vFire

Single Sign-On Technical Reference Guide Version 1.3





Table of Contents

Version Details
Online Support
Comments and Feedback 4
Copyright
About this Document
Intended Audience
Standards and Conventions
About Single Sign-On using the SAML based Connector
The SAML Transaction Steps for vFire7
Glossary of Terms
Technical and Access Requirements
Supported Interfaces
Configuring vFire for Single Sign-On
Importing Identity Provider Metadata
Adding an Identity Provider13
Deleting an Identity Provider
Installing a Service Provider Signing Certificate
Adding a Signing Certificate15
Configuring the Service Provider
Adding a Service Provider



Deleting a Service Provider	23
Exporting Service Provider Metadata	24
Importing Service Provider metadata into the Identity Provider	
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	
Adding New Claims to the ICNF File	
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	
Technical Support	59
Comments and Feedback	



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

Nou 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.
Ţ	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

It is 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	\checkmark
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.

Menu +	💐 Integra
Links	
Favorites	Main
🗸 Integra	ation
Integ	pration Platform Settings
Conn	ectors
Sour	ces
Sche	duling
Reso	urces
Links	
Even	ts
Outb	ound Actions
Inbo	und Actions
Activ	ity
Single :	Sign On
Signi	ng Certificates
Iden	tity Providers
Servi	ce Providers

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:

- 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.

Version 1.3 © Alemba 2017



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.

Single Sign On Identity Provider Details	
Name *	
Secure Hash Algorithm	
SHA-1	
Metadata	
	^
	\sim

3. Complete the details.

Name Add a Display Name for the Identity Provider.



Secure Hash	Choose SHA-1 or SHA-256 from the dropdown list.
Algorithm	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 同 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. 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.

Contraction of the second of the secon							
	vFire System1 - Trigg, Kris (Central) - [Integration]				-		×
Image: Second	VHIPCORE V9.3.0						
Image: Bargener Image: Bar	🖌 v 🁙 v 📴 v 🏥 v	🛨 - 🔎 - 🔯 🦉 - 🚊 - 🌌 - 🖄 - 🔀	Call No	* *	Central		v
Indulation Sping Contributions Indulation	HEAU - 👯 Integration					- 6	×
Image:		Installed Signing Certificates					
Image: Second Contract Image: Second Contract<	Links						
Internal Today Control		In the ball ball ball ball ball ball ball bal					-
Second	Favorites Nain	IB Express Development Certificate					
Conversion of the second secon	 Integration Integration Rations 	Alerba code Signing					
Rear Banar B	Connectors						
Restores Here The Constraints Server Server Server Server Server Server Server Server Se	Sources Extend date						
produced and an an and an	Resources						
Subset Agen Share a "Web Agen Better Needen Detter Needen Detter Needen	Links Duestr						
i Referin Con Elipsopo Con Elipsopo Elipsop	Dutbound Actions						
- Public Bug Box Here Brown Berte Brown Berte Brown Here Brown	Inbound Actions Activity						
Includes Serve Produce	→ Single Sign On						
	Signing Certificates Identity Providers						
	Service Providers						
· · · · · · · · · · · · · · · · · · ·							
							v

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



Complete the details.

NameAdd a Display Name for the Signing Certificate

CertificateChoose a Certificate to make this available to your ServiceProvider (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



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

Private key protection To maintain security, the private key was protected with a password.
Type the password for the private key.
Next Can



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

General Details Certification Path Show: Field Value Version V3 Serial number Signature algorithm sha256RSA Signature hash algorithm sha256 Valid from Valid to	General Details Certification Path Show: <all> Field Value Version V3 Serial number Signature algorithm Signature hash algorithm sha256RSA Signature hash algorithm sha256 Valid from Valid to Valid to Subject</all>	General Details Certification Path Show: <all> Field Value Version V3 Serial number Signature algorithm Signature hash algorithm sha256RSA Issuer Valid from Valid to Subject</all>	🗾 Certificate				>
Show: <all></all>	Show: <all></all>	Show: <all></all>	General Details C	ertification Path			
Field Value Version V3 Serial number Signature algorithm Signature hash algorithm sha256RSA Signature hash algorithm sha256 Issuer Valid from Valid to Value Subject V	Field Value Wersion V3 Serial number Signature algorithm Signature hash algorithm sha256 Issuer Valid from Valid to Valie Subject V	Field Value Version V3 Serial number Signature algorithm Signature hash algorithm sha256 Issuer Valid from Valid to valid to Subject valid	Show: <all></all>		\sim		
Signature algorithm sha256RSA Signature hash algorithm sha256 Issuer Valid from Valid to	Edit Properties	Edit Properties	Field	N	/alue	^	
Signature hash algorithm sha256 Signature hash algorithm sha256 Valid from Valid to	Signature hash algorithm sha256 Issuer Valid from Valid to Valid to Subject V	Signature hash algorithm sha256 Issuer Valid from Valid to Valid to Subject V	Signature algor	ithm s	sha256RSA		
Valid to	Edit Properties	Edit Properties	Signature hash	algorithm s	sha256		
	Edit Properties Copy to File	Edit Properties Copy to File	Valid to			~	
	Edit Properties Copy to File	Edit Properties Copy to File					
	Edit Properties Copy to File	Edit Properties Copy to File					
				Edit	Properties	Copy to File	

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.

• vFire core					- 0 ×
🕜 x 🧶 x 🜔 x 🟥 x 1	🛨 - 🖉 - 🐚 👖 - 🗎	- 🔜 - 🛒 - 🔀 -		Cal No	Central v
HIAU - Kategra.					• _ 8 ×
	Service Providers				
Links					0
	Unique Identifier	Partition	Source	URL	Certificate ^
Pavonses Plan	Ny Special Service	Unspecified	Service Desk	https://localhast/Infra.Web	IIS Express Deve
✓ Integration	fad 4fc 14-bbf7-4280-a90d-ebdbc7fc60e6	Unspecified	Self Service Portal	https://localhost/Infra.Web	Alemba Code Sig
Connectors	3236200 0915 4106-8883 (1546691412	Unspectred	VHIC POILS	https://iocanosq1ma.web	Herios Coce sig
Sources					
Resources					
Unis					
Dutbound Actions					
Inbound Actions					
v Single Sign On					
Signing Certificates					
Service Providers					
					~
	٨				>



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

🗘 vFire System1 - Trigg, Kris (Central) - (Single Sign On Service Provider Details)			-		×
VEIRe constant					
$\left(\begin{array}{cccc} & \cdot & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot & \cdot \\ & \cdot & \cdot$	Call No	- *	Central		×
HTNU + 🐹 Integration Stable State On Service Provider Deta.				- 1	XR
Nada Cian On Consider Devider Debile			_	-	-
mige sign on service provider becaus					^
					9
User Interface *					
vitie Core v					
Service Identifier *					
ol Selon seuros					
Male LM *					
Insue (possible op an et new					
MPR V					
re					
IS Fourse Development Certificate					
Resource Mazzina					
SAME Import - Person					
Service Provider Netadata					
Automatical and a standard and a					

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.



ldentity 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 by 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

Call Nequel: Viox View	n New Search Times Bulleon	Reports Dashbid Admin	Eat		
ENJ - 👯 Integra	0				· _ 6
	Service Providers				
inks					
Fevorites Nain	Unique Identifier	Partition	Source	URL	Certificate
Intraration	fed4fc14-bbf7-4239-e50d-ebcbc7fct0e5	Unspecified	Self Service Portal	https://ocahoet,Enfra.Web	Alemba Code
Integration Platform Settings	323ec200-0915-4336-8ba3-c15ff6691f12	Unspecified	vFire Portal	https://localhost/thifea.Web	Alemba Code
Connectors					
Scherkeinn					
Resources					
Links					
Events					
Initia and Actions					
Activity					
Single Sign On					
Signing Certificates					
Loensty Providers Service Droviders	_				
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.

	Service Providers
Links	🔳 🔂 🔜 🕞 🕒
	Unique Identifier
Pavorites Main	651fbef3-d570-493c-93fe-2bd5a779462f
 Integration 	
Integration Platform Settings	
Connectors	
Sources	
Scheduling	
Resources	
Links	
Events	
Outbound Actions	
Inbound Actions	
Activity	
▼ Single Sign On	
Signing Certificates	
Identity Providers	
Service Providers	



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

ingle Sign On Service Provi	ider Details
Iser Interface *	
vFire Core	×
ervice Identifier *	
551fbef3-d570-493c-93fe-2bd5a779462f	×
Public Url	
https://localhost/vsm	
dentity Provider *	
SAML idP	\checkmark
Signing Certificate *	
MyCertificate	V
Resource Mapping	
SAML - SAML Mappings	✓
ervice Provider Metadata	
VindLinky Opeon QWD Ammissamp ¹² units Samp ²³	n anie a custerie 2000 (100000000000000000000000000000000
cds:X509Cerbifacte >MIDDDCCAFSqwiBAg1 QDERWOSQLWIJTGU JPMUTQUEYCES WMDAWWJAMSDWKYDVQQE/RWOSQLW JDERAUQAHEDWAWGB/CABABC + 1458 307H1VGRU2ahdonAfpdHazE + 420,0WY 44 247H1VGRU2ahdonAfpdHazE + 420,0WY 44 2462 * 30,4MOQ29 499ER J, 0HV 672,258W 44 PJ 247BH0240 AB 100,000 AB 100,000 AB 100,000 247BH0240 AB 100,000 AB 100,000 AB 100,000 AZ 7BH0240 AB 100,000 AB 100,000 AB 100,000 AZ 7BH0240 AB 100,000 AB 100,000 AB 100,000 AD 100,000 AB 100,000 AB 100,000 AD 100,000 AB 100,000 AB 100,000 AB 100,	IQIW: IBDXAFLZNIA:spelbb 2DDANBgichiloG9W0BAQLFADA/M50wKW1DV IbbQYImFnem9 (LS5)b2wihch01YWhizIMTDy12A2Who1MYCw12MMD /dTTjFyU JFMMTQU/29yCS5h6VYImFnem9 LC5b20wg0EMA0GC5qGSb /g5/lk.wc/4226W08qTfw0izQCV/U0GTo5e4C9/Vp06qScf07RvR-R948ULap55 caWihNum19YWB6b3c5Gd2vgF1CJxsFBygI4qqzy7TAxdpHc12CFCQU2 0023dBabCv9x9anHt5j6ewAy2g71SD2.cK9MPQsfc07RvR-R946ULap55 D023dBabCv9x9anHt5j6ewAy2g71SD2.cK9MPQsfc07RvR-R946ULap57 JBBgTBWchBigKi2HSX5+ug8BbL/JV72x9T+07+XYQ4P4A5QJDAWA M6gFBQCATABdqk/dk59W0BQLFAACCQC4PAB(JFauv)eV14V1/Zjep pslv xL1PmW19Fh0Ts+1281aEb6fw1V72y9T+02-55fc8/ft503LSYNCYC+ #H0W2Mh1MU/QdEb2La+x55fc20/19dmeKx8ft7WU7nSPc1L9FCU2 W101La = xc/6V590Partificase

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.

🗭 🔿 🖄 📰 📓 📷	· ·	
Consoler Adult AD FS A Service Endpoints Certificates Claim Descriptions Dutinopione	Add or Remove Snap-ins Vou can select anap-ins for this console from those available on your computer and configure the sele- extended may-ray, you can configure which extensions are enabled. Available may-ins: Selected anap-ins:	ted set of snap-ins. For
Trust Kelationships Claims Provider Trusts Relying Party Trusts Attribute Stores	Snap-in Vendor Come University County County AD FS Management Microsoft Cor Console Root Console Root Cons	Edit Extensions Remove
A A Authentication Policies Per Relying Party Trust	Computer Services Moraselt Car Computer Managem Moraselt Car Computer Managem Moraselt And Moraselt And Moraselt Car Grave Policy Object Moraselt Car Grave Policy Object	Move Up Move Down
	B P Security Monitor Microsoft Cor B P Security Noticy Microsoft Cor Description:	Advanced
	The ActiveX Control snap-in enables you to add an MMC node with a results view containing an Activ	OK Cancel

- 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.

\$	Add Relying Party Trust Wizard
Select Data Source	
Select Data Source Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance 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 the federation metadata and 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. New relation metadata file location: C:\Users\Desktop\wetadata tod C:\Users\Desktop\wetadata tod Import data about the relying party organization. Import data about the relying party manually Use this option to import the necessary data about this relying party organization.
	< Previous Next > Cancel

13. Click Next

14. Enter a **Display Name** for the party trust.

\$	Add Relying Party Trust Wizard	
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	Test	
Specify Display Name	Notes:	
Configure Multi-factor Authentication Now?	<u>^</u>	
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
 Finish 	· · · · · · · · · · · · · · · · · · ·	
	< Previous Next > Cancel	
	< Previous Next > Cancel	

Version 1.3 © Alemba 2017



- 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.

\$ 1	Add Relying Party Trust Wizard
Steps Welcome Select Data Source Select Data Source Specify Display Name Configure Muti-factor Authentication Now? Choose Issuance Authentication Nules Ready to Add Trust Finish	Add Relying Party Trust Wizard Corfigure multifactor authentication settings for this relying party trust. Multifactor authentication is required if there is a match for any of the specified requirements. Multifactor Authentication Global Settings Requirements Users/Groups Not configured Device Not configured Location Not configured Location Not configured Configure multifactor authentication settings for this relying party trust at this time. Orifigure multifactor authentication settings for this relying party trust at this time. Configure multifactor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u> .
	< Previous Next > Cancel

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



- 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.

Display Name	Enabled	Туре	Identifier
Device Registration Service	Yes	WS-Trust / SAML / WS-Federation	um:ms-drs:it-a
Service Desk	Yes	WS-Trust / SAML / WS-Federation	My Special Se
Self Service	Yes	WS-Trust / SAML / WS-Federation	fad4fc14-bbf7
Dev System	Yes	WS-Trust / SAML / WS-Federation	5d3bb22f-7ce
vFire Officer	Yes	WS-Trust / SAML / WS-Federation	c45f3a3d-53d
	Edit Claim Ru Disable Properties Delete Help	iles	

- 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.

LI DEV OVSLETI	THS VV.5-TUUSEZ. 28/00 Z.VV.5-TRUBHUDD 30.3007Z1-Z089-9312-200-808704011009
Q	Add Transform Claim Rule Wizard
Select Rule Template	
Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
 Configure Claim Rule 	Claim rule template: Send LDAP Attributes as Claims
	Claim rule template description.
	Using the Serd 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 authoriccated users from the displayNume and ItelphoneNumber Active Directory attributes and them send those values as two different outgoing claims. This rule may also be used to send all of the user's group methodenships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.
	< Previous Next > Cancel

- 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.

	Edi	t Ri	ule - test Rule	×
You which issu	can configure this rule to send the values ch to extract LDAP attributes. Specify how ed from the rule.	s of L / the	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be	F
Clair	m rule name:			F
test	Rule			
Bule	e template: Send I DAP Attributes as Claim	19		-
Attri	bute store:			
Acti	ive Directory		v	
Mar	pping of LDAP attributes to outgoing claim	type	e'	
	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)	
	User-Principal-Name	~	Name ID Name ID	7
	Given-Name	~	first name	7
	Sumame	~	Sumame	7
	E-Mail-Addresses	~	E-Mail Address	7
•		~		7
				ノ
Vie	ew 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.

	Relyin	g Party Pro	opertie	S	x
Organization	Endpoints	Proxy Endpoints Notes Advance		Advanced	
Monitoring	Identifiers	Encryption	Signatu	ure Acc	cepted Claims
Specify the display name and identifiers for this relying party trust. Display name: Relying Party Relying party identifier:					
	Toornamor.				Add
Example: htt	ns://fs.contos	com/adfs/se	arvices/tr	ust	7 1010
Palice and state that					
CE1fbof2.dE	70 4020 0260	bd5-770463		r	_
L		ОК	C	ancel	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.



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

Relying Party Properties
Monitoring Identifiers Encryption Signature Accepted Claims
Specify the secure hash algorithm to use for this relying party trust.
Secure hash algorithm: SHA-1
OK Cancel Apply

Identity Provider details.

16. 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 formal, 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 Attrib ute Displa y	ADFS Outbo und Claim Displa y *	ADFS Outbound Claim Actual rted To		vFire ICNF
Nam e ID	Name ID	Name ID	Name ID	User Name	User Nam e
First Nam e	Given- Name	Given Name	http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/givenname	First Name	First Nam e
Surna me	Surna me	Surna me	http://schemas.xmlsoap.org/ws/2005/05/identit y/claims/surname	Surna me	Surna me
Email Addr ess	E- Mail- Addre sses	E- Mail Addre ss	http://schemas.xmlsoap.org/claims/EmailAddre ss	Email Addre ss	Email Addr ess
First Nam e	Given- Name	First Name	First Name		First Nam e

*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 (must be same as User Qualified Name)	
Login ID	User Name	User Name (must be unique)	
NT Domain Name	Must be blank	Must be blank	

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

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

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

lssue:	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



Resolution	Add the following to the configuration section of the web.config
	<runtime></runtime>
	<assemblybinding xmlns="urn:schemas-microsoft-com:asm.v1"></assemblybinding>
	<dependentassembly></dependentassembly>
	<assemblyidentity <="" name="Newtonsoft.Json" th=""></assemblyidentity>
	publicKeyToken="30ad4fe6b2a6aeed" culture="neutral"/>
	<bindingredirect <br="" oldversion="0.0.0.0-8.0.0.0">newVersion="8.0.0.0"/></bindingredirect>

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

Assertion Subject does not define a NameID
--



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

lssue:	I can't see my signing certificate
Resolution	 Digital certificates must have a private key must be installed in the local machine certificate store be accessible to the account running the app pool Core runs under Network Service by default The app pool must have full control of the certificate The friendly name of the certificate should be set to make management easier. SAML connector should now appear in the list of integration connectors:

lssue:	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: Set the trusted URL as default Index: Set the trusted URL as default Index: Set the trusted URL as default Encode URL: Set the trusted URL:
	Example: https://sts.contoso.com/logout OK Cancel
	OK Cancel Apply
	Should match this:



Single Sign On Service Provider Details
User Interface *
vFire Core
service Identifier *
651fbef3-d570-493c-93fe-2bd5a779462f
Public ori
https://localhost/vsm
Identity Provider *
SAML idP
Solution 2:
If you have created a new self-signed certificate, make sure that the
Relving Party properties have been updated by importing the new
certificate (and removing the old one).
Export the current certificate:



Use this feature Filter:	• to request and manage certif	show All	Group by: No Group	ing •	
Name	•	Issued T WIN-UA	o SROCS4GQR1.alemba. WIN LONEREGORIS	Issued E WIN-UA	
MyCertific TestCertifi	Import Create Certificate Request Complete Certificate Reque Create Domain Certificate Create Self-Signed Certificat View Export Remove Enable Automatic Rebind of Help	f Renewed	d Certificate	V9-2-W V9-2-W	



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 Subject Issuer Effective Date Expiration 20/07/2016 13 20/07/2016 13 20/07/2016 13 CN=V9-2-WI CN=V9-2-WIN1 20/07/2016 13 20/07/2016 13 20/07/2016 13 Add View Remove OK Cancel Apply		Relying Par	ty Properties	X
Monitoring Identifiers Encryption Signature Accepted Claims Specify the signature verification certificates for requests from this relying party. Subject Issuer Effective Date Expiration Subject Issuer 20/07/2016 13: 20/07/2016 13: Add View Remove Add OK Cancel Apply	Organization	Endpoints Proxy En	dpoints Notes	Advanced
Specify the signature verification certificates for requests from this relying party. Subject Issuer Effective Date Expirative party is the second	Monitoring la	dentifiers Encryption	Signature Acc	epted Claims
Subject Issuer Effective Date Expiration CN=V9-2-WI CN=V9-2-WIN1 20/07/2016 13 20/07/2 <	Specify the signa party.	ature verification certificat	es for requests from th	is relying
Image: CN=V9-2-WI CN=V9-2-WIN1 20/07/2016 13: 20/07/2 Image: CN=V9-2-WI Image: CN=V9-2-WIN1 20/07/2 20/07/2 Image: CN=V9-2-WI CN=V9-2-WI X X Image: CN=V9-2-WI X X X X Image: CN=V9-2-WI X X X X X Image: CN=V9-2-WI X X X X X X <td>Subject</td> <td>Issuer</td> <td>Effective Date</td> <td>Expiratio</td>	Subject	Issuer	Effective Date	Expiratio
III > Add View Remove OK Cancel Apply	🕮 CN=V9-2-	WI CN=V9-2-WIN1	. 20/07/2016 13:	. 20/07/:
Add View Remove OK Cancel Apply	<			>
OK Cancel Apply	Add	View	Remove	
		ОК	Cancel	<u>A</u> pply



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.

File	View Help					
Conne	ctions					
Q- [i 🚈 象					
····	Start Page					
⊿¶	V9-2-WIN12SQL14 (V9-2-WIN12SQL14\Adı					
	Application Pools					
(Gites Gites Default Web Site Default Client					
	⊳ 😭 vsm					

3. Right click on SSL Settings and select Bindings.

ASP Authenti	c Authorizat CGI Cor Rules
8	
Request SSL	Open Feature
Filtering	Explore
Management	Edit Permissions
	Bindings
Configurat IIS N 🗐	Basic Settings
Editor Perr	View Applications
	View Virtual Directories
	Manage Website 🔹 🕨
	Help



4. In the Site Bindings window, select Add.

orizat	· · · · ·	List Lompressu	n Llet	ault Directory	Fror Varier	Failed H	andler HITP	нп
				Site Bir	dings		? X	Respo
						1		
F	Туре	Host Name	Port	IP Address	Binding Informa		Add	
	http		80	*				
	net.tcp				808:*		Edit	
	net.pi				*			
	net.m				localhost		Remove	
	msm				localhost			
	https		443	*	localitost		Browse	
	nups		449					
							Close	
							Close	

5. Configure the binding as follows:

	0100-011	rannga	
	Add Site Binding	I	? X
Type: https ✓	IP address: All Unassigned	Port:	
Host name:			
Require Server Nan	ne Indication	I	
SSL certificate:			
MyCertificate	~	Select	View
	[ОК	Cancel

🚫 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.





5. Assign a friendly name to the certificate.

لح	002 V0.7 WINT7SCU 14 corp alombagroup.com 10/07/2017/01/00/00 54E195/ 02ELEE2952A.6	/0E /EQ	Borcon
1	Create Self-Signed Certificate	?	× m
	Specify Friendly Name		
	Specify a file name for the certificate request. This information can be sent to a certificate authority for signing:		
	Specify a friendly name for the certificate:		
	TestCertificate		
	Select a certificate store for the new certificate:		
	Personal V		
	ОК С	ancel	

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

aliable shap-INS:		_	1	Selected snap-ins:	
nap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Certificates (Local Computer)
Alemba vFire 9.3 Se	Alemba				Kemove
Authorization Manager	Microsoft Cor	≡			
Certificates	Microsoft Cor				Move Up
Component Services	Microsoft Cor				
Computer Managem	Microsoft Cor				Move Down
Device Manager	Microsoft Cor		Add >		
🔮 Disk Management	Microsoft and				
🛃 Event Viewer	Microsoft Cor				
🗎 Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor	~			Advanced
scription:					
scripuon:					

- 10. Select Computer Account.
- 11. Click Next.
- 12. Select Local Computer.
- 13. Click Finish.

Version 1.3 © Alemba 2017



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

File Action View Favorites Window He	ip				
🗢 🔿 🙍 🛅 📋 🤕 📷					
Console Root	Issued To A	Issued By	Expiration Date	Intended Purposes	Friendly Name
a 🙀 Certificates (Local Computer)	💱 V9-2-WIN12SQL14.corp.alembagroup.com	V9-2-WIN12SQL14.corp.alembagr	19/07/2017	Server Authenticati	MyCertificate
4 🚞 Personal	💱 V9-2-WIN12SQL14.corp.alembagroup.com	V9-2-WIN12SQL14.corp.alembagr	19/07/2017	Server Authenticati	AnotherCertificat
Certificates	💱 V9-2-WIN12SQL14.corp.alembagroup.com	V9-2-WIN12SQL14.corp.alembagr	19/07/2017	Server Authenticati	TestCertificate
a 🚞 Trusted Root Certification Authorities	WIN-UASROCS4GQR1.alembatest.local	WIN-UASROCS4GQR1.alembatest	13/11/2024	Server Authenticati	<none></none>
Certificates	WMSvc-WIN-L2NFBEGGBJS	WMSvc-WIN-L2NFBEGGBJS	06/01/2025	Server Authenticati	<none></none>
Enterprise Trust					
Intermediate Certification Authorities					
Irusted Publishers					
Untrusted Certificates					
p Inird-Party Root Certification Authorities					
p in trusted People					
p Citeric Authentication issuers					
b Smart Card Trusted Boots					
b Trusted Devices					
y Mak Usalan					

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.

Group or user names:		
& SYSTEM & Administrators (V9-2-WII & S-1-5-5-0-1323316	N12SQL14\Administrator	5)
Permissions for SYSTEM	Add	Remove
Full control Read Special permissions		
For special permissions or adv click Advanced.	vanced settings,	Advanced

17. Click Add.



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

Select Users, Computers, Service Accounts, or	r Groups 🛛 🗙
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
corp.alembagroup.com	Locations
Enter the object names to select (examples):	
Network	Check Names
Advanced OK	Cancel

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

	Multiple Names Found		X
More than one object matched the na names from this list, or, reenter the na <u>M</u> atching names:	ame "Network". Select one or more me.		
Name	Logon Name (pr E-Mail Address	Description	In Folder
NETWORK NETWORK SERVICE			
NETWORK SQLBACKUP	SQLBACKUP		corp.alemb;
<			>
		ОК	Cancel

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

🔎 · 🔞 🛃	
MENU - 💐 Integration	Single Sign On Certificate Details
Single Sign On Identity F	Provider Details
Name *	
Certificate *	
TestCertificate AnotherCertificate MyCertificate	

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>

SieldID 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";
```

}

Version 1.3 © Alemba 2017



```
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
g 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.



eg 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 signins 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





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

vFi	re Test - Blogs, Joe /Fire c o	RE	V9.4.4
Ç	- 😥		
MENU	-		
	Dashboards	•	Windows
+	New	٠	Cascade
ali	Reports	•	Close Open Window(s)
Ē	Bulletin Board	٠	Opened Windows
	View	۲	
P	Search	٠	
2	Saved Searches	٠	
	Admin	٠	

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		
a 🖬 🐱		
Name *	Status	
MultiTestDomain Pull	Active	~
Connector	(Assembly.TypeName)	
Microsoft Active Directory Connector	Infra.Connector.LDAP.AD.ADConnector	
▼ Connection Parameters		
Ionix Service Manager Active Directory Conn	ector	
LDAP Server Path		
LDAP://AZURE.alembatest.com		
Login ID		
bob@alembatest.com		
Password		
•••••		
Server Bind SSL Kerberos/NTLM		
Advanced		
NT Domain Name		
Delete Disabled Person Records		
▼ Authentication		
Authenticate Imported People against Source		

eg *.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 MatchingFields 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.

domain services PREMEW		
ENABLE DOMAIN SERVICES FOR THIS DIRECTORY	YES NO	0
		_
DNS DOMAIN NAME OF DOMAIN SERVICES	alembatest.com	0
CONNECT DOMAIN SERVICES TO THIS VIRTUAL NETWORK	Virtual Network Subnet-1(10.0.0.0/11) North Europe sub v	0
IP ADDRESS	10.0.0.5; 10.0.0.4	Ø
SECURE LDAP (LDAPS)	Configure certificate	Ø
SECURE LDAP CERTIFICATE	Thumbprint: EA60EABC5D9C98ED89F4D6CC81960A8F1396373A Certificate expires: Fri, 06 Oct 2017 10:05:15 GMT	Ø
ENABLE SECURE LDAP ACCESS OVER THE INTERNET	YES NO	0
EXTERNAL IP ADDRESS FOR LDAPS ACCESS	52.169.72.184	0

- ^{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





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-directoryds-admin-guide-configure-secure-Idap/#requirements-for-the-secure-Idapcertificate



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.