certificate store• be accessible to the account running the app pool <p>Core runs under Network Service by default</p> <p>The app pool must have full control of the certificate</p> <p>The friendly name of the certificate should be set to make management easier.</p> <p>SAML connector should now appear in the list of integration connectors:</p>

Issue:	Page Cannot Be Displayed Error after logging into authentication server:
---------------	--



Resolution

Solution 1:

Check that service provider ID in Core matches the SPID in the endpoint url configured in the relying party on the ADFS server

This:

Edit Endpoint

Endpoint type:
SAML Assertion Consumer

Binding:
POST

Set the trusted URL as default

Index: 0

Trusted URL:
i:/localhost/vsm/sso.aspx?spid=651fbef3-d570-493c-93fe-2bd5a779462f
Example: https://sts.contoso.com/adfs/ls

Response URL:
Example: https://sts.contoso.com/logout

OK Cancel

Should match this:



Single Sign On Service Provider Details

User Interface *
vFire Core

Service Identifier *
651fbef3-d570-493c-93fe-2bd5a779462f

Public URI
https://localhost/vsm

Identity Provider *
SAML idP

Solution 2:

If you have created a new self-signed certificate, make sure that the Relying Party properties have been updated by importing the new certificate (and removing the old one).

Export the current certificate:



Server Certificates

Use this feature to request and manage certificates that the Web server can use with web

Filter: [dropdown] Go [dropdown] Show All | Group by: No Grouping [dropdown]

Name	Issued To	Issued E
	WIN-UASROCS4GQR1.alemba...	WIN-UA
	WMSvc-WIN-L2NFBEGGBJS	WMSvc
MyCertific	V9-2-WIN1360114	m... V9-2-W
TestCertifi	m...	V9-2-W

- Import...
- Create Certificate Request...
- Complete Certificate Request...
- Create Domain Certificate...
- Create Self-Signed Certificate...
- View...
- Export...
- Remove
- Enable Automatic Rebind of Renewed Certificate
- Help

Import new certificate to the relying party and remove the old one:



Relying Party Properties [X]

Organization | Endpoints | Proxy Endpoints | Notes | Advanced
Monitoring | Identifiers | Encryption | **Signature** | Accepted Claims

Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiration
CN=V9-2-WI...	CN=V9-2-WIN1...	20/07/2016 13:...	20/07/...

< [Progress Bar] >

Add.. View... Remove...

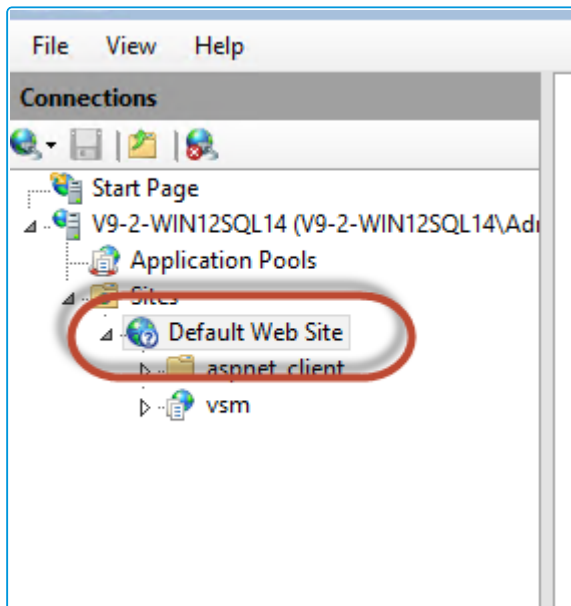
OK Cancel Apply



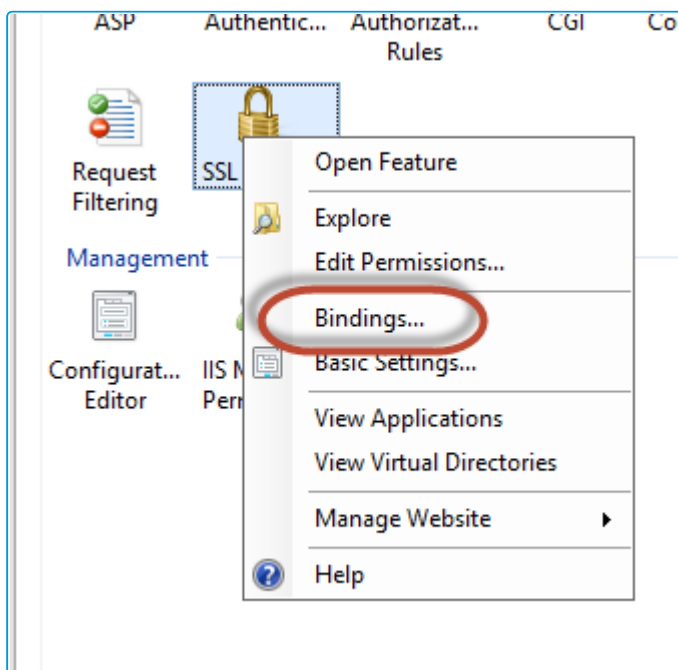
SSL Binding

This topic provides useful information on how to bind an SSL Certificate to your vFire System. This is a requirement for SAML and is therefore needed in order to enable vFire for Single Sign-On.

1. Open **Internet Information Services(IIS) Manager**.
2. Select **Default Web Site** from the **Connections** tree.

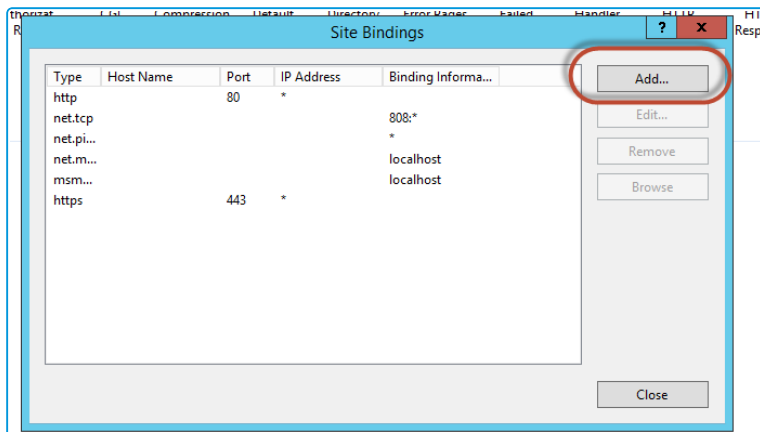


3. Right click on **SSL Settings** and select **Bindings**.

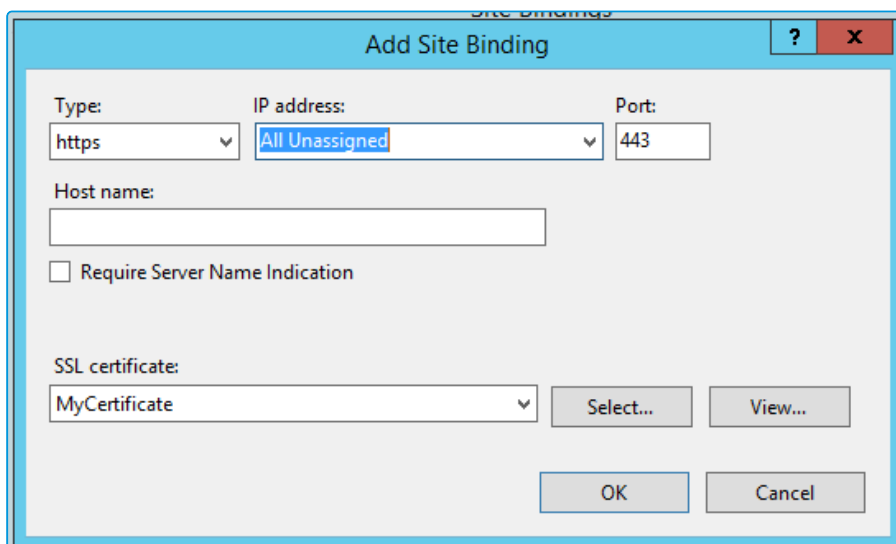




4. In the **Site Bindings** window, select **Add**.



5. Configure the binding as follows:



Set the SSL certificate to the one you have created or installed

6. Click OK.
7. Close the IIS Manager window.
8. Open a command line prompt and reset IIS by using the **iisreset** command.



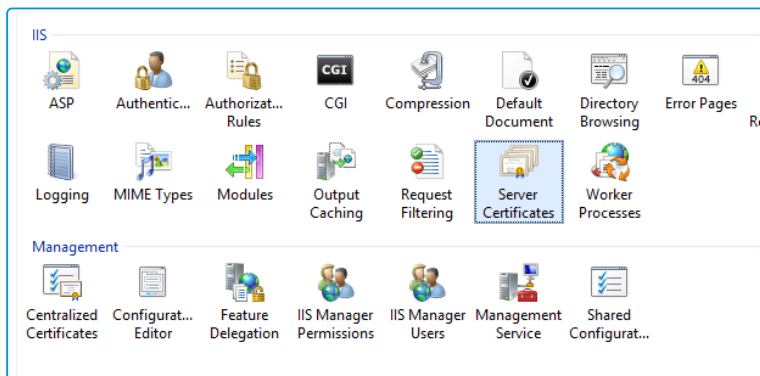
Creating a Self Signed Certificate

This appendix provides useful information on how to create a Self-Signed Certificate on the vFire Web Server. SAML requires an SSL Certificate so for testing purposes you may wish self-signing certificate to be added to the certificate store.

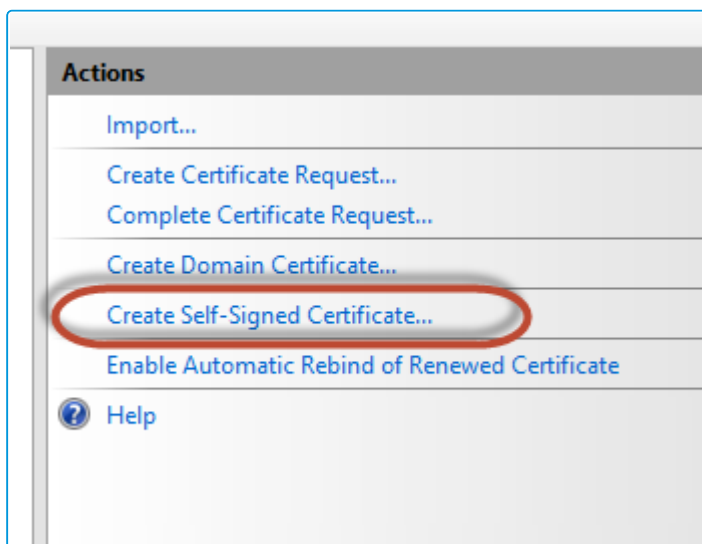


You are also able to use a 3rd Party Certificate as long as this has been installed to the Local Certificate store.

1. Open **Internet Information Services(IIS) Manager**.
2. Select the **Local Machine** from the **Connections** tree
3. Select **Server Certificates** from the IIS section.

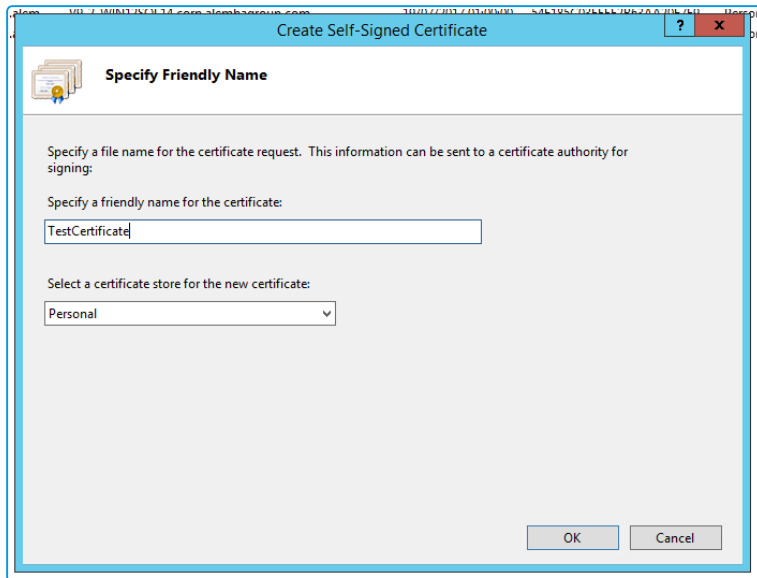


4. Select **Create Self-Signed Certificate**.

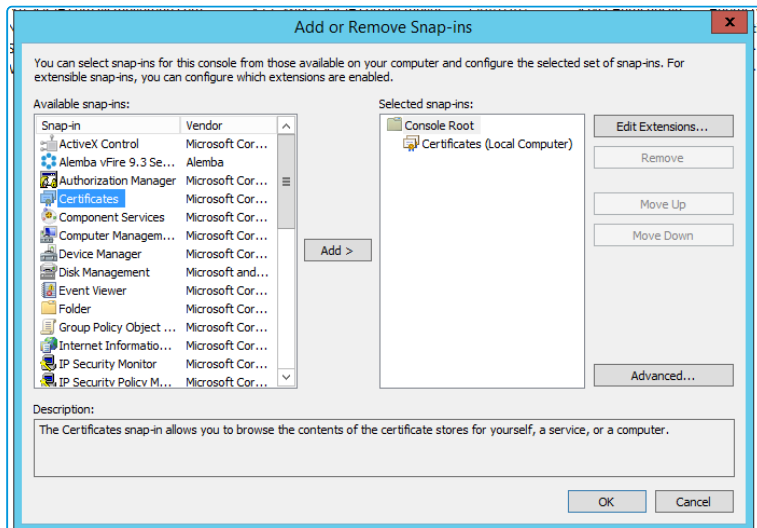




- Assign a friendly name to the certificate.



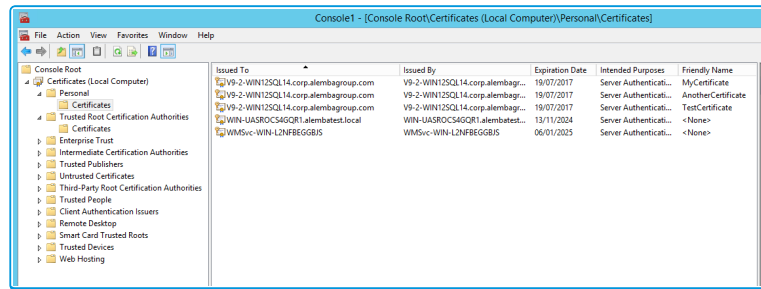
- Click OK.
- Open the **Microsoft Management Console** (type MMC in app search).
- Select **File > Add/Remove Snap-in**.
- Select **Certificates** from the list and click **Add**.



- Select **Computer Account**.
- Click **Next**.
- Select **Local Computer**.
- Click **Finish**.

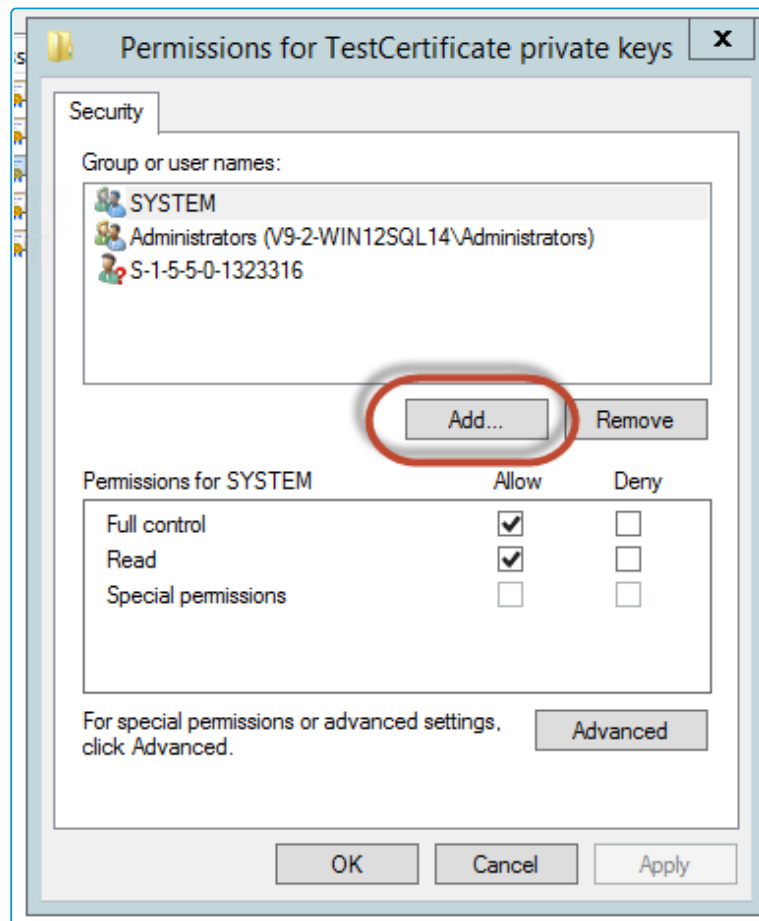


14. Within the MMC Console, expand **Certificates** tree, expand **Personal Tree**, and then



select **Certificates**.

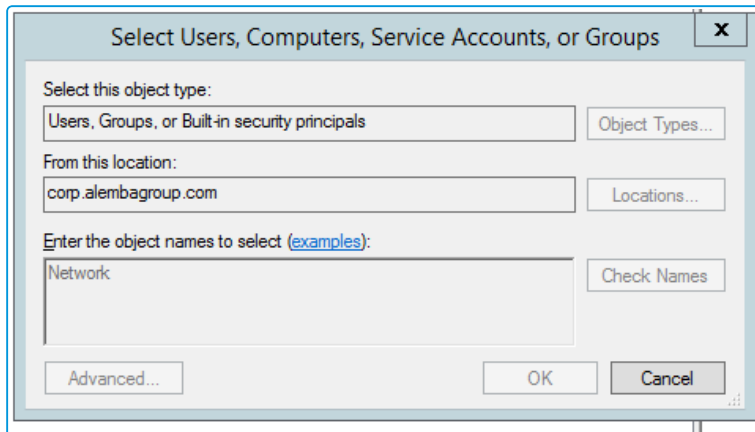
15. Right Click your certificate from the list (check **Friendly Name** column to find the one you just created).
16. Select **All Tasks > Manage Private Keys**.



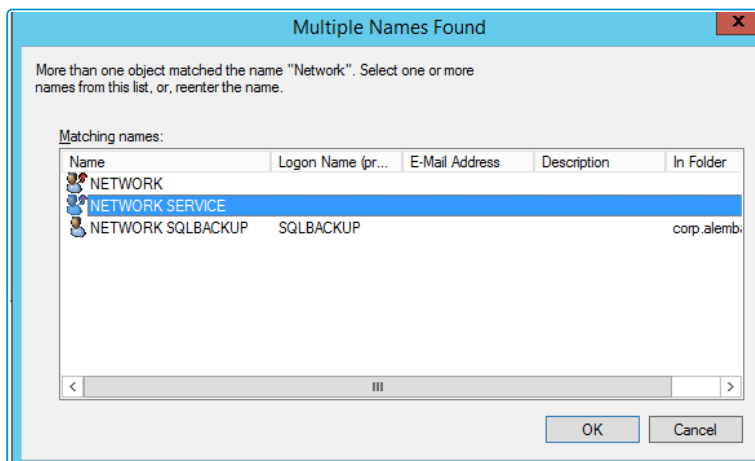
17. Click **Add**.



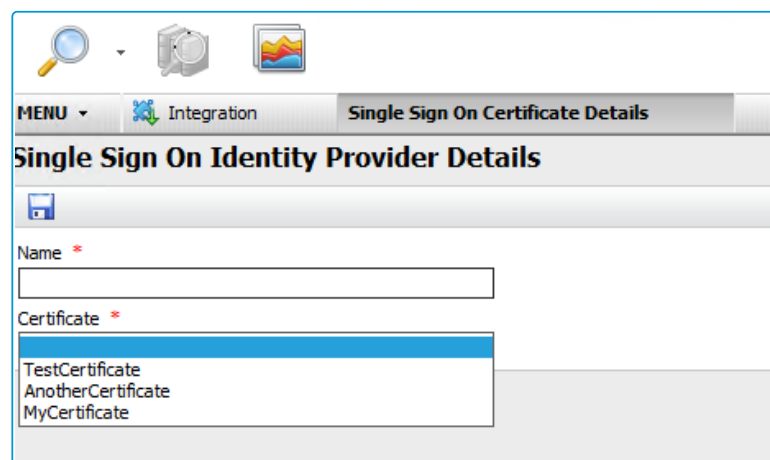
18. In the **Enter the object name to Select** field, type **Network**.



19. Click the **Check Names** button.
20. If prompted, login with your standard domain credentials.
21. Select Network Service from the list.



22. Click **OK**, **Apply** and **OK** again. The certificate should now appear in the list of Signing



Certificates in vFire Core.



Extending the Single Sign-On Connector

The Identity Provider sends a list of key value pairs as claims. Common attributes have been added to the connector, however, this list is not exhaustive or there may be custom attributes that you wish to add.

The ICNF file for the connector is configured with a basic fieldset which makes those claims available in the vFire resource mapping for Field Matching.

```
<fieldSets>

<fieldSet xsi:type="mappedFieldSet" fieldSetID="UserProperties" queryID="TheRow">

<field xsi:type="mappedField" fieldID="Email Address" fieldDisplay="Email Address"
dataType="string" select="Email Address" />

<field xsi:type="mappedField" fieldID="User Name" fieldDisplay="User Name"
dataType="string" select="User Name" />

<field xsi:type="mappedField" fieldID="First Name" fieldDisplay="First Name"
dataType="string" select="First Name" />

<field xsi:type="mappedField" fieldID="Surname" fieldDisplay="Surname"
dataType="string" select="Surname" />

<field xsi:type="mappedField" fieldID="Member Of" fieldDisplay="Member Of"
dataType="string" select="Member Of" />

<field xsi:type="mappedField" fieldID="User Principal Name" fieldDisplay="User
Principal Name" dataType="string" select="User Principal Name" />

<field xsi:type="mappedField" fieldID="Account Name" fieldDisplay="Account Name"
dataType="string" select="Account Name" />

<field xsi:type="mappedField" fieldID="Company" fieldDisplay="Company"
dataType="string" select="Company" />

</fieldSet>
```




</fieldSets>



fieldID in the mappedField corresponds to the name of the claim.

The claim names are user defined, although ADFS uses some standardised names by default.



Given Name in ADFS is sent as

<http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname>

Some of these names are mapped in code to a more user friendly value:


```
Dictionary<string, string> claimTypeAliases = new Dictionary<string, string>
{
    { ClaimTypes.Email, InternalClaimTypes.EmailAddress },
    { GlobalClaimTypes.EmailAddress, InternalClaimTypes.EmailAddress },
    { ClaimTypes.GivenName, InternalClaimTypes.FirstName },
    { ClaimTypes.Surname, InternalClaimTypes.Surname },
    { GlobalClaimTypes.MemberOf, InternalClaimTypes.MemberOf }
};


static class GlobalClaimTypes
{
    public const string EmailAddress =
"http://schemas.xmlsoap.org/claims/EmailAddress";

    public const string MemberOf = "http://schemas.xmlsoap.org/claims/Group";
}
```



```
static class InternalClaimTypes
{
    public const string UserName = "User Name";
    public const string FirstName = "First Name";
    public const string Surname = "Surname";
    public const string EmailAddress = "Email Address";
    public const string MemberOf = "Member Of";
}
```


 SAML supports free text definition of key names for claims (Outgoing Claim Types)


 All Claims are included in the standard vFire Diagnostic Tracing to assist with troubleshooting issues.

Adding New Claims to the ICNF File

Additional claims can be defined by the Identity Provider. To make them available to the connector, those claims must be added to the ICNF File.


To add support for a custom claim, you simply need to add a new field to the existing fieldSet.

 `<field xsi:type="mappedField" fieldID="Custom Claim Name" fieldDisplay="The name to display in the resource mapping drop down" dataType="string" select="Custom Claim Name" />`

 Each SAML claim can define one or more values. E.g. a user could have multiple Email Addresses.

In this case, the claim values are received as a list. This list is then converted to a semi-colon separated string.



 a.user@alembagroup.com;auser@alembagroup.com

This value can then be parsed in the Resource Mapping by using a Transform.



Azure Multi-factor Authentication

This documentation provides a high level introduction to vFire Core and Azure Multi-factor Authentication with Azure Active Directory.

Multi-factor authentication (MFA) is a method of authentication that requires the use of more than one verification method and adds a critical second layer of security to user sign-ins by requiring the following verification methods:

- Something you know (typically a password)
- Something you have (a trusted device that is not easily duplicated, like a phone)

The security of multi-factor authentication lies in its layered approach. Compromising multiple authentication factors presents a significant challenge for attackers. Even if an attacker manages to learn the user's password, it is useless without also having possession of the trusted device. Should the user lose the device, the person who finds it won't be able to use it unless he or she also knows the user's password.

Azure Multi-factor Authentication helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It delivers strong authentication via a range of easy verification options —phone call, text message, mobile app notification or verification code.

Alemba use **Azure Multi-factor Authentication*** in conjunction with the Alemba SSO integration module, to provide connectivity to **Azure Active Directory*** with SAML authentication.

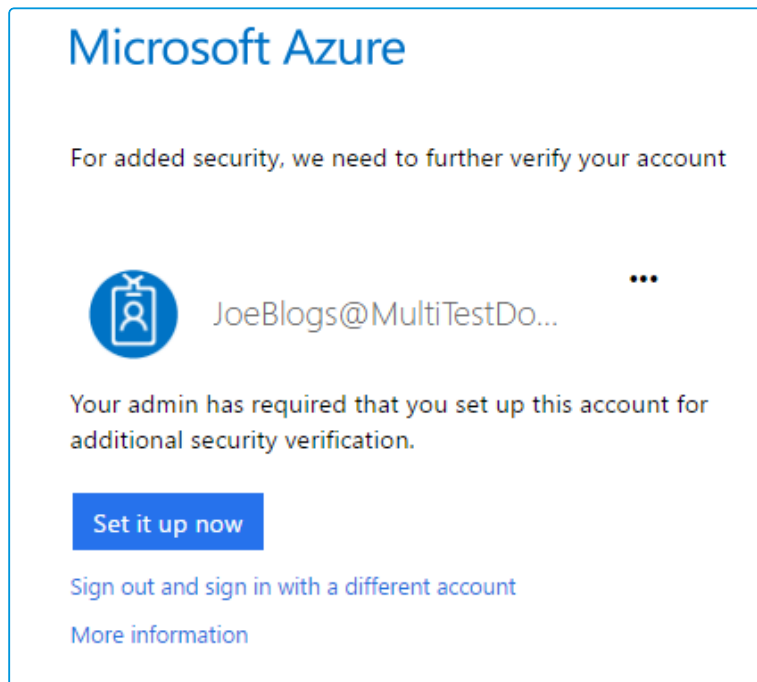


*Azure Services are not provided as part of the Alemba Cloud offering, pricing and further information on Azure can be found at <https://azure.microsoft.com>



Multi-factor Authentication User Transaction Steps for vFire

The vFire User or Analyst makes a request to access the application by loading an appropriate vFire URL in a Browser. The vFire application will detect this request and generate a SAML request, vFire then redirects the User/Analyst's browser to the Azure



Portal URL.

The Azure Authentication Service detects that the user has been configured to use the Multi-factor Authentication Service and the user is directed to a configuration page. The Users selects from a predefined set of verification methods:


- Phone call
- Text message
- Mobile app notification – allowing users to choose the method they prefer
- Mobile app verification code



Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Azure Authenticator app for *Windows Phone, Android* or *iOS*.
2. In the app, tap on 'Add account'. This will launch the camera.
3. Scan the image below.



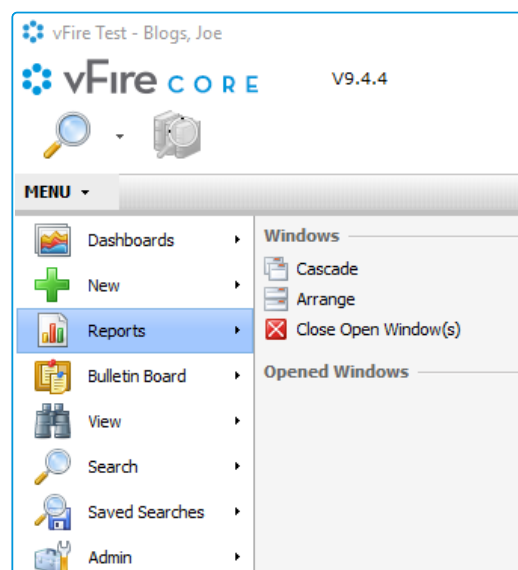
Configure app without notifications

If you are unable to scan the image, enter the following information in your app.
 Code: 128 333 207
 Url: <https://cys01pfpad01.phonefactor.net/pad/489885263>

If the app displays a six-digit code, you are done!

Done

Once the user has chosen and configured their preferred verification method the setup of MFA is complete. The user is then able to login and verify their account with the method selected. User Configuration of MFA is only required on the User/Analyst first login with



Azure Multi-factor authentication.

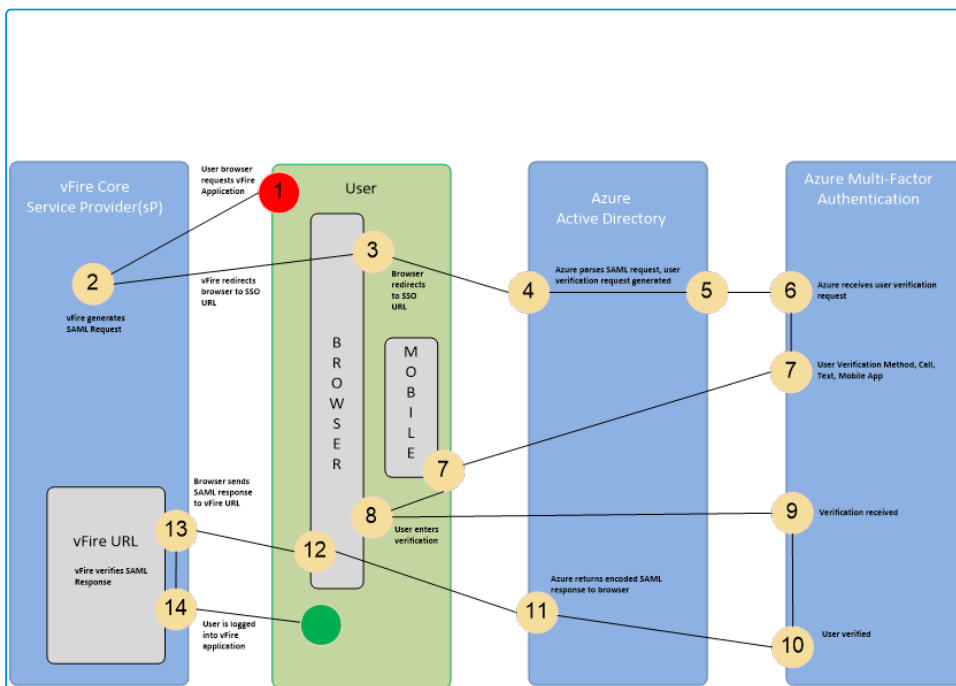
Azure Multi-Factor Authentication authenticates the User/Analyst. The SAML Response is then passed back to the User/Analyst's Browser which is then sent to the vFire URL, once vFire verifies this response the User/Analyst is logged into the vFire application.



Multi-Factor Authentication Technical Transaction Steps for vFire

The User/Analyst browser requests the vfire url to login to the application. vFire SSO intercepts the request and redirects the User/Analyst browser to the Azure portal login. The Azure portal login accepts the User/Analyst AD credentials and request multi-factor authentication from the User/Analyst. At the same time the Azure MFA service provides the User/Analyst with the method for multi-factor authentication.

The User/Analyst supplies the multi-factor authentication to the Azure portal login, which is then passed to the MFA service. Once the MFA verification is authorized, the Azure AD service will generate a SAML assertion which is passed back to the User/Analyst browser. This in turn is passed back to the vFire Core SSO service for verification. Once the SAML assertion is verified the User/Analyst is logged in and redirected to the vFire Core application.





Configuring Azure Active Directory discovery

This topic describes how to configure Azure Active Directory discovery through Secure Lightweight Directory Access Protocol (TLS 1.2).

Configuring vFire Core

Core can be easily configured to scan your Azure Active Directory using the Active Directory Connector secured with SSL.

1. Configure your active Directory Connector integration with the Azure Domain in the LDAP server path. This must match the certificate name. If you are using a wild card SSL certificate for your domain, then you will need to preface the address with Azure.

Integration Source Details

Name: MultiTestDomain Pull | Status: Active

Connector: Microsoft Active Directory Connector | (Assembly.TypeName) Infra.Connector.LDAP.AD.ADConnector

Connection Parameters

Ionix Service Manager Active Directory Connector

LDAP Server Path: LDAP://AZURE.alembatest.com

Login ID: bob@alembatest.com

Password: [Redacted]

Server Bind SSL Kerberos/NTLM


Advanced

NT Domain Name: [Empty]


Delete Disabled Person Records

Authentication

Authenticate Imported People against Source

 *.alembatest.com would be configured as LDAP://Azure.alembatest.com

2. Configure your security settings per your requirements, if you are using the SSO connector for authentication do not check “authenticate imported people at source”.
3. Configure your Resource and Filed mapping values as per the AD connector guide.

 If you are using the SSO connector for authentication you must ensure your Matching Fields are configured to match existing user on the AD and SSO connectors.



Configuring Azure Active Directory.

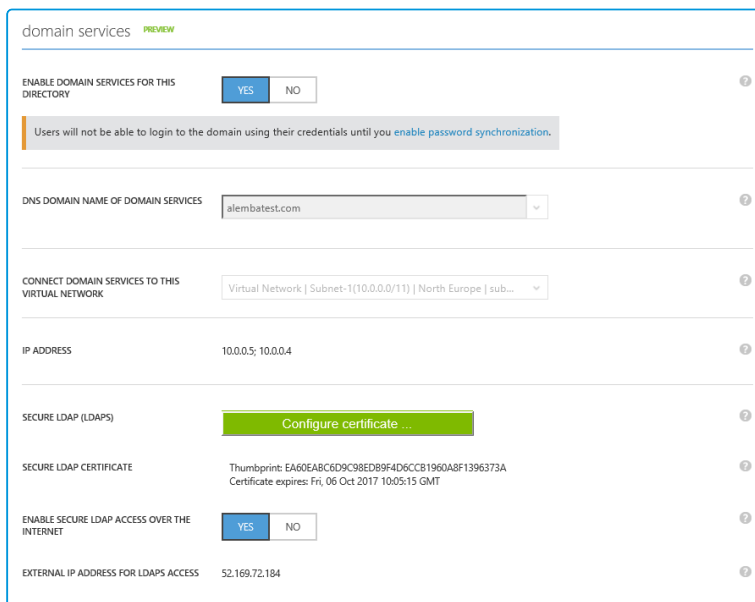
To configure the Azure Active Directory to allow LDAPS connections you will need to navigate to your Azure Active Directory using the older Azure portal at <https://manage.windowsazure.com>

1. Navigate the Active Directory and Domain you wish to configure and select the



Configure tab.

2. Scroll down to the “domain service” section and enable Domain Services.



3. You will then need to configure your LDAPS certificate which will need to be uploaded to Azure in PFX format.
4. Once you have configured your certificate enable. Enable **Secure LDAP Access over**



the Internet.



5. Once enabled, you will need to ensure you have the relevant Entries in your Domain DNS records to point to the IP address shown in the “External IP Address for LDAPS Access” field.



Further information on configuring AZURE LDAPS can be found at <https://azure.microsoft.com/en-gb/documentation/articles/active-directory-ds-admin-guide-configure-secure-ldap/#requirements-for-the-secure-ldap-certificate>



Further Information

Product Information and Online Support

For information about Alemba products, licensing and services, visit www.alemba.com.

For release notes and software updates, go to www.alemba.help.

Up-to-date product documentation, training materials and videos can be found at www.alemba.help/help.



You may need to register to access some of these details.

Technical Support

For technical support, please visit: www.alemba.com and select the **vfire support** link. You will need to log in to the alemba self service portal to contact the Alemba Service Desk.

Comments and Feedback

If you have any comments or feedback on this documentation, submit it to info@alembagroup.com.

