Manuals+ — User Manuals Simplified.

SEAGATE LYVE Cloud Configuring Federated Login User Guide

S E A G A T E

Contents

Configuring Federated Login

LYVE™ Cloud

Overview

Federated Login provides authentication without revealing user login credentials to the Lyve Cloud service. Federated Login enables your users to use a single authentication method with the help of your organization's Identity Provider (or IdP) for Lyve Cloud.

Once a Lyve Cloud user signs in and has access to your organization's domain, they have direct access to the Lyve Cloud console. The user does not need to perform a separate login process. To use Federated Login feature, your organization must have an authentication system which uses the SAML 2.0 protocol.

To configure Federated Login, contact your organization's IdP administrator to obtain the metadata file in XML format. Upload this file to configure Federated Login.

Security Asser on Markup Language (SAML) Protocol

The Security Assertion Markup Language (SAML) protocol is an open-standard, XML-based framework for authentication and authorization between two entities without a password:

- A **Service Provider** (SP) agrees to trust the identity provider to authenticate users.
- An **Identity Provider** (IdP) authenticates users and provides service providers an authentication assertion that indicates a user has been authenticated.

In this scenario, Lyve Cloud is a Service Provider that will connect with your organization's Identity Provider to establish a Single Sign-On (SSO) access to your users.

Configuring Lyve Cloud as a SAML Service Provider

To configure Lyve Cloud as a SAML service provider:

1. Obtain metadata from your IdP administrator.
2. Configure Lyve Cloud as a service provider.
3. Add service provider metadata to the identity provider.
4. Configure the identity provider to send email attribute.
5. Update the metadata file.

Obtain metadata and certificate from your IdP Administrator

Contact your organizations IdP administrator and obtain the metadata file in XML format to upload and configure Federated Login.
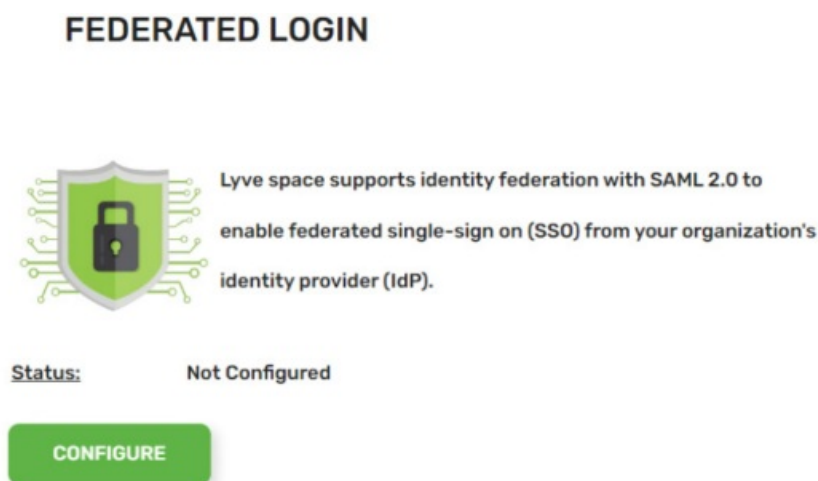
For more information on generating a metadata file for Okta, see **Generating XML Metadata files for IdP** .

Configure Lyve Cloud as a service provider

1. Log in to the Lyve Console either as Root or an Admin user. From the top menu, select the **Feederated Login** tab.

2. On the Federated Login page, select **Configure**.

3. Select Update Metadata file.

CONFIGURE FEDERATED LOGIN

Please upload your SAML metadata file below to complete this configuration

⬆ UPDATE METADATA FILE

4. Navigate to the location of the XML file and select it. Select **Open**.
5. After the Metadata file is uploaded successfully, the configuration data is displayed with its status ('Configured'), the name of the identity provider, and the metadata file expiry date. Example:

FEDERATED LOGIN

Lyve space supports identity federation with SAML 2.0 to enable federated single-sign on (SSO) from your organization's identity provider (IdP).

Status:	Configured
Provider:	qa2-lyvecloud-sso-qa2-saml
Expires on:	16/07/2034

⬆ UPDATE METADATA FILE

IDENTITY PROVIDER CONFIGURATION DATA

Provider URL:	https://lyvespace-dev.us.auth0.com/login/callback?connection=qa2-lyvecloud-sso-qa2-saml
Entity ID:	urn:lyvecloud:qa2-lyvecloud-sso-qa2-saml

DELETE IDP

In addition, the identity provider configuration details are provided. The following attributes are used to configure the IdP:

- Provider URL
- Entity ID

Add service provider metadata to the iden ty provider

1. Add some information to the IdP that allows it to receive and respond to SAML-based authentication requests from the Lyve Cloud service provider. The following instructions are generic. You will need to find the appropriate screens and fields on the identity provider.
2. Locate the screens from the Identity Provider that allow you to configure SAML.

The IdP must know where to send the SAML assertions after it has authenticated a user. This is the Provider URL in Lyve Cloud. The IdP might call this Assertion Consumer Service URL or Application Callback URL.

https://authenticate.lyve.seagate.com/login/callback?connection=<RESELLER><TENANT>-saml

The connection URL parameter is required for identity provider-initiated flow.

i **Note–**If you have custom domeains set up, use the custom domain-based URL rather than your Lyve Cloud domain in the following format:

https://authenticate.lyve.seagate.com/login/callback?connection=–saml

3. Enter the entity ID in the Audience or Entity ID field from Lyve Cloud:urn:lyvecloud: <RESELLER>-<TENANT>-saml
4. If IdP provides a choice for bindings, selectHTTP-Redirect from the Authentication Requests dropdown.
5. The Single Logout Service URLfield contains the destination for SAML logout requests and/or responses from the identity provider. Enterhttps://LYVECLOUD_CONSOLE_URL/signout

i **Signing Logout Requests–**When configuring the IdP, make sure that SAML Logout Requests sent to the service provider are signed.

Configure the identity provider to send email attribute

Lyve Cloud reads an "email" attribute from the identity profile. Some IdPs send "email" by default, while some require you to configure it to send "email".

Okta

Okta must be configured to send an email attribute.

1. Select Applications from the sidebar, and then selectApplications. 2. Select an application to edit, and then selectGeneral. 3. Select Edit in 'SAML settings'. 4. Leave the 'General Settings' as they are and selectNext. 5. In the 'Attribute Statements (optional)' section, select Add Another. Update the attributes as follows:
• **Name** = email
• **Value** = user.email

Update the metadata file

You will need to update the metadata file before the certificate expires. Contact your IdP administrator to get the updated XML file. If you make any updates and regenerate metadata.xml, you must delete the old metadata file before uploading the updated file. If you upload the file without first deleting the old file, it may not update the old file.

1. From the top menu, select theFederated Login tab. 2. On the Federated Login page, selectUpdate Metadata file. 3. Navigate to the location of the updated XML file. Select the file, and then selecOt pen.

After the metadata file is uploaded successfully, the configuration data is displayed along with its status ('Configured'), the name of the identity provider, and the metadata file expiry date.
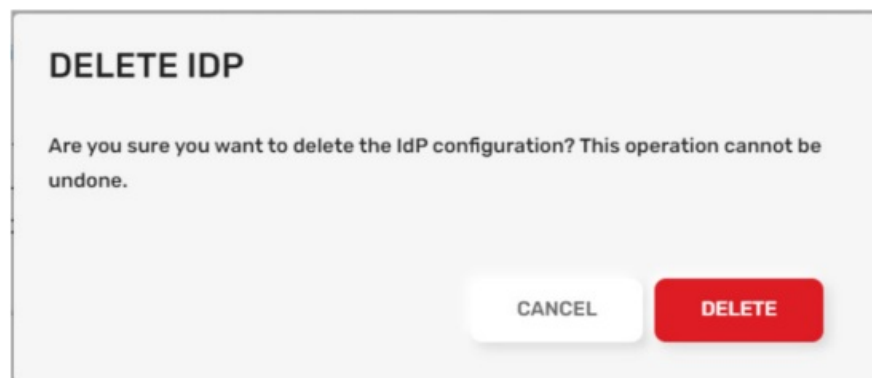
Delete an exis ng IdP configura on

To delete an IdP configuration:

1. From the top menu, select theFederated Login tab. 2. On the Federated Login page, selectDelete IdP.

Entity ID: urn:lyvecloud:qa2-lyvecloud-sso-qa2-saml
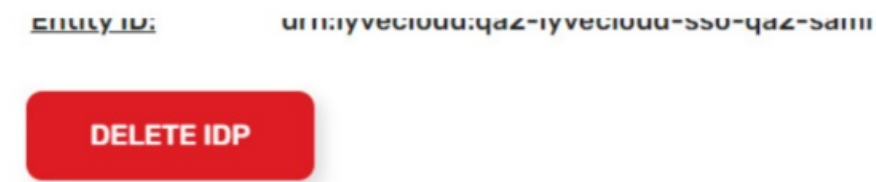
3. In the Delete IdP dialog, selectDelete.

Troubleshoo ng Federated Login

If your application doesn't work the first time, clear your browser history and cookies before you test again. If you don't, the browser may not pick up the latest version of your HTML page, or it may have outdated cookies that impact execution.

To troubleshoot Federated Login:

Capture an HTTP trace of the interaction: Use any of the available tools to capture the HTTP traffic from your browser for analysis.
Search for HTTP Trace. Capture the login sequence from start to finish, and analyze the sequence of GETs to determine how much of the sequence was successful. See a redirect from your original site to the service provider and then to the identity provider.
A post of credentials if you had to log in. A redirect back to the callback URL or the service provider. Finally, a redirect to the callback URL specified in your application. Ensure the cookies and JavaScript are enabled for your browser. Check to make sure that the callback URL specified by your application in its authentication request is listed in the Allowed Callback URLs field. The http://samltool.io tool can decode a SAML assertion and is a useful debugging tool.

Genera ng XML metadata files for IdP

Different types of IdP products have their own way of generating XML metadata files.

Okta

Prerequisites

Create an Okta account and add a user as an administrator for configuration. Lyve Cloud reseller name, account name (tenant name), and administrators account in the console.

Reseller name can be found using the console URL, for examplec: onsole. <RESELLER>.lyve.seagate.com

Account or tenant name is the name of the account you typically enter in the Login screen.

Generate an XML file for Okta

1. In Okta, create an application for Lyve Cloud and log in as administrator. 2. In the sidebar, select the Applications dropdown, and then selectApplications. 3. Select Create App Integration .
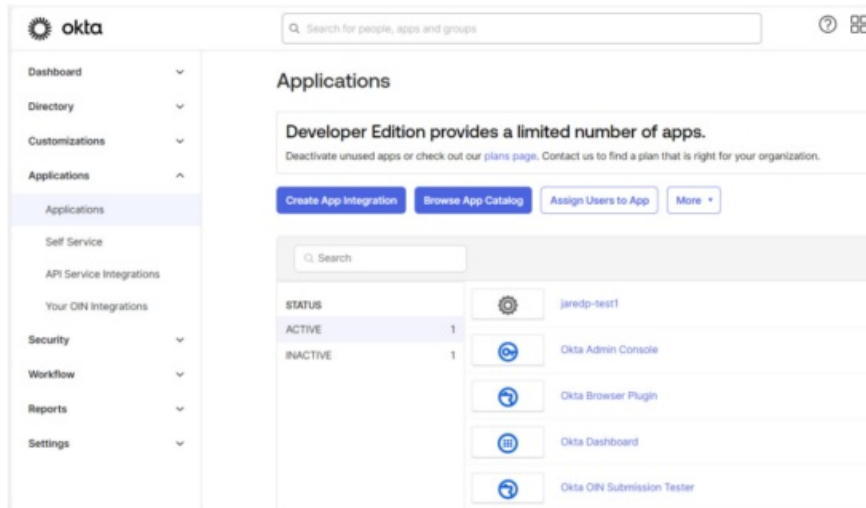
4. In the dialog, selectSAML 2.0, and then selectNext.
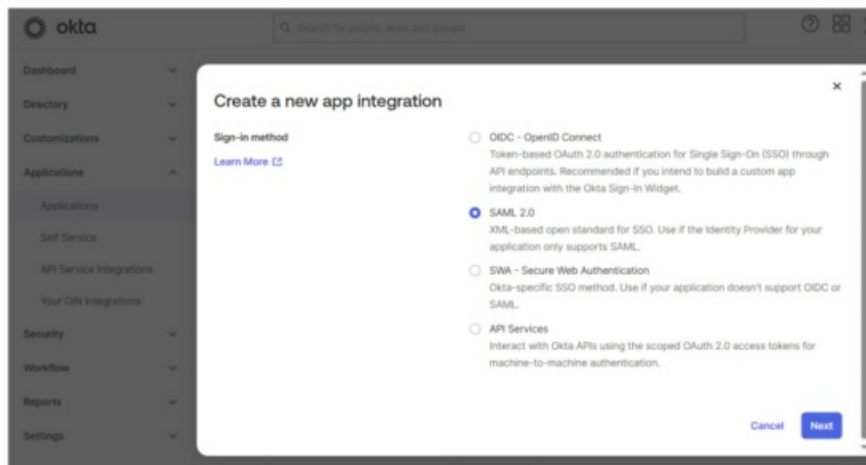
5. In the 'General Settings' section, enter the app name.

Create SAML Integration

	1 General Settings	2 Configure SAML	3 Feedback

1 General Settings

App name	lyvecloud-v2-sso
App logo (optional)	[logo upload area with SEAGATE LYVE Cloud logo]
App visibility	○ Do not display application icon to users

Cancel   Next

---

6. In the 'Configure SAML' section, enter a URL in theSingle sign on URLfield using the following format:

https://authenticate.lyve.seagate.com/login/callback?connection=<RESELLER><TENANT>-saml

For example, if your Lyve Cloud account (tenant) is mytenant and your reseller is myreseller, your single sign on URL would be:

https://authenticate.lyve.seagate.com/login/callback?connection=myresellermytenant-saml
7. In the Audience URI (SP Entity ID) field, enter the SP Entity ID in the following format:

urn:lyvecloud:<RESELLER>-<TENANT>-saml

For example, if your SP Entity ID is urn:lyvecloud:myreseller-mytenant-saml:

Create SAML Integration

	1 General Settings	2 Configure SAML	3 Feedback

A SAML Settings

General

Single sign-on URL	https://authenticate.lyve.seagate.com/login/callback?c
	☑ Use this for Recipient URL and Destination URL
Audience URI (SP Entity ID)	urn:lyvecloud:qa2-lyvecloud-sso-qa2-saml
Default RelayState	|
	If no value is set, a blank RelayState is sent
Name ID format	Unspecified ▾
Application username	Okta username ▾
Update application username on	Create and update ▾

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.

---

8. In the 'Attribute Statements' section, set the following values: Name: email Value: user.email

Select Next.

9. In the 'Feedback' section, provide feedback to help Okta Support understand how the application was configured. Select the appropriate option, and then selectFinish.

Retrieve the XML metadata file

After the application is generated, you must retrieve the XML metadata file.

1. Select the Sign On tab. 2. In the 'Settings' section under 'View SAML setup instructions', extract the IdP metadata and save it to
file with .xml extension.

This is the XML file that is used to configure Lyve Cloud federation.

Logging In to Lyve Cloud as an Okta User

Add users to Okta

1. In Lyve Cloud, ensure that user has afederated authentication type:

CREATE USER

Email *
siva.gurunathan+sso2@seagate.com

Choose Authentication Type *
federated

CANCEL   CREATE USER

2. In Okta, add the user to your Okta account. 3. Assign the Lyve Cloud application to the user.

Applications   Groups   Profile   Devices   Admin roles

Assigned Applications

Assign Applications   🔍 lyve   ⓧ

Application   Assignment & App Username

[LYVE Cloud] lyvecloud-v2-sso   👤 Individual
                                  siva.gurunathan+sso2@seagate.com   ✏️   ✕

Log in to Lyve Cloud

There are two ways for an Okta user to log in to Lyve Cloud.

Okta home page

Select the Lyve Cloud tile on the Okta Home page. You will be redirected to the Lyve Cloud console and logged in automatically using Federated Login.

My Apps

⊙ Work

jaredp-test1

SEAGATE
LYVE™Cloud
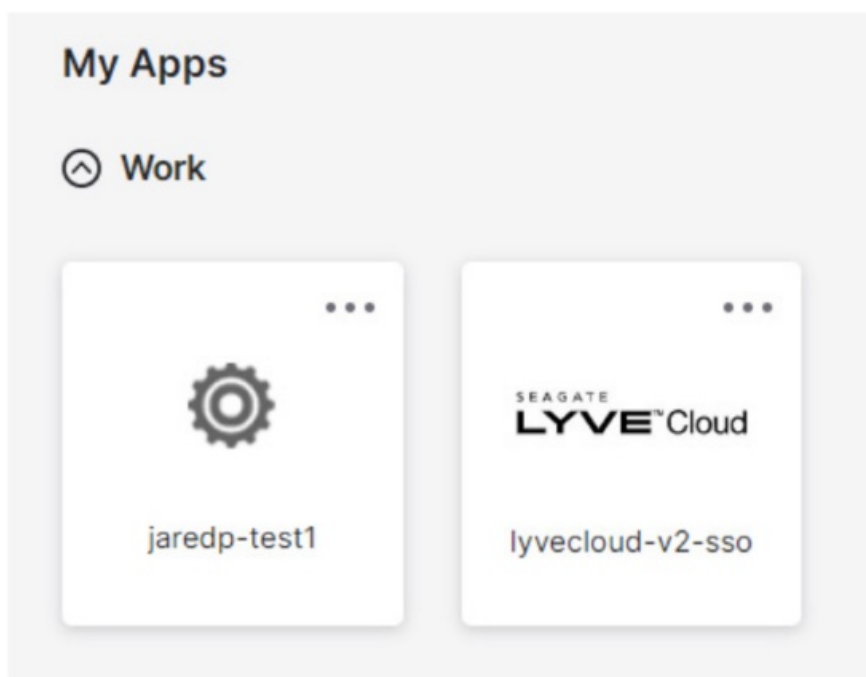
lyvecloud-v2-sso

Embedded link

1. Copy the App Embed Link from the General tab of the Okta application. 2. Paste the link into a browser.

App Embed Link   Edit

Embed Link

You can use the URL below to sign into lyvecloud-v2-sso from a portal or other location outside of Okta.

https://dev-70573509.okta.com/home/dev-
70573509_lyvecloudv2sso_1/0oaidno4nbaA3Fpe05d7/alnidnv5b6jRk9Kz75d7

8/13/24

Documents / Resources

	SEAGATE LYVE Cloud Configuring Federated Login [pdf] User Guide LYVE Cloud Configuring Federated Login, Cloud Configuring Federated Login, Configuring Federated Login, Federated Login, Login

References

- 🌀 **lyve.seagate.com**
- **User Manual**