## polarıs

## Polaris OAuth 2.0 Integration with Microsoft AD FS Guide

7.2

© 2022



World Headquarters 1900 Powell Street, Suite 400 Emeryville, CA 94608 +1.510.655.6200

### **Legal Notices**

© Innovative (Part of Clarivate) and/or its affiliates. All rights reserved. All trademarks shown are the property of their respective owners.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

The software and related documentation are provided under an agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of the software, unless required by law for interoperability, is prohibited.

### Contents

Introduction	1
Minimum Requirements	2
Polaris System Administration (Web-Based)	2
Leap with Active Directory and AD FS Authentication	2
Process Overview	3
Install Active Directory Federation Services	4
Configure Active Directory Federation Services	14
Verify Active Directory Federation Services Is Running	24
Verify that OAuth 2.0 is Enabled	26
Create an Application Group	28
Configure the AD FS Web Application: Claims and Permitted Scopes	34
Enable CORS on AD FS To Accept Requests from Polaris APIs	40
Set Up Web Services and Applications	. 41
Set Up Polaris.AdminServices	41
Set Up PolarisAdmin	45
Set Up Polaris.ApplicationServices	50
Set Up LeapWebApp	54
Enable Session Storage for LeapWebApp	58
Add a URL Rewrite Rule for LeapWebApp	59
Sample Rewrite Rule Text	60
Additional URL Rewrite Resources	60
Customize the AD FS Pages	62
Change the Access Token Lifetime	63
Bind a New SSL Certificate	64
Troubleshoot	65

Force a logout	. 65
AD FS in one-way trust	. 65
Receiving "User is not a valid Polaris user." error	65
Troubleshoot Redirect URIs	65

### Introduction

Polaris System Administration (web-based) requires OAuth 2.0 with OpenID and PKCE. As of version 7.2, Leap supports using OAuth 2.0 with OpenID.

When configured, staff authentication for Polaris System Administration (web-based) and Leap is handled by Active Directory and Active Directory Federation Services.

### Important:

The mechanism used to connect an Active Directory user to a Polaris user is the user principal name (UPN) in the format of an email address. For example, user@mydomain.com. During the account verification process, we request the UPN claim from Active Directory. This must return a UPN in the name@domain format. The Polaris.AdminServices (API) can then use that information to map the AD user to a Polaris user.

### **Minimum Requirements**

Polaris System Administration (Web-Based)

To use Polaris System Administration (web-based), you must have the following installed:

- Windows Server 2019 Standard
  - Polaris requires OAuth 2.0 with PKCE support
  - AD FS on Windows Server 2019 supports PKCE
- Active Directory Domain Services
- SSL Certificate
  - Publicly trusted CA signed certificate
- Polaris 7.1

Leap with Active Directory and AD FS Authentication

To use Leap with Active Directory and AD FS authentication, you must have the following installed:

- Windows Server 2019 Standard
  - Polaris requires OAuth 2.0 with PKCE support
  - AD FS on Windows Server 2019 supports PKCE
- Active Directory Domain Services
- SSL Certificate
  - Publicly trusted CA signed certificate
- Polaris 7.2

### **Process Overview**

To configure Polaris OAuth Support with AD FS, perform the following tasks:

- 1. Install Active Directory Federation Services.
- 2. Configure Active Directory Federation Services.
- 3. Verify that Active Directory Federation Services is running.
- 4. Verify that OAuth 2.0 is Enabled.
- 5. <u>Create an Application Group for Polaris LeapWebApp</u>.
- 6. Configure the AD FS Web Application: Claims and Permitted Scopes.
- 7. Enable CORS on AD FS to accept requests from Polaris APIs.
- 8. Set up web services and applications.
- 9. Enable session storage for LeapWebApp.
- 10. Add a URL rewrite rule for LeapWebApp.
- 11. <u>Customize the AD FS pages</u>.
- 12. <u>Change the access token lifetime</u>.
- 13. Bind a new SSL certificate.
- 14. Troubleshoot.

### **Install Active Directory Federation Services**

### To install AD FS

- 1. Sign in to Windows Server 2019 with administrative privileges.
- 2. Start the Server Manager desktop application.

🚡 Server Manager				– 🗆 X
Server Mana	ager • Dashboard	• (	🔊   🚩 Manage <u>T</u> ools	<u>V</u> iew <u>H</u> elp
Image: Dashboard     V       Image: Local Server     Image: Local Servers       Image: AD DS     DNS       Image: File and Storage Services     Image: Display Services	VELCOME TO SERVER MANAGER QUICK START QUICK START QUICK START QUICK START QUICK START QUICK CONTRACTOR CONTRAC	gure this local server roles and features other servers to manage ate a server group nect this server to cloud service	25	
R	LEARN MORE	DNS     1       ①     Manageability       Events     Services       Performance     BPA results	File and Storage Services Manageability Events Services Performance BPA results	1

3. On the Server Manager Dashboard view, select Add roles and features.

The Add Roles and Features Wizard opens.



4. On the Before You Begin tab, select Next.



5. On the **Installation Type** tab, select **Role-based or feature-based installation**, and then select **Next**.

📥 Server Mar	nager							- 🗆	$\times$
	- Server Manag	ger • Dashboard	- 	2. 2.	• @	Manage	Tools	View	Help
	🚘 Add Roles and Features Wizar	rd			- 🗆 ×				^
Local :	Select destinatio	n server		Po	DESTINATION SERVER plarisOauth.pol-qa-oauth.local				
All Ser	Before You Begin Installation Type	Select a server or a virtual hard	d disk on which to inst	all roles and features.					
B DNS	Server Selection	<ul> <li>Select a virtual hard disk</li> </ul>							
File ar	Server Roles Features	Server Pool							
		Name	IP Address Op	erating System					
		PolarisQauth.pol-qa-oau	10.25.197.8 Mid	rosoft Windows Server 20	19 Standard		1	Hide	
		and that have been added by newly-added servers from whi	using the Add Servers ch data collection is s	command in Server Mana ill incomplete are not sho	ager. Offline servers and wn.	lity	-		
			< <u>P</u> revious	<u>N</u> ext >	Install Cancel				
		Performance BPA results	Pert BPA	ormance results	Performa BPA resu	ance			
		File and Storage	1 Loc	al Server	1 All Serv	ers	1		Ŷ

6. On the Server Selection tab, select the server, and then select Next.

🚡 Server Manager						-	- 0	×
Server Manage	er • Dashboard		• ③	I <b>r</b>	<u>M</u> anage X	<u>T</u> ools	<u>V</u> iew	<u>H</u> elp
<ul> <li>Dasht</li> <li>Local</li> <li>All Set</li> <li>DNS</li> <li>DNS</li> <li>File ar</li> <li>Server Selection</li> <li>Server Roles</li> <li>Features</li> <li>AD FS</li> <li>Confirmation</li> <li>Results</li> </ul>	Select one or more roles to install o Roles  Active Directory Certificate Active Directory Domain Se Active Directory Commin Se Active Directory Cightweigh Active Directory Rights Man Device Health Attestation DHCP Server DHCP Server DHCP Server DHC Guardian Services Hyper-V Network Policy and Access Remote Access Remote Access Volume Activation Services	n the selected server.	DES Polaris Oauth Active Directory Fed (AD FS) provides sim identity federation a sign-on (SSO) capab includes a Federation enables browser-bas	TINATION SERV pol-ga-oauth lo plified, secure nd Web single lifties. AD FS 5 Service that wed Web SSO.	es ed e tora	age	Hidd	e
		< <u>P</u> revious <u>N</u> ext >	. <u>I</u> nstall	Cancel	I			
	Performance BPA results	Performance BPA results		Perfo BPA	ormance results			

- 7. On the Server Roles tab, do the following:
  - a. Verify that Active Directory Domain Services are installed.
  - b. Select the Active Directory Federation Services role.
  - c. Select Next.

Server Mar	Server Manac	ger 🕨 Dashboard		• ②	▶ Mana	ge <u>T</u> ools	<u>V</u> iew	] X
Image: Deshter in the second secon	Select features Before You Begin Installation Type Server Selection Server Roles Features AD FS Confirmation Results	Select one or more features to instal Features       Network Load Balancing     Network Virtualization     Peer Name Resolution Proto     Quality Windows Audio Vide     RAS Connection Manager Ar     Remote Assistance     Remote Assistance     Remote Server Administratic     SMPC over HTP Proxy     Setup and Boot Event Collecc     Simple TCP/IP Services     SMB 10/CISF File Sharing Sc     MB Bandwidth Limit     SMIP Service     Storage Migration Service Proces     Storage Regica     Storage Regica     System Data Archiver (Instal     System Data Archiver (Instal	I on the selected server.	DESTI PolarisOauth.pc Description Provides services to co archive Windows Serve	NATION SERVER I-qa-oauthJocai	torage	Hic	le
		Performance BPA results	< Previous Next > Performance BPA results	Install	Cancel Performar BPA result	ts		v

8. On the **Features** tab, select **Next**.

🚖 Server Mar	nager					- 0	$\times$
	Server Manage	er • Dashboard		• ③   <b>『</b> Mana	age <u>T</u> ools	<u>V</u> iew	<u>H</u> elp
Local     Local     All Ser     AD DS     DNS     File ar	Active Directory Fe Before You Begin Installation Type Server Roles Features AD FS Confirmation Results	torage	Hide				
			< Previous Next >	Install Cancel			
		Performance BPA results	Performance BPA results	Performa BPA resul	nce Its		Ų

9. On the **AD FS** tab, read the Active Directory Federation Services (AD FS) information, and then select **Next**.

📥 Server Ma	anager				_	
	Server Mana	ager 🕨 Dashboard		• 🕄   🚩 Man - 🗆 X	age <u>T</u> ools <u>'</u>	<u>V</u> iew <u>H</u> elp
Local : Local : All Ser AD DS DNS File ar	Confirm installa Before You Begin Installation Type Server Selection Server Roles Features AD FS Confirmation Results	tion selections	vices, or features on selected server, cli utomatically if required ation tools) might be displayed on this p lo not want to install these optional feat	DESTINATION SERVER PolarisOauth.pol-qa-oauth.local ck Install. page because they have tures, click Previous to clear	torage	Hide
			< Previous Next >	Install Cancel		
		Performance BPA results	Performance BPA results	Performa BPA resu	ince Its	

10. On the **Confirmation** tab, confirm your selections, and then select **Install**.



11. On the **Results** tab, select **Close** when the installation is complete.



- 12. On the Server Manager dashboard, verify that AD FS is an installed role.
- 13. Restart the server.

### **Configure Active Directory Federation Services**

#### To configure Active Directory Federation Services

1. Start the Server Manager desktop application.

The system generates a configuration notification.



2. Open the notification, and select **Configure the federation service on this server**.

The Active Directory Federation Services Configuration wizard opens.



3. On the Welcome tab, select Next.

📥 Active Directory Federation Serv	ices Configuration Wizard	– 🗆 X
Connect to Active	Directory Domain Services	TARGET SERVER PolarisOauth.pol-qa-oauth.local
Welcome Connect to AD DS	Specify an account with Active Directory domain adminis federation service configuration.	strator permissions to perform the
Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	iï\jeff.young	Change
	< Previous Ne:	kt > Configure Cancel

4. Select **Change**, and provide an administrator account. Then select **Next**.

pecify Service Pr	operties	TARGET SE PolarisOauth.pol-qa-oauth
Welcome Connect to AD DS Specify Service Properties	SSL Certificate:	*.polarislibrary.com v Import View
Specify Service Account Specify Database	Federation Service Name:	dev-fs.polarislibrary.com ~ Example: fs.contoso.com
Pre-requisite Checks Installation Results	Federation Service Display Name:	Polaris R&D Federation Service Users will see the display name at sign in. <i>Example: Contoso Corporation</i>

5. If not already installed on the server, select **Import** to install an SSL certificate.

Connect to AD DS	SSL Certificate:	*.polarislibrary.com v	Import
Specify Service Properties		View	
Specify Service Account	Federation Service Name:	dev-fs.polarislibrary.com	
Specify Database		Example: fs.contoso.com	
Review Options			
Pre-requisite Checks	Federation Service Display Name:	Polaris R&D Federation Service	
Installation		Users will see the display name at sign in.	
Results		Example: Contoso Corporation	

- 6. Enter the following, and then select **Next**:
  - Federation Service Name
  - Federation Service Display Name

📥 Active Directory Federation Serv	vices Configuration Wizard		-	- 🗆	×
Specify Service A	ccount		PolarisOauth.p	TARGET SE ool-qa-oauth	RVER I.local
▲ Group Managed Service Ac Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	<ul> <li>Specify a domain user acco</li> <li>Create a Group Manage</li> <li>Account Name:</li> <li>Use an existing domain</li> <li>Account Name:</li> <li>Account Name:</li> <li>Account Password:</li> </ul>	use the KDS Root Key has not been set ount or group Managed Service Account POL-QA-OAUTH\ o user account or group Managed Serv POL-QA-OAUTH\Po OL-QA-OAUTH\Po	t. Use the foll Si int. vice Account <u>Clear</u>	Select	×
		< Previous Next >	Configure	Cano	el

7. Specify a service account, and then select **Next**.

📥 Active Directory Federation Serv	vices Configuration Wizard		_		×
Specify Configura	ition Database	Ро	TAI IarisOauth.pol-q	RGET SEF a-oauth.	(VER local
Welcome Connect to AD DS Specify Service Properties	Specify a database to store the Active D Create a database on this server usir Specify the location of a SQL Server	irectory Federation Service co ng Windows Internal Database database	nfiguration data. e.		
Specify Database Review Options	Database Host Name:				
Pre-requisite Checks Installation Results	Database Instance:	To use the default instance, le	eave this field bla	nk.	
	< Pr	evious Next >	Configure	Cance	ł

8. Specify the location of the AD FS configuration database, and then select **Next**.

For simple scenarios, creating the local database is acceptable.

Active Directory Federation Servi	ces Configuration Wizard	_		×
Review Options	Pol	T/ arisOauth.pol-	ARGET SEI qa-oauth.	RVER local
Welcome	Review your selections:			
Connect to AD DS	This server will be configured as the primary server in a new AD FS far	m 'dev-		
Specify Service Properties	is polarisi brary.com .			
Specify Service Account	AD FS configuration will be stored in Windows Internal Database.			
Specify Database	Windows Internal Database feature will be installed on this server if it	is not already i	installed.	
Review Options	Federation service will be configured to run as POL-QA-OAUTH\Polari	sServices.		
Pre-requisite Checks	-			
Installation				
Results				
	These settings can be exported to a Windows PowerShell script to auto additional installations	omate	View scrip	t
	< Previous Next >	Configure	Cance	el 🛛

9. Review your selections, and then select **Next**.

All prerequisite checks pass	ed successfully. Click 'Configure' to begin installation.
Welcome Connect to AD DS	Prerequisites must be validated before Active Directory Federation Services is configured on this computer.
Specify Service Properties	Rerun prerequisites check
Specify Service Account	
Specify Database	
Review Options	Prerequisites Check Completed
Pre-requisite Checks	All prerequisite checks passed successfully. Click 'Configure' to begin installation.
Installation	
Results	

10. After you complete all pre-requisite checks, select **Configure**.

This server was successful	lly configured Show more
Welcome	View detailed operation results
Connect to AD DS	A machine restart is required to complete ADFS service configuration. For more
Specify Service Properties	Information, see: https://go.microsoft.com/fwlink/?LinkId=/98/25
Specify Service Account	fs.polarislibrary.com'. Configuring certificate authentication binding on port '49443' and
specify Database	hostname 'dev-fs.polarislibrary.com'.
Review Options	Failed to register SSL bindings for Device Registration Service: An item with the same key has already been added.
Pre-requisite Checks	
Installation	
Results	

11. When the configuration wizard has completed successfully, select **Close**, and then restart the server.

### **Verify Active Directory Federation Services Is Running**

### To verify that Active Directory Federation Services is running

1. Start the Server Manager desktop application.

AD FS should be green.

📥 Server Manager					
Server M	anager • Da	shboard			
<ul> <li>Dashboard</li> <li>Local Server</li> <li>All Servers</li> <li>AD DS</li> <li>AD FS</li> <li>DNS</li> <li>File and Storage Services ▷</li> </ul>	LEARN MORE ROLES AND SER Roles: 4 Server of AD DS Managea Events Services Performa BPA resu	5 Co VER GROUPS proups: 1   Servers total 1 bility nce ts	nnect	this server to cl AD FS Manageability Events Services Performance BPA results	oud services

2. Start the Services application and check the status.

🔍 Services					_		×
File Action View	Help						
<= ⇒   📰 🖾 🤇	à 🔒 🛛 📰 🕨 🔲 II 🕩						
Services (Local)	Name	Description	Status	Startup Type	Log On As		^
	Active Directory Domain Services	AD DS Dom	Running	Automatic	Local Syste		
	Active Directory Federation Services Enables Acti Running Automatic (Delayed POL-QA-O						
	Active Directory Web Services	This service	Running	Automatic	Local Syste		
	🎑 ActiveX Installer (AxInstSV)	Provides Us		Disabled	Local Syste		
	🔍 AllJoyn Router Service	Routes AllJo		Manual (Trigger Start)	Local Service		

- 3. Open the Edge (or Chrome) web browser and go to https://localhost/adfs/fs/federationserverservice.asmx
  - If you want to ignore certificate errors, select Advanced.

A page similar to the following image opens:

https://localhost/adfs/fs/federati x +			-	0	×
$\leftarrow$ $\rightarrow$ C 🔺 Not secure   https://localhost/adfs/fs/federationserverservice.asmx	τõ	£≡	Ē		
This XML file does not appear to have any style information associated with it. The document tree is shown below.					
<pre>vsubl:definitions xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/0 xmlns:i0="http://schemas.microsoft.com/ActiveDirectory/FederationService/2005/07/" xmlns:wsu="http://docs.oasis 200401-wss-wssecurity-utility-1.vsd" xmlns:wsa0e="http://www.w3.org/2005/08/addressing" xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" xmlns:wsap="http://schemas.xmlsoap.org/ws/2004/08/addr xmlns:msc="http://schemas.xmlsoap.org/ws/2004/01/2/ xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/01/2/ xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/01/2/ xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/01/2/ xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/01/2/ xmlns:wsa="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/" xmlns:soap="http://schemas.xmlsoap.org/wsd1" xmlns:wsa="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://tempuri.org/" xmlns:soap="http://schemas.xmlsoap.org/wsd1" xmlns:wsa="http://www.w3.org/2001/XMLSchema" xmlns:soaper="http://schemas.xmlsoap.org/soap/encoding/ name="ADFSTIrustInformationService" targetNamespace="http://tempuri.org/"&gt; vswsp:Policy vswsp:Policy vswsp:Policy vswsp:Policy vswsp:Policy vswsp:Policy vswsp:Policy vsy:piransportBinding xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"&gt; vswsp:Policy vsp:Policy vsp:Policy vsp:Policy vsp:Policy vsp:Policy vsp:Palicy vsp:Polic</pre>	9/mex" -open.c essing/ /soap12 etadata .org/ws "	rg/wss/ policy" /" dl/soap	2004/0	1/oasis	-

This indicates that Active Directory Federation Services is running.

### Verify that OAuth 2.0 is Enabled

### To verify that OAuth 2.0 is enabled

1. Open the AD FS Management desktop application.



2. Open the **Service** folder, and then select the **Endpoint** folder.

File       Action       View       Window       Help	
Image: Process of the second seco	ē ×
Image: Service     Endpoints     Actions       Image: Service     Enabled     Proxy Enabled     URL Path     Type       Image: Service     Image: Service     No     //adfs/services/trust/13/usemamebasictransport     WS-Trust 1.3       Image: Service     Ves     Yes     //adfs/services/trust/13/usemamebasictransport     WS-Trust 1.3       Image: Service     Ves     Yes     //adfs/services/trust/13/usemamemixed     WS-Trust 1.3	
Enabled     Proxy Enabled     URL Path     Type     Enabled     Enabled     Enabled       Attribute Stores     No     No     /adfs/services/trust/13/usemamebasictransport     WS-Trust 1.3     View       Yes     Yes     Yes     /adfs/services/trust/13/usemamebasictransport     WS-Trust 1.3     View	
No       No       /adfs/services/trust/13/ssuedtokenasymmethcbasic256       WS-Trust 1.3         Device Registration       Yes       /adfs/services/trust/13/ssuedtokenasymmethcbasic256       WS-Trust 1.3         Endpoints       No       No       /adfs/services/trust/13/ssuedtokenasymmethcbasic256       WS-Trust 1.3         Scope Descriptions       Yes       /adfs/services/trust/13/ssuedtokenmixedasymmethcbasic.       WS-Trust 1.3         Web Application Proxy       No       No       /adfs/services/trust/13/ssuedtokenmixedasymmethcbasic2.       WS-Trust 1.3         Relying Party Trusts       No       No       /adfs/services/trust/13/ssuedtokensymmethcbasic256       WS-Trust 1.3         Paplication Groups       No       No       /adfs/services/trust/13/ssuedtokensymmethcbasic256       WS-Trust 1.3         No       No       No       /adfs/services/trust/13/ssuedtokensymmethcbasic256       WS-Trust 1.3         Mo       No       /adfs/services/trust/13/ssuedtokensymmethcbasic256       WS-Trust 1.3         No       No	*
Metadata     ~        >	

- 3. Search for the oauth2 path.
- 4. In either the Edge or Chrome web browser, go to https://localhost/adfs/.wellknown/openid-configuration
  - If you want to ignore certificate errors, select Advanced.

A page similar to the following image opens:



This indicates that OAuth 2.0 is available.

### **Create an Application Group**

To create an application group for use with Polaris Admin and LeapWebApp

1. Open the AD FS Management desktop application.



- 2. Select the **Application Groups** folder.
- 3. Under Actions, select Add Application Group.

The Add Application Group wizard opens.

输 Add Application Group W	/izard X
Welcome	
Steps	Name:
Welcome	Polaris
<ul> <li>Native application</li> <li>Apply Access Control Policy</li> </ul>	Description:
Summary	Polaris web applications
Complete	Template:         Client-Server applications         Image: Native application accessing a web API         Image: Web browser accessing a web application         Standalone applications         Image: Native application         Image: Server application         Image: Server application         Image: Server application         Image: Native application         Image: Server application         Image: Serv

- 4. On the **Welcome** tab, do the following:
  - a. In the Name box, enter Polaris.
  - b. In the Description box, enter Polaris web applications.
  - c. From the Template section, select **Web browser accessing a web application**.
- 5. Select Next.

翰 Add Application Group W	fizard	×
Native application		
Steps	Name:	
Welcome	Polaris - Native application	
Native application	Client Identifier:	
Apply Access Control Policy	0a586b1e-eeb0-4c8a-8381-50e9cafec240	
Summary		
Complete	Redirect UKI:	LL A
	Example. https://contoso.com	Add
	https://rd-polaris.polarislibrary.com/PolarisAdmin/login https://rd-polaris.polarislibrary.com/PolarisAdmin/oauth-success	Remove
	https://rd-polaris.polarislibrary.com/Polaris.AdminServices/swagger/oauth2-redirect.html	
	< >	
	Description:	
	< Previous Next >	Cancel

- 6. On the Native application tab, in the Redirect URI box, enter the following URIs:
  - https://server address/PolarisAdmin/
  - https://server address/PolarisAdmin/login
  - https://server address/PolarisAdmin/oauth-success
  - https://server address/Polaris.AdminServices/swagger/oauth2-redirect.html
  - https://server address/LeapWebApp/signin-oidc
  - https://server address/LeapWebApp/signin-override-oidc
  - https://server address/LeapWebApp/signout-callback-oidc
  - https://server address/Polaris.ApplicationServices/swagger/oauth2redirect.html

#### Note:

Replace server address with the FQDN that matches your Polaris

System Administration (web-based) or Leap server name and certificate.

7. Copy the value in the **Client Identifier** box to Notepad.

You'll need this when you set up PolarisAdmin's appsettings.user.json.

8. Select Next.



9. On the **Apply Access Control Policy** tab, select an access control policy, and then select **Next**.

훾 Add Application Group W	izard	×
Summary		
Steps	Review the following settings and click 'Next' to create the application.	
<ul> <li>Welcome</li> <li>Native application</li> <li>Apply Access Control Policy</li> <li>Summary</li> <li>Complete</li> </ul>	Application Group         Name: Polaris         Description: Polaris web applications         Native application         Name: Polaris - Native application         Identifier: 0a586b 1e-eeb0-4c8a-8381-50e9cafec240         Redirect URIs:         https://rd-polaris polarislibrary.com/PolarisAdmin/         https://rd-polaris polarislibrary.com/PolarisAdmin/ogin         https://rd-polaris polarislibrary.com/PolarisAdmin/oauth-success         https://rd-polaris polarislibrary.com/Polaris.AdminServices/swagger/oauth2-redirect.html         Web application         Identifiers: 0a586b 1e-eeb0-4c8a-8381-50e9cafec240         Access control policy: Permit everyone         Application permissions:	
	< Previous Next > Cancel	

10. On the **Summary** tab, review the settings and then select **Next**.



11. On the **Complete** tab, select **Close**.

### Configure the AD FS Web Application: Claims and Permitted Scopes

### To configure the AD FS web application

1. Open the AD FS Management desktop application.



- 2. Select the Application Groups folder.
- 3. Select the **Polaris** application group, and then select **Properties**.

Polaris Properties	×
General	
Name:	
Polaris	
Description:	
Polaris web applications	
Applications:	
Name	Description
Native application	
Polaris - Native application	
Web application	
Polaris - Web application	
Add application	Edit Remove
	OK Cancel Apply

4. Select **Polaris** - **Web application**, and then select **Edit**.



5. Select the Issuance Transform Rules tab, and then select Add Rule.

National Add Transform Claim Rule Wizard				
Select Rule Template				
Steps	Select the template for the claim rule that you want to create from the following list. The description provides	3		
Choose Rule Type	details about each claim rule template.			
<ul> <li>Configure Claim Rule</li> </ul>	Claim rule template:			
	Send Claims Using a Custom Rule $\qquad \qquad \lor$			
	Claim rule template description:			
	Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include: • Sending claims from a SQL attribute store • Sending claims from a custom attribute store using a custom LDAP filter • Sending claims only when 2 or more incoming claims are present • Sending claims only when 2 or more incoming claims are present • Sending claims only when an incoming claim value matches a complex pattern • Sending claims with complex changes to an incoming claim value • Creating claims for use only in later rules			
	< Previous Next > Cancel			

6. On the Add Transform Claim Rule Wizard, select **Send Claims Using a Custom Rule** from the **Claim rule template** list, and then select **Next**.

🏟 Add Transform Claim Rule	e Wizard	×
Configure Rule		
Configure Rule Steps Choose Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language. Claim rule name: Forward UPN Claim Rule template: Send Claims Using a Custom Rule Custom rule: c: [Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"] => issue(claim = c);	~ ~
	< Previous Finish Cancel	

- 7. In the Claim rule name box, enter Forward UPN Claim.
- 8. In the **Custom rule** box, enter the following rule:

```
c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]
=> issue(claim = c);
```

- 9. Select Finish.
- 10. On the Issuance Transform Rules tab, select Add Rule.
- 11. On the Add Transform Claim Rule Wizard, select **Send Claims Using a Custom Rule** from the **Claim rule template** list, and then select **Next**.
- 12. In the Claim rule name box, enter Add Tenantld.
- 13. In the **Custom rule** box, enter the following rule:

```
=> issue(Type =
"http://schemas.microsoft.com/identity/claims/tenantid",
Value = "polaris");
```

14. Select Finish.

Polaris - Web application Properties					×		
Identifiers Notes Acc	cess control policy	ssuance Transform	Rules Clier	nt Permissions			
Configure application permissions to enable client applications to acess this Web API							
Client application (caller):							
Name		Description			]		
Polaris - Native app	lication						
L			Add	Remove	1		
<b>D</b>			<u>M</u> uu	<u>N</u> emove			
Permitted scopes:	1				1		
Scope Name	Description			^			
allatclaims	Requests the access token claims in the identity token.						
aza	Scope allows broker client to request primary refresh token.						
	Request the email claim for the signed in user.						
logon_cert	The logon_cert scope allows an application to request logo						
	Prequest use of the OpenID Connect authonization protocol.						
				· · · · · · · · · · · · · · · · · · ·			
				New scope			
		OK	Cancel	Acobe			
		UN	Cancer	~@piy			

- 15. On the **Client Permissions** tab, verify that **email** and **openid** are selected.
- 16. Select **OK** to close the **Web application Properties** dialog.
- 17. Select **OK** to close the **Polaris properties** dialog.
- 18. Using the services applet, restart the Active Directory Federation Services service.

# Enable CORS on AD FS To Accept Requests from Polaris APIs

### To enable CORS on AD FS to accept requests from Polaris APIs

- 1. Refer to the information on the following page:
  - <u>https://docs.microsoft.com/en-us/windows-server/identity/ad-</u> <u>fs/operations/customize-http-security-headers-ad-fs#cross-origin-resource-</u> <u>sharing-cors-headers</u>
- 2. Use the following commands:
  - Set-AdfsResponseHeaders -EnableCORS \$true
  - Set-AdfsResponseHeaders -CORSTrustedOrigins https://rdpolaris.polarislibrary.com, https://example2.com

#### Note:

Replace https://rd-polaris.polarislibrary.com and https://example2.com with your own URL or list of URLs.

### Set Up Web Services and Applications

To set up each of the following web services and applications, you must configure a .json file for each of the following:

- Polaris.AdminServices (the API service)
- PolarisAdmin (the web-based Polaris System Administration application)
- Polaris.ApplicationServices (Leap's API service)
- LeapWebApp (Leap)

The four .json files are all named appsettings.user.json, but they reside in different directories:

- C:\Program Files\Polaris\7.2\Polaris.AdminServices
- C:\Program Files\Polaris\7.2\PolarisAdmin\assets
- C:\Program Files\Polaris\7.2\Polaris.ApplicationServices
- C:\Program Files\Polaris\7.2\Polaris\LeapWebApp

This section contains the following topics:

- <u>Set Up Polaris.AdminServices</u>
- Set Up PolarisAdmin
- Set Up Polaris.ApplicationServices
- Set Up LeapWebApp

Set Up Polaris.AdminServices

### To set up Polaris.AdminServices

Verify that OAuth is Enabled

• Open C:\Program Files\Polaris\7.2\Polaris.AdminServices\appsettings.user.json and verify Polaris.OAuth.Enabled is set to true.

```
"Polaris": {
 "CachePermissions": true,
 "CORS": {
   "AllowedHosts": "https://rd-polaris.polarislibrary.com"
 },
 "BasicAuth": {
   "Enabled": false
 },
 "OAuth": {
   "Enabled": true,
   "ClientID": "0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "Authority": "https://dev-fs.polarislibrary.com/adfs/",
   "Audience": "microsoft:identityserver:0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "ValidIssuer": "http://dev-fs.polarislibrary.com/adfs/services/trust",
   "ValidAudience": "microsoft:identityserver:0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "AuthorizationUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/authorize",
   "TokenUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/token"
 },
```

### Update the Client Id

1. On the AD FS server, open AD FS Management desktop application.



- 2. Copy the Client Id from the Polaris Native application properties dialog.
- 3. Paste the copied Client Id into the appsettings.user.json file.
- 4. If you started from the template, replace [client-id-that-might-look-like-a-guid] with the copied Client Id.

It should look like the following image when complete (your Client Id will be different):

```
'Polaris": {
 "CachePermissions": true,
 "CORS": {
   "AllowedHosts": "https://rd-polaris.polarislibrary.com"
 },
 "BasicAuth": {
   "Enabled": false
 },
 "OAuth": {
   "Enabled": true,
   "ClientID": "0a586b1e-eeb0-4c8a-8381-50e9cafec240"
   "Authority": "https://dev-fs.polarislibrary.com/adfs/",
   "Audience": "microsoft:identityserver:0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "ValidIssuer": "http://dev-fs.polarislibrary.com/adfs/services/trust",
   "ValidAudience": "microsoft:identityserver:0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "AuthorizationUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/authorize",
   "TokenUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/token"
 },
```

Update the AD FS Server Location

- 1. If you started from the template, replace [my-adfs-server-domain-name] with the AD FS server address.
- 2. It should look like the following when complete (your AD FS server address will be different):

```
"Polaris": {
 "CachePermissions": true,
  "CORS": {
   "AllowedHosts": "https://rd-polaris.polarislibrary.com"
 },
  "BasicAuth": {
   "Enabled": false
 },
  "OAuth": {
   "Enabled": true,
    "ClientID": "0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "Authority": "https://dev-fs.polarislibrary.com/adfs/",
   "Audience": "microsoft:identityserver:0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "ValidIssuer": "http://dev-fs.polarislibrary.com/adfs/services/trust",
   "ValidAudience": "microsoft:identityserver:0a586b1e-eeb0-4c8a-8381-50e9cafec240",
   "AuthorizationUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/authorize",
   "TokenUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/token"
 },
```

### Set Up PolarisAdmin

#### To set up PolarisAdmin

Verify that OAuth is Enabled

• Open C:\Program Files\Polaris\7.2\PolarisAdmin\assets\appsettings.user.json and verify that oauthEnabled is set to true.

```
"apiUrlRoot": "https://rd-polaris.polarislibrary.com/polaris.adminservices/api/",
"oauthEnabled": true,
 'msal':{
    "auth": {
      "clientId": "0a586b1e-eeb0-4c8a-8381-50e9cafec240",
      "authority": "https://dev-fs.polarislibrary.com/adfs/",
      "knownAuthorities": ["dev-fs.polarislibrary.com"],
      "redirectUri": "https://rd-polaris.polarislibrary.com/PolarisAdmin/oauth-success",
      "postLogoutRedirectUri": "https://rd-polaris.polarislibrary.com/PolarisAdmin",
      "protocolMode": "OIDC",
      "navigateToLoginRequestUrl": false
    },
    "cache": {
        "cacheLocation" : "localStorage",
        "storeAuthStateInCookie": false,
        "secureCookies": true
    },
     'guard": {|
        "interactionType": "redirect",
        "authRequest": {
            "scopes": ["openid", "profile", "email", "urn:microsoft:userinfo"]
        },
"loginFailedRoute": "/login-failed"
    },
    "interceptor": {
        "interactionType": "redirect",
        "protectedResourceMap": [
            ["https://rd-polaris.polarislibrary.com/Polaris.AdminServices/api/protected/", ["email"]]
        1
    }
}
```

#### Update the Client Id

1. On the AD FS server, open AD FS Management desktop application.



- 2. Copy the Client Id from the Polaris Native application Properties dialog.
- 3. Paste the copied Client Id into the appsettings.user.json file.
- 4. If you started from the template, replace [CLIENTID-ASSIGNED-IN-ADFS] with the copied Client Id.

It should look like the following when complete (your Client Id will be different):



Update AD FS Server Location

• If you started from the template, replace [ADFS-SERVER-ADDR] with the AD FS server address.

It should look like the following when complete (your AD FS server address will be different):



Update Polaris Admin Server Location

• If you started from the template, replace [POLADMIN-SERVER-ADDR] with the AD FS server address.

It should look like the following image when complete (your AD FS server address will be different):



Update Polaris Admin Services (API) Server Location

• If you started from the template, replace [POLADMINSVC-SERVER-ADDR] with the AD FS server address.

It should look like the following image when complete (your AD FS server address will be different):



### Set Up Polaris.ApplicationServices

#### To set up Polaris.ApplicationServices

Verify that OAuth Is Enabled

Open C:\Program

Files\Polaris\7.2\Polaris.ApplicationServices\appsettings.user.json and verify that OAuth.Enabled is set to true.

"OAuth": { "Enabled": true, "Authorities": [ "Name": "ADFS", "Authority": "https://dev-fs.polarislibrary.com/adfs/", "Audience": "microsoft:identityserver:3eb2a79f-db5a-4ba0-b22f-e7dl6a6l6d4a", "MetaAddress": "https://dev-fs.polarislibrary.com/adfs/.well-known/openid-configuration", "RequireHttpsMetadata": true, "RequireSignedTokens": true, "ValidateIssuer": true, "ValidIssuers": [ "https://dev-fs.polarislibrary.com/adfs", "http://dev-fs.polarislibrary.com/adfs/services/trust" 1. "ValidateAudience": true, "ValidAudiences": [ "3eb2a79f-db5a-4ba0-b22f-e7d16a616d4a", "microsoft:identityserver:3eb2a79f-db5a-4ba0-b22f-e7dl6a616d4a" 1, "ClaimTypeUPN": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" ł 1, "Swagger": { "ClientID": "3eb2a79f-db5a-4ba0-b22f-e7dl6a616d4a", "AppName": "Polaris.ApplicationServices", "AuthorizationUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/authorize", "TokenUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/token", "RefreshTokenUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/token", "LogoutUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/logout" } },

Update the AD FS Server Location

• If you started from the template, replace *adfs-server-address* with the AD FS server address.

It should look like the following when complete (your AD FS server address will be different):

```
"OAuth": {
  "Enabled": true,
  "Authorities": [
    Ł
      "Name": "ADFS",
      "Authority": "https://dev-fs.polarislibrary.com/adfs/",
      "Audience": "microsoft:identityserver:3eb2a79f-db5a-4ba0-b22f-e7d16a616d4a",
      "MetaAddress": "https://dev-fs.polarislibrary.com/adfs/.well-known/openid-configuration",
      "RequireHttpsMetadata": true,
      "RequireSignedTokens": true,
      "ValidateIssuer": true,
      "ValidIssuers": [
        "https://dev-fs.polarislibrary.com/adfs",
        "http://dev-fs.polarislibrary.com/adfs/services/trust"
      1,
      "ValidateAudience": true,
      "ValidAudiences": [
        "3eb2a79f-db5a-4ba0-b22f-e7d16a616d4a",
        "microsoft:identityserver:3eb2a79f-db5a-4ba0-b22f-e7dl6a6l6d4a"
      1,
      "ClaimTypeUPN": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"
    ł
 1,
  "Swagger": {
   "ClientID": "3eb2a79f-db5a-4ba0-b22f-e7dl6a616d4a",
   "AppName": "Polaris.ApplicationServices",
   "AuthorizationUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/authorize",
"TokenUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/token",
   "RefreshTokenUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/token",
   "LogoutUrl": "https://dev-fs.polarislibrary.com/adfs/oauth2/logout"
 }
},
```

#### Update the Client ID

1. On the AD FS server, open the AD FS Management desktop application.

<ul> <li>Ŷ AD FS</li> <li>Ŷ File Action View Window Help</li> <li>↓ ♪ □ □</li> </ul>		
AD FS Service Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups	Application Groups Name Polaris Polaris Properties Genera Polaris - Native ag General Pola Desc Pola Client Id: Da586b1e-eeb0 Redirect URI: Na https://rd-polaris https://rd-polaris https://rd-polaria Client Id: Appl Na https://rd-polaria Client Id: Description: Add	Description Polaris web applications
		OK Cancel Apply

- 2. Copy the Client ID from the **Polaris Native application Properties** dialog.
- 3. Paste the copied Client ID into the appsettings.user.json file.
- 4. If you started from the template, replace *client-id-configured-in-adfs* with the copied Client ID.

It should look like the following when complete (your client ID will be different):



### Set Up LeapWebApp

### To set up LeapWebApp

Verify that OAuth Is Enabled

 Open C:\Program Files\Polaris\7.2\LeapWebApp\appsettings.user.json and verify that OAuthEnabled is set to true.

```
"OAuthEnabled": true,
"OAuth": {
    "Authority": "https://dev-fs.polarislibrary.com/adfs/",
    "ClientSecret": null,
    "MetadataAddress": "https://dev-fs.polarislibrary.com/adfs/.well-known/openid-configuration",
    "KnownAuthorities": [ "dev-fs.polarislibrary.com" ],
    "CallbackPath": "/signin-oidc",
    "SignedOutCallbackPath": "/signout-callback-oidc",
    "SignedOutCallbackPath": "/login",
    "RemoteAuthenticationTimeout": 15,
    "RemoteFailureRedirectUri": "/leapwebapp/logout",
    "ResponseMode": "form_post",
    "ResponseType": "code id_token token",
    "UsePkce": false
    "UsePkce": false
},
```

Update the AD FS Server Location

• If you started from the template, replace [adfs-server-address] with the AD FS server address.

It should look like the following when complete (your AD FS server address will be different):

```
"OAuthEnabled": true,
"OAuth": {
    "Authority": "https://dev-fs.polarislibrary.com/adfs/",
    "ClientId": "0a586ble-eeb0-4c8a-8381-50e9cafec240",
    "ClientSecret": null,
    "MetadataAddress": "https://dev-fs.polarislibrary.com/adfs/.well-known/openid-configuration",
    "KnownAuthorities": [ "dev-fs.polarislibrary.com" ],
    "CallbackPath": "/signin-oidc",
    "SignedOutCallbackPath": "/signout-callback-oidc",
    "SignedOutCallbackPath": "/login",
    "RemoteAuthenticationTimeout": 15,
    "RemoteFailureRedirectUri": "/leapwebapp/logout",
    "ResponseMode": "form_post",
    "ResponseType": "code id_token token",
    "UsePkce": false
}.
```

#### Update the Client ID

1. On the AD FS server, open the AD FS Management desktop application.



- 2. Copy the Client ID from the Polaris Native application Properties dialog.
- 3. Paste the copied Client ID into the appsettings.user.json file.
- 4. If you started from the template, replace the *client-id-configured-in-adfs* with the copied Client ID.

It should look like the following when complete (your client ID will be different):

```
"OAuthEnabled": true,
"OAuth": {
    "Authority": "https://dev-fs.polarislibrary.com/adfs/",
    "ClientId": '@a586b1e-eeb0-4c8a-8381-50e9cafec240",
    "ClientSecret": null,
    "MetadataAddress": "https://dev-fs.polarislibrary.com/adfs/.well-known/openid-configuration",
    "KnownAuthorities": [ "dev-fs.polarislibrary.com" ],
    "CallbackPath": "/signin-oidc",
    "SignedOutCallbackPath": "/signout-callback-oidc",
    "SignedOutCallbackPath": "/signout-callback-oidc",
    "SignedOutRedirectUri": "/login",
    "RemoteAuthenticationTimeout": 15,
    "RemoteFailureRedirectUri": "/leapwebapp/logout",
    "ResponseMode": "form_post",
    "ResponseType": "code id_token token",
    "UsePkce": false
}.
```

### Enable Session Storage for LeapWebApp

Enable session storage for the best user experience when using OAuth and OIDC.

Microsoft SQL Server Express 2019 (or a newer version) must be installed to use session storage. You install SQL Server Express separately. It is not part of the Leap installation.

#### To enable session storage

• Open C:\Program Files\Polaris\7.2\LeapWebApp\appsettings.user.json and set SessionStore.Enabled to true.

```
"SessionStore": {
    "Enabled": true,
    "ConnectionString": "Data Source=.\\Polaris; Initial Catalog=PolarisCache; Integrated Security=True;",
    "SessionTimeoutMinutes": "1440",
    "SchemaName": "dbo",
    "TableName": "Sessions"
},
```

### Add a URL Rewrite Rule for LeapWebApp

Adding a URL rewrite rule redirects incoming URLs to the correct address for the LeapWebApp. This must be done manually, since the library may already use other URL rewrite rules.

The Microsoft IIS URL Rewrite 2.1 extension is required to add a URL rewrite rule. For more information, see <u>https://www.iis.net/downloads/microsoft/url-rewrite</u>.

### To add a URL rewrite rule

1. Open the root IIS web.config file, found in the following location:

C:\inetpub\wwwroot\web.config

2. Add a rewrite rule to the **system.webServer** node.



#### Note:

For sample rewrite rule text that you can copy and paste, see Sample Rewrite Rule Text.

In the example above, if the incoming URL includes a path that contains any of the following, the rewrite rule redirects to /leapwebapp:

- /LeapWebApp
- /Leapwebapp
- /LEAPWEBAPP
- 3. Save the web.config file.

#### Note:

When registering redirect URIs for LeapWebApp in AD FS, the URIs should

be lowercase. For example:

- https://rd-polaris.polarislibrary.com/leapwebapp/signin-oidc
- https://rd-polaris.polarislibrary.com/leapwebapp/signin-overrideoidc
- https://rd-polaris.polarislibrary.com/leapwebapp/signout-callbackoidc

### Sample Rewrite Rule Text

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
     <rewrite>
        <rules>
          <rule name="UrlToLowercase" stopProcessing="true">
             <match url="(.*)" ignoreCase="true" />
               <action type="Redirect" url="https://{HTTP HOST}</pre>
                {ToLower:{PATH_INFO}}" redirectType="Found"
               appendQueryString="true" />
               <conditions>
                  <add input="{PATH INFO}" pattern="^/LeapWebApp
                  (.*) | ^/Leapwebapp(.*) | ^/LEAPWEBAPP(.*) "
                  ignoreCase="false" />
               </conditions>
          </rule>
        </rules>
     </rewrite>
  </system.webServer>
</configuration>
```

### Additional URL Rewrite Resources

See Microsoft's URL Rewrite Module Configuration Reference for additional information:

<u>https://docs.microsoft.com/en-us/iis/extensions/url-rewrite-module/url-rewrite-module-configuration-reference</u>

### **Customize the AD FS Pages**

Use the following resources to customize AD FS pages:

- <u>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn280950(v=ws.11)</u>
  - Get-AdfsGlobalWebContent
  - Set-AdfsGlobalWebContent

#### **Examples:**

Customize the examples below to suit your library's needs.

**PS** C:\Windows\system32> **Set-AdfsGlobalWebContent -SignOutPageDescriptionText** "You have successfully signed out.<br>If you have been directed here immediately after signing in, your session may have timed out."

PS C:\Windows\system32> Set-AdfsWebTheme -TargetName
default -Logo @{path="c:\ADFS Custom\leap logo.png"}

PS C:\Windows\system32> Set-AdfsGlobalWebContent -CompanyName "Polaris R&D"

- Advanced customization:
  - <u>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn636121(v=ws.11)</u>

### Change the Access Token Lifetime

The default token lifetime for both access and ID tokens is 60 minutes. Execute the following command to increase the expiration time to 24 hours:

```
Set-AdfsWebApiApplication -TokenLifetime 1440 -TargetIdentifier "0a586ble-eeb0-4c8a-8381-50e9cafec240"
```

#### Note:

Replace *TargetIdentifier* with the Polaris Application Group native application client ID.

### **Bind a New SSL Certificate**

If your web server certificate expires, use the instructions below to bind a new SSL certificate.

#### To bind a new SSL certificate

- 1. Install the certificate using Certificates Management.
- 2. Set the service communications certificate using the AD FS Management Console:
  - a. Expand the Services folder.
  - b. Select a new certificate.
  - c. Restart the AD FS service.
- 3. Attach the certificate to AD FS using PowerShell:
  - a. Get the certificate's thumbprint by viewing the certificate.

c:\> Set-AdfsSslCertificate -Thumbprint e8fd5016542796214e94f72d76095f9fc587c731

b. Restart the AD FS service.

### Troubleshoot

### Force a logout

https://AD FS server address/adfs/oauth2/logout

**Note:** Replace *AD FS server address* with your library's AD FS server address.

AD FS in one-way trust

Problem: Only local accounts are authenticating

**Solution**: Make sure the account running the AD FS service is a parent domain account and not a local account.

Receiving "User is not a valid Polaris user." error

• Check the setting Polaris.OAuth.ValidIssuer in the Polaris.AdminServices appsettings.user.json file.

Example value: http://AD FS server address/adfs/services/trust

**Note:** Replace *AD FS server address* with your library's AD FS server address.

• Verify a domain is attached to AD user accounts so the UPN claim can be added to the ID token's claims.

The UPN claim should look like user@mydomain.com.

Troubleshoot Redirect URIs

Redirect URIs are case-sensitive.