



Configuring SAML single sign-on authentication for Quest® QoreStor™

Technical White Paper

Quest Engineering
February 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 QoreStor

Updated – February 27, 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 QoreStor UI.....25**

Executive summary

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

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

<http://support.quest.com/qorestor>

Setting up SAML in an identity provider

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

Understanding the SAML 2.0 enterprise application

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

- Azure Active Directory
- Okta
- OneLogin

Limitations

The SAML authentication integration with QoreStor includes the following limitations:

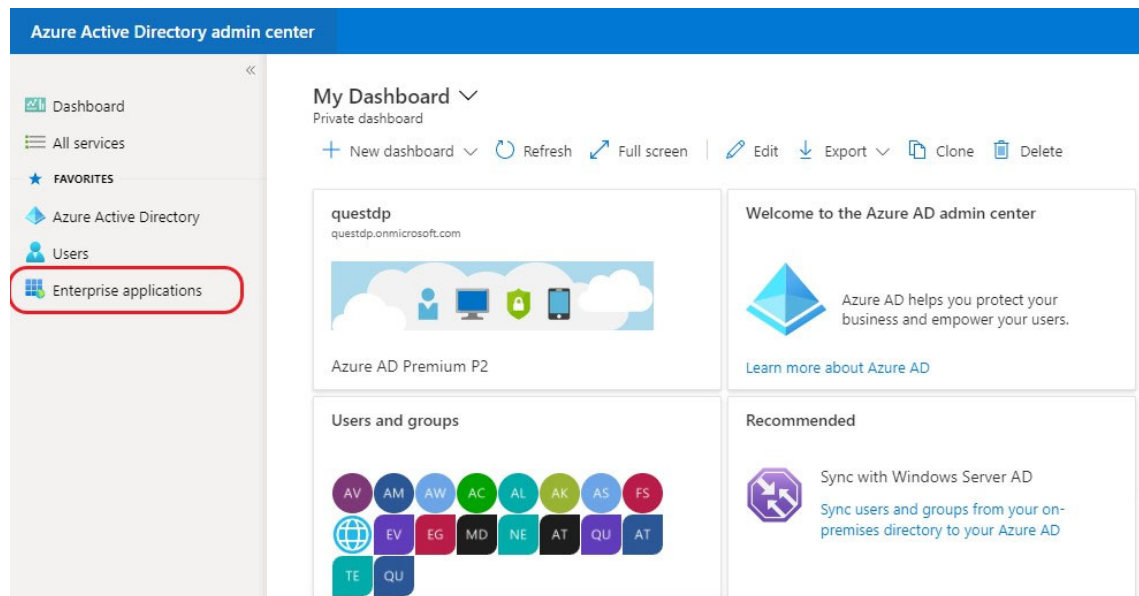
- SAML works only when accessing QoreStor through FQDN, not with an IP address
- Single log-out (SLO) is not supported.
- Firefox is not supported.
- To prevent login failures, the system clock of the machine where QoreStor is installed must be synchronized with the IdP clock.
- Only users are supported.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

Configuring SAML in Azure Active Directory

To configure SAML in Azure Active Directory

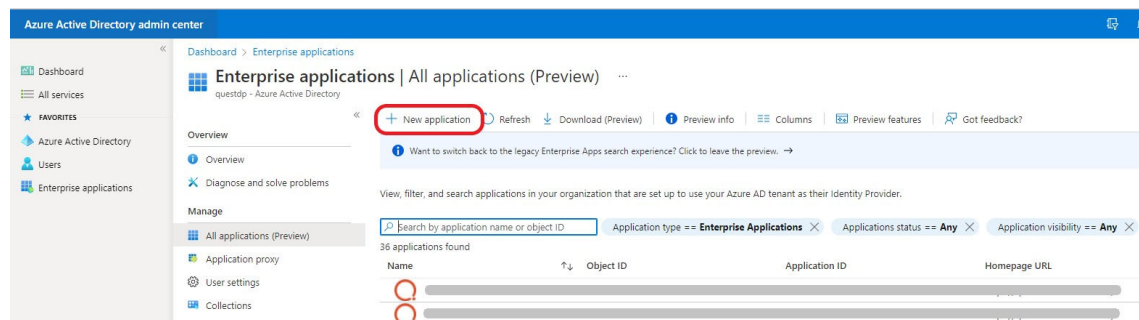
- 1 From the Azure Active Directory (AD) user interface (UI), in the left navigation, click **Enterprise applications**.

Figure: Azure AD – Enterprise applications



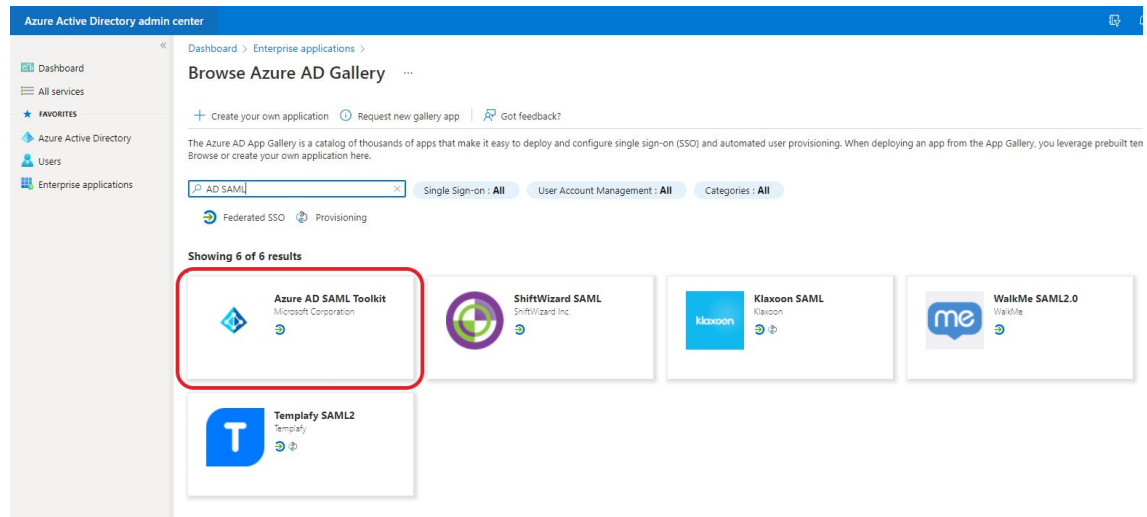
- 2 On the Enterprise applications page, click **New application**.

Figure: Azure AD – New application



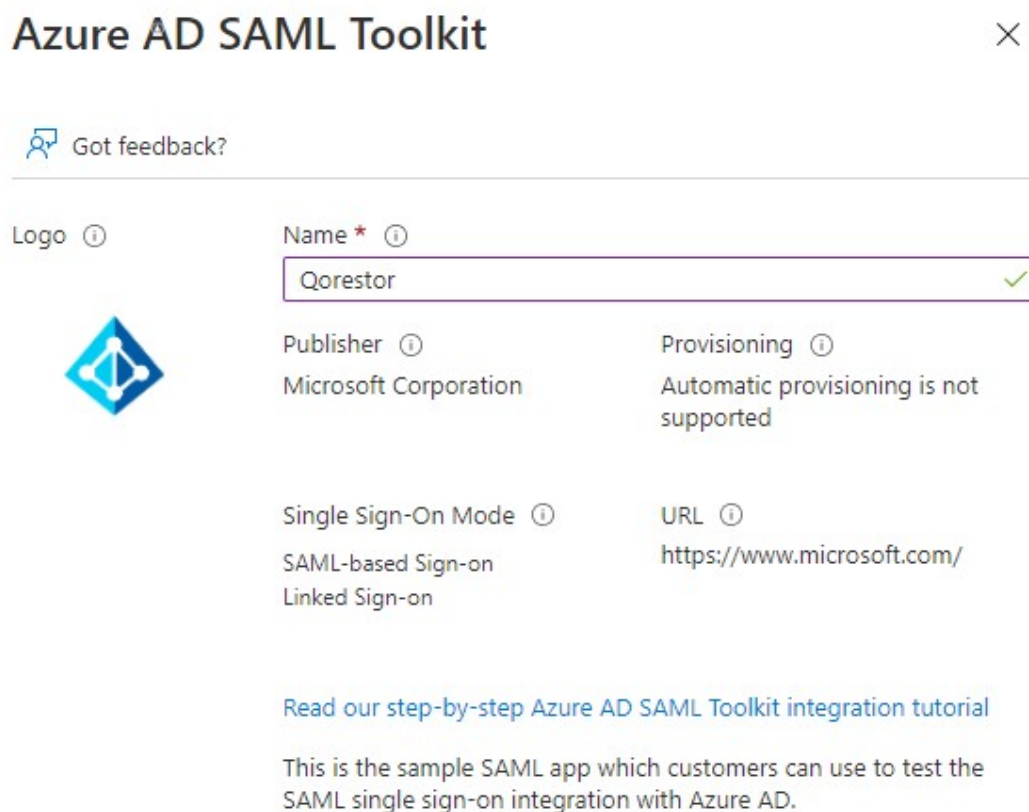
- 3 In the Azure AD Gallery, search for **AD SAML**, and then click **Azure AD SAML Toolkit**.

Figure: Azure AD Gallery



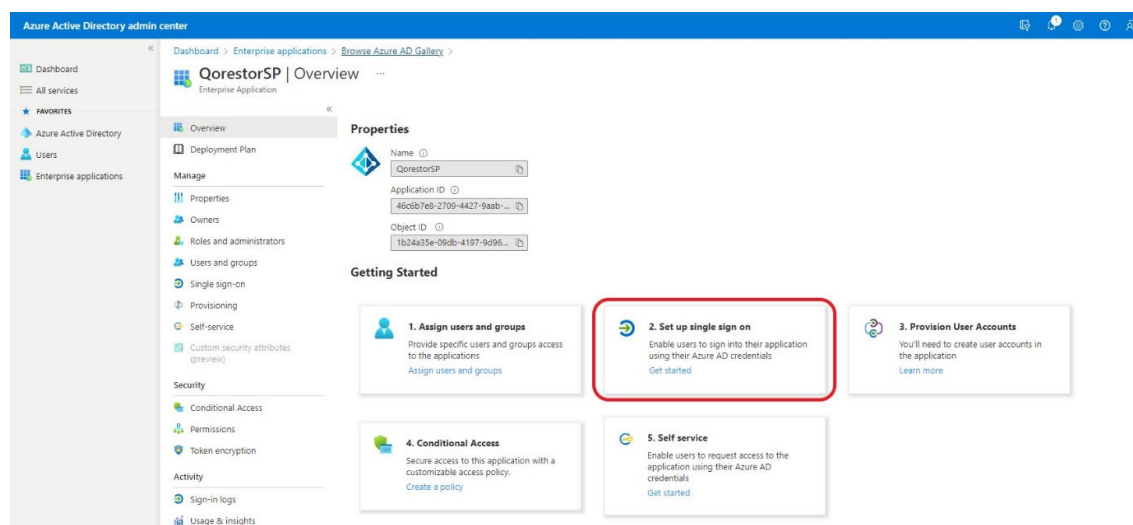
- 8 In the Azure AD SAML Toolkit, enter a name for the configuration, such as the hostname of the QoreStor server.

Figure: Azure AD SAML Toolkit



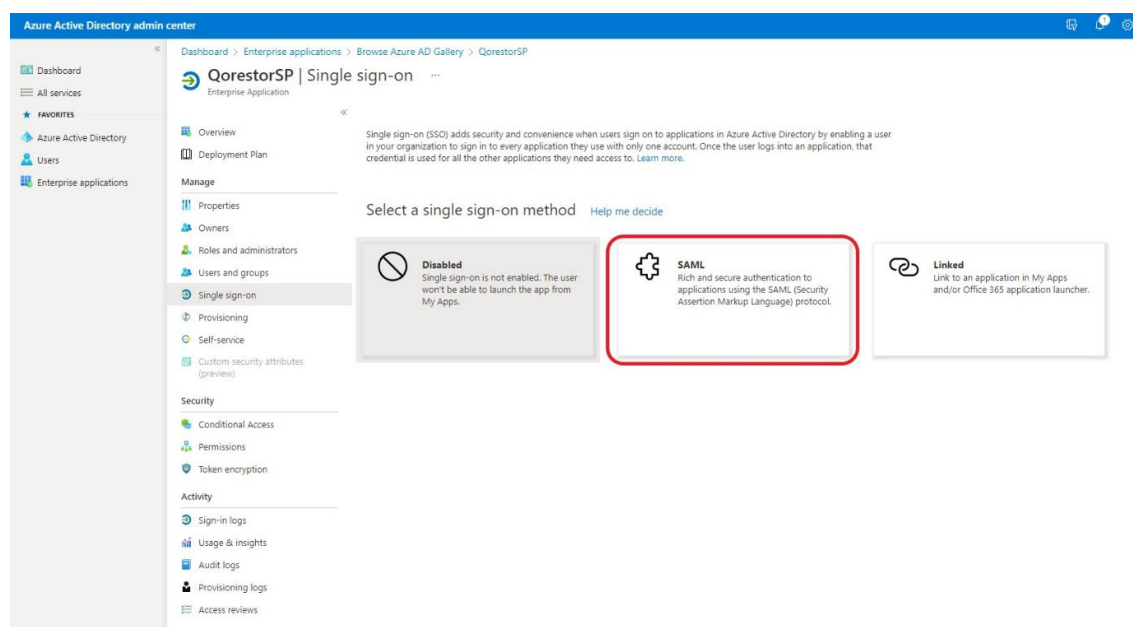
- 9 On the Overview page, under Getting Started, click **Set up single sign on**.

Figure: SAML Overview page



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

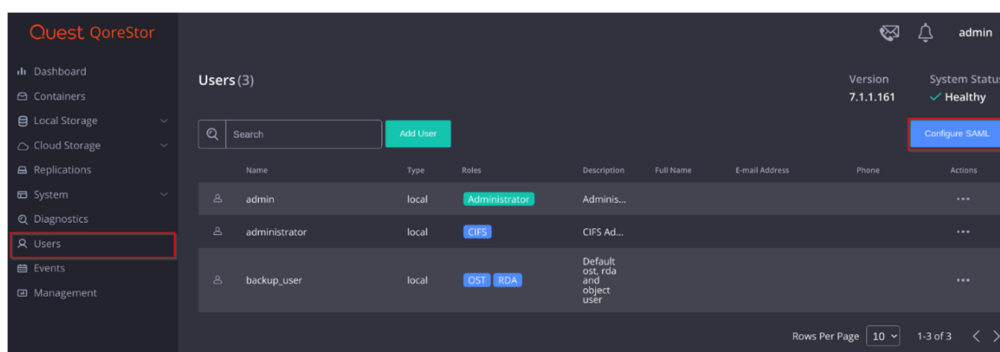
Figure: Single sign-on page



- 8 Go to the Qorestor UI and, in the left navigation, click **Users**.

- 9 On the Users page, click **Configure SAML**.

Figure: QoreStor Users page

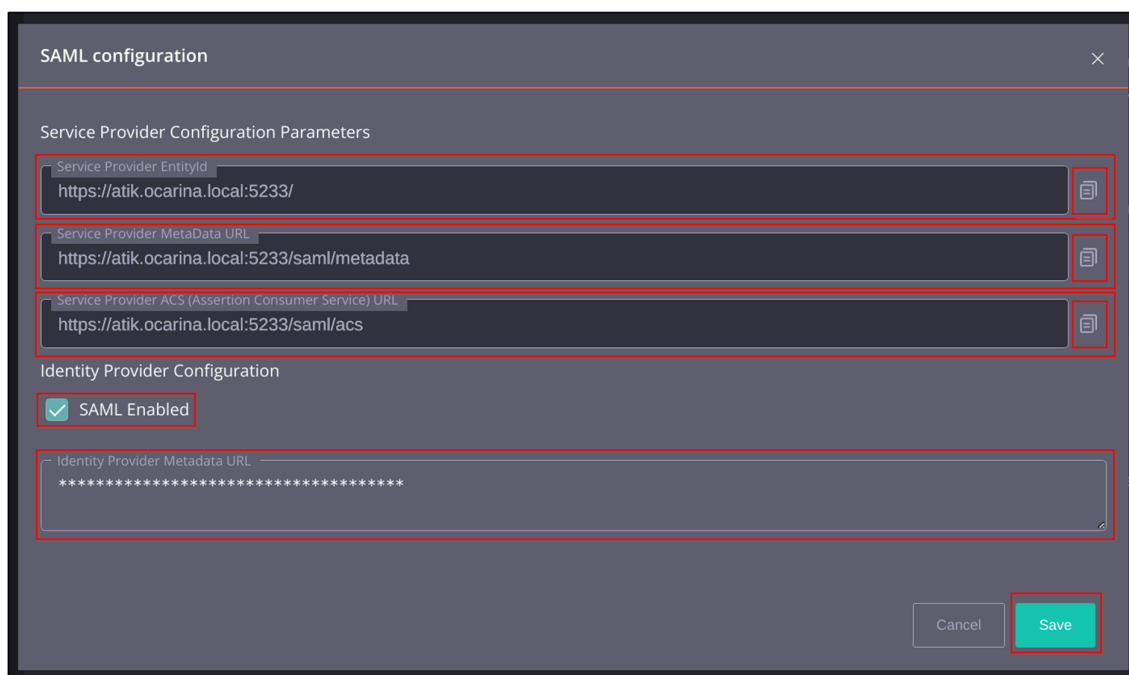


The SAML configuration window opens with the Service Provider Configuration Parameters pre-populated.

10 In the SAML configuration window, copy the following URLs:

- **Service Provider EntityId**
- **Service Provider MetaData URL**
- **Service Provider ACS (Assertion Consumer Service) URL**

Figure: SAML configuration window



11 Return to the Azure AD UI and, on the Set up Single Sign-On with SAML page, complete the following actions:

- In the Basic SAML Configuration section, click **Edit** and enter the following details you obtained from the QoreStor UI:
 - For **Identifier (Entity ID)**, enter the **Service Provider EntityId**.

- For **Reply URL (Assertion Consumer Service URL)**, enter the **Service Provider MetaData URL**.
- For **Sign on URL**, enter the **Service Provider ACS (Assertion Consumer Service) URL**.
- For **Relay State (Optional)** and **Logout Url (Optional)**, leave them blank.
- In the SAML Signing Certificate section, copy the **App Federation Metadata Url** link.

Figure: Set up Single Sign-On with SAML page

Basic SAML Configuration

Identifier (Entity ID)	https://QorestorFQDN:5233/saml/metadata
Reply URL (Assertion Consumer Service URL)	https://QorestorFQDN:5233/saml/acs
Sign on URL	https://QorestorFQDN:5233/
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

Attributes & Claims

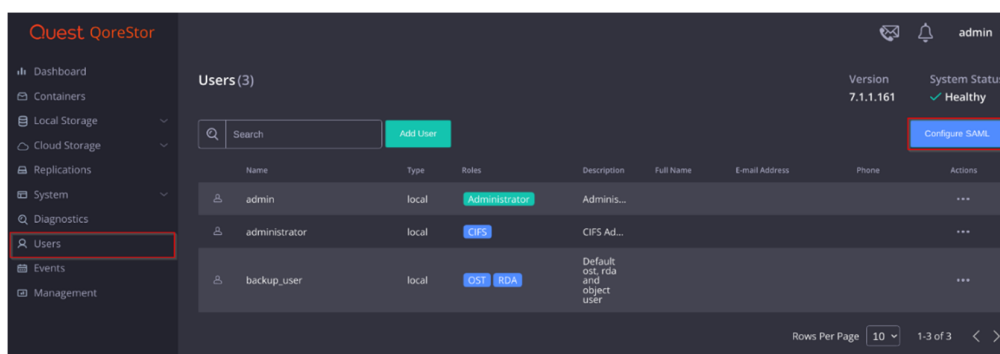
givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

Status	Active
Thumbprint	01360F1010870C2F546082145B574A06B1A4DBC2
Expiration	2/19/2025, 11:58:05 PM
Notification Email	Koteswara.Rao.Annavarapu@questdp.com@microsoft.com
App Federation Metadata Url	https://login.microsoftonline.com/d3981170-ed81...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- 11 To add user identities to the SAML application in Azure AD, see Microsoft Azure Active Directory documentation.
- 12 To add users to the SAML integration in QoreStor, return to the QoreStor UI.
- 13 In the left navigation, click **Users**.
- 14 On the Users page, click **Configure SAML**.

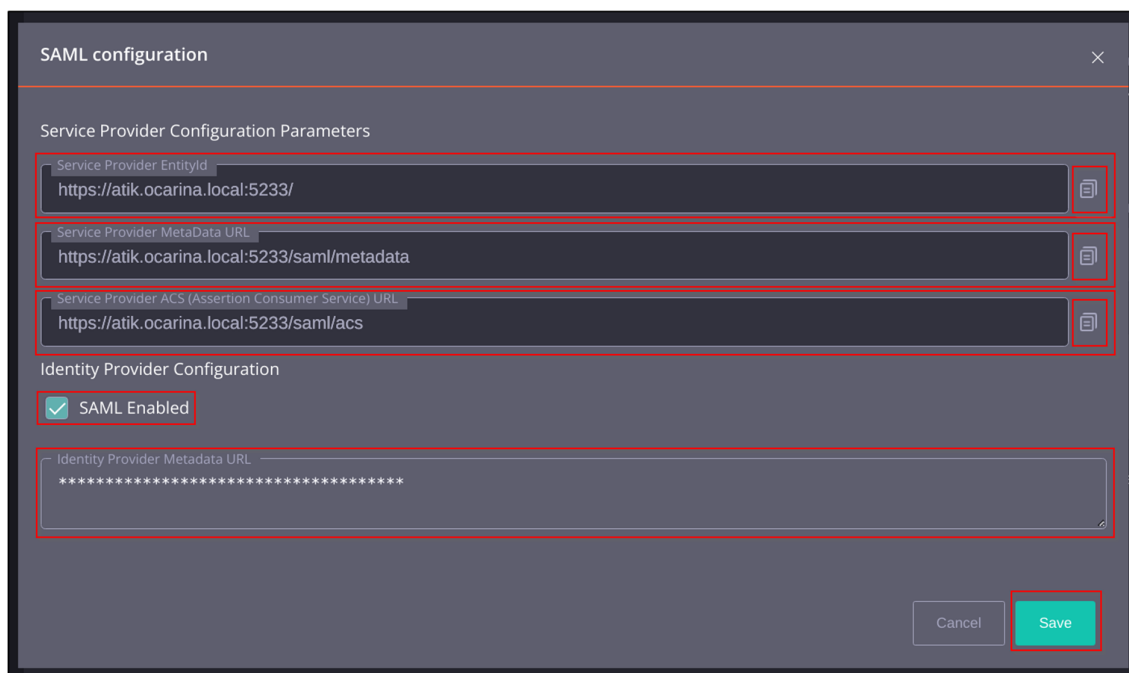
Figure: QoreStor Users page



The SAML configuration window opens with the Service Provider Configuration Parameters pre-populated.

- 15 In the SAML configuration window, in the **Identity Provider Metadata URL** text box, paste the App Federation Metadata URL that you copied in Step 7b, and then click **Save**.

Figure: SAML configuration window



i **NOTE:** Any user identities that you added to the SAML application in Azure AD, you must also add to QoreStor. For more information, see the “Registering an SSO user with the QoreStor Server” in the *QoreStor User Guide*.

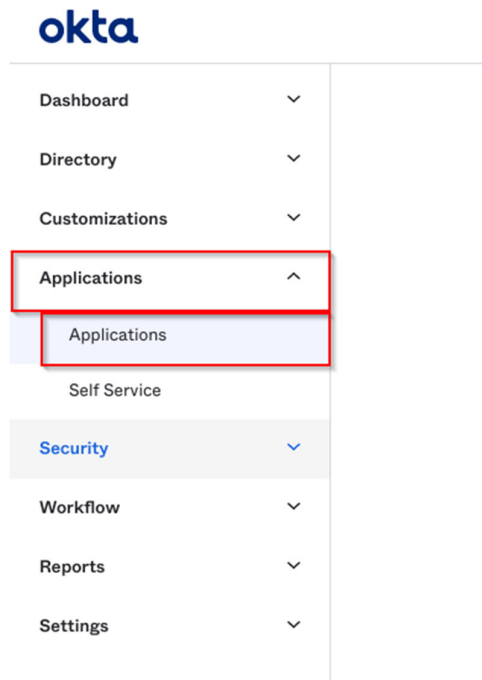
- 17 Restart the ocaui service.

Configuring SAML in Okta

To configure SAML in Okta

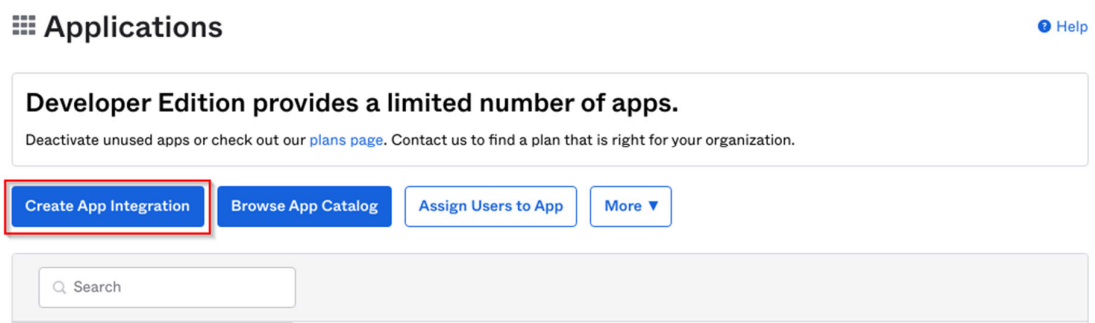
- 1 In the Okta UI, in the left navigation menu, expand the **Applications** menu, and then click **Applications**.

Figure: Okta Applications menu



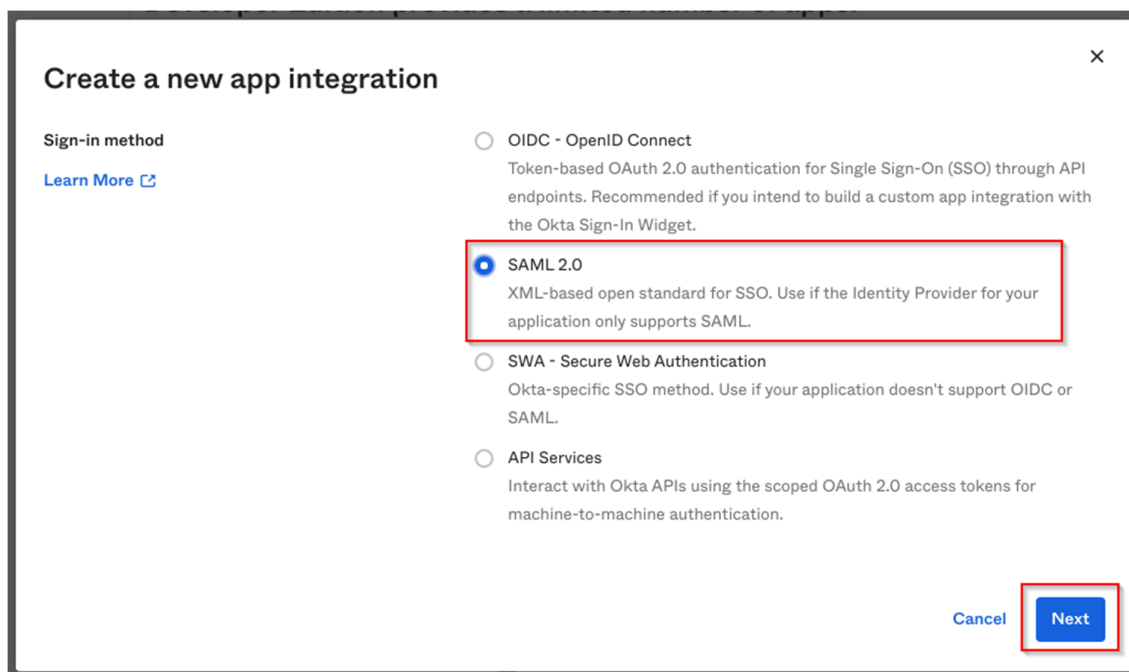
- 2 On the Applications page, click **Create App Integration**.

Figure: Okta Application page



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

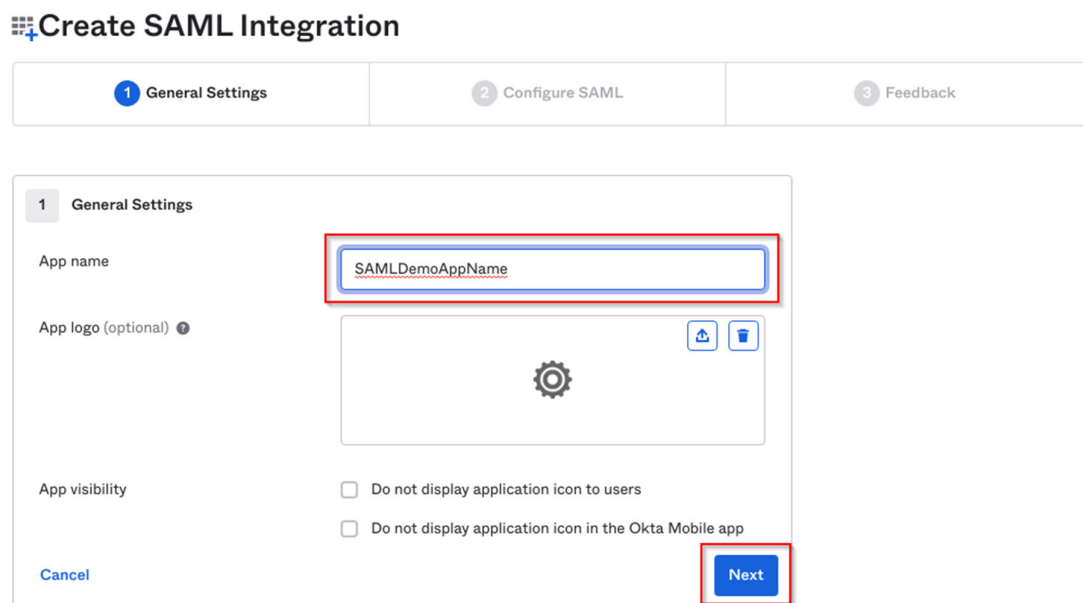
Figure: Okta Create a new app integration window – SAML 2.0



The image shows a modal window titled "Create a new app integration" with a close button (X) in the top right corner. On the left, under "Sign-in method", there is a link "Learn More". The main area lists three options: "OIDC - OpenID Connect" (unselected), "SAML 2.0" (selected and highlighted with a red box), and "SWA - Secure Web Authentication" (unselected). Below "SAML 2.0", there is a description: "XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML." At the bottom right, there are "Cancel" and "Next" buttons, with the "Next" button highlighted by a red box.

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

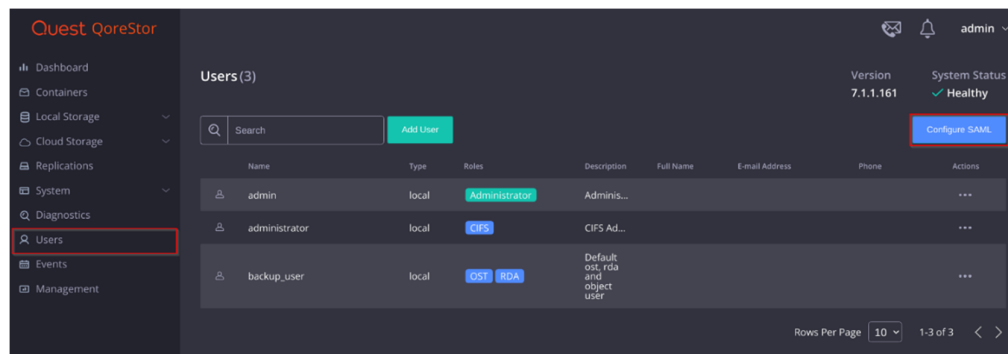
Figure: Create SAML Integration - General Settings tab



The image shows the "Create SAML Integration" page with three tabs: "1 General Settings", "2 Configure SAML", and "3 Feedback". The "General Settings" tab is active. It contains the following fields: "App name" (with the value "SAMLDemoAppName" entered and highlighted by a red box), "App logo (optional)" (with a gear icon and upload/delete buttons), and "App visibility" (with two checkboxes: "Do not display application icon to users" and "Do not display application icon in the Okta Mobile app", both unchecked). At the bottom left is a "Cancel" button and at the bottom right is a "Next" button highlighted by a red box.

- 5 Go to the QoreStor UI and, in the left navigation, click **Users**.
- 6 On the Users page, click **Configure SAML**.

Figure: QoreStor Users page

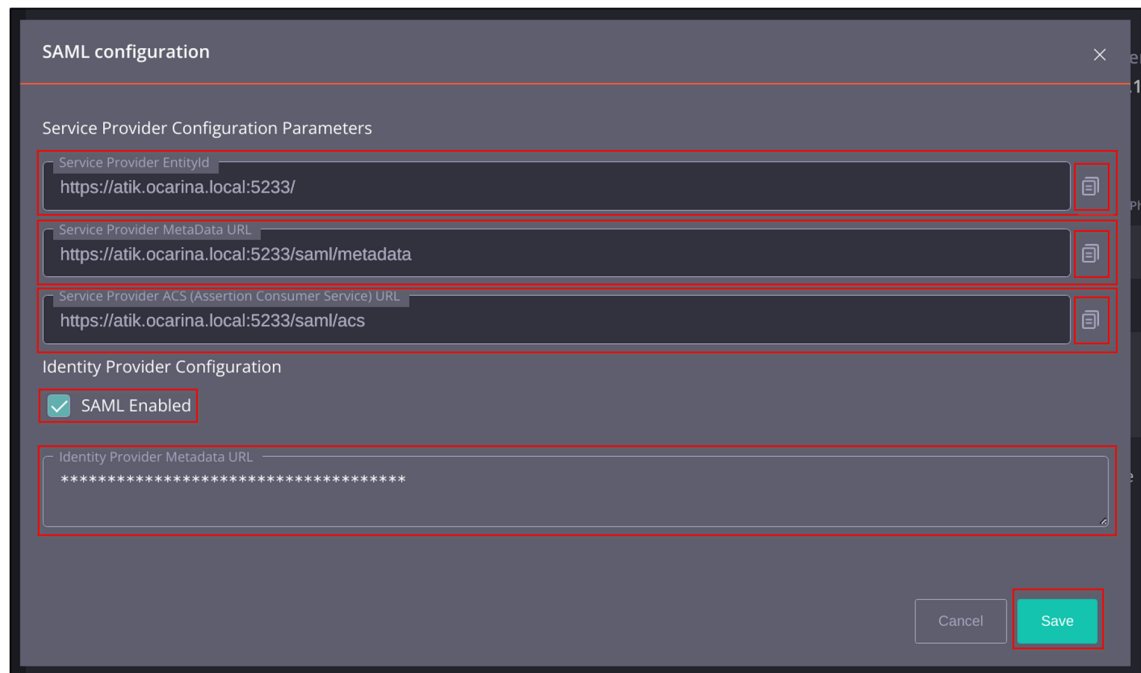


The SAML configuration window opens with the Service Provider Configuration Parameters pre-populated.

7 In the SAML configuration window, copy the following URLs:

- **Service Provider EntityId**
- **Service Provider MetaData URL**
- **Service Provider ACS (Assertion Consumer Service) URL**

Figure: SAML configuration window



8 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 **EmailAddress**.

- 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](#)

- 8 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

Create SAML Integration

1 General Settings

2 Configure SAML

3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

☒ I'm an Okta customer adding an internal app

☐ I'm a software vendor. I'd like to integrate my app with Okta

1

The optional questions below assist Okta Support in understanding your app integration.

App type

☒ This is an internal app that we have created

Previous

Finish

Why are you asking me this?

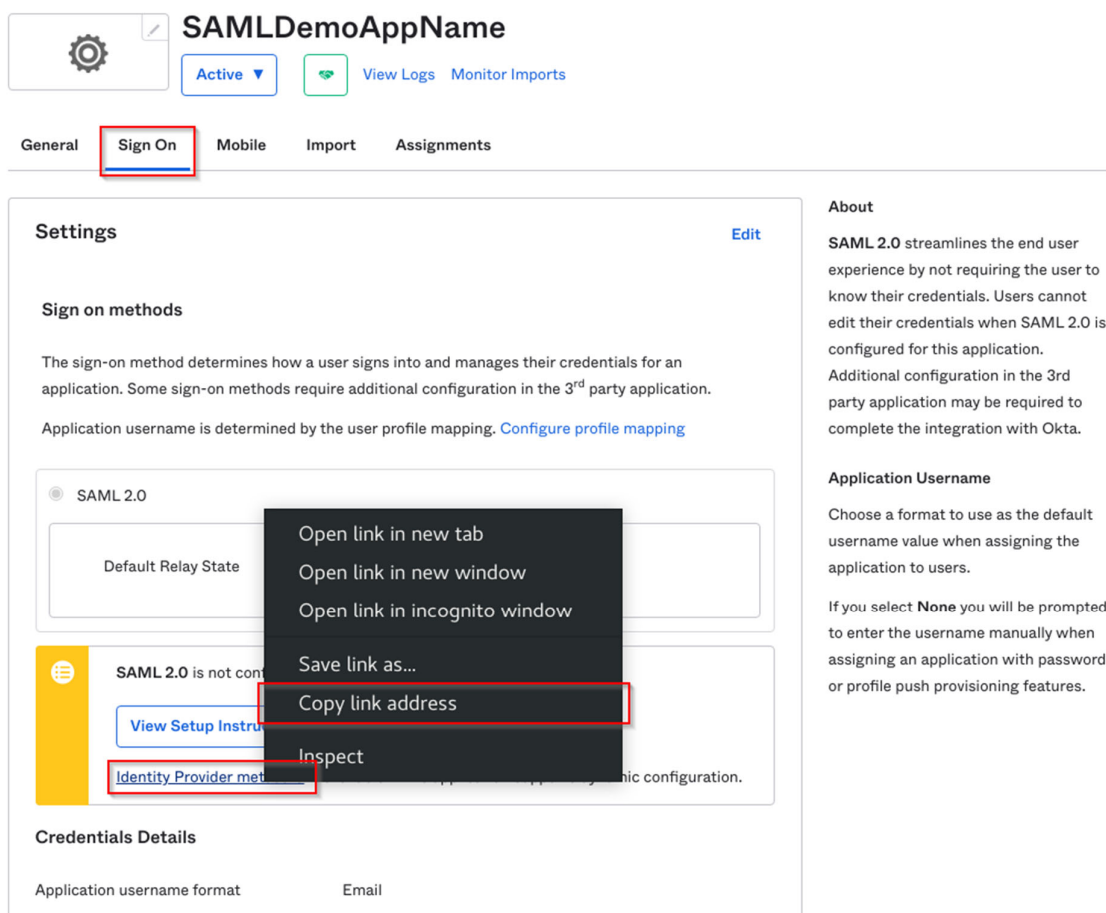
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

9 Click **Finish**.

The UI opens the page for the SAML app integration.

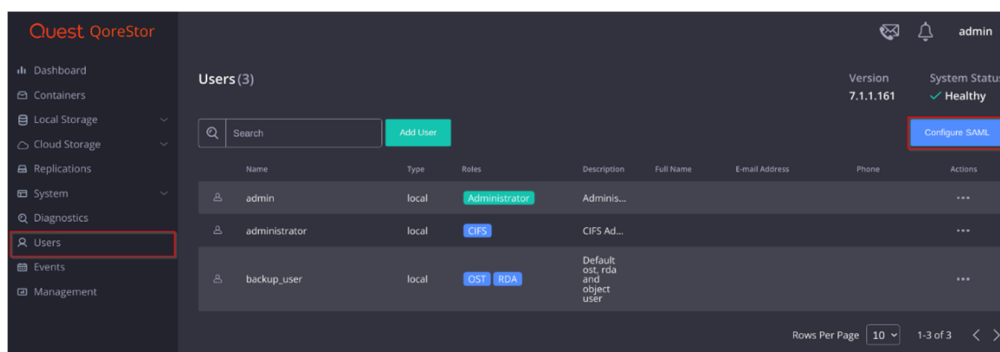
10 On the SAML integration page, go to the **Sign On** tab, and then right-click **Identity Provider metadata** and select **Copy link address**.

Figure: SAML app integration IdP metadata



- 11 To add user identities to the SAML application in Okta, see Okta documentation.
- 12 To add users to QoreStor, return to the QoreStor UI and, in the left navigation, click **Users**.
- 13 On the Users page, click **Configure SAML**.

Figure: QoreStor Users page



The SAML configuration window opens with the Service Provider Configuration Parameters pre-populated.

- 14 In the SAML configuration window, in the **Identity Provider Metadata URL** text box, paste the Identity Provider metadata link that you copied in Step 8, and then click **Save**.

Figure: SAML configuration window

The screenshot shows a 'SAML configuration' window with a close button (X) in the top right corner. The window is divided into two main sections: 'Service Provider Configuration Parameters' and 'Identity Provider Configuration'. In the 'Service Provider Configuration Parameters' section, there are three text input fields, each with a copy icon to its right. The first field is 'Service Provider EntityId' with the value 'https://atik.ocarina.local:5233/'. The second field is 'Service Provider MetaData URL' with the value 'https://atik.ocarina.local:5233/saml/metadata'. The third field is 'Service Provider ACS (Assertion Consumer Service) URL' with the value 'https://atik.ocarina.local:5233/saml/acs'. In the 'Identity Provider Configuration' section, there is a checkbox labeled 'SAML Enabled' which is checked. Below this is a text input field for 'Identity Provider Metadata URL' containing a series of asterisks. At the bottom right of the window are two buttons: 'Cancel' and 'Save'.

i **NOTE:** Any user identities that you added to the SAML application in Azure AD, you must also add to QoreStor. For more information, see the “Registering an SSO user with the QoreStor Server” in the *QoreStor User Guide*.

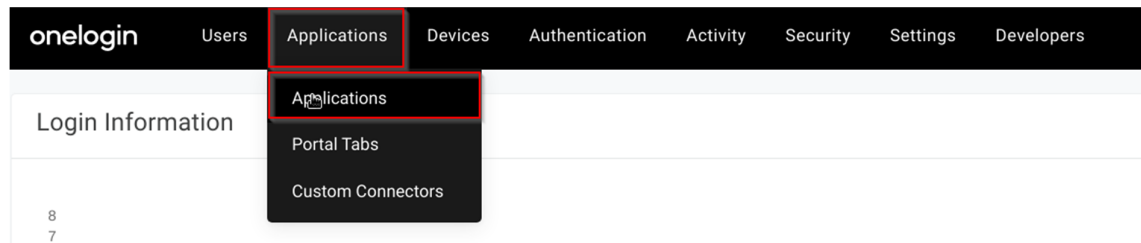
- 15 Restart the ocaui service.

Configuring SAML in OneLogin

To configure SAML in OneLogin

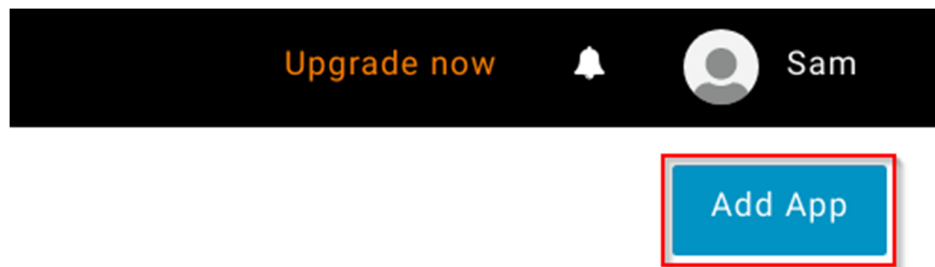
- 1 In the OneLogin UI, in the **Applications** menu, click **Applications**.

Figure: OneLogin Applications



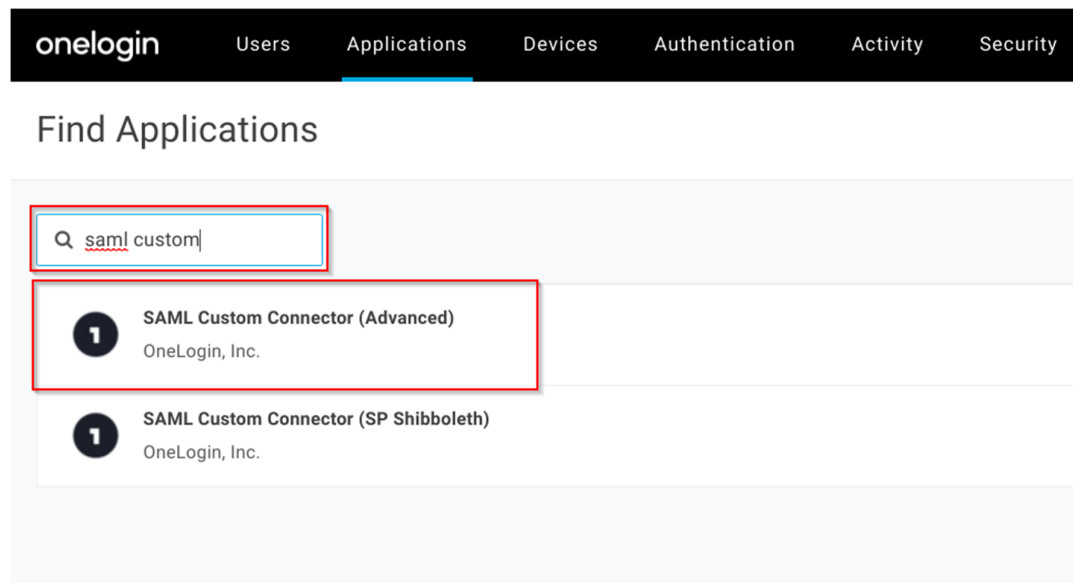
- 2 On the Applications page, click **Add App**.

Figure: OneLogin Add App



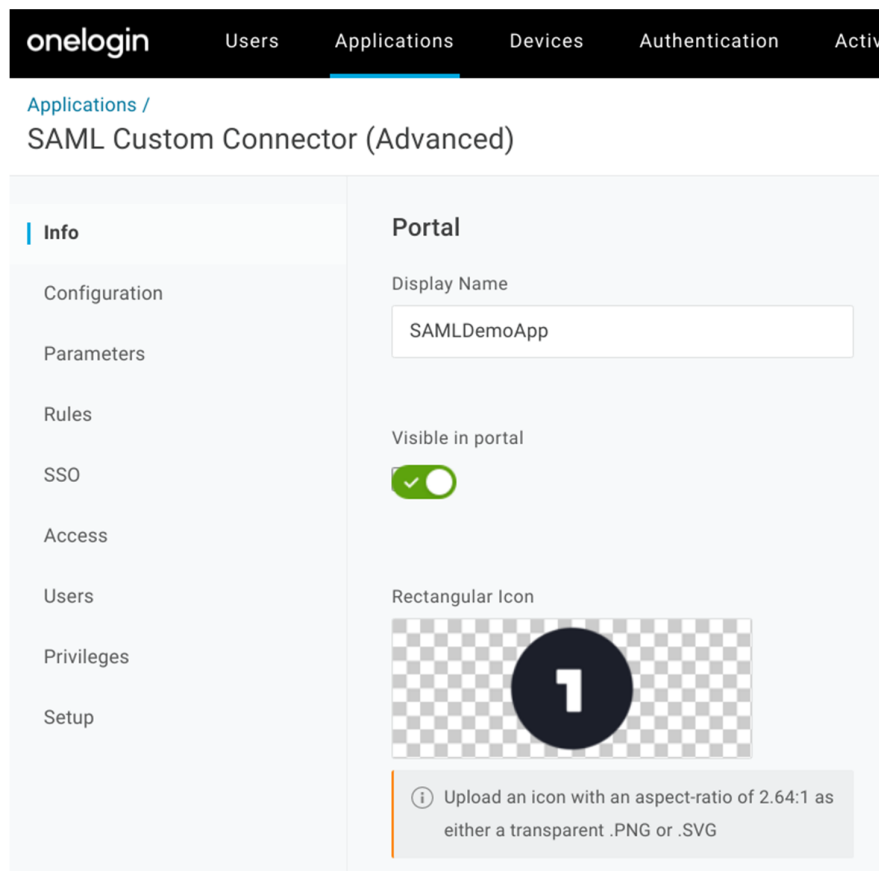
- 3 On the Find Applications page, search for **saml custom**, and then click **SAML Custom Connector (Advanced)**.

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 QoreStor Server, and then select **Visible in portal**.

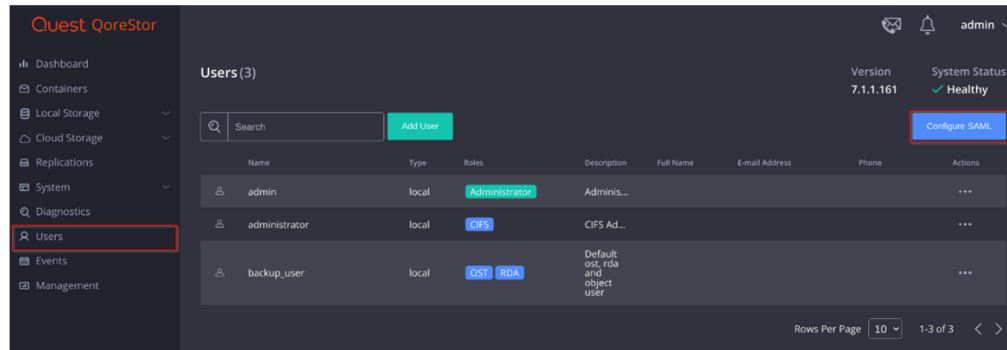
Figure: SAML Custom Connector (Advanced) – Info page



15 Go to the QoreStor UI and, in the left navigation, click **Users**.

16 On the Users page, click **Configure SAML**.

Figure: QoreStor Users page

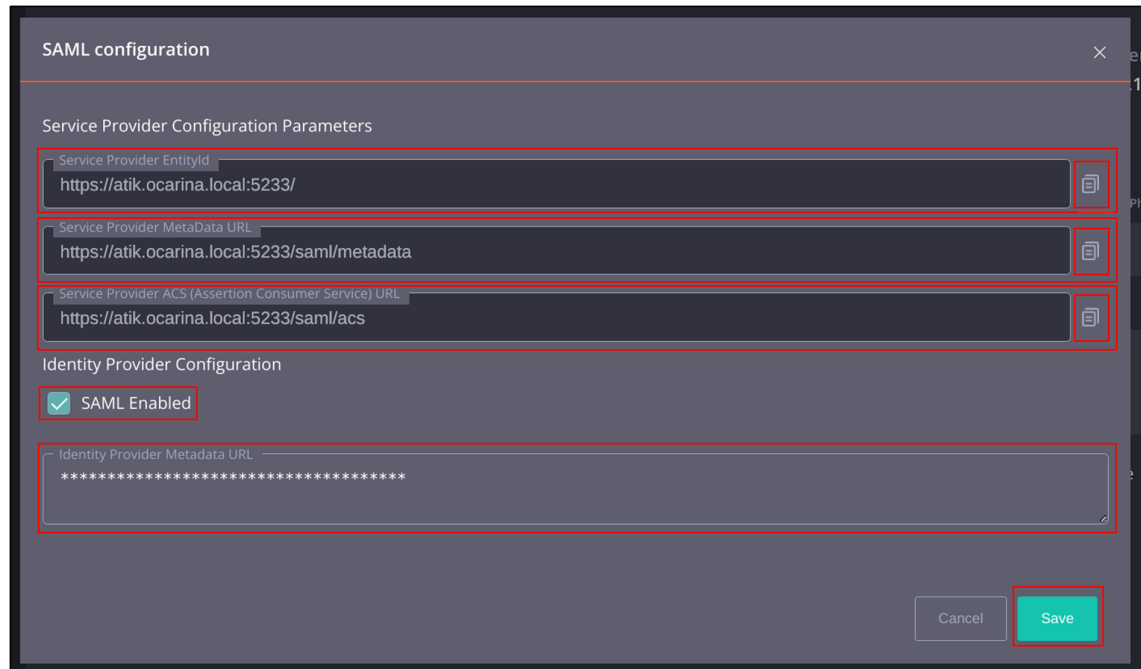


The SAML configuration window opens with the Service Provider Configuration Parameters pre-populated.

17 In the SAML configuration window, copy the following URLs:

- **Service Provider EntityId**
- **Service Provider MetaData URL**
- **Service Provider ACS (Assertion Consumer Service) URL**

Figure: SAML configuration window



9 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: \ / \`
`/hostname_of_qorestor_server.domainname_of_qorestor_server:5233/.*`
- For **ACS (Consumer) URL***, enter the **Service Provider EntityId**.

Figure: SAML Custom Connector (Advanced) - Configuration page

The screenshot shows the 'SAML Custom Connector (Advanced)' configuration page in the OneLogin console. The left sidebar contains a menu with options: Info, Configuration (highlighted with a red box), Parameters, Rules, SSO, Access, Users, Privileges, and Setup. The main content area is titled 'Application details' and contains several configuration fields:

- RelayState**: An empty text input field.
- Audience (EntityID)**: A text input field containing the value `https://qorestorFQDN:5233/saml/metadata`, highlighted with a red box.
- Recipient**: A text input field containing the value `https://qorestorFQDN:5233/saml/acs`, highlighted with a red box.
- ACS (Consumer) URL Validator***: A text input field containing the value `^https:\\\\qorestorFQDN:5233/.*`, highlighted with a red box. Below this field is a required field indicator (info icon and text '*Required').
- ACS (Consumer) URL***: A text input field containing the value `https://qorestorFQDN:5233/saml/acs`, highlighted with a red box. Below this field is a required field indicator (info icon and text '*Required').

- 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

onelogin Users Applications Devices Authentication Activity Security Settings Developers

Applications / SAML Custom Connector (Advanced)

Info Configuration Parameters Rules **SSO** Access Users Privileges Setup

Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)
[Change](#) [View Details](#)

SAML Signature Algorithm
SHA-1

Issuer URL
<https://app.onelogin.com/saml/metadata/6e5b5bc7-5f74-4c46-acb6-9c8bbadb0e24>

SAML 2.0 Endpoint (HTTP)
<https://srikanths-dev.onelogin.com/trust/saml2/http-post/sso/6e5b5bc7-5f74-4c46-acb6-9c8bbadb0e24>

SLO Endpoint (HTTP)
<https://srikanths-dev.onelogin.com/trust/saml2/http-redirect/slo/1680026>

- 6 Click **Save**.
- 7 To add user identities to the SAML application in OneLogin, see OneLogin documentation.
- 8 To add users to QoreStor, return to the QoreStor UI and, in the left navigation, click **Users**.
- 9 On the Users page, click **Configure SAML**.

Figure: QoreStor Users page

Quest QoreStor

Dashboard Containers Local Storage Cloud Storage Replications System Diagnostics **Users** Events Management

Users (3)

Search [Add User](#) [Configure SAML](#)

Name	Type	Roles	Description	Full Name	E-mail Address	Phone	Actions
admin	local	Administrator	Adminis...				...
administrator	local	CIFS	CIFS Ad...				...
backup_user	local	OST RDA	Default ost, rda and object user				...

Rows Per Page 10 1-3 of 3

The SAML configuration window opens with the Service Provider Configuration Parameters pre-populated.

- 10 In the SAML configuration window, in the **Identity Provider Metadata URL** text box, paste the Issuer URL that you copied in Step 6, and then click **Save**.

Figure: SAML configuration window

The screenshot shows a 'SAML configuration' window with a close button (X) in the top right corner. The window is divided into two main sections: 'Service Provider Configuration Parameters' and 'Identity Provider Configuration'. In the 'Service Provider Configuration Parameters' section, there are three text input fields, each with a copy icon to its right. The first field is 'Service Provider EntityId' with the value 'https://atik.ocarina.local:5233/'. The second field is 'Service Provider MetaData URL' with the value 'https://atik.ocarina.local:5233/saml/metadata'. The third field is 'Service Provider ACS (Assertion Consumer Service) URL' with the value 'https://atik.ocarina.local:5233/saml/acs'. In the 'Identity Provider Configuration' section, there is a checkbox labeled 'SAML Enabled' which is checked. Below this is a text input field for 'Identity Provider Metadata URL' containing a series of asterisks. At the bottom right of the window are two buttons: 'Cancel' and 'Save'.

i **NOTE:** Any user identities that you added to the SAML application in Azure AD, you must also add to QoreStor. For more information, see the “Registering an SSO user with the QoreStor Server” in the *QoreStor User Guide*.

- 11 Restart the ocaui service.

Managing SAML in the QoreStor UI

For information about managing the SAML integration and managing SAML users, see the *QoreStor User Guide*.