



Configuring SAML single sign-on authentication for Quest® Rapid Recovery™

Technical White Paper

Quest Engineering
August 2022



© 2022 Quest Software Inc.

ALL RIGHTS RESERVED.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Zmanda is a trademark of Zmanda Incorporated in the USA. All other trademarks and registered trademarks are property of their respective owners.

Legend



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death



CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.



IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Setting up SAML single sign-on authentication for Quest Rapid Recovery

Updated – August 30, 2022

Contents

- Setting up SAML in an identity provider5**
 - Understanding the SAML 2.0 enterprise application5
 - Limitations.....5
 - Configuring SAML in Azure Active Directory6
 - Configuring SAML in Okta12
 - Configuring SAML in OneLogin.....19
- Managing SAML in the Rapid Recovery UI24**

Executive summary

This white paper provides information about how to set up SAML single sign-on authentication for Rapid Recovery. This document is a quick reference guide and includes the three supported identity providers.

For additional information, see the Rapid Recovery documentation and other data management application best practices whitepapers at:

<http://support.quest.com/rapid-recovery>

Setting up SAML in an identity provider

The following chapter describes how to configure SAML 2.0 with Rapid Recovery based on your identity provider.

Understanding the SAML 2.0 enterprise application

Before you can establish SAML authentication with Rapid Recovery, you must install the SAML 2.0 application in an identity provider (IdP). Rapid Recovery supports the following IdPs:

- Azure Active Directory
- Okta
- OneLogin

Limitations

The SAML authentication integration with Rapid Recovery includes the following limitations:

- SAML works only when accessing Rapid Recovery through FQDN, not with an IP address
- Single log-out (SLO) is not supported.
- Firefox is not supported.
- To prevent login failures, the system clock of the machine where Rapid Recovery is installed must be synchronized with the IdP clock.
- Only users are supported. Rapid Recovery does not support IdP roles and groups.
- Rapid Recovery does not support IdP-initiated SSO. You must initiate the login from Rapid Recovery.

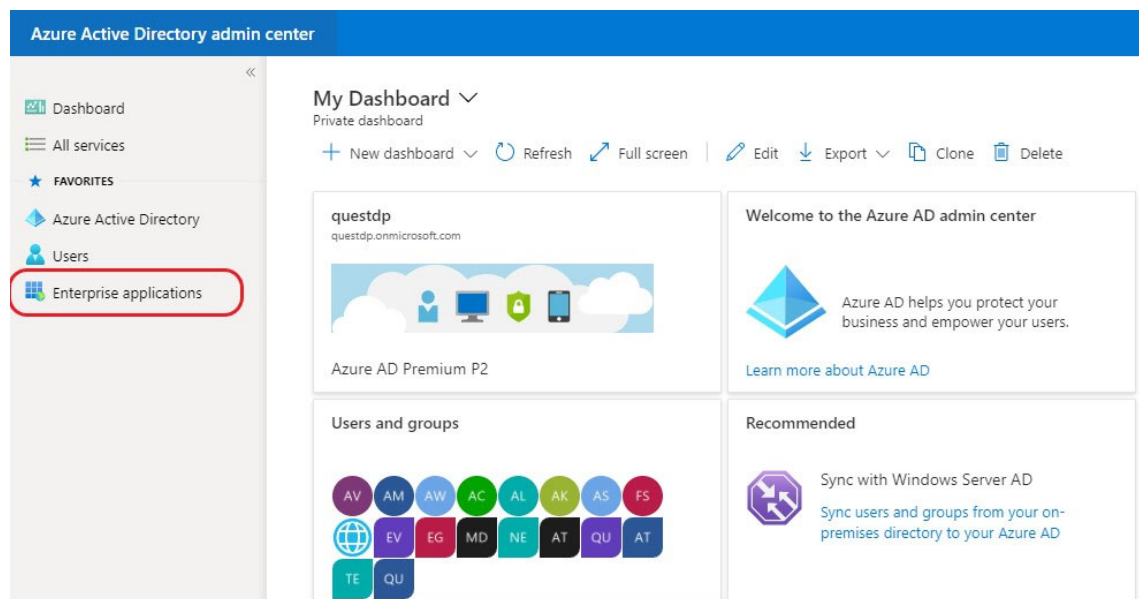
Configuring SAML in Azure Active Directory

CAUTION: After you configure the SAML settings, you must restart the Core Service for the changes to take effect. Before you restart the Core Service, you must complete all of the steps in the configuration procedure. If you restart the Core service before completing the SAML configuration, the Core Console becomes inaccessible.

To configure SAML in Azure Active Directory

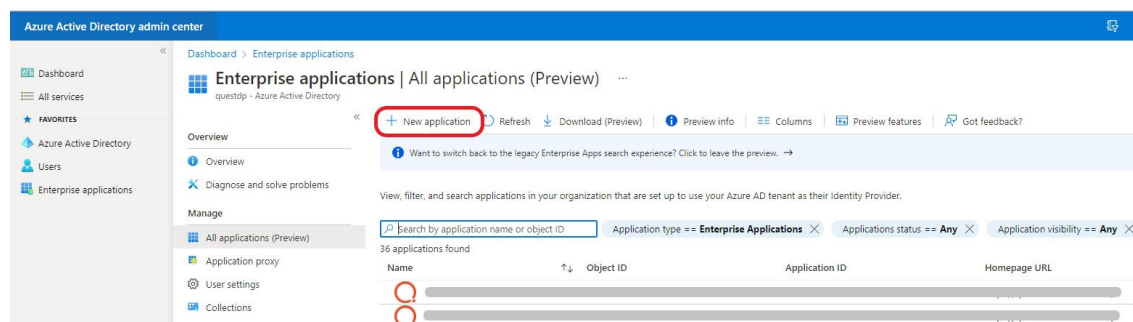
- 1 Go to <https://aad.portal.azure.com> and create an account.
- 2 Complete the steps for registering a new enterprise application in Azure Active Directory.
- 3 From the Azure Active Directory (AD) user interface (UI), in the left navigation, click **Enterprise applications**.

Figure: Azure AD – Enterprise applications



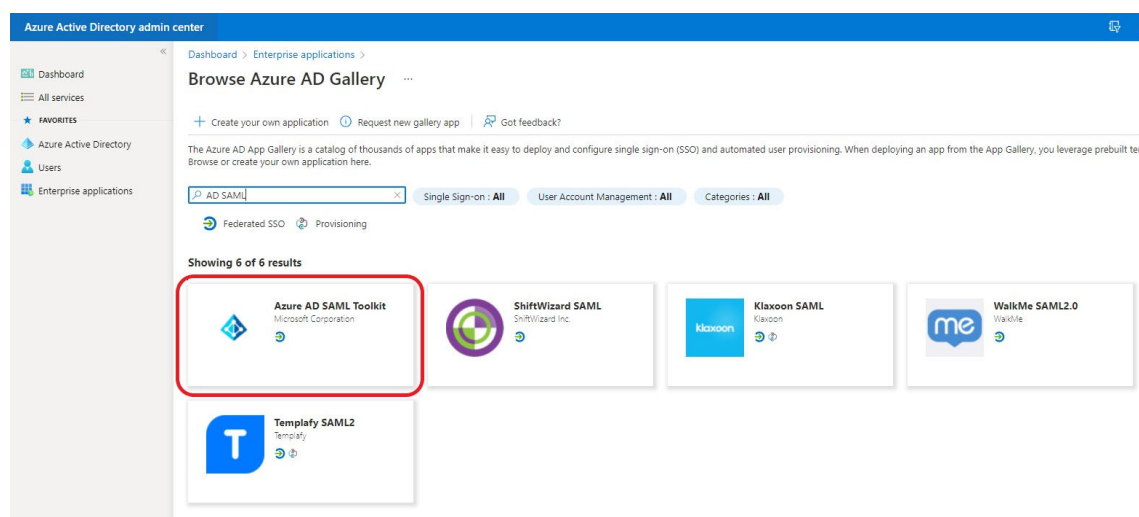
- 4 On the Enterprise applications page, click **New application**.

Figure: Azure AD – New application



- 5 In the Azure AD Gallery, search for **AD SAML**, and then click **Azure AD SAML Toolkit**.


Figure: Azure AD Gallery





- 8 In the Azure AD SAML Toolkit, enter a name for the configuration, such as the hostname of the Rapid Recovery server.



Figure: Azure AD SAML Toolkit


Azure AD SAML Toolkit ✕

 Got feedback?


Logo 




Name  

Publisher 


Microsoft Corporation

Provisioning 

Automatic provisioning is not supported

Single Sign-On Mode 

SAML-based Sign-on
Linked Sign-on

URL 

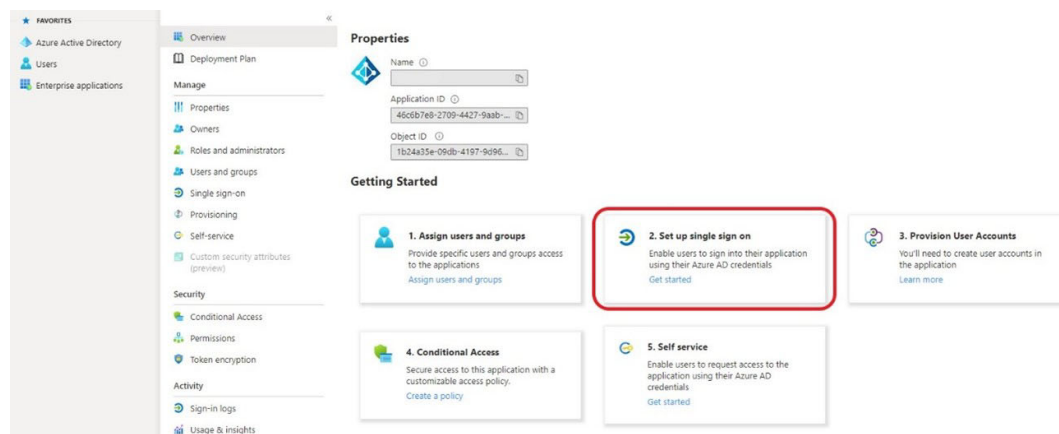
<https://www.microsoft.com/>

[Read our step-by-step Azure AD SAML Toolkit integration tutorial](#)


This is the sample SAML app which customers can use to test the SAML single sign-on integration with Azure AD.


- 9 On the Overview page, under Getting Started, click **Set up single sign on**.


Figure: SAML Overview page



Properties

Name 

Application ID 

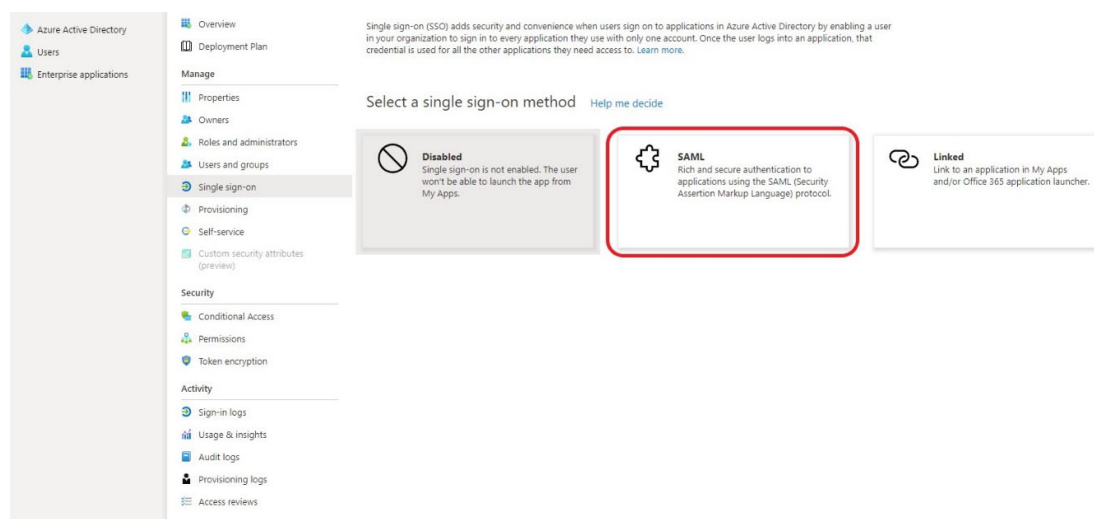
Object ID 

Getting Started

- 1. Assign users and groups**
Provide specific users and groups access to the applications.
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials.
[Get started](#)
- 3. Provision User Accounts**
You'll need to create user accounts in the application.
[Learn more](#)
- 4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)
- 5. Self service**
Enable users to request access to the application using their Azure AD credentials.
[Get started](#)

- 10 On the Single sign-on page, under Select a single sign-on method, click **SAML**.

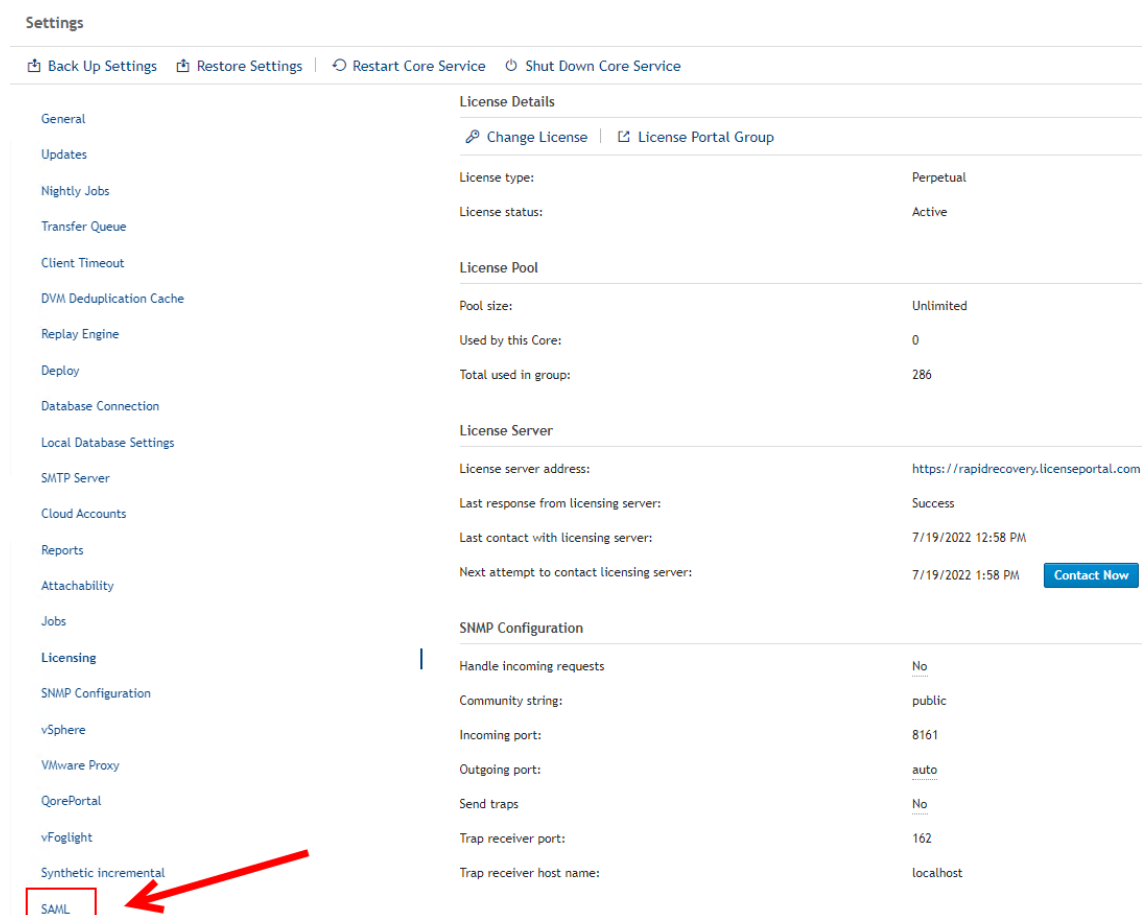
Figure: Single sign-on page



11 Go to the Rapid Recovery UI and, in the left navigation for the Core, click the **Settings**  icon.

12 On the Settings page, scroll down or click **SAML**.


Figure: Rapid Recovery Settings page



13 On the Settings page, under SAML, next to Enable configuration, click the setting. If the setting is currently No, complete the following steps:


- Click **No**.
- Select the empty check box.
- To apply the change, click the check mark ✓.

The SAML settings appear.

14 Click the **Copy**  icon for each of the following URLs:

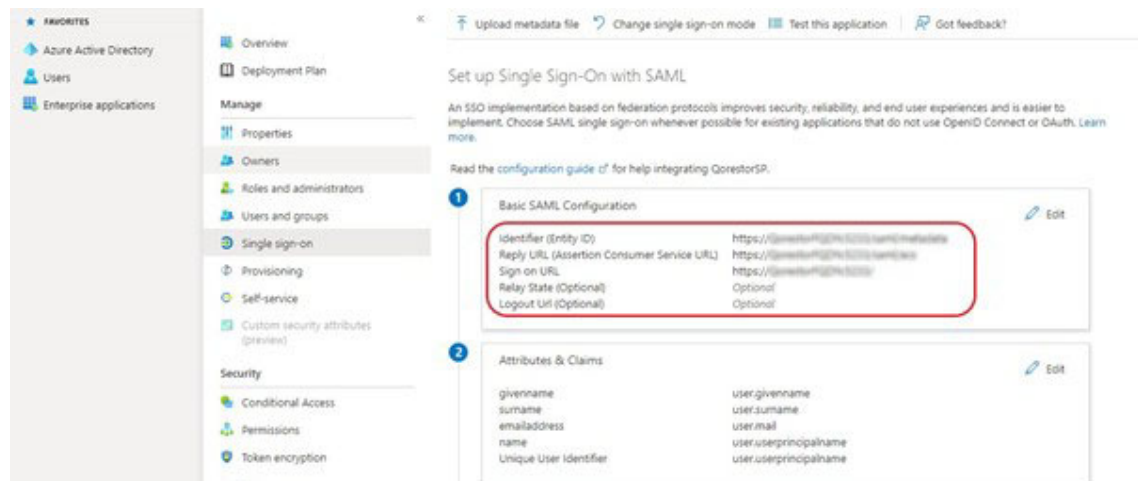
- **Sign on URL**
- **Reply URL (Assertion Consumer Service URL)**
- **Logout URL**


Figure: SAML configuration settings URLs


SAML	
Enable configuration:	Yes
	<p>⚠ The Rapid Recovery Core service must be restarted after enabling and/or disabling SAML authentication. Please note that Rapid Recovery Core supports two types of authentication: Windows-based and SAML-based (Windows-based authentication is by default. After enabling SAML you are switching from Windows-based authentication to SAML and vice versa)</p>
Sign on URL:	https://functest-core3:8006/apprecovery/admin/Auth/Login 
Reply URL (Assertion Consumer Service URL):	https://functest-core3:8006/apprecovery/admin/Auth/AssertionConsumerService 
Logout URL:	https://functest-core3:8006/apprecovery/admin/Auth/Logout 

15 Return to the Azure AD UI and, on the Set up Single Sign-On with SAML page, paste the URLs into the corresponding areas.:

Figure: Set up Single Sign-On with SAML page



Basic SAML Configuration		
Identifier (Entity ID)	https://f1a6e1f0-0000-4000-b000-000000000000	
Reply URL (Assertion Consumer Service URL)	https://f1a6e1f0-0000-4000-b000-000000000000	
Sign on URL	https://f1a6e1f0-0000-4000-b000-000000000000	
Relay State (Optional)	Optional	
Logout URL (Optional)	Optional	

Attributes & Claims		
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

16 In the SAML Signing Certificate section, click **Edit**.

17 In the SAML Signing Certificate section, copy the following details:

- **App Federation Metadata URL**
- **Certificate**

- **Signing Algorithm**

18 Click **OK**.

19 To add user identities to the SAML application in Azure AD, see Microsoft Azure Active Directory documentation.

20 Return to the Rapid Recovery Core Settings page.

21 On the Settings page, under SAML, paste the SAML details in the corresponding areas.

22 Click **Check SAML**.

23 Restart the Core service.

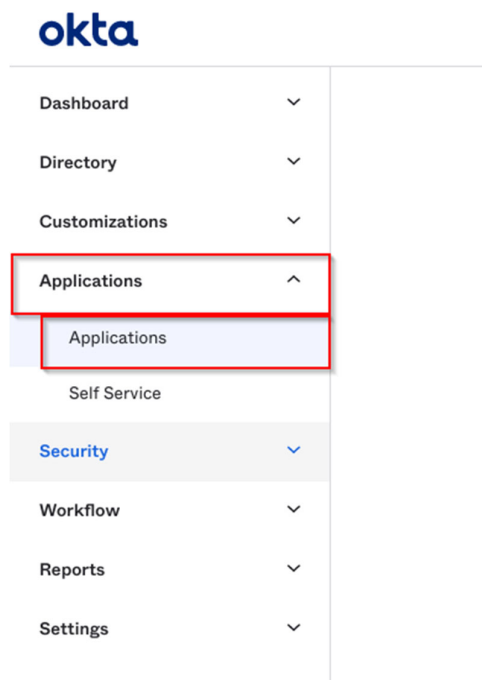
Configuring SAML in Okta

CAUTION: After you configure the SAML settings, you must restart the Core Service for the changes to take effect. Before you restart the Core Service, you must complete all of the steps in the configuration procedure. If you restart the Core service before completing the SAML configuration, the Core Console becomes inaccessible.

To configure SAML in Okta

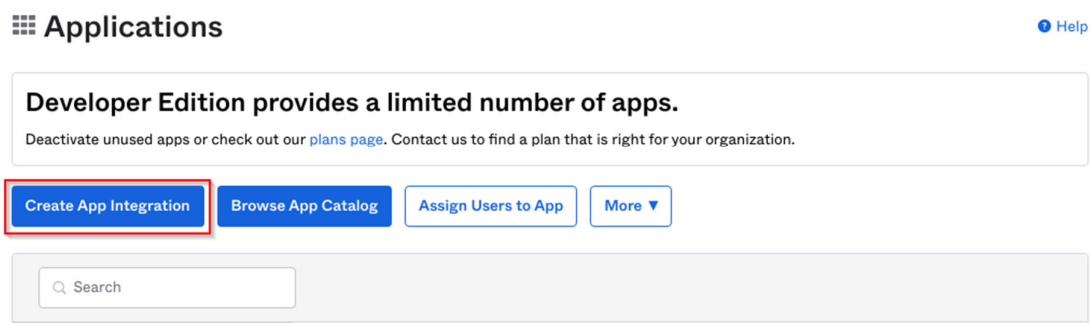
- 1 Go to <https://login.okta.com> and create an account.
- 2 In the Okta UI, in the left navigation menu, expand the **Applications** menu, and then click **Applications**.

Figure: Okta Applications menu



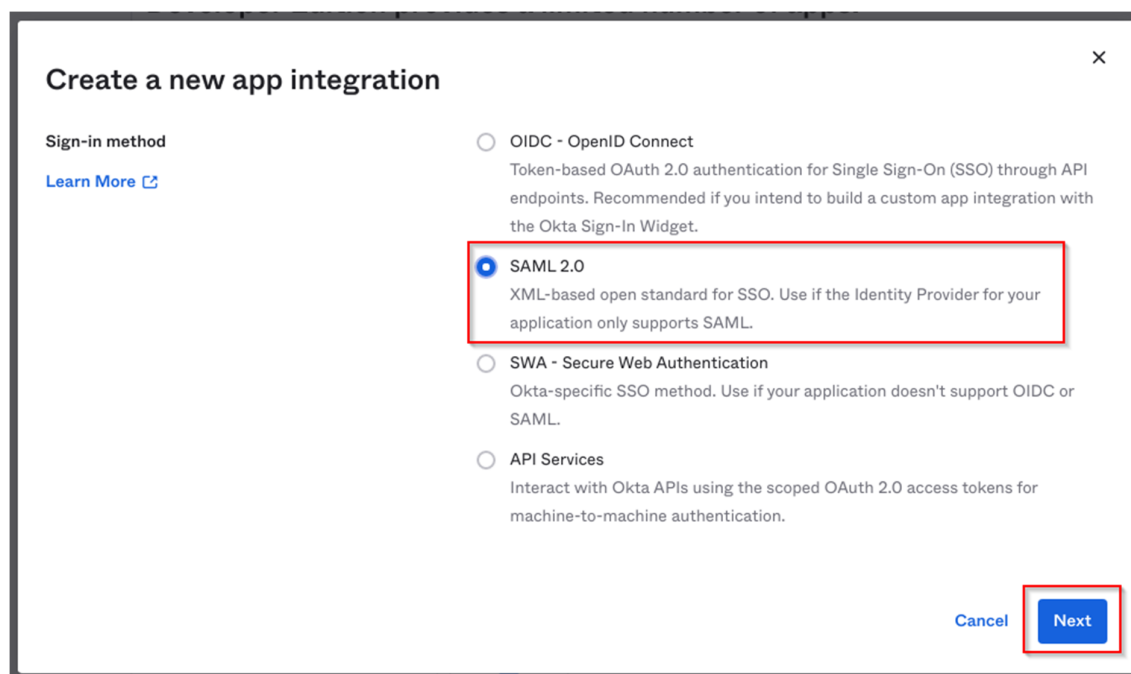
- 3 On the Applications page, click **Create App Integration**.

Figure: Okta Application page



- 4 In the Create a new app integration window, select **SAML 2.0**, and then click **Next**.

Figure: Okta Create a new app integration window – SAML 2.0



- 5 On the Create SAML Integration page, on the General Settings tab, enter an **App name** for the integration, such as the hostname of the Rapid Recovery Server, and then click **Next**.

Figure: Create SAML Integration - General Settings tab

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name: SAMLDemoAppName

App logo (optional): [Gear icon]

App visibility:

- ☐ Do not display application icon to users
- ☐ Do not display application icon in the Okta Mobile app

Cancel Next


- 8 On the Configure SAML tab, enter the following details found on the Rapid Recovery Core Settings page:
 - **Single sign on URL**
 - **Audience URI (SP Entity ID)**
- 9 Select **Use this for Recipient URL and Destination URL**.
- 10 Optionally, to add encryption, click **Show Advanced Settings** and following the instructions provided by Okta documentation.
- 11 Click **Next**.
- 12 On the Feedback tab, select I'm an **Okta customer adding an internal app**.
- 13 Click **Finish**.
- 14 Return to the Applications page and click the **Sign On** tab.
- 15 Copy the URL for Identity Provider metadata for use in the Rapid Recovery Core settings.
- 16 Go to the Rapid Recovery UI and, in the left navigation for the Core, click the **Settings**  icon.
- 17 On the Settings page, scroll down or click **SAML**.

Figure: Rapid Recovery Settings page

Settings

[Back Up Settings](#) |
 [Restore Settings](#) |
 [Restart Core Service](#) |
 [Shut Down Core Service](#)

General	License Details
Updates	Change License License Portal Group
Nightly Jobs	License type: Perpetual
Transfer Queue	License status: Active
Client Timeout	License Pool
DVM Deduplication Cache	Pool size: Unlimited
Replay Engine	Used by this Core: 0
Deploy	Total used in group: 286
Database Connection	License Server
Local Database Settings	License server address: https://rapidrecovery.licenseportal.com
SMTP Server	Last response from licensing server: Success
Cloud Accounts	Last contact with licensing server: 7/19/2022 12:58 PM
Reports	Next attempt to contact licensing server: 7/19/2022 1:58 PM Contact Now
Attachability	SNMP Configuration
Jobs	Handle incoming requests: No
Licensing	Community string: public
SNMP Configuration	Incoming port: 8161
vSphere	Outgoing port: auto
VMware Proxy	Send traps: No
QorePortal	Trap receiver port: 162
vFoglight	Trap receiver host name: localhost
Synthetic incremental	
SAML	

18 On the Settings page, under SAML, next to Enable configuration, click the setting. If the setting is currently No, complete the following steps:

- Click **No**.
- Select the empty check box.
- To apply the change, click the check mark

The SAML settings appear.

19 Click the **Copy** icon for each of the following URLs:

- **Sign on URL**
- **Reply URL (Assertion Consumer Service URL)**
- **Logout URL**

20 Return to the Okta UI and, on the SAML Settings page, enter the following details:

- For **Single sign on URL**, enter the **Service Provider ACS (Assertion Consumer Service) URL**, and then select **Use this for Recipient URL and Destination URL**.
- For **Audience URI (SP Entity ID)**, enter the **Service Provider MetaData URL**.

- For **Name ID format**, select **Email Address**.
- For **Application username**, select **Email**.

Figure: Create SAML Integration – Configure SAML tab

Create SAML Integration

1 General Settings
2 **Configure SAML**
3 Feedback

A SAML Settings

General

Single sign on URL ⓘ

☒ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ⓘ

Default RelayState ⓘ

If no value is set, a blank RelayState is sent

Name ID format ⓘ

Application username ⓘ

Update application username on

[Show Advanced Settings](#)

What does this form do?

This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

- 21 On the Feedback tab, select **I'm an Okta customer adding an internal app**, and then select **This is an internal app that we have created**.

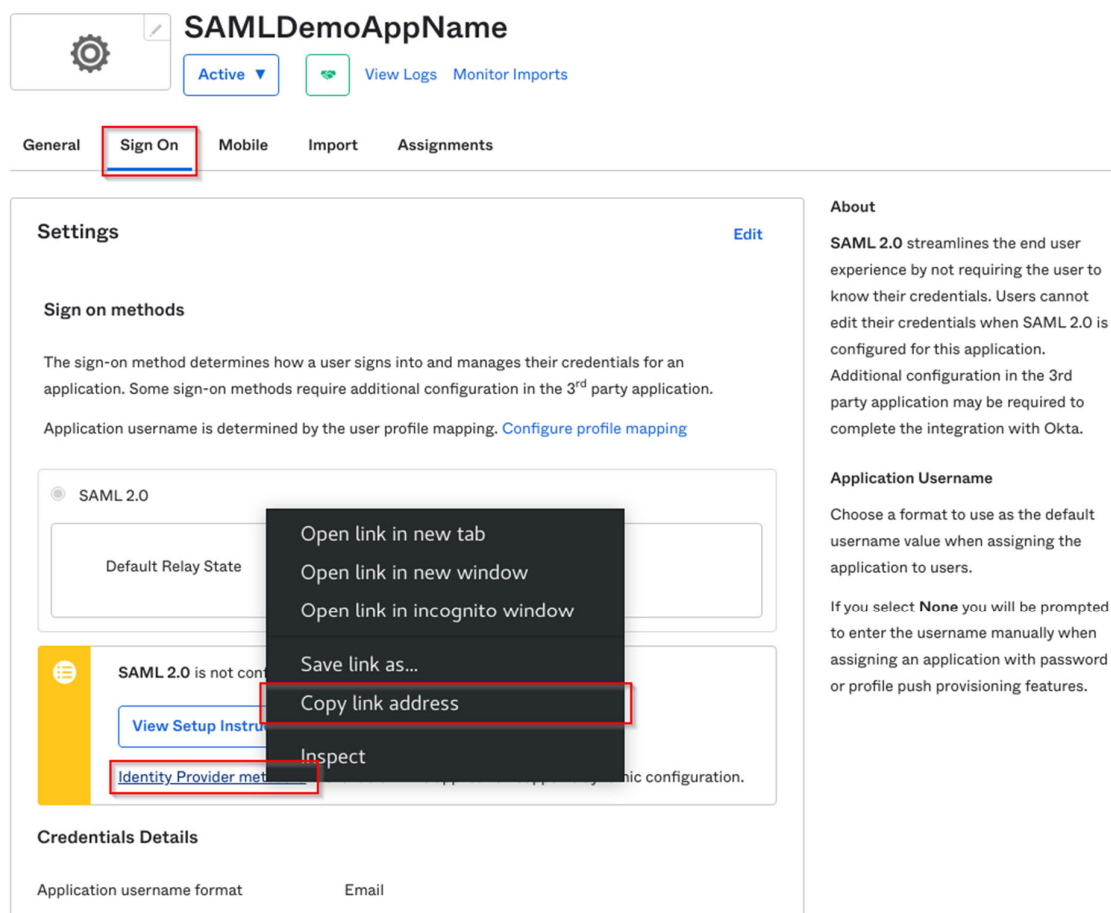
Figure: Create SAML Integration – Feedback tab

22 Click **Finish**.

The UI opens the page for the SAML app integration.

23 On the SAML integration page, go to the **Sign On** tab, and then right-click **Identity Provider metadata** and select **Copy link address**.

Figure: SAML app integration IdP metadata



- 24 To add user identities to the SAML application in Okta, see Okta documentation.
- 25 Return to Core Settings page of the Rapid Recovery Core Console.
- 26 On the Settings page, under SAML, paste the SAML details in the corresponding areas.
- 27 Click **Check SAML**.
- 28 Restart the Core service.

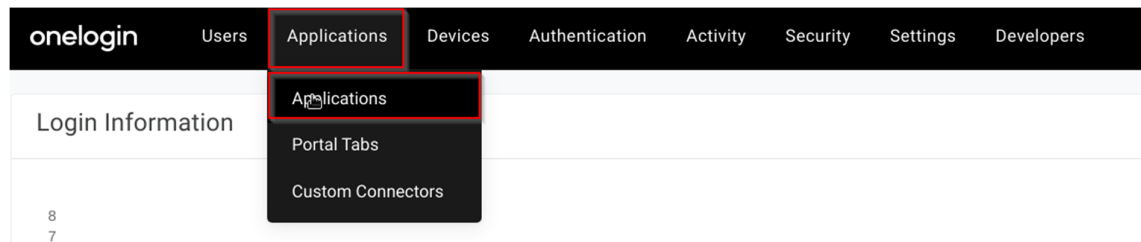
Configuring SAML in OneLogin

CAUTION: After you configure the SAML settings, you must restart the Core Service for the changes to take effect. Before you restart the Core Service, you must complete all of the steps in the configuration procedure. If you restart the Core service before completing the SAML configuration, the Core Console becomes inaccessible.

To configure SAML in OneLogin

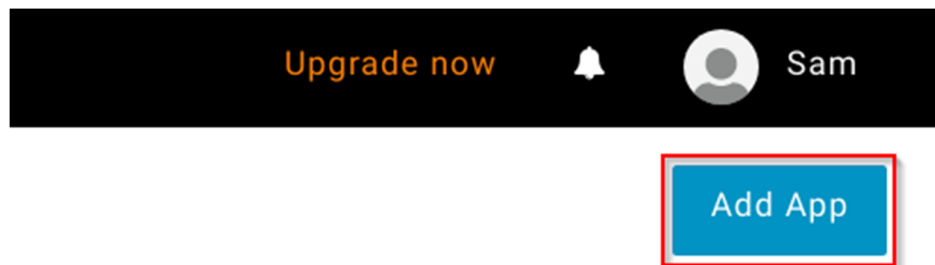
- 1 In the OneLogin UI, in the **Applications** menu, click **Applications**.

Figure: OneLogin Applications



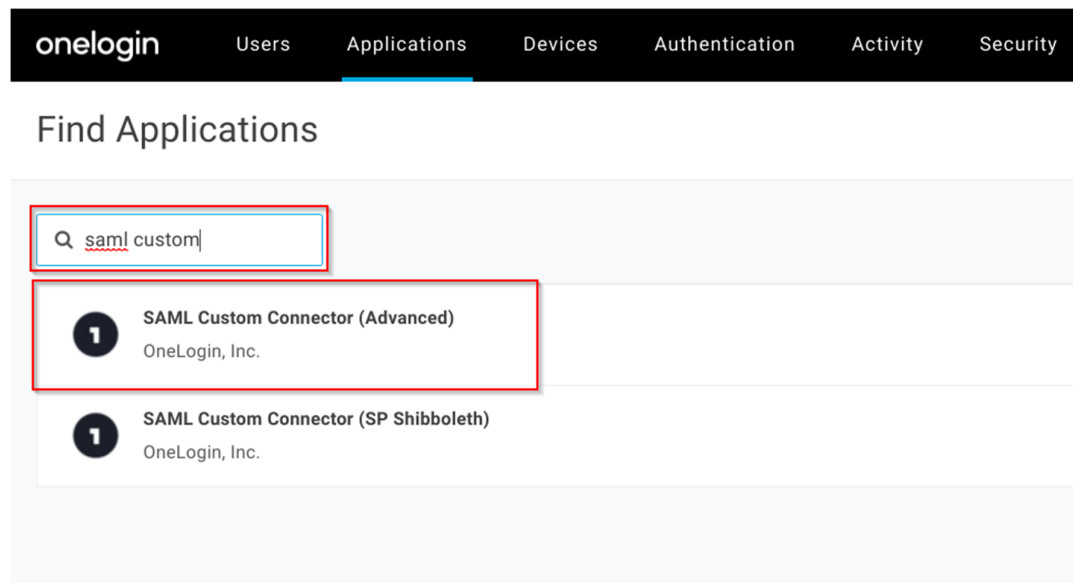
- 2 On the Applications page, click **Add App**.

Figure: OneLogin Add App



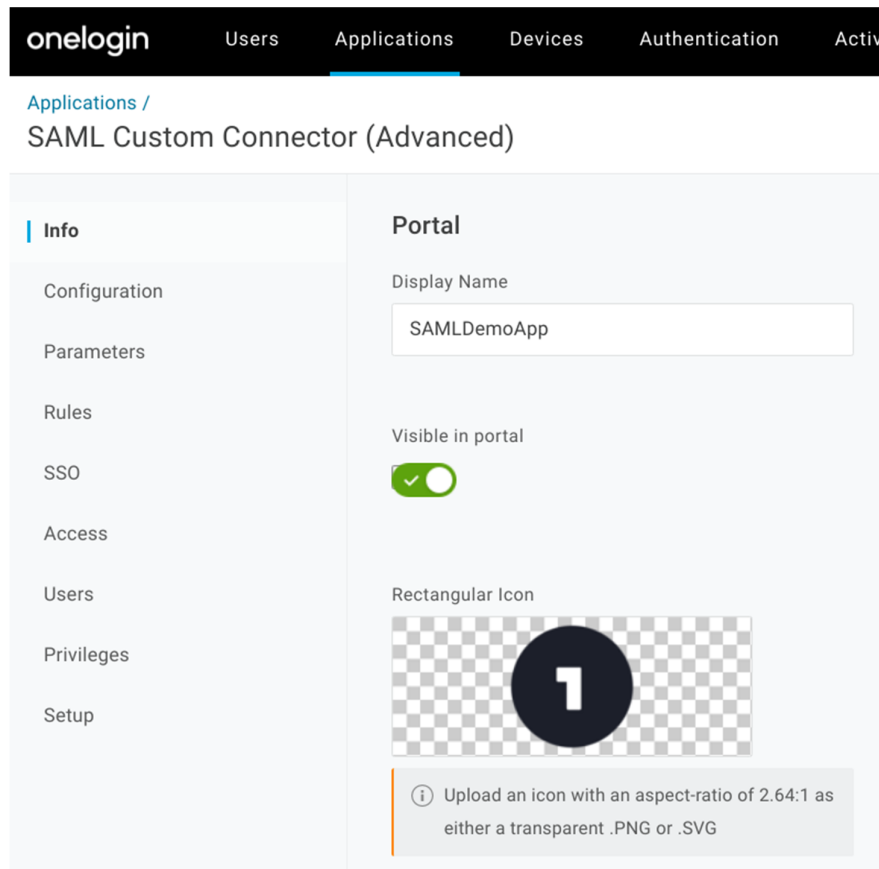
- 3 On the Find Applications page, search for **saml custom**, and then click **SAML Custom Connector (Advanced)**.

Figure: Find Applications page – SAML application



- 4 On the Info page of SAML Custom Connector (Advanced), enter a **Display Name** for the application integration, such as the hostname of the Rapid Recovery Server, and then select **Visible in portal**.

Figure: SAML Custom Connector (Advanced) – Info page




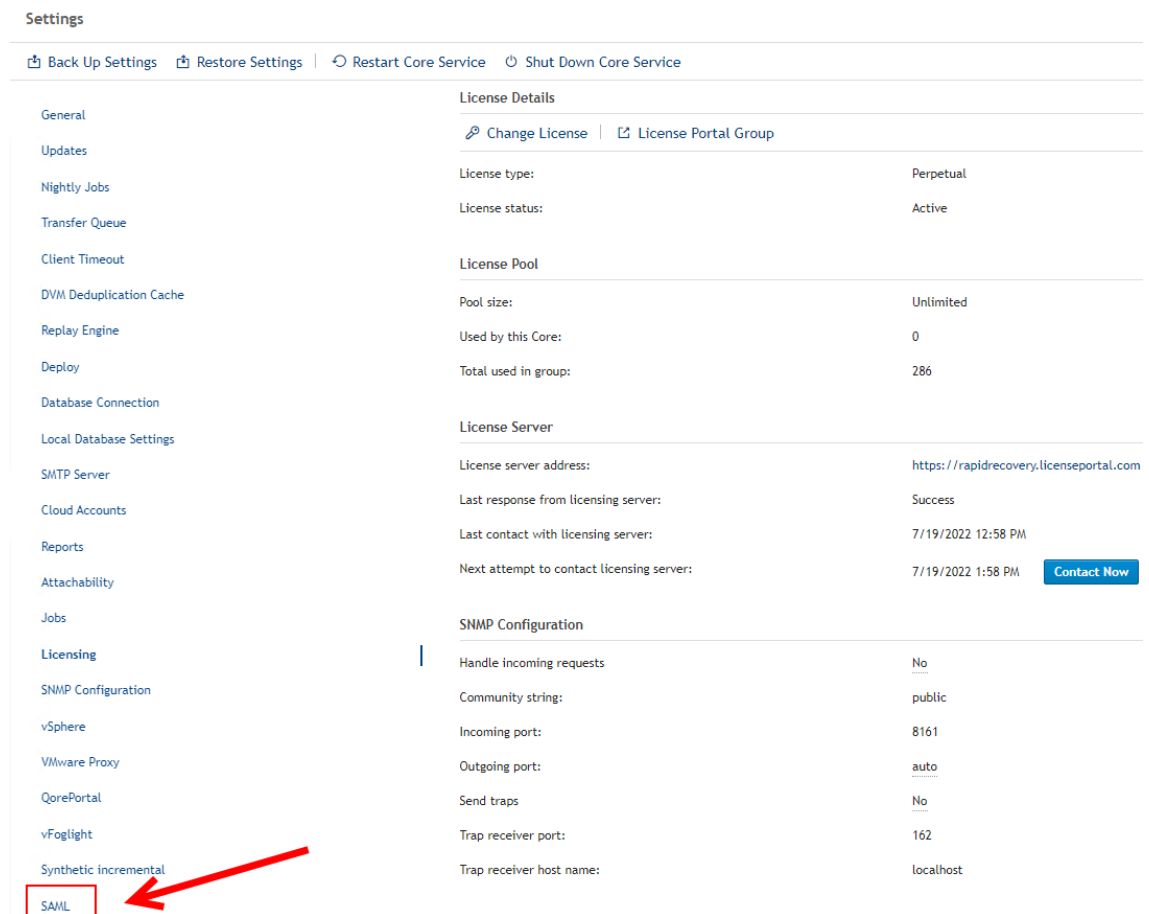
- 21 Go to the Rapid Recovery UI and, in the left navigation for the Core, click the **Settings**  icon.
- 22 On the Settings page, scroll down or click **SAML**.

Figure: Rapid Recovery Settings page




Settings

Back Up Settings | Restore Settings | Restart Core Service | Shut Down Core Service

General	License Details
Updates	Change License License Portal Group
Nightly Jobs	License type: Perpetual
Transfer Queue	License status: Active
Client Timeout	License Pool
DVM Deduplication Cache	Pool size: Unlimited
Replay Engine	Used by this Core: 0
Deploy	Total used in group: 286
Database Connection	License Server
Local Database Settings	License server address: https://rapidrecovery.licenseportal.com
SMTP Server	Last response from licensing server: Success
Cloud Accounts	Last contact with licensing server: 7/19/2022 12:58 PM
Reports	Next attempt to contact licensing server: 7/19/2022 1:58 PM Contact Now
Attachability	SNMP Configuration
Jobs	Handle incoming requests: No
Licensing	Community string: public
SNMP Configuration	Incoming port: 8161
vSphere	Outgoing port: auto
VMware Proxy	Send traps: No
QorePortal	Trap receiver port: 162
vFoglight	Trap receiver host name: localhost
Synthetic incremental	
SAML	

- 23 On the Settings page, under SAML, next to Enable configuration, click the setting. If the setting is currently No, complete the following steps:

- Click **No**.
- Select the empty check box.
- To apply the change, click the check mark .

The SAML settings appear.

- 24 Click the **Copy**  icon for each of the following URLs:

- **Sign on URL**
- **Reply URL (Assertion Consumer Service URL)**
- **Logout URL**

- 25 Return to the OneLogin UI and, on the Configuration page, enter the following details:

- For **Audience (EntityID)**, enter the **Service Provider MetaData URL**.
- For **Recipient**, enter the **Service Provider ACS (Assertion Consumer Service) URL**.
- For **ACS (Consumer) URL Validator***, enter string in the following format:
`^https:\\/[IP or hostname + port
pattern]\\/apprecovery\\admin\\/auth\\/AssertionConsumerService`
- For **ACS (Consumer) URL***, enter the **Service Provider EntityId**.

Figure: SAML Custom Connector (Advanced) - Configuration page

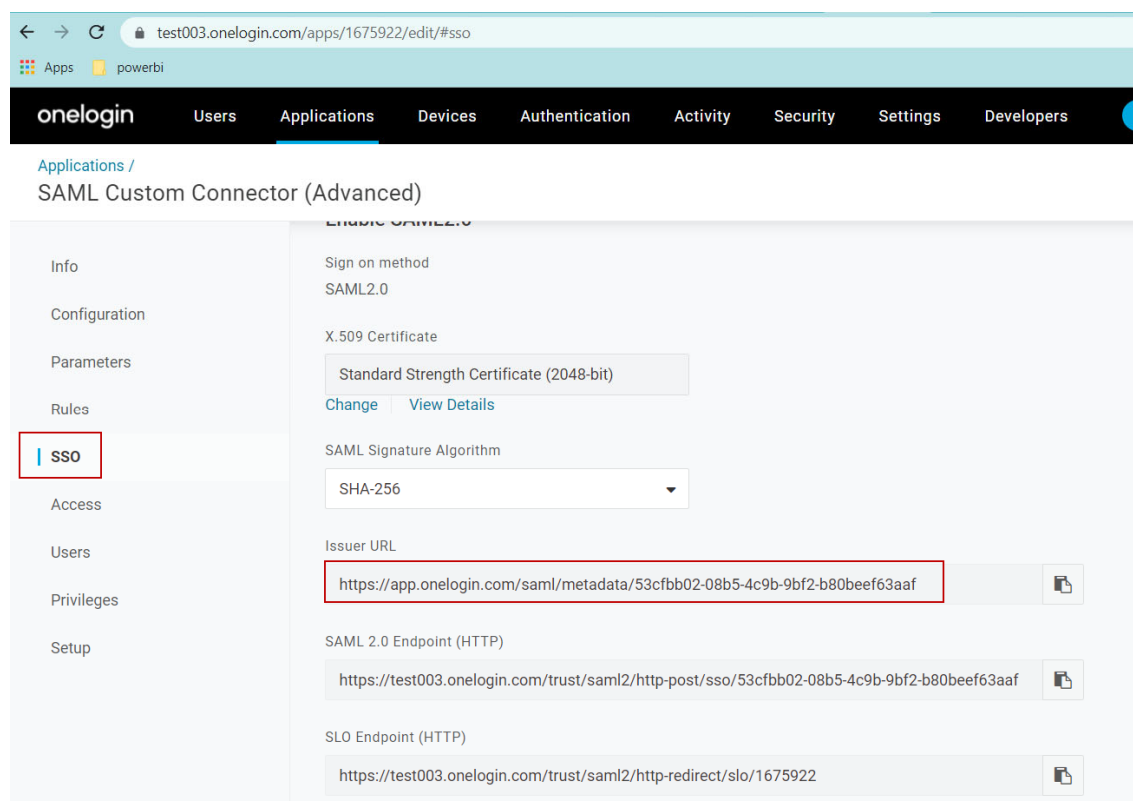
The screenshot displays the OneLogin SAML Custom Connector (Advanced) Configuration page. The left sidebar shows the navigation menu with 'Configuration' selected. The main content area contains the following fields:

- ACS (Consumer) URL Validator***: A text input field containing the regex pattern `^https:\\/[IP or hostname + port pattern]\\/apprecovery\\admin\\/auth\\/AssertionConsumerService`.
- ACS (Consumer) URL***: A text input field containing `https://localhost:44327/Auth/AssertionConsumerService`.
- Single Logout URL**: A text input field containing `https://localhost:44327/Auth/Logout`.
- Login URL**: A text input field containing `https://localhost:44327/Auth/Login`.

A note at the bottom of the configuration section states: "Only required if you select Service Provider as the SAML Initiator." The page also includes a 'More Actions' dropdown and a 'Save' button in the top right corner.

- 5 On the SSO page, to copy the **Issuer URL**, click the icon on the right side of the URL.

Figure: SAML Custom Connector (Advanced) – SSO page



- 6 Click **Save**.
- 7 To add user identities to the SAML application in OneLogin, see OneLogin documentation.
- 8 Return to Core Settings page of the Rapid Recovery Core Console.
- 9 On the Settings page, under SAML, paste the SAML details in the corresponding areas.
- 10 Click **Check SAML**.
- 11 Restart the Core service.

Managing SAML in the Rapid Recovery UI

For information about managing the SAML integration, see the *Rapid Recovery User Guide*.