

Asset Performance Management APM Classic V4.6.11.0.0

Single Sign On

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	46
About Enabling APM SSO	47
About Host Names	47
Enable SSO On Site Authentication Using Active Directory	47
Enable SSO Off-Site Authentication Using APM Server Setup	48
Chapter 4: Configure APM Server	50
Configure APM Server	51
Chapter 5: Troubleshooting	54
Troubleshooting Scenarios	55
Frequently Asked Questions	57

Copyright Digital, part of GE Vernova

© 2025 GE Vernova and/or its affiliates. All rights reserved.

GE, the GE Monogram, and Predix are trademarks of General Electric Company used under trademark license.

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

Overview

Topics:

- Overview of Single Sign-OnSSO Workflow

Overview of Single Sign-On

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

- $\leftarrow \rightarrow \ {
 m C}$ $\ \,$ $\ \,$ portal.azure.com/#home 😒 🗯 🔔 📅 Anns 🔟 FASTAG RECHARGE 🙈 Rally 😤 Gold Team - Dev CL. 📃 SDI 📃 Deployment Validat. 📃 Patches 📃 Automation 📃 AD 😤 Patches - Gold team 🔗 Allocation 📃 Coverity » Other bookmarks 🔠 Reading I ,P Search reso Microsoft Azure Welcome to Azure! Don't have a subse Check out the following options Start with an Azure free trial Manage Azure Active Directory Access student benefits Manage access, set smart policies, and enhance security with Azure Active Directory. Get free software, Azure credit, or access Azure Dev Tools for Teaching after you verify your academic status. Get \$200 free credit toward Azure products and services, plus 12 months of popular free services. Start Learn more D View Learn more Explore Learn more 🗗 Azure services +SQL **W** 8 Create a
- 1. Sign in to the Azure portal and select **Azure Active Directory**.

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

	The transmission of the state o	• • • • • • • • • • • • • • • • • • •								
 Create a resource 	Enterprise applications	s - All appli	cations							
Home		« + Nev	w application	Columns						
Dashboard	Overview	^								
All services	 Overview 	Applicatio	ion Type rise Applications	\sim	Applications status Any	~	Application visibility Any	~	Apply Rese	
FAVORITES	Manage	Enterpr	ise Applications	Ŷ	Any	v	Any	Ŷ	мрру кезе	с ч
App Services	All applications	First 50) shown, to search all c	f your ap	plications, enter a display	name or the app	olication ID.			
Function App	Application proxy	NAME			HOMEPAGE URL			OBJECT ID		APPLICATION ID
SQL databases	User settings	2	Asset Performan	e Mana	gemei			a5055119-db45	4923-956d-d7570621	46ed8f77-e062-4bce-bb95
Azure Cosmos DB	Security	•	Asset Performant	e Mana	gemei			96d803e5-3016	-4896-81db-d28a75e9	2e54f355-2498-4a5a-93e9.
Virtual machines	Conditional Access	0	Office 365 Exchan	nge Onli	ne http://office.mi	crosoft.com/o	utlook/	3b0e3709-93cc	-4830-a33d-b96defd4	00000002-0000-0ff1-ce00-
Load balancers	Activity	ø	Office 365 Manag	gement /	APIs			5008761a-19dd-	48ed-b043-4e25bac0	c5393580-f805-4401-95e8-
Storage accounts	Sign-ins	0	Office 365 Sharel	Point On	line http://office.mi	crosoft.com/sl	harepoint/	dd333e69-4b2c	-4bda-bdf3-792fb39a	00000003-0000-0ff1-ce00
Azure Active Directory	🛍 Usage & insights (Preview)		onprem-apm-tes	t-NEW				ebe17c60-5f38-	4724-b8a8-330edb1f5	01c7ee4f-2f13-4119-b454-8
Monitor	Audit logs		Outlook Groups					7-4-6d0o.4dc8	4bo6 ab99 4d8b41oc	925eb0d0-da50-4604-a19f-
Advisor	듣 Access reviews									
Security Center	Troubleshooting + Support	- <u>-</u>	Same Sign on					2f37ea7d-9962-	4694-bc77-d4f9d413	b12afa8d-6ecb-4fb6-b761
Cost Management + Bill	Virtual assistant (Preview)	SF	Skype for Busine	s Online	2			822dcb0d-e9a2	-44ff-aa0c-65d94227	00000004-0000-0ff1-ce00

3. Select **New application**. The **Add an application** section appears.

	« Home > Enterprise applications	- All applications >	Categories > Add an applicatio	n	
+ Create a resource	Categories	×	Add an application		☆ □ ×
A Home	All (3171)	A	Add your own app		
	Business management (400)		Application	On-premises	Non-gallery
+ FAVORITES	Collaboration (454)		you're developing	application	application
··· • • •	Construction (7)		Register an app you're	Configure Azure AD Application Proxy to	Integrate any other application that you
App Services Function App	Consumer (44)		working on to integrate 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	.9	
👤 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		
Monitor	Finance (258)		CON		
Advisor	Health (63)		Box Con	cur Cornerstone C)
Security Center	Human resources (290)				
 Cost Management + Bill Help + support 	IT infrastructure (194)		DC	•• O	

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

<	Home > apmtestad > Enterprise applie	cations - All	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)		Application	On-premises	Non-gallery		The display name for your new application
	Collaboration (454)		you're developing	On-premises application	application		Once you decide on a name for your new
All resources	Construction (7)	_	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		configuration steps to get the application working.
🔕 App Services	Content management (153)						working.
🤣 Function App	CRM (155)		Add from the gallery				Supports: 🚯
👼 SQL databases	Data services (149)		riad norm the gallery				SAML-based single sign-on Learn more
🖉 Azure Cosmos DB	Developer services (109)		Enter a name				
👰 Virtual machines	E-commerce (75)		Featured applications				Automatic User Provisioning with SCIM Learn more
Load balancers	Education (145)						Password-based single sign-on
Storage accounts	ERP (92)		box	C • C			Learn more
••• Virtual networks	Finance (258)						
Monitor	Health (63)		Box Con	cur Cornerstone C)		
👎 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.

0	Home > apmtestad > Enterprise app	ications - All applications > Asset Performance Management - Single sign-on	
Create a resource	Asset Performance Ma Enterprise Application	nagement - Single sign-on	
🛧 Home		«	
🛄 Dashboard	📕 Overview	Select a single sign-on method Help me decide	
■ All services	💅 Getting started		
+ FAVORITES	Deployment Plan	Disabled දිරි 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.	
S App Services	Owners		
۶ Function App	R ^R Users and groups		
SQL databases	 Single sign-on 		
Azure Cosmos DB	Provisioning	Password-based Cinked Password storage and replay using a Linked	
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.

*	Home > apmtestad > Enterprise ap	pplications - All a	pplications > Asset Performance Management -	Single sign-on > SAML-based sign-on	
+ Create a resource	Asset Performance Manage	gement - SA	ML-based sign-on		
A Home		≪ 🕇 Upl	oad metadata file 🏾 🍤 Change single sign-on n	node 🔚 Validate this application 📔 💙 Got	feedback?
🛄 Dashboard	Overview	A			
All services	💅 Getting started	Set u	p Single Sign-On with SAML		
* FAVORITES	聞 Deployment Plan				
All resources	Manage		he configuration guide of for help integrating As	set Performance Management.	
(🐑 Resource groups	-	0	Basic SAML Configuration		
Services	Properties		Identifier (Entity ID)	Required	
Function App	🍰 Owners		Reply URL (Assertion Consumer Service URL)	Required	
	x ^R Users and groups		Sign on URL Relay State	Optional Optional	
SQL databases	Single sign-on		Logout Url	Optional	
2 Azure Cosmos DB	Provisioning				
👰 Virtual machines	Application proxy	2	User Attributes & Claims		/
💠 Load balancers	Self-service		Givenname	user.givenname	
🧮 Storage accounts	C Sell-Selvice		Surname	user.surname	
Virtual networks	Security		Emailaddress	user.mail	
Azure Active Directory	Conditional Access		Name Unique User Identifier	user.userprincipalname user.userprincipalname	
Monitor	👫 Permissions		•		
	Token encryption (Preview)	8			
🌪 Advisor		• •	SAML Signing Certificate		

8. In the **Basic SAML Configuration** section, select <a>. 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 👩	
Sign on URL I	
Enter a sign on URL	
Enter a sign on URL Relay State 💿	
Enter a sign on URL Relay State 💿	

9. Enter the following details.

ldentifier (Entity ID)	Enter a unique ID. Note: This ID will be used in the saml.json file for the service provider name. Therefore, note the ID.
Reply URL (Assertion Consumer Service URL)	The application callback URL where the response will be posted. Enter the URL in the following format: https:// <apm name="" server="">/ Meridium/api/core/security/ssologinauth, where <apm server<br="">Name> is the name of the APM server.</apm></apm>
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	C
Azure AD Identifier	https://sts.windows.net/78dd76d6-f3b7-4b89-9ef	Q
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 42, 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/
```

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 21
- 3. Add Certificates on page 27
- 4. Federation Service Identifier from ADFS on page 44

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.

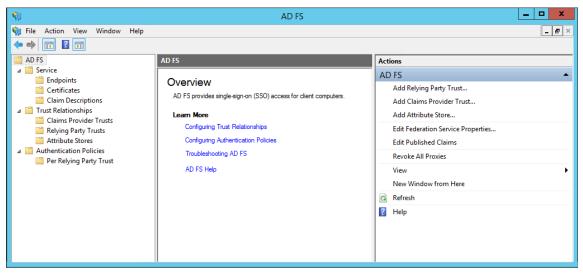
Note: To add adfs/ls endpoint, refer to the AD FS documentation.

• 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.

\$ 0	Add Relying Party Trust Wizard
Welcome	
Steps • Velcome • Select Data Source • Configure Multi-factor Authentication Now? • Choose Issuance Authorization Rules • Ready to Add Trust • Finish	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.

\$	Add Relying Party Trust Wizard
Select Data Source	
 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 	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 and or on a local network. Eederation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Erderation metadata file location: @ Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization.
	< Previous Next > Cancel

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

\$	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>
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
 Finish 		
	< <u>P</u> revious <u>N</u> ext > Cance	1

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

\$	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	
Choose Profile	security token encryption and the SAML 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 Multifactor Authentication Now?		
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
Finish		
	< <u>P</u> revious <u>N</u> ext > Cance	el

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

\$	Add Relying Party Trust Wizard	x
Configure Certificate		
Steps Welcome Select Data Source Select Data Source Choose Profile Configure Certificate Configure URL Configure URL 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 Issuer: Subject: Effective date: Expiration date: Mew Browse Remove	4

8. Select **Next**. The **Configure URL** page appears.

\$	Add Relying Party Trust Wizard	x
Configure URL		
 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 	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 URLs to use. Support for the WS-Trust 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: 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 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: Integration Net/SSO protocol. Relying party SAML 2.0 SSO service URL: Integration Integration Com/Meridium/api/core/security/ssologinauth Example: https://www.contoso.com/adfs/ls/	the

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.

\$	Add Relying Party Trust Wizard	×
Configure Identifiers	;	
Steps	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers	s for this relving
Welcome	party trust.	
Select Data Source	Relying party trust identifier:	
Specify Display Name		Add
Choose Profile	Example: https://fs.contoso.com/adfs/services/trust	
Configure Certificate	Relying party trust identifiers:	
Configure URL	um:componentspace:Meridium	Remove
Configure Identifiers		
Configure Multi-factor Authentication Now?		
 Choose Issuance Authorization Rules 		
Ready to Add Trust		
Finish		
	< Previous Next >	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.

\$	Add Relying Party Trust Wizard
Steps Welcome	Configure multi-factor authentication settings for this relying party trust. Multi-factor authentication is required if there is a match for any of the specified requirements.
 Select Data Source Specify Display Name Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules 	Multi-factor Authentication Global Settings Requirements Users/Groups Not configured Device Not configured Location Not configured
 Ready to Add Trust Finish 	 I do not want to configure multi-factor authentication settings for this relying party trust at this time. Configure multi-factor authentication settings for this relying party trust. You can also configure multi-factor authentication settings for this relying party trust by navigating to the Authentication Policies node. For more information, see <u>Configuring Authentication Policies</u>.
	< 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		
Steps	Issuance authorization rules determine whether a user is permitted to receive claims for the relving party.	
Welcome	Choose one of the following options for the initial behavior of this relying party's issuance authorization rules.	
Select Data Source	Permit all 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	
Configure Identifiers	later add issuance authorization rules to enable any users to access this relying party.	
Configure Multi-factor Authentication Now?	You can change the issuance authorization rules for this relying party trust by selecting the relying party trust	
 Choose Issuance Authorization Rules 	and clicking Edit Claim Rules in the Actions pane.	
Ready to Add Trust		
 Finish 		
	< <u>P</u> revious <u>N</u> ext > Cancel	

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

\$	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 configuration database. Encryption Signature Accepted Claims Organization Endpoints Notes Advanced Specify the encryption certificate for this relying party trust. Encryption Encryption Subject: Issuer: Subject: Effective date: Expiration date: View View View Cancel Encryption Issuer:	

14. Select **Next**. The **Finish** page appears.

\$	Add Relying Party Trust Wizard
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.
	Qlose

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 21

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.

Edit Claim Rule	es for urn:componentspace:Meridium 📃 🗖 🗙		
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules The following transform rules specify the claims that will be sent to the relying party.			
Order Rule Name	Issued Claims		
Add Rule	Rule <u>R</u> emove Rule		
	OK Cancel Apply		

3. Select Add Rule. The Add Transform Claim Rule Wizard window appears.

\$ #	Add Transform Claim Rule Wizard
Select Rule Templa	te
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 nule 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.

\$ 1	Add Transform Claim Rule Wizard	x
Configure Rule		
Steps Choose Rule Type Configure Claim Rule	You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule. Claim rule name: 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 Attribute (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** dropdown 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.

\$		Add Transform Claim Ru	le	Wizard	x
Configure Rule					
Configure Rule Steps • Choose Rule Type • Configure Claim Rule	which issued Qlaim Meridi Rule t Attribu Active		pes	DAP attributes as claims. Select an attribute store from attributes will map to the outgoing claim types that will be v : Outgoing Claim Type (Select or type to add more) Name ID E-Mail Address	
				< <u>P</u> revious Finish Cancel	

7. Select Finish.

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

翰 🛛 Edit Claim Rules	s for urn:componentspace:Meridium	
Issuance Transform Rules	Issuance Authorization Rules Delegation Authorization R	ules
The following transform n	les specify the claims that will be sent to the relying party.	
Order Rule Name	Issued Claims	
1 Meridium Claim	s E-Mail Address,Given Na	
Add Rule Edit 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 27

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 28
- 2. Export the Public Key Certificate on page 32

- 3. Copy the Certificate to Active Directory on page 39
- 4. Install the Token Signing idp.cer Certificate on the Application Server on page 42

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.

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.

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: Microsoft Windows			
Show detail	s 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.

🗧 嵾 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	Password
port option	s:
	strong private key protection. You will be prompted every time the key is used by an application if you enable this option.
	is key as exportable. This will allow you to back up or transport your a later time.
Protect	private key using virtualized-based security(Non-exportable)
🗸 Include	all extended properties.

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

Sertificate Import Wizard	
Certificate Store Certificate stores are system areas where certific	ates are kept.
Windows can automatically select a certificate sto the certificate.	ore, or you can specify a location for
 Automatically select the certificate store ba 	ased on the type of certificate
O Place all certificates in the following store	
Certificate store:	
	Browse
	Next Ca

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

	X
📀 🌛 Certificate Import W	izard
Completing the C	ertificate Import Wizard
The certificate will be import You have specified the follow	
	Automatically determined by the wizard
Content	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 32

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	Microsoft Cor				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	_			
IP Security Policy M	Microsoft Cor	\sim			Advanced
scription:					
cription:					

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: • Local computer: (the computer this console is running on)	
O Another computer: Browse	
Allow the selected computer to be changed when launching from the command line. The only applies if you save the console.	is
< Back Finish Ca	ncel

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

iap-in	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Gertificates (Local Computer)	
Authorization Manager	Microsoft Cor				Remove
Certificates	Microsoft Cor	=			
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				
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	_			
IP Security Policy M	Microsoft Cor	~			Advanced

- 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.

	Console1 -	Console Root\Certificates (Loc	al Computer)\Pers	onal\Certificates]				X
File Action View Favorites	Window Help						-	8
• 🔿 🙍 📰 🤞 🖬 🗶 🖬 🛙	🔒 🛛 💼							
	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	State	Actions	
	BLRQAVM23.meridium.com	BLRQAVM23.meridium.com	09-05-2019	Server Authenticati	ssotest		Certificates	
	localhost	localhost	26-08-2021	Server Authenticati	IIS Express Develop		More Actions	
	localhost	localhost WMSvc-WIN-ARLO9PKINBO	19-05-2020 17-04-2026	Server Authenticati Server Authenticati	IIS Express Develop <none></none>			
	WMSvc-WIN-ARLO9PKINBQ		31-12-2049	<pre>Server Authenticati</pre>	<none> CN=www.sp.com</none>		www.sp.com	
Intermediate Certification	sa www.sp.com	www.sp.com	51-12-2049	SAII2	Civ=www.sp.com		More Actions	
Trusted Publishers								
Untrusted Certificates								
Third-Party Root Certificat								
Trusted People								
Client Authentication Issue								
Remote Desktop								
Certificate Enrollment Req								
Smart Card Trusted Roots								
Trusted Devices								
Web Hosting								
III > 4	<	ш				>		
								-

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, click Next.

Y

9. Select Next.

📀 🍠 Certificate Export Wizard
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.

 Select the format you want to use: DER encoded binary X.509 (.CER) Base-64 encoded X.509 (.CER) Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties Microsoft Serialized Certificate Store (.SST) 	E	xport File Format Certificates can be exported in a variety of file formats.
 Base-64 encoded X.509 (.CER) Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties 		Select the format you want to use:
 Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties 		• DER encoded binary X.509 (.CER)
 Include all certificates in the certification path if possible Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties 		O Base-64 encoded X.509 (.CER)
 Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties 		Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 Include all certificates in the certification path if possible Delete the private key if the export is successful Export all extended properties 		Include all certificates in the certification path if possible
 Delete the private key if the export is successful Export all extended properties 		O Personal Information Exchange - PKCS #12 (.PFX)
Export all extended properties		Include all certificates in the certification path if possible
		Delete the private key if the export is successful
O Microsoft Serialized Certificate Store (.SST)		Export all extended properties
		 Microsoft Serialized Certificate Store (.SST)

Y

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

	X
📀 🛃 Certificate Export Wizard	
File to Export Specify the name of the file you wa	nt to export
File name:	Browse
	Next Cancel

- 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 42, steps 5
 - 8 for detailed process of installing the certificate.

Next Steps

• Copy the Certificate to Active Directory on page 39

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.

File Action View Window Help				_
• 🔿 📶 🖬 🖬	Relying Party Trusts	_		Actions
Service Service Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies	Keying Yarty Trusts Display Name Device Registration Service um componentspace Mendum um componentspace Mendumsour um componentspace Mendumsoor	Yes WS Yes WS	T um:ms-drs:blmgmtad.abc.com	Actions Relying Party Trusts Add Relying Party Trust Add Non-Claims-Aware R. View New Window from Here Image: Refresh Help urn:componentspace:Me. Update from Federation Edit Claim Rules Disable Properties Delete Help

- 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.

Irganization	Endpoints	Proxy End	dpoints	Notes	Advance
lonitoring	Identifiers	Encryption	Signatu	ure Ac	cepted Clain
becify the sig arty.	nature verifica	tion certificate	s for requ	ests from t	his relying
Subject	Issu	ier	Effecti	ve Date	Expirat
<		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**.

urn	component:	tspace:Me	eridium Pr	operti	es X
Monitoring	Identifiers	Encryption	Signature	Acce	epted Claims
Organization	Endpoints	Proxy End	points N	lotes	Advanced
Specify the	secure hash alg	orithm to use	for this relyin	g party t	rust.
Secure hash	algorithm: SH	IA-1			~
		OK	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 42

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 Current Machine
To continue, dick Next.
Next Cancel

6. Select Local Machine, and then select Next.

Sertificate Import Wizard	
Certificate Store Certificate stores are system areas where ce	rtificates are kept.
Windows can automatically select a certificate the certificate.	e store, or you can specify a location for
 Automatically select the certificate stor 	e based on the type of certificate
O Place all certificates in the following sto	ore
Certificate store:	
	Browse
	Next Car

- 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 47

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 47
- Enable SSO Off-Site Authentication Using APM Server Setup on page 48

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 51

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.

	à	🎝 Ho	ost Name	s ×
Host Names		F	ป พ.15.02	
				Name
				64m19x002mmonidium.uem
				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 51

Chapter Δ

Configure APM Server

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 Alias
•	
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://myadfsserver/adfs/ls.
 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"
                         }
                    ]
                },
                "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"
                             }
                         ]
                    }
                1
            }
        1
    }
}
```

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 55

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.;</td></tr><tr><th>3</th><th><pre>xmlns:xsi=" xmlschema-inst<=""></nlog>
4	autoReload="true"
5	internalLogLevel="Warn"
6	<pre>internalLogFile="internal-nlog.txt"></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:\</td></tr><tr><th>16</th><td><pre><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:</td></tr><tr><th>21</th><td>- </targets></td></tr><tr><th>22</th><td></td></tr><tr><th>23</th><td><! rules to map from logger name to target></td></tr><tr><th>24</th><td>₽ <rules></td></tr><tr><th>25</th><td><pre><!Skip Microsoft logs and so log only own logs</pre></td></tr><tr><th>26</th><td><pre><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="</pre></td></tr><tr><th>29</th><td><pre><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 55.