

# Single Sign On



© 2024 General Electric Company

## Contents

Chapter 1: Overview	1
Overview of Single Sign-On	2
SSO Workflow	2
Chapter 2: Set up APM SSO	3
About Setting Up APM SSO	4
Configure Azure Active Directory as the Identity Provider (IDP)	4
Configure Identity Provider (IDP) on Active Directory	9
Chapter 3: Enable SSO	44
About Enabling APM SSO	45
About Host Names	45
Enable SSO On Site Authentication Using Active Directory	45
Enable SSO Off-Site Authentication Using APM Server Setup	45
Chapter 4: Configure APM Server	48
Configure APM Server	49
Chapter 5: Troubleshooting	51
Troubleshooting Scenarios	52
Frequently Asked Questions	54

## **Copyright Digital, part of GE Vernova**

 $^{\odot}$  2024 GE Vernova and/or its affiliates.

GE Vernova, the GE Vernova logo, and Predix are either registered trademarks or trademarks of GE Vernova. All other trademarks are the property of their respective owners.

This document may contain Confidential/Proprietary information of GE Vernova and/or its affiliates. Distribution or reproduction is prohibited without permission.

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Access to and use of the software described in this document is conditioned on acceptance of the End User License Agreement and compliance with its terms.

# Chapter 1

# Overview

## **Topics:**

- Overview of Single Sign-On
- SSO Workflow

## **Overview of Single Sign-On**

SSO is a process that allows pre-authenticated users to access APM, without having to re-enter their credentials.

The APM user logs on initially using a form-based enterprise login screen. SSO is a common procedure in enterprises, where a user logs in once and gains access to different applications without the need to reenter log-in credentials at each application. SSO authentication facilitates seamless network resource usage. SSO mechanisms vary, depending on application type.

SSO advantages include:

- Eliminates credential re-authentication.
- Streamlines local and remote application and desktop workflow.
- Minimizes phishing.
- Improves compliance through a centralized database.
- Provides detailed user access reporting.

APM supports the following types of authentication for SSO:

- Pass-through authentication Enables the users to enter their Windows credentials in the APM login page and APM validates the credentials against Active Directory.
- Security Assertion Markup Language (SAML) authentication
   Enables the users to navigate to the SSO URL (hosted on the APM Application Server) that redirects
   the browser to a preconfigured URL (not hosted on the APM Application Server), which is the Identity
   Provider (IDP). If there are multiple databases, and when the user selects a database, the user account
   is then authenticated and the IDP provides the web browser a token through a cookie. If the token is
   valid, the user can access APM.

## **SSO Workflow**

This workflow provides the basic, high-level steps for using this module. The steps and links provided in the workflow do not necessarily reference every possible procedure.

#### Procedure

- 1. Set up APM SSO by configuring an identity provider.
- 2. Enable SSO on-site or off-site authentication.
- 3. Configure the APM server.

# Chapter

2

## Set up APM SSO

**Topics:** 

- About Setting Up APM SSO
- Configure Azure Active Directory as the Identity Provider (IDP)
- Configure Identity Provider (IDP) on Active Directory

## **About Setting Up APM SSO**

### **About Setting up APM SSO**

To set up APM SSO, perform one of the following tasks:

- Configure Azure Active Directory as the Identity Provider (IDP)
- Configure IDP on Active Directory

## Configure Azure Active Directory as the Identity Provider (IDP)

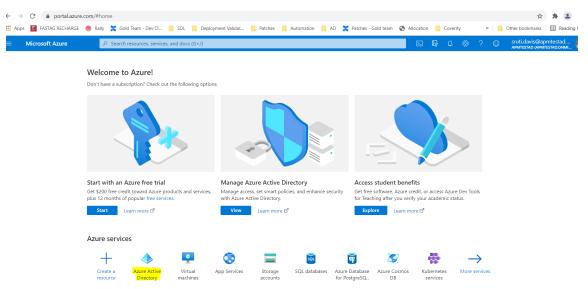
## Configure Azure Active Directory as the Identity Provider (IDP)

#### **Before You Begin**

You must have an Azure Active Directory (Azure AD) instance.

#### Procedure

1. Sign in to the Azure portal and select Azure Active Directory.



In the navigation pane, select Enterprise applications.
 The Enterprise applications – All applications page appears.

0	Home > Enterprise applications - All a	applica	tions								
Create a resource	enterprise applications	s - Al	l applications								
🛧 Home		«	+ New application	Column	s						
🗔 Dashboard	Overview	1									
All services	<ol> <li>Overview</li> </ol>		Application Type	~	Applications status	~	Application visibilit	/ 		P	
+ FAVORITES			Enterprise Applications	~	Any	~	Any	~	Apply	Reset	
	Manage		First 50 shown, to search all	of your ap	plications, enter a displi	y name or the app	olication ID.				
App Services	All applications		NAME		HOMEPAGE URL			OBJECT ID		APPLICATION ID	
> Function App	Application proxy		Asset Performar								
SQL databases	User settings		Asset Performan	ce Mana	gemer			a5055119-db45	-4923-956d-d75	70621 46ed8f77-e062-4	bce-bb95
Azure Cosmos DB	Security		Asset Performar	ce Mana	gemei			96d803e5-3016	-4896-81db-d28	a75e9 2e54f355-2498-4	a5a-93e9
Virtual machines	Conditional Access	L.	Office 365 Excha	inge Onli	ne http://office.	microsoft.com/c	utlook/	3b0e3709-93cc	-4830-a33d-b96	defd4 00000002-0000-0	lff1-ce00
Load balancers	Activity	L.	Office 365 Mana	gement	APIs			5008761a-19dd	-48ed-b043-4e2	5bac0 c5393580-f805-44	401-95e8
Storage accounts	Sign-ins	Е	Office 365 Share	Point Or	line http://office.	nicrosoft.com/s	harepoint/	dd333e69-4b2	c-4bda-bdf3-792	2fb39a 00000003-0000-0	lff1-ce00
Azure Active Directory	👔 Usage & insights (Preview)	Ŀ	onprem-apm-te	st-NEW				ebe17c60-5f38	-4724-b8a8-330e	edb1f5 01c7ee4f-2f13-411	9-b454-8
Monitor	Audit logs		Outlook Groups					7.4.640.444		8b41ec 925eb0d0-da50-4	
Advisor	듣 Access reviews							/a4abd0e-4dc8	s-4beb-ab99-4d8	5041ec 925eb0d0-da50-4	1604-a19t
Security Center	Troubleshooting + Support		Same Sign on					2f37ea7d-9962	-4694-bc77-d4f9	9d413 b12afa8d-6ecb-4f	b6-b761
Cost Management + Bill	Virtual assistant (Preview)		SF Skype for Busine	ss Onlin	e			822dcb0d-e9a	2-44ff-aa0c-65d9	94227 00000004-0000-0	)ff1-ce00

#### 3. Select New application.

The **Add an application** section appears.

«	Home > Enterprise applications - All app	lications	> Categories > Add an applicatio	n	
+ Create a resource	Categories	×	Add an application		\$ 🗆 X
A Home	All (3171)	-	Add your own app		
<ul> <li>Dashboard</li> <li>All services</li> </ul>	Business management (400)		Application	On-premises	Non-gallery
+ FAVORITES	Collaboration (454)		you're developing	application	application
🔇 App Services	Construction (7)	_	Register an app you're working on to integrate	Configure Azure AD Application Proxy to	Integrate any other application that you
Function App	Consumer (44)	_	it with Azure AD	enable secure remote access	don't find in the gallery
🡼 SQL databases	Content management (153)	_			
🖉 Azure Cosmos DB	CRM (155)	_	Add from the gallery		
👰 Virtual machines	Data services (149)	_			
🚸 Load balancers	Developer services (109)		Enter a name		
Storage accounts	E-commerce (75)		Featured applications		
↔ Virtual networks	Education (145)				
Azure Active Directory	ERP (92)		box	<b>C.</b>	
Monitor	Finance (258)				
Advisor	Health (63)		Box Cond	cur Cornerstone O	
<ul> <li>Security Center</li> <li>Cost Management + Bill</li> </ul>	Human resources (290)				
Help + support	IT infrastructure (194)	-	<b>D</b> 5	<b>★</b>	

 Select Non-gallery application. The Add your own application section appears.

	« Home > apmtestad > Enterprise applica	ations - Al	I applications > Categories > Ad	d an application > Add your c	own application		
+ Create a resource	Categories	×	Add an application		\$	×	Add your own application $\ \ \Box \ \times$
A Home	All (3171)	-	Add your own app			-	* Name
All services	Business management (400)	- 1	Application	On-premises	Non-gallery		The display name for your new application
	Collaboration (454)		you're developing	application	application		Once you decide on a name for your new
All resources	Construction (7)	- 1	Register an app you're	Configure Azure AD Application Proxy to	Integrate any other application that you		application, click the "Add" button below and we'll walk you through some simple
( Resource groups	Consumer (44)		working on to integrate it with Azure AD	enable secure remote access	don't find in the gallery	а.	configuration steps to get the application working.
🔇 App Services	Content management (153)	- 1					working.
Inction App	CRM (155)		Add from the gallery				Supports: 🛛
👼 SQL databases	Data services (149)	- 5					SAML-based single sign-on Learn more
🖉 Azure Cosmos DB	Developer services (109)		Enter a name				Automatic User Provisioning with SCIM
👤 Virtual machines	E-commerce (75)		Featured applications				Learn more
Load balancers	Education (145)						Password-based single sign-on
Storage accounts	ERP (92)		box	<b>C</b> • <b>C</b>			Learn more
Azure Active Directory	Finance (258)		<b>GOX</b>				
Monitor	Health (63)		Box Con	cur Cornerstone C	D		Add
Advisor	Human resources (290)	-				-	Add

5. In the **Name** box, enter a name for the application that you want to configure with Azure AD, and then select **Add**.

The page of the added application appears.

6. In the navigation pane of the application page, select **Single sign-on**. The **Select a single sign-on method** section appears.

«	Home > apmtestad > Enterprise applica	ions - All applications 🗧 Asset Performance Management - Single sign-on				
+ Create a resource	Asset Performance Management - Single sign-on					
🛧 Home	Cherphice Application		-			
Dashboard	Soverview	Select a single sign-on method Help me decide				
E All services	💅 Getting started					
* FAVORITES	Deployment Plan	Disabled දි SAML				
All resources	Manage	User must manually enter their username and password. Rich and secure authentication to applications using the SAML (Security				
(🐑 Resource groups	Properties	Assertion Markup Language) protocol.				
🔇 App Services	M Owners					
Function App	x <sup>R</sup> Users and groups					
🗟 SQL databases	<ul> <li>Single sign-on</li> </ul>					
🖉 Azure Cosmos DB	Provisioning	Password-based Password storage and replay using a Linked Link to an application in the Azure				
👰 Virtual machines	Application proxy	web browser extension or mobile app. Active Directory Access Panel and/or				
💠 Load balancers	Self-service	Office 365 application launcher.				
Storage accounts						
Virtual networks	Security					
Azure Active Directory	Conditional Access					
🕒 Monitor	A Permissions					
🜪 Advisor	Token encryption (Preview)					

#### 7. Select SAML.

The Set up Single Sign-On with SAML section appears.

+ Create a resource	Asset Performance Manager	ment - SAML-based sign-on	>
	Enterprise Application		
🛧 Home	٥	K Upload metadata file ♥ Change single sign-on mode	
Dashboard	Soverview	·	
■ All services	💅 Getting started	Set up Single Sign-On with SAML	
* FAVORITES	Deployment Plan	Read the configuration guide of for help integrating Asset Performance Management.	
All resources	Manage		
Resource groups	Properties	Basic SAML Configuration	
S App Services		Identifier (Entity ID) Required	
Function App	🗳 Owners	Reply URL (Assertion Consumer Service URL) Required Sian on URL Optional	
SQL databases	g <sup>R</sup> Users and groups	Relay State Optional	
_	Single sign-on	Logout Url Optional	
Azure Cosmos DB	Provisioning		
👰 Virtual machines	Application proxy	User Attributes & Claims	
💠 Load balancers	Self-service	Givenname user.givenname	
Storage accounts		Surname user.surname	
🐡 Virtual networks	Security	Emailaddress user.mail Name user.userprincipalname	
Azure Active Directory	Conditional Access	Unique User Identifier user.userprincipalname	
Monitor	& Permissions		
Advisor	Token encryption (Preview)	SAML Signing Certificate	

8. In the **Basic SAML Configuration** section, select  $\checkmark$ . The **Basic SAML Configuration** window appears.

Basic SAML Configuration	×
R Save	
* Identifier (Entity ID) 👩	
The default identifier will be the audience of the SAML response for IDP-initiated SSO	.
* Reply URL (Assertion Consumer Service URL) 👩 The default reply URL will be the destination in the SAML response for IDP-initiated SSO	
Sign on URL 🚯	
Enter a sign on URL	
Relay State 🙃	_
Enter a relay state	
Logout Url 😝	_
Enter a logout url	

#### 9. Enter the following details.

Identifier (Entity	Enter a unique ID.
ID)	<b>Note:</b> This ID will be used in the saml.json file for the service provider name. Therefore, note the ID.
Reply URL	The application callback URL where the response will be posted.
(Assertion	Enter the URL in the following format: https:// <apm name="" server="">/</apm>
Consumer Service	Meridium/api/core/security/ssologinauth, where <apm server<="" td=""></apm>
URL)	Name> is the name of the APM server.
Sign on URL	The application URL, which initiates the same sign-on. Enter the URL in the following format: https:// <apm name="" server="">/ meridium/index.html, where <apm name="" server=""> is the name of the APM server.</apm></apm>

#### 10. Select **Save**.

- 11. In the SAML Signing Certificate section, select Download corresponding to Certificate (Base 64).
- 12. From the **Set up <Identifier>,** section copy the Login URL and Azure AD Identifier.

Set up sdsso

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/78dd76d6-f3b7	D
Azure AD Identifier	https://sts.windows.net/78dd76d6-f3b7-4b89-9ef	0
Logout URL	https://login.microsoftonline.com/78dd76d6-f3b7	0

**Note:** The Login URL and Azure AD Identifier will be used in the saml.json file for SingleSignOnServiceURL and PartnerIdentityProviderConfigurations Name, respectively.

- 13. In the application server, copy the downloaded Certificate (Base 64) to C:\Program Files\Meridium\ApplicationServer\api. Please refer to section Install the Token Signing idp.cer Certificate on the Application Server on page 40, steps 5 - 8 for installing the certificate.
- 14. Modify the saml.json file as follows:
  - LocalServiceProviderConfiguration Name with the value that you entered and noted for the Identifier (Entity ID) box.
  - PartnerIdentityProviderConfigurations Name with the Azure AD Identifier.
  - SingleSignOnServiceURL with the Login URL.
  - AssertionConsumerServiceUrl with the URL that you entered in the Reply URL (Assertion Consumer Service URL) box.
  - PartnerCertificates FileName with the downloaded certificate name.

```
{
    "SAML": {
        "$schema": "https://www.componentspace.com/schemas/saml-
config-schema-v1.0.json",
        "Configurations": [
            {
                "LocalServiceProviderConfiguration": {
                     "Name": "sdsso",
                     "AssertionConsumerServiceUrl": "https://<APM
Server Name>/Meridium/api/core/security/ssologinauth",
                    "LocalCertificates": [
                         {
                             "FileName": "sp.pfx",
                             "Password": "password"
                    1
                },
                "PartnerIdentityProviderConfigurations": [
                         "Name": "https://sts.windows.net/78dd76d6-
f3b7-4b89-9efc-ef8d5483b7ea/",
                         "Description": "Azure AD",
                         "SignAuthnRequest": true,
                         "WantSamlResponseSigned": false,
                         "WantAssertionSigned": true,
                         "WantAssertionEncrypted": false,
                         "UseEmbeddedCertificate": false,
                         "SingleSignOnServiceUrl": "https://
login.microsoftonline.com/78dd76d6-f3b7-4b89-9efc-ef8d5483b7ea/
saml2",
                        "DigestAlgorithm": "http://www.w3.org/
2001/04/xmlenc#sha256",
                         "SignatureAlgorithm": "http://www.w3.org/
```

15. Add users to the enterprise application by accessing the Users and groups section.

- a) Select Users and groups section in the left navigation pane.
- b) Click on Add user/group button to add a new user to this enterprise application. Search for the user in the Users list and then click on Assign.

Users are added to the enterprise application.

#### **Next Steps**

Enable SSO

## **Configure Identity Provider (IDP) on Active Directory**

### About Configuring Identity Provider (IDP) on Active Directory

#### **About This Task**

You must configure IDP on Active Directory using the Active Directory Federation System (AD FS) Management Console.

Note: The strings and the URLs in AD FS are case-sensitive.

To configure IDP on Active Directory, you must perform the following tasks:

#### Procedure

- 1. Add Relying Party Trusts on page 9
- 2. Add Claim Rules on page 20
- 3. Add Certificates on page 26
- 4. Federation Service Identifier from ADFS on page 42

### Add Relying Party Trusts

#### **Before You Begin**

- You must have administrative privileges to configure AD FS.
- Ensure that the /adfs/Is endpoint exists for SAML v2.0.

**Note:** To add adfs/ls endpoint, refer to the AD FS documentation.

• Ensure that the token encrypting certificates exist.

#### Procedure

- 1. Access Control Panel, then select System and Security, and then select Administrative Tools.
- 2. Select **AD FS Management**. The **AD FS** window appears.

3. In the Actions section, select Add Relying Party Trust. The Add Relying Party Trust Wizard appears.

<b>\$</b>	Add Relying Party Trust Wizard
Welcome	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Configure Multi-factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	Welcome to the Add Relying Party Trust Wizard This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions. The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.
	< Previous Start Cancel

#### 4. Select Start.

The Select Data Source page appears.

<b>\$</b>	Add Relying Party Trust Wizard	x
Select Data Source		
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Profile</li> <li>Configure Certificate</li> <li>Configure URL</li> <li>Configure Identifiers</li> <li>Configure Multi factor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	Select an option that this wizard will use to obtain data about this relying party:          Import data about the relying party published online or on a local network         Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata address (host name or URL):	S
	< <u>P</u> revious <u>N</u> ext > Cancel	]

5. Select Enter data about relying party manually, and then select Next. The Specify Display Name page appears.

<b>\$</b>	Add Relying Party Trust Wizard	x
Specify Display Name		
Steps	Enter the display name and any optional notes for this relying party.	
Welcome	Display name:	
Select Data Source	um:componentspace:Meridium	
Specify Display Name	Notes:	
Choose Profile		
Configure Certificate		
Configure URL		
Configure Identifiers		
Configure Multi-factor Authentication Now?		<u> </u>
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
Finish		
	< <u>P</u> revious <u>N</u> ext > Cance	

6. In the **Display name** box, enter **urn:componentspace:Meridium**, and then select **Next**. The **Choose Profile** page appears.

<b>\$</b>	Add Relying Party Trust Wizard	x
Choose Profile		
Steps	This wizard uses configuration profiles to aid in creating the relying party trust. Choose the appropriate	
Welcome	configuration profile for this relying party trust.	
Select Data Source	AD <u>F</u> S profile	
Specify Display Name	This profile supports relying parties that are interoperable with new AD FS features, such as security token encryption and the SAML 2.0 protocol.	
Choose Profile	security token encryption and the SAMIL 2.0 protocol.	
Configure Certificate	O AD FS 1.0 and 1.1 profile	
Configure URL	This profile supports relying parties that are interoperable with AD FS 1.0 and 1.1.	
Configure Identifiers		
Configure Multi-factor Authentication Now?		
<ul> <li>Choose Issuance Authorization Rules</li> </ul>		
Ready to Add Trust		
Finish		
	< <u>P</u> revious <u>N</u> ext > Cance	1

7. Select the AD FS profile option, and then select Next. The Configure Certificate page appears.

<b>\$</b>	Add Relying Party Trust Wizard	X
Configure Certificate		
Configure Certificate Steps  Welcome Select Data Source Select Data Source Choose Profile Configure Certificate Configure URL Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to it. To specify the certificate, click Browse	
	< <u>P</u> revious <u>N</u> ext > Cance	:

8. Select Next.

The **Configure URL** page appears.

<b>\$</b>	Add Relying Party Trust Wizard
Configure URL	
<ul> <li>Steps</li> <li>Welcome</li> <li>Select Data Source</li> <li>Specify Display Name</li> <li>Choose Profile</li> <li>Configure Certificate</li> <li>Configure URL</li> <li>Configure Identifiers</li> <li>Configure Multifactor Authentication Now?</li> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If         WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Frust protocol is always enabled for a relying party.         □       Enable support for the WS-Federation Passive protocol         The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol URL:         □       Example: https://fs.contoso.com/adfs/ls/         Image:       Enable support for the SAML 2.0 WebSSO protocol         The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.         Relying party SAML 2.0 SSO service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.         Relying party SAML 2.0 SSO service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.         Relying party SAML 2.0 SSO service URL:         https://cmeridiumserver>.       organisation>.com/Meridium/api/core/security/ssologinauth         Example: https://www.contoso.com/adfs/ls/       Evenple: https://www.contoso.com/adfs/ls/

- 9. Select the Enable Support for the SAML 2.0 WebSSO protocol check box.
- 10. In the **Relying Party SAML 2.0 SSO service URL box**, enter https://<APM Server Name>/ Meridium/api/core/security/ssologinauth, and then select Next.

**Note:** The word Meridium is case-sensitive. Therefore, ensure that the first letter of the word is capitalized. Also, the URL must be same as the AssertionConsumerServiceUrl in the saml.json file.

The **Configure Identifiers** page appears.

<b>\$</b>	Add Relying Party Trust Wizard	x
Configure Identifiers		
Configure Identifiers Steps  Welcome Select Data Source Select Data Source Configure Uslaw Configure Certificate Configure URL Configure Identifiers Configure Multifactor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	Relying parties may be identified by one or more unique identifier strings. Specify the identifier party trust. Relying party trust identifier: Example: https://fs.contoso.com/adfs/services/trust Relying party trust identifiers: Umicomponentspace:Meridium	s for this relying Add Remove
	< <u>P</u> revious <u>N</u> ext >	Cancel

11. In the Relying party trust identifier box, enter urn:componentspace:Meridium, then select Add, and then select Next.

The **Configure Multi-factor Authentication Now** page appears.

<b>\$</b>	Add Relying Party Trust Wizard	x
Steps	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if	
Welcome	there is a match for any of the specified requirements.	
Select Data Source     Specify Display Name     Choose Profile     Configure Certificate     Configure URL     Configure Identifiers     Configure Multi-factor     Authentication Now?     Choose Issuance	Multi-factor Authentication       Global Settings         Requirements       Users/Groups       Not configured         Device       Not configured         Location       Not configured	
Authorization Rules Ready to Add Trust Finish	<ul> <li>I do not want to configure multi-factor authentication settings for this relying party trust at this time.</li> <li>Configure multi-factor authentication settings for this relying party trust.</li> <li>You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.</li> </ul>	
	< Previous Next > Cancel	]

12. Select I do not want to configure multi-factor authentication settings for this relying party trust at this time, and then select Next. The Choose Issuance Authorization Rules page appears.

Add Relying Party Trust Wizard       Choose Issuance Authorization Rules		
Welcome	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.	
Select Data Source	Permit <u>all</u> users to access this relying party	
Specify Display Name	The issuance authorization rules will be configured to permit all users to access this relying party. The relying	
Choose Profile	party service or application may still deny the user access.	
Configure Certificate	O Deny all users access to this relying party	
Configure URL	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.	
Configure Identifiers	later add issuance authorization rules to enable any users to access this reiging party.	
Configure Multi-factor Authentication Now?	You can change the issuance authorization rules for this relying party trust by selecting the relying party trust	
<ul> <li>Choose Issuance Authorization Rules</li> </ul>	and clicking Edit Claim Rules in the Actions pane.	
Ready to Add Trust		
<ul> <li>Finish</li> </ul>		
	< Previous Next > Cancel	

13. Select **Permit all users to access this relying party**, and then select **Next**. The **Ready to Add Trust** page appears.

<b>\$</b>	Add Relying Party Trust Wizard	x
Ready to Add Trust		
Steps Welcome Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish	The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.           Encryption       Signature       Accepted Claims       Organization       Endpoints       Notes       Advanced       <         Specify the encryption certificate for this relying party trust.       Encryption certificate:       Issuer:       Subject:       Effective date:       Expiration date:         View       View       View       Issuer:       Issuer	
	< <u>P</u> revious <u>N</u> ext > Cancel	

14. Select Next.

The **Finish** page appears.

<b>\$</b> 1	Add Relying Party Trust Wizard	x
Finish		
Steps  Welcome  Select Data Source  Specify Display Name  Choose Profile  Configure Certificate  Configure URL  Configure Identifiers  Configure Multi factor Authentication Now?  Choose Issuance Authorization Rules  Ready to Add Trust  Finish	The relying party trust was successfully added to the AD FS configuration database. You can modify this relying party trust by using the Properties dialog box in the AD FS Management snap in ✓ Open the Edit Claim Rules dialog for this relying party trust when the wizard closes	٦.
	Glose	

15. Clear the **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes** check box, and then select **Close**.

#### **Next Steps**

• Add Claim Rules on page 20

## **Add Claim Rules**

#### Procedure

1. In the AD FS window, expand the Trust Relationships folder, and then select Relying Party Trusts. The Relying Party Trusts page appears.

2. Select urn:componentspace:Meridium, and then, in the Actions section, select Edit Claim Rules. The Edit Claim Rules for urn:componentspace:Meridium window appears. Select Issuance Transform Rules tab.

Section 2015 Participation Components Pace: Meridia	im 🗕 🗆 🗙
Issuance Transform Rules Issuance Authorization Rules Delegation Au	thorization Rules
The following transform rules specify the claims that will be sent to the re	ying party.
Order Rule Name Issued Claims	
Add Rule	
OK Car	icel Apply

3. Select Add Rule.

The Add Transform Claim Rule Wizard window appears.

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

4. In the **Claim rule template** drop-down list box, select **Send LDAP Attributes as Claims**, and then select **Next**.

The **Configure Rule** page appears.

<b>\$</b>	Add Transform Claim Rule Wizard				
Configure Rule					
Steps • Choose Rule Type • Configure Claim Rule	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the nule.  Claim rule name:  Rule template: Send LDAP Attributes as Claims Attribute store: Select an attribute store  Mapping of LDAP attributes to outgoing claim types:  LDAP Attributes to outgoing claim types:  LDAP Attribute (Select or type to add more)  *  Voltagoing Claim Type (Select or type to add more)  *  Voltagoing Claim Type (Select or type to add more)				
	< Previous Finish Cancel				

- 5. In the **Claim rule name** box, enter **Meridium Claims**, and then, in the **Attribute store** drop-down list box, select **Active Directory**.
- 6. Perform the following steps:
  - In the first drop-down list box in the LDAP Attribute column, select User-Principal-Name, and then, in the corresponding Outgoing Claim Type drop-down list box, select Name ID.
  - In the second drop-down list box in the LDAP Attribute column, select E-mail-Addresses, and then, in the corresponding Outgoing Claim Type drop-down list box, select E-Mail Address.

The **Configure Rule** page is populated with the selected values.

<b>%</b>		Add Transform Claim Ru	ıle	Wizard
Configure Rule				
Configure Rule Steps Choose Rule Type Configure Claim Rule	which issued Claim Meridi Rule t Attribu Active		the a	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be v s: Outgoing Claim Type (Select or type to add more) Name ID v E-Mail Address v
				< Previous Finish Cancel

7. Select Finish.

The Edit Claim Rules for urn:componentspace:Meridium window appears.

	s for urn:componentspace:Meridium	<b>x</b>
Issuance Transform Rules	Issuance Authorization Rules Delegation Authorization Ru	iles
The following transform n	les specify the claims that will be sent to the relying party.	
Order Rule Name	Issued Claims	
1 Meridium Claims	s E-Mail Address,Given Na	
		•
Add Rule Edit F	Rule Remove Rule	
	OK Cancel	Apply

#### 8. Select OK.

The claim rule is added to the Edit Claim Rules for urn:componentspace:Meridium window.

#### **Next Steps**

• Add Certificates on page 26

## **Add Certificates**

#### **About This Task**

To add certificates, you must perform the following tasks:

#### Procedure

- 1. Install the Service Provider certificate (sp.pfx) on page 27
- 2. Export the Public Key Certificate on page 31
- 3. Copy the Certificate to Active Directory on page 38

4. Install the Token Signing idp.cer Certificate on the Application Server on page 40

#### Install the Service Provider certificate (sp.pfx)

#### Procedure

1. Navigate to C:\Program Files\Meridium\ApplicationServer\api, where the service provider certificate file (sp.pfx) is located.

**Note:** GE Vernova provides the service provider certificate file (sp.pfx). pfx is personal information exchange.

2. Right-click **sp**, and then select **Install PFX**. The **Certificate Import Wizard** appears.

9 \$	Certificate Import Wizard
	Welcome to the Certificate Import Wizard
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
	Store Location
	O Current User
	Local Machine
	To continue, dick Next.
	Next Cancel

3. Select Local Machine, and then select Next. The User Account Control window appears.

•	User Account Control				
Do you want to allow the following program to make changes to this computer?					
	Program name: Windows host process (Rundll32) Verified publisher: <b>Microsoft Windows</b>				
Show deta	ils Yes No				
	Change when these notifications appear				

4. Select Yes.

The **Certificate Import Wizard** appears, and the **File Name** box displays the file path where the certificate is located.

📀 🍠 Certificate Import Wizard
File to Import Specify the file you want to import.
File name:         C:\Program Files\Meridium\ApplicationServer\api\sp.pfx         Browse
Note: More than one certificate can be stored in a single file in the following formats: Personal Information Exchange-PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B) Microsoft Serialized Certificate Store (.SST)
Next Cancel

5. Select Next.

🗧 😺 Certificate Import Wizard

#### Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

🗸 Display Pa	sword	
port options:		
	ng private key protection. You will be prompted e is used by an application if you enable this option	
Mark this k Mark this k Mark this k	ey as exportable. This will allow you to back up or ater time.	r transport your
Protect pri	vate key using virtualized-based security(Non-exp	portable)
🗸 Include all	extended properties.	

6. Enter a password *password*, and then select **Next**.

3	Certificate Import Wizard
c	ertificate Store Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for the certificate.
	<ul> <li>Automatically select the certificate store based on the type of certificate</li> </ul>
	O Place all certificates in the following store
	Certificate store:
	Browse
	Next Canc

7. Select Automatically select the certificate store based on the type of certificate. The Completing the Certificate Import Wizard appears.

	X
📀 🍠 Certificate Import V	Vizard
Completing the	Certificate Import Wizard
The certificate will be impo You have specified the foll	
	Automatically determined by the wizard PFX
File Name	C:\Program Files\Meridium\ApplicationServer\api\sp.pfx
	Finish         Cancel

8. Select Finish.

#### **Next Steps**

• Export the Public Key Certificate on page 31

#### **Export the Public Key Certificate**

#### Procedure

- 1. Access Microsoft Management Console.
- 2. In the main navigation bar, select **File**, then select **Add/Remove Snap-in**, and then select **Certificates**.

The Add or Remove Snap-ins window appears.

nap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor				
Authorization Manager					Remove
Certificates	Microsoft Cor	≣			
Component Services	Microsoft Cor				Move Up
Computer Managem					
Device Manager	Microsoft Cor				Move Down
Disk Management	Microsoft and		Add >		
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
Internet Informatio	Microsoft Cor				
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor				1
IP Security Policy M	Microsoft Cor	~			Advanced
IP Security Monitor IP Security Policy M scription:	Microsoft Cor Microsoft Cor	~	contents of the	certificate stores for yourself, a	Advanc

#### 3. Select Add.

The **Certificates snap-in** window appears.

Certificates snap-in
This snap-in will always manage certificates for: My user account Service account Computer account
< Back Next > Cancel

4. Select the **Computer account** option, and then select **Next**. The **Select Computer** window appears.

Select Computer	X
Select the computer you want this snap-in to manage. This snap-in will always manage: <ul> <li>Local computer: (the computer this console is running on)</li> </ul>	
Another computer:     Browse      Allow the selected computer to be changed when launching from the command line. This     only applies if you save the console.	
< Back Finish Can	cel

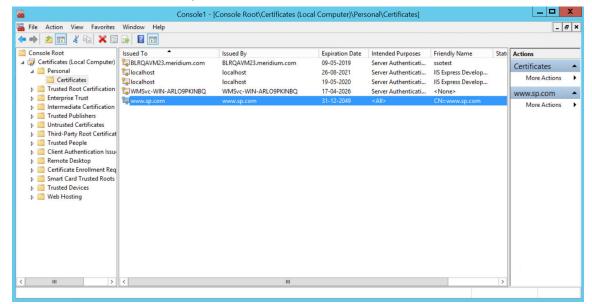
5. Select the Local computer option, and then select Finish.

ap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Gertificates (Local Computer)	Demous
Authorization Manager					Remove
Certificates	Microsoft Cor	=			
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				Marco Decision
Device Manager Disk Management	Microsoft Cor		Add >		Move Down
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object					
Internet Informatio					
Internet Informatio					
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor	~			Advanced
iption:					

6. In the Add or Remove Snap-ins window, select OK.

The certificate appears in the **Personal** > **Certificates** folder of the **Certificates (Local Computer)** folder.

7. Select Certificates (Local Computer), then select Personal, and then select Certificates.



8. Right-click the certificate that you have installed, select **All Tasks**, and then select **Export**. The **Certificate Export Wizard** appears.

Welcome to the Certificate Export Wizard
•
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, dick Next.

9. Select Next.

×

←
Export Private Key You can choose to export the private key with the certificate.
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.
Do you want to export the private key with the certificate?
○ Yes, export the private key
No, do not export the private key
Note: The associated private key is marked as not exportable. Only the certificate can be exported.
Next Cancel

10. Select the **No, do not export the private key** option, and then select **Next**.

Export File Format Certificates can be export	ed in a variety of file formats.
Select the format you war	nt to use:
OER encoded binar	y X.509 (.CER)
◯ Base-64 encoded >	(.509 (.CER)
🔿 Cryptographic Mes	sage Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certi	ficates in the certification path if possible
🔿 Personal Informati	on Exchange - PKCS #12 (.PFX)
Include all certi	ficates in the certification path if possible
Delete the priv	ate key if the export is successful
Export all exte	nded properties
O Microsoft Serialized	Certificate Store (.SST)

11. Select DER encoded binary X.509 (.CER), and then select Next.

Y

	X
📀 🌛 Certificate Export Wizard	
File to Export Specify the name of the file you want to export	
File name:	
Next	ancel

- 12. Select **Browse**, and then navigate to the location to which you want to export the certificate.
- 13. In the **File name** box, enter the same name that was mentioned while installing the certificate, and then, in the **Save as type** drop-down list box, select **DER Encoded Binary X.509 (.cer)**.
- 14. Select Next, and then select Finish.
- 15. Copy the exported certificate to Active Directory and install it. Please refer to section Install the Token Signing idp.cer Certificate on the Application Server on page 40, steps 5 - 8 for detailed process of installing the certificate.

#### **Next Steps**

• Copy the Certificate to Active Directory on page 38

#### **Copy the Certificate to Active Directory**

#### Procedure

- 1. Access Control Panel, then select System and Security, and then select Administrative Tools.
- 2. Select **AD FS Management**. The **AD FS** window appears.

<b>S</b>	AD FS	
翰 File Action View Window Help		_ <i>B</i> ×
🗢 🔿 🖄 📰 🚺 🗊		
AD FS	Relying Party Trusts	Actions
<ul> <li>Service</li> <li>Trust Relationships</li> <li>Claims Provider Trusts</li> <li>Relying Party Trusts</li> <li>Athibute Stores</li> <li>Authentication Policies</li> </ul>	Display Name         Enabled         Type         Identifier           Device Registration Service         Yes         WS-Tumms-dis-bimginitial abc.com           um componentispace Mediumso         Yes         WS-Tumcomponentispace Mendum           um componentispace Mediumso         Yes         WS-Tumcomponentispace Mendumso           um componentispace Mediumso         Yes         WS-Tumcomponentispace Mendumso           um componentispace Mediumsocr         Yes         WS-T         um componentispace Mendumso	Relying Party Trusts         Add Relying Party Trust         Add Non-Claims-Aware R         View       >         New Window from Here         Refresh         I Help         urnccomponentspace:Me         Update from Federation         Edit Claim Rules         Disable         Properties         X         Delte         I Help
Opens a new window rooted at this node.	1	1

- 3. Expand Trust Relationships, and then select Relying Party Trusts.
- 4. Select urn:componentspace:Meridium, and then, in the Actions section, select Properties. The urn:componentspace:Meridium Properties window appears.

Organization	Endpoin	ts Proxy End	points	Notes	Advanced
Nonitoring	Identifiers	Encryption	Signatu	re Acc	epted Claims
arty.	nature verifi	cation certificate			
Subject	Is	suer	Effectiv	ve Date	Expiratio
<		111			>

- 5. Select the **Signature** tab, and then select **Add**.
- 6. Navigate to the location in which you have saved the certificate, and then select the file.

- 7. Select **Yes** to ignore the warning about certificate key length.
- 8. Select the **Advanced** tab.
- 9. In the **Secure hash algorithm** drop-down list box, based on the policy of your organization, select **SHA-1** or **SHA-256**.

urr	n:componer	ntspace:Me	eridium Pr	opert	ies X
Monitoring	Identifiers	Encryption	Signature	Acc	epted Claims
Organization	Endpoints	Proxy End	lpoints N	lotes	Advanced
Specify the	secure hash al	gorithm to use	for this relyin	ig party	trust.
Secure has	h algorithm: S	HA-1			~
		ОК	Cano	el	Apply

10. Select **Apply**, and then select **OK**.

#### **Next Steps**

• Install the Token Signing idp.cer Certificate on the Application Server on page 40

#### Install the Token Signing idp.cer Certificate on the Application Server

#### Procedure

- 1. Access the Active Directory.
- 2. Export the token signing certificate and save the certificate.
- 3. Select Finish.
- 4. Copy the certificate to the api folder of the application server.
- 5. Right-click the file, and then select **Install Certificate**. The **Certificate Import wizard** appears.

· · · · · · · · · · · · · · · · · · ·
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location Current User Local Machine
To continue, dick Next.
Provide Cancel

6. Select Local Machine, and then select Next.

Ð 3	Certificate Import Wizard
	Certificate Store Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for the certificate.
	<ul> <li>Automatically select the certificate store based on the type of certificate</li> </ul>
	O Place all certificates in the following store
	Certificate store:
	Browse
	Next Cancel
	Next Concer

- 7. Select Automatically select the certificate store based on the type of certificate.
- 8. Select **Next**, and then select **Finish**.

#### **Federation Service Identifier from ADFS**

To get Federation Service Identifier from ADFS.

#### Procedure

- 1. Open AD FS management console.
- 2. Select AD FS from left navigation and select 'Edit Federation Service Properties' from Actions pane on the right.
- 3. On the **Federation Service Properties** dialog window, you can find the Federation Service identifier value.
- 4. Navigate to C:\Program Files\Meridium\ApplicationServer\api folder and open saml.json file in a text editor. Update the PartnerIdentityProviderConfigurations Name value with the Federation Service Identifier.

#### Next Steps

• About Enabling APM SSO on page 45

## Chapter

3

### **Enable SSO**

#### **Topics:**

- About Enabling APM SSO
- About Host Names
- Enable SSO On Site
   Authentication Using Active
   Directory
- Enable SSO Off-Site
   Authentication Using APM
   Server Setup

#### **About Enabling APM SSO**

To enable APM SSO, perform one of the following tasks:

- Enable SSO On Site Authentication Using Active Directory on page 45
- Enable SSO Off-Site Authentication Using APM Server Setup on page 45

#### **About Host Names**

Using the Host Names feature, you can:

- Enable Single Sign-On (SSO) off-site authentication and SSO on-site authentication.
- Filter Data Sources to access the related APM database.
- Create a unique URL to access APM.

When you use a URL to access APM, you can access the data sources that are mapped to the host name. For example, if two data sources (data\_source1 and data\_source2) are associated with a APM server, you can create two different URLs (https://data\_source1/meridium/index.html and https://data\_source2/ meridium/index.html) using the host names that are mapped to the data sources. If you log in to APM with https://data\_source1/meridium/index.html or https://data\_source2/meridium/index.html, you can access data\_source1 or data\_source2, respectively.

In the **Host Names** page, you can add multiple host names. However, only the host name of the URL with which you have logged in to APM is listed.

#### **Enable SSO On Site Authentication Using Active Directory**

#### Procedure

- 1. Run the LDAP Synchronization Process Manually or Schedule a LDAP Synchronization Process .
- 2. Log out of APM.
- 3. Log in to APM with the Windows user name and password. You are logged in.

#### Results

• SSO On-Site Authentication is enabled.

#### **Next Steps**

Configure APM Server on page 49

#### **Enable SSO Off-Site Authentication Using APM Server Setup**

#### **About This Task**

Note: The settings shown below may vary depending on your system.

#### Procedure

1. In the module navigation menu, select Admin > Operations Manager > Host Names. The Host Names page appears.



2. In the left pane, select +

The workspace for a new host name appears, displaying default values.

🔓 📥 🎄 Host Nam	es X
Host Names	<del>ประวัติหนึ่ง</del>
	Name
	64-18-08
	IDP URL
	Enter PartnerldentityProviderConfigurations -> Name value from saml.json
	SSO Enabled
	Changing these values could cause SSO to stop working. Please update with caution.

3. In the Name box, replace the default text with the APM Server's fully qualified hostname.

**Note:** This value must match with the server name in the URL used to navigate to APM in the browser. i.e. https://<Server Name>/Meridium.

- 4. In the **IDP URL** box, enter the PartnerIdentityProviderConfigurations **Name** value that was configured on the C:\Program Files\Meridium\ApplicationServer\api \saml.json file.
- 5. Select the **SSO Enabled** check box.
- 6. Select 🛅.

The host name is saved.

7. Log out of APM.

8. On the APM Server, in the APM program files, navigate to the folder ... \ApplicationServer \api.

#### Note:

- If you installed the software in the default location, the folder location will be C:\Program Files\Meridium\ApplicationServer\api.
- The settings in saml.json must be configured to match the environment to which you are connecting. For example, the URL listed in SingleSignOnServiceUrl should point to the URL where you want to authorize the users.
- 9. Modify the assertion and response signing settings to match the signing settings that are specified on the IDP, and then save and close the file.

#### 10. Reset IIS.

IIS is reset.

11. Access APM via a web browser.

The user is logged in, and SSO off-site authentication is enabled.

#### Next Steps

• Configure APM Server on page 49

# Chapter 4

## **Configure APM Server**

**Topics:** 

Configure APM Server

#### **Configure APM Server**

#### **Before You Begin**

- Ensure that the APM Server is installed and the server is configured to use SSL.
- Ensure that you can access the APM application in a web browser using HTTPS protocol.
- Ensure that the GE Vernova data source is configured and you can log in with administrative privileges.

#### Procedure

- 1. Using a web browser, log in to APM as an Administrator.
- 2. In the module navigation menu, select **Admin**, then select **Operations Manager**, and then select **Data Sources**.

#### The **Data Sources** page appears.

V4030100_BASE_QA_LAST	
Data Source ID	Database Server
V4030100_BASE_QA_LAST	BLRDEVDB01\SQL2012
Data Source Description	Database Name
V4030100_BASE_QA_LAST	V4030100_BASE_QA_LAST
Data Source Host	Database Allas
*	
Database Type	Oracle Host
SQL Server	¥
Database User Name	Oracle Port
V4030100_BASE_QA_LAST	
Password	Oracle Service
Preload Cache	
Datasource Offline	

- 3. In the **Data Source Host** box, enter the name of the APM server, and then select **Save**.
- 4. Enable LDAP Integration, configure Domain Record, and then schedule and run LDAP synchronization.

**Note:** For more information on how to enable LDAP Integration, configure a Domain Record, and schedule LDAP synchronization, refer to the Lightweight Directory Access Protocol documentation.

The users from Active Directory are now imported to APM and are assigned the appropriate Security Roles and Groups.

- 5. Stop IIS, the Redis service, and all Meridium Windows services.
- 6. Navigate to C:\Program Files\Meridium\ApplicationServer\api
- 7. Using a json or text editor, access the file saml.json.
- 8. Add a new configuration to <PartnerIdentityProviderConfigurations>json array or update the existing configuration by setting the following attributes:
  - Name: As described in sections Configure Azure Active Directory as the Identity Provider (IDP) on page 4 and About Configuring Identity Provider (IDP) on Active Directory on page 9.
  - WantSAMLResponseSigned: false
  - WantAssertionSigned: true
  - WantAssertionEncrypted: false
  - UseEmbeddedCertificate: false

• SingleSignOnServiceUrl: In the case of ADFS, it is of the form: {https version of Federation Service identifier} + "/adfs/ls". For example, https://myadfsserver/adfs/ls. This information must be obtained from the ADFS team. In the case of Azure AD, please refer to section Configure Azure Active Directory as the Identity Provider (IDP) on page 4.

#### Note:

For SHA-256, you must add the following two attributes to the saml.json file:

- "DigestAlgorithm":"http://www.w3.org/2001/04/xmlenc#sha256"
- "SignatureAlgorithm":"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"

The following example shows the configured saml.json file:

```
{
    "SAML": {
        "$schema": "https://www.componentspace.com/schemas/saml-
config-schema-v1.0.json",
        "Configurations":
            {
                "LocalServiceProviderConfiguration": {
                     "Name": "urn:componentspace:Meridium",
                     "AssertionConsumerServiceUrl": "~/core/security/
ssologinauth",
                     "LocalCertificates": [
                         {
                             "FileName": "sp.pfx",
                             "Password": "password"
                         }
                     1
                "PartnerIdentityProviderConfigurations": [
                     {
                         "Name": "http://fs.xyz.com/adfs/services/
trust",
                         "Description": "ADFS",
                         "SignAuthnRequest": true,
                         "WantSamlResponseSigned": false,
                         "UseEmbeddedCertificate": true,
                         "WantAssertionEncrypted": false,
                         "WantAssertionSigned": true,
                         "SingleSignOnServiceUrl": "https://
fs.xyz.com/adfs/ls/idpinitiatedsignon.aspx",
                         "PartnerCertificates": [
                                 "FileName": "idp.cer"
                         ]
                    }
                ]
            }
        ]
    }
}
```

9. Save and close the file saml.json.

10. Start IIS, the Redis service, and all Meridium Windows Services.

# Chapter 5

## Troubleshooting

**Topics:** 

- Troubleshooting Scenarios
- Frequently Asked Questions

#### **Troubleshooting Scenarios**

#### **Troubleshooting Scenarios**

The following topics can help you troubleshoot issues that you may have with the SSO module:

• Enable ComponentSpace SAML trace on page 52

#### Enable ComponentSpace SAML trace

#### Description

Enable ComponentSpace SAML trace for troubleshooting SSO issues

#### Cause

None

#### Solution

Perform the following steps:

- 1. Navigate to C:\Program Files\Meridium\ApplicationServer\api
- 2. Access Nlog.config
- 3. In the <Targets> section, add the following line of code: <target xsi:type="File"
   name="spFile" fileName="c:\ProgramData\Meridium\Logs\sp.log" layout="\$
   {liteLayout}" />
- 4. In the <Rules> section, add the following line of code: <logger name="ComponentSpace.\*"
   minlevel="Debug" writeTo="spFile" />

As shown below:

1	<pre><?xml version="1.0" encoding="utf-8" ?></pre>
2	<nlog 2001="" http:="" pre="" www.w3.org="" xmlns="http://www.nlog-project.org/schemas/NLog.;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;3&lt;/th&gt;&lt;th&gt;&lt;pre&gt;xmlns:xsi=" xmlschema-inst<=""></nlog>
4	autoReload="true"
5	internalLogLevel="Warn"
6	<pre>internalLogFile="internal-nlog.txt"&gt;</pre>
7	
8	<pre><!-- import extensions and liteLayout--></pre>
9	<include file="nlog.Shared.config"></include>
10	
11	the targets to write to
12	中 <targets></targets>
13	write logs to file
14	<target <="" file"="" filename="c:\&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;16&lt;/th&gt;&lt;td&gt;&lt;pre&gt;&lt;target xsi:type=" name="mechanicalIntegrity" pre="" scheduler"="" type="File" xsi:type="File"></target>
	/>
17	<target filenam<="" name="dlFramework" th="" xsi:type="File"></target>
18	<pre><!-- write to the void aka just remove--></pre>
19	<target name="blackhole" xsi:type="Null"></target>
20	<target filename="c:&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;21&lt;/th&gt;&lt;td&gt;- &lt;/targets&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;22&lt;/th&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;23&lt;/th&gt;&lt;td&gt;&lt;! rules to map from logger name to target&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;24&lt;/th&gt;&lt;td&gt;₽ &lt;rules&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;25&lt;/th&gt;&lt;td&gt;&lt;pre&gt;&lt;!Skip Microsoft logs and so log only own logs&lt;/pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;26&lt;/th&gt;&lt;td&gt;&lt;pre&gt;&lt;logger name=" microsoft.*"="" minlevel="Trace" name="spFile" pre="" writeto<="" xsi:type="File"></target>
27	<pre><!--Skip Quartz logs till Info and so log only own</pre--></pre>
28	<pre><logger maxlevel="&lt;/pre&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;th&gt;29&lt;/th&gt;&lt;td&gt;&lt;pre&gt;&lt;logger name=" meridium.core.scheduling.*"="" minlevel="Info" minlevel<="" name="Quartz.*" pre=""></logger></pre>
30	<pre><logger minl<="" name="Meridium.MechanicalIntegrity.*" pre=""></logger></pre>
31	<pre><logger componentspace.*"="" meridium.integration.*"="" minlevel="Debug" name="Meridium.Api.Connect.*" pre="" w<=""></logger></pre>
34	<pre><logger <="" minlevel="Info" name="*" pre="" writeto="allfile"></logger></pre>
35	-
36	L
27	

The ComponentSpace SAML trace is enabled.

IIS reset and Redis restart are not required after this change. You must refresh the browser and complete the SSO workflow. This will create a file, sp.log in the C:\ProgramData\Meridium\Logs folder and write the SAML trace to it.

**Note:** It is recommended to disable the SAML trace after the troubleshooting is complete as it may impact performance of the production system.

#### **Frequently Asked Questions**

#### **FAQs for SSO**

#### Is Azure AD supported as an Identity Provider in APM?

Yes, Azure AD for SAML SSO can be configured in APM. For more information, refer to Configure Azure Active Directory as the Identity Provider (IDP) on page 4.

#### How to enable ComponentSpace SAML trace?

You can enable ComponentSpace SAML trace to generate logs for troubleshooting. For more information, refer to Enable ComponentSpace SAML trace on page 52.