

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	45
About Enabling APM SSO	46
About Host Names	46
Enable SSO On Site Authentication Using Active Directory	46
Enable SSO Off-Site Authentication Using APM Server Setup	46

Chapter 4: Configure the Server	48
---------------------------------	----

Configure APM Server

49

Copyright Digital, part of GE Vernova

© 2024 General Vernova and/or its affiliates.

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

This document may contain Confidential/Proprietary information of and/or its suppliers or vendors. 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)

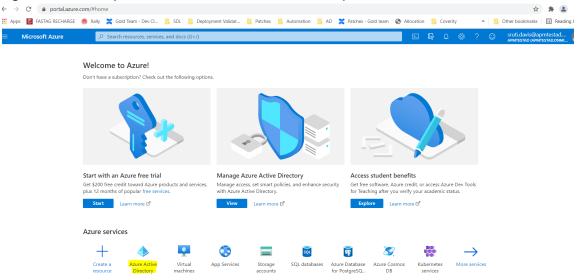
Configure Azure Active Directory as the Identity Provider (IDP)

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.

	« Home > Enterprise applications - All a	applications				
Create a resource	Enterprise applications apmtestad - Azure Active Directory	- All applications				
A Home		≪ + New application ■ Columns				
Dashboard	Overview	·				
■ All services	1 Overview	Application Type Enterprise Applications	Applications status Any V	Application visibility	Apply Reset	
FAVORITES	Manage				nuppy nearer	
App Services	All applications		plications, enter a display name or the app			
Function App	Application proxy	NAME	HOMEPAGE URL	OBJECT ID	APPLICATION ID	
SQL databases	User settings	Asset Performance Mana	gemei	a5055119-db4	-4923-956d-d7570621 46ed8f77-e062-4b	oce-bb95
Azure Cosmos DB	Security	Asset Performance Mana	gemei	96d803e5-301	5-4896-81db-d28a75e9 2e54f355-2498-4a	a5a-93e9
Virtual machines	Conditional Access	Office 365 Exchange Onli	ne http://office.microsoft.com/o	utlook/ 3b0e3709-93c	-4830-a33d-b96defd4 00000002-0000-0f	ff1-ce00
Load balancers	Activity	Office 365 Management	APIs	5008761a-19do	l-48ed-b043-4e25bac0 c5393580-f805-44	401-95e8
Storage accounts	Sign-ins	Office 365 SharePoint On	line http://office.microsoft.com/s	harepoint/ dd333e69-4b2	c-4bda-bdf3-792fb39a 00000003-0000-0f	ff1-ce00
Azure Active Directory	🚻 Usage & insights (Preview)	onprem-apm-test-NEW		ebe17c60-5f38	-4724-b8a8-330edb1f5 01c7ee4f-2f13-4119	9-b454-8
Monitor	Audit logs	Outlook Groups		7a4a6d0e-4dc	8-4be6-ab99-4d8b41ec 925eb0d0-da50-46	604-a19f-
Advisor	E Access reviews	Same Sign on			-4694-bc77-d4f9d413 b12afa8d-6ecb-4fb	
Security Center	Troubleshooting + Support			213/ea/d-996	-4094-DC//-04190415 D1281880-86CD-410	00-0761
Cost Management + Bill	Virtual assistant (Preview)	SF Skype for Business Online	2	822dcb0d-e9a	2-44ff-aa0c-65d94227 00000004-0000-0f	ff1-ce00

3. Select New application.

The **Add an application** section appears.

Create a resource	Categories	×	Add an application		2 🗅
🛧 Home	All (3171)	^	Add your own app		
All services	Business management (400)			On-premises	Non-gallery application
+ FAVORITES	Collaboration (454)		you're developing	application	
App Services	Construction (7)		Register an app you're	Configure Azure AD Application Proxy to	Integrate any other application that you
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	P	
👤 Virtual machines	Data services (149)	_	,,,, ,		
铃 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)				
🜪 Advisor	Health (63)		Box Cond	cur Cornerstone C)
Security Center	Human resources (290)				
Cost Management + Bill	IT infrastructure (194)				

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.

*	Home > apmtestad > Enterprise applica	ions - All applications > Asset Performance Management - Single sign-on	
+ Create a resource	Asset Performance Mana Enterprise Application	gement - Single sign-on	\times
🛧 Home	 Encland Approximit « 		
🖪 Dashboard	Soverview	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.	
🔇 App Services	Owners		
Function App	x ^R Users and groups		
SQL databases	 Single sign-on 		
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.

<	K Home > apmtestad > Enterprise appli	ications - All applications > Asset Performance Manage	ment - Single sign-on / SAML-based sign-on	
Create a resource	Asset Performance Manager	ment - SAML-based sign-on		
🛧 Home	0	≪ ↑ Upload metadata file	n-on mode 🛛 \Xi Validate this application 📗 🂙 Got fi	eedback?
💷 Dashboard	📕 Overview			
All services	💅 Getting started	Set up Single Sign-On with SAML		
* FAVORITES	Deployment Plan	Read the configuration guide of for help integra	ting Asset Parformance Management	
All resources	Manage		ang Asset Performance Management.	
🐑 Resource groups	Properties	Basic SAML Configuration		
🔇 App Services	Owners	Identifier (Entity ID)	Required	
🦘 Function App	-	Reply URL (Assertion Consumer Service Sign on URL	e URL) Required Optional	
💀 SQL databases	g ^R Users and groups	Relay State	Optional	
Azure Cosmos DB	Single sign-on	Logout Url	Optional	
Virtual machines	Provisioning	2		
Load balancers	Application proxy	User Attributes & Claims		/
ř.	Self-service	Givenname	user.givenname	
Storage accounts		Surname	user.surname	
Virtual networks	Security	Emailaddress Name	user.mail	
Azure Active Directory	Conditional Access	Name Unique User Identifier	user.userprincipalname user.userprincipalname	
Monitor	A Permissions			
Advisor	Token encryption (Preview)	 SAML Signing Certificate 		1

8. In the Basic SAML Configuration section, select 🖋.

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)	Note: 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/v1/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			
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 and install it. Please refer to section Install the Token Signing idp.cer Certificate on the Application Server on page 41, steps 5 - 8 for installing the certificate.

```
14. Modify the saml.json file found in C:\Program Files\Meridium\ApplicationServer \api 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/v1/core/security/ssologinauth",
            "LocalCertificates":
            ſ
            {
                "FileName": "sp.pfx",
                "Password": "password"
            1
        },
        "PartnerIdentityProviderConfigurations":
        Γ
        {
            "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/2001/04/xmldsig-
more#rsa-sha256",
            "PartnerCertificates":
            {
                 "FileName": "sdsso.cer"
            1
        1
    }
    1
}
```

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 10
- 2. Add Claim Rules on page 21
- 3. Add Certificates on page 27
- 4. Federation Service Identifier from ADFS on page 43

Add Relying Party Trusts

Before You Begin

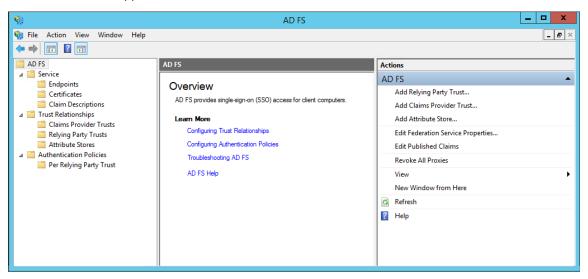
- You must have administrative privileges to configure AD FS.
- Ensure that the /adfs/Is endpoint exists for SAML v2.0.

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.

\$	Add Relying Party Trust Wizard
Welcome	
Steps • Velcome • Select Data Source • Configure Multifactor 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 Cettificate 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 online or on a local network.

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	I

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	!

7. 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 • Specify Display Name • 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	
	< <u>P</u> revious <u>N</u> ext > Cance	:

8. Select Next.

The **Configure URL** page appears.

\$	Add Relying Party Trust Wizard	x
Configure URL		
Steps Velcome 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/ ✓ 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: Intps://comerciteumserver>. Net/SO protocol. Relying party SAML 2.0 SSO service URL: Intps://www.contoso.com/adfs/ls/ Example: https://www.contoso.com/adfs/ls/ Previous Next > Cancel	le

- 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/v1/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	x
Configure Identifiers		
Configure Identifiers Steps Welcome Select Data Source Select Data Source Choose Profile Configure Certificate Configure URL Configure Identifiers Configure Identifiers Configure Multi-factor 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: Um.componentspace: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.

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

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 Au	thorization 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 <u>D</u> eny 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			
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 Encryption Encryption Signature Accepted Claims Organization Endpoints Notes Advanced Specify the encryption certificate for this relying party trust. Encryption Encrypti	

14. Select Next.

The **Finish** page appears.

\$ 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 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.

翰 🛛 Edit Claim Rule	s for urn:componentsp	ace:Meridium	• x
Issuance Transform Rules	Issuance Authorization Rules	Delegation Authorization F	Rules
The following transform	ules specify the claims that will	be sent to the relying party.	
Order Rule Name		Issued Claims	
			₽
Add Rule	Rule <u>R</u> emove Rule		
	OF	K 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.

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

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

7. Select Finish.

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

	s for urn:componentspace:Meridium	□ X
Issuance Transform Rules Issuance Authorization Rules Delegation Authorization Rules		
The following transform n	les specify the claims that will be sent to the relying party.	
Order Rule Name	Issued Claims	
1 Meridium Claime	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 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 41

Install the Service Provider certificate (sp.pfx)

Procedure

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

Note: GE Vernova provides the public key certificate file (sp.pfx). pfx is personal information exchange.

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

Welcome to	the Certificat	e Import Wiza	ard
	ou copy certificates, c to a certificate store.		nd certificate revocation
and contains inform	ation used to protect	ation authority, is a co data or to establish s stem area where certi	
Store Location			
O Current User			
Local Machine			
To continue, dick Ne	ext.		

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 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.

🕞 🍠 Ce	rtificate Import Wizard
File to	Import
	pecify the file you want to import.
E	le name:
-	C: \Program Files \Meridium \ApplicationServer \api \sp.pfx Browse
Ľ	Diowaciii
N	ote: 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.

\checkmark	Display Password
mpo	rt options:
	Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
] Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
	Protect private key using virtualized-based security(Non-exportable)
\checkmark	Include all extended properties.

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

 \times

3	Certificate Import Wizard
G	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.
	 Automatically select the certificate store based on the type of certificate
	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 fol	
	d 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 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.

ap-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	~			Advanced

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: Image: Image:	\$
< Back Finish Ca	ncel

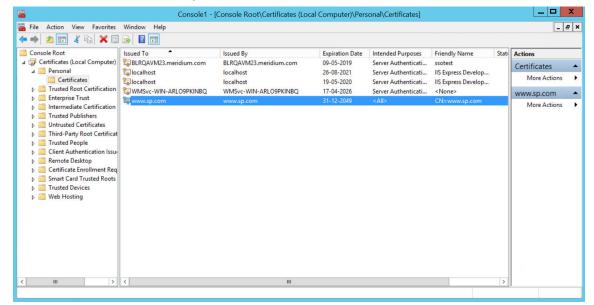
5. Select the Local computer option, and then select Finish.

	Vendor	^		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			Gertificates (Local Computer)	-
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					
Internet Informatio					
Internet Informatio					
IP Security Monitor	Microsoft Cor	-			Advanced
IP Security Policy M	Microsoft Cor	Y			Advanced

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.

V

	X
📀 🍠 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 Cance	1

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

Export File Format Certificates can be exported in a var	riety of file formats.
Select the format you want to use:	
DER encoded binary X.509 (.	CER)
O Base-64 encoded X.509 (.CE	R)
🔘 Cryptographic Message Synta	ax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in t	he certification path if possible
O Personal Information Exchange	ge - PKCS #12 (.PFX)
Include all certificates in t	he certification path if possible
Delete the private key if t	the export is successful
Export all extended prope	erties
O Microsoft Serialized Certificat	e Store (.SST)

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

X

	X
📀 🛃 Certificate Export Wizard	
File to Export Specify the name of the file you want to export	
File name: Browse	
Next Can	cel

- 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 41, 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		_ (
• 🔿 🙍 🖬 🖬 🖬		
AD FS	Relying Party Trusts	Actions
 Service Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies 	Display Name Enabled Type Identifier Device Registration Service Yes WS-T	

- 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	Endpoints	Proxy End	points	Notes	Advanced
Nonitoring	Identifiers	Encryption	Signatu	ure Acc	cepted Claim
pecify the sig arty.	nature verificat	ion certificate	s for reque	ests from th	his relying
Subject	Issue	er	Effecti	ve Date	Expiratio
<		III			>

- 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	operti	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	g party f	trust.
Secure has	h algorithm: S	HA-1			~
		ОК	Canc	el	Apply

10. Select Apply, and then select OK.

Next Steps

• Install the Token Signing idp.cer Certificate on the Application Server on page 41

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.

	X
💿 🝠 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.	
😵 Next 🛛 Can	icel

6. Select Local Machine, and then select Next.

📀 🥏 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.
 Automatically select the certificate store based on the type of certificate
O Place all certificates in the following store
Certificate store:
Browse
Next Cancel

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

Next Steps

• Enable SSO On Site Authentication Using Active Directory on page 46

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

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 46
- Enable SSO Off-Site Authentication Using APM Server Setup on page 46

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 Applications menu, navigate to ADMIN > Operations Manager > SSO Configuration. The SSO Configuration page appears.
- 2. In the IDP URL box, enter the PartnerIdentityProviderConfigurations Name value configured in the C:\Program Files\Meridium\ApplicationServer\api \saml.json file.
- 3. Select the SSO Enabled check box.
- 4. Select 🛅. The SSO configuration is saved.
- 5. Log out of APM.
- 6. 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 the saml.json file must 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.
- 7. 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.
- 8. Reset IIS.
- 9. Access APM via a web browser. SSO off-site authentication is enabled.

Next Steps

Configure APM Server on page 49.

Chapter 4

Configure the 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 Applications menu, navigate to ADMIN > Operations Manager > Data Sources. The Data Sources page appears.
- 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: {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": "https://<APM Server
Name>/Meridium/api/v1/core/security/ssologinauth",
            "LocalCertificates":
            Γ
            {
                "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"
        }
        1
    }
    1
```

9. Save and close the file saml.json.

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