Qmlativ SSO / LDAP Launch Kit

Qmlativ SSO / LDAP Launch Kit

Table of Contents

What options are available for Single Sign-On?

LDAP (Lightweight Directory Access Protocol)

LDAP is an industry-standard protocol that allows an application like Skyward to authenticate to a 3rd party LDAP directory like Microsoft's Active Directory or Micro Focus's eDirectory.

In general terms, you can think of an LDAP server as a phone book that has the usernames and passwords for the district users. Skyward can take advantage of this "phone book" by allowing it to be used to log into Skyward. The advantage is end users have one less password to remember. The o*ptional* LDAP Group Integration feature allows Qmlativ to read group memberships from your Network directory and then add them to linked Security Groups, automating the assignment of Group Membership in Qmlativ.

SSO (Single Sign-On)

Single Sign-On allows Qmlativ users to log in to Qmlativ using a username and password from a 3rd party system. SSO relies on a 3rd party Identity Provider (IdP) to authenticate Qmlativ users utilizing security tokens provided by a SAML or Active Directory Federated Services IdP. To use SSO you must configure the 3rd party to be an Identify Provider by creating a SAML App in the 3rd party Admin Console.

For an overview video of the Single Sign-On process for your Skyward end-users and other recommended Skyward Security Best Practices, please visit our link to the Skyward Security Best Practices Blog.

Can Cloud Hosted Customers use SSO?

Yes, Cloud Hosted Customers can implement Secure LDAP or SSO across the internet using Secure protocol (LDAPS, LDAP w/ TLS, SAML/wsFed/HTTPS) to encrypt the data between the district's network and the Data Center. Cloud Hosted customers cannot use Kerberos encryption for LDAP.

What are the SSO Firewall Requirements?

ISCorp Cloud Hosted customers must allow access to access to your LDAP servers from the following ISCorp Data Center source IP Addresses:

ISCorp LDAP Source IP Addresses
Adding both ISCorp LDAP source address(es) is recommended for disaster recovery.
Mequon, WI: 192.222.0.56
Dallas, TX: 8.12.72.20

LDAP / SAML Port Information
LDAPS Default Port: TCP 636 (Inbound)
District must provide their LDAPS server Certificate to the Cloud Provider

LDAP/TLS Default Port: TCP 389 (Inbound)
District must provide their LDAP/TLS Server Certificate to the Cloud Provider

SAML 2.0 Default Port: TCP 443 (Outbound)
When a Metadata URL will be used, the district provides the SSO Metadata URL to the Cloud Provider so they can allow the outbound traffic through the data center firewall.

User Management Options

What if the existing user's logins do not match the LDAP or SSO login names?

Many customer's looking to implement LDAP or SSO face this challenge. Good News! We have built several tools to help you!

Account Automation / Identity Management (IDM)

If your district wishes to implement Identity Management beyond the capabilities of the utilities provided in Qmlativ, your district should consider a 3rd party solution that can automate the creation of accounts.

3rd Party solutions

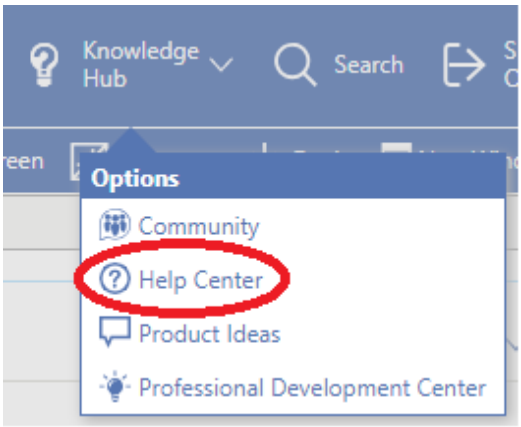
Skyward has partnered with the Tools4ever UMRA solution to provide an Identity Management solution that provisions user accounts from Skyward Student or Business Suites to a variety of systems, including Active Directory. UMRA is our preferred IDM partner but Skyward can be used with any 3rd party IDM solution.

User Import Tools

Importing your Security Users from a third-party software enables you to import a .csv or .txt file of a list of individuals who need secure access. This enables you to create multiple users at once instead of adding them individually. For example, if you have a file that contains your user and security information and you wish to import that information into the Skyward software, you will use this import.

There are two types of imports you can process: importing new users and updating existing users or importing new users and updating and removing existing users.

Details of the User Import options can be found by clicking Help Center and searching for User Import, including sample file formats.



Configure the Security User Import

The following User Import Settings are used when the security user import is processed as a scheduled task.

1. View Menu -> Administrative Access -> Security -> Settings -> System Configuration
2. Under the User Import Heading, enter the User Import Change Threshold (percentage) if appropriate.
3. Enter the User Import Delete Threshold (percentage) if appropriate.
4. Enter the User Import File Path if appropriate (UNC path for Automation)
5. Choose the appropriate User Import File Type Code from the drop-down list -> Save Changes

Processing the Security User Import

1. View Menu -> Administrative Access -> Security -> Utilities -> User Import
2. Select Run User Import -> Choose File -> Next -> If prompted, choose File Type (Only New/Updated Users or All Users) -> Next -> Run
3. Review User Import Results

Configuring the Username Structure can be defined by the system admin, this optional feature ensures that new users are entered using the customer-defined username and email formats.

Configure Username Structure by User Type - Student

Student Management - Configure Student User Name Structure

1. **View Menu** -> Administrative Access -> Student -> Settings -> System Configuration -> Security User Creation

2. Select R – Required on Student Add -> Click Add Username Structure -> Select Desired Part Type Code and character options

    1. Repeat for each desired part code -> Save

3. Test Username Structure on Security User Creation page -> Select sample student -> Generate Username

4. Email Creation can also be configured using **View Menu** -> Administrative Access -> Student -> Settings -> System Configuration -> Email Creation

Configure Username Structure by User Type - Family

Student Management - Configure Family Username Structure

1. **View Menu** -> Administrative Access -> Security -> Settings -> System Configuration

2. Set Authentication mode for Family user type -> S-Skyward or L-LDAP

3. **View Menu** -> Administrative Access -> Family -> Settings -> System Configuration -> Security User Creation

4. Select R – Required on Guardian Add -> Click Add User Name Structure -> Select Desired Part Type Code and character options

    1. Repeat for each desired part code -> Save

5. Test Username Structure on Security User Creation page -> select sample Guardian -> Generate Username

Configure Username Structure by User Type - Staff

Student Management - Configure Staff User Name Structure

1. **View Menu** -> Administrative Access -> Security -> Settings -> System Configuration
2. Set Authentication mode for Admin Employee Teacher Activity user type -> S-Skyward or L-LDAP
3. **View Menu** -> Administrative Access -> Staff -> Settings -> System Configuration -> Security User Creation
4. Select R – Required on Staff Add -> Click Add User Name Structure -> Select Desired Part Type Code and character options
    1. Repeat for each desired part code -> Save
5. Test Username Structure on Security User Creation page -> select sample Staff -> Generate Username

Configure Username Structure by User Type - Employee

Business Management - Configure Employee User Name Structure

1. **View Menu** -> Administrative Access -> Employee -> Settings -> System Configuration -> Security User Creation
2. Select R - Required -> Click Add User Name Structure -> Select Desired Part Type Code and character options
    1. Repeat for each desired part code -> Save
3. Test Username Structure on Security User Creation page -> select sample Employee -> Generate New Username
4. Email Creation can also be configured using **View Menu** -> Administrative Access -> Employee -> Settings -> System Configuration -> Email Creation

Configuring LDAP Provider(s)

Complete the Configuring LDAP Provider steps if you intend to use LDAP as an Authentication source or the optional LDAP Group Integration. You can create multiple LDAP Providers. If you are using SSO Authentication and not LDAP you can skip to Configure SSO Authentication Provider(s).

Step 1 - Create LDAP Provider(s)

1. **View Menu** -> Administrative Access -> Security -> Features -> LDAP Provider

2. Add LDAP Provider -> At a minimum enter the required fields of Host, Port, Protocol Code, and Order.

3. Repeat Steps 1 and 2 if you wish to Add Multiple LDAP Providers.

   Note: The Qmlativ system updates the system cache every 60 seconds so you may need to wait up to 1 minute before your LDAP configuration changes will be used.

   The following pages describe the LDAP Provider fields in detail.

Host

Identifies the Host Name or IP Address of the LDAP server.

Port

Identifies the port of the LDAP server.
The Default Kerberos, LDAP, and SSL/TLS port is TCP 389.
The Default LDAPS port is TCP 636.

ISCorp Cloud Hosted customers must review the SSO Firewall Requirements.

Protocol Code

Specifies the encryption method used to communicate to the LDAP server.

- **S - Simple*** - LDAP with no encryption (port 389 clear text)
  Simple should only be used for testing. When Simple LDAP is used usernames and passwords are transmitted in clear text, it might allow an attacker to intercept your usernames and passwords.
- **K - Kerberos –** Secure LDAP using Kerberos encryption (on-premises only)
- **T - SSL/TLS –** Secure LDAP using TLS Encryption
- **L - LDAPS** -Secure LDAP using LDAPS

Cloud Hosted customers must use either SSL/TLS or LDAPS, Kerberos will only work for on-premises hosted customers.

SSL Certificate Requirements

SSL Certificate Requirement

If the SSL Certificate is self-signed, the LDAP Host Certificate Authority must be installed on the Qmlativ Web and Workflow Servers.
Cloud Hosted Customers must send the exported certificate to their hosting provider to be installed on their Qmlativ Web and Workflow Servers.

SSL Wildcard Certificate Requirement

If used, a Wildcard certificate needs to have a Subject Alternative Name (SAN) that matches the LDAP server hostname.

Domain Name

If using Active Directory enter the short (NETBIOS) name of the Active Directory domain.

The domain field is optional and should NOT be entered when:

- You are not using Active Directory.
- You have entered a Search Base DN
- You have entered a Search Base User

Note: Important for Active Directory Environments:
Check your Active Directory configuration to ensure that the guest account is not enabled. Microsoft and Skyward strongly recommends against enabling the Active Directory guest account for security purposes.
How do I disable the Guest Account for LDAP**?**
https://support.skyward.com/FAQ/View.aspx?ID=1110789

Order

Identifies the order in which the providers are used by the Qmlativ system. The first provider would typically be set as 1, the second provider as 2, and so on.

Ignore Certification Errors

Enables Skyward to trust a misconfigured/untrusted SSL certificate.

Ignore Certification Errors should only be used for testing. When an invalid certificate is accepted, it might allow an attacker to spoof a trusted LDAP Host by using a man-in-the-middle (MITM) attack.

Disable Referrals

Skyward recommends enabling this setting for the best LDAP query performance. Referrals may be required if the LDAP server being quired does not hold a copy of the entire Network Directory, but this configuration is rare.

Search Base DN (optional)

The Search Base DN can be used to improve the lookup performance for large directories. By default, the system will search the entire directory to find the DN of the user. If you would like to limit the search to a specific location in your directory, specify the DN of the location where the search should start.

If you are using LDAP/LDAPS the Search Base DN must be entered using LDAP notation (example: ou=users. Sites that use Kerberos would enter the container name without LDAP notation (example: users)

Search Filter (optional)

The Default Search Filter field will populate automatically after you enter the Search Base DN. After entering the Search Base DN, tab through the Filter field to automatically populate the default filter.

The default search filter includes the attributes of cn and sAMAccountName.
Default: DN(&(objectclass=person)(|(cn=%s)(sAMAccountName=%s)))

You can improve LDAP performance by specifying a specific LDAP attribute.
Modified: DN(&(objectclass=person)(|(sAMAccountName=%s)))

Search User DN (optional)

When you enter a Search User Distinguished Name (DN), the Search User is used to connect and search your LDAP directory when your Qmlativ users authenticate. Typically, a search user is a service account set up by your organization's IT staff. You should enter the Search User DN information using LDAP Notation and enter the Search Users' Password in the Search User Password field.

For Example, you could enter CN=searchuser,ou=users,dc=constoso,dc=com for the Search User DN.

If you leave this field blank the system will attempt an anonymous connection to search your LDAP directory when your Qmlativ users authenticate.

Search User Password (optional)

If a Search User DN field is used, enter the password for that user.

4. Optionally, continue to -> Configure the LDAP Group Membership Integration, or skip to Test LDAP Provider(s)

Step 2 - Configure the LDAP Group Membership Integration

The ***optional*** LDAP Group Integration feature allows Qmlativ to read group memberships from your LDAP directory and sync them to linked Security Groups, automating the assignment of Group Membership in Qmlativ.

Group Base DN

The Group Base DN can be used to improve the lookup performance for large directories. By default, the system will search the entire directory to find the DN of the user. If you would like to limit the search to a specific location in your directory, specify the DN of the location where the search should start.

If you are using LDAP/LDAPS the Search Base DN must be entered using LDAP notation (example: ou=users. Sites that use Kerberos would enter the container name without LDAP notation (example: users).

Group Filter

The Default Group Filter field will populate automatically after you enter the Group Base DN. After entering the Group Base DN, tab through the Group Filter field to automatically populate the default Group Filter.

The default Group search filter includes the objectclass of the group.
Default: (objectClass=group)

Group Member Filter

The Default Group Member Filter field will populate automatically after you enter the Group Filter. After entering the Group Filter, tab through the Group Member Filter field to automatically populate the default Group Member Filter.

The default Group Member search filter includes the objectclass of the user.
Default: (objectClass=user)

Username Attribute

The Default Username Attribute field will populate automatically after you enter the Group Member Filter. After entering the Group Member Filter, tab through the Username Attribute field to automatically populate the default Username Attribute.

The default Username Attribute is the attribute sAMAccountName.
Default: sAMAccountName

Continue to -> Test LDAP Provider(s)

Step 3 - Test LDAP Provider(s)

1. **View Menu** -> Administrative Access -> Security -> Features -> LDAP Provider

2. Choose an LDAP Provider -> In the TEST LDAP PROVIDER DETAILS enter a valid LDAP Username and Password -> Click Run LDAP Provider Test.

3. The LDAP test should report success, also note that a typical login query should not take very long, typically completing in milliseconds. Long queries will cause delays when your users' login and can typically be corrected by tweaking your LDAP Provider configuration.

   LDAP User Requirements

   The Qmlativ usernames match the LDAP usernames. Example: If the user's network login name is "John.Doe" then the skyward login name must also be "John.Doe".

   To use LDAP in the Qmlativ software, users must either be Super Users or be in a security group that gives access to the relevant portals, such as the Admin Portal or Teacher Portal. The group must have menu security configured for the relevant portals. These portals directly correspond to the authentication mode codes on the System Configuration Details screen of the Security module.

   If the user does not meet these requirements, they will not be allowed to log in using LDAP.

4. To test the ***optional*** LDAP Group Membership feature to go **View Menu** -> Administrative Access -> Security -> Features -> LDAP Groups. The screen should populate with groups from your LDAP Directory.

5. Optionally, continue to -> Configure SSO Authentication Provider(s), or skip to Configure Authentication Role(s)

Configure SSO Authentication Provider(s)

If you will be using SAML Identity Providers for authentication, create a new Authentication Method that defines the Identity Provider details. A corresponding SAML application needs to be configured in your 3rd party Identity Provider. If you are only using LDAP for authentication, you can skip to Configure Authentication Role(s).

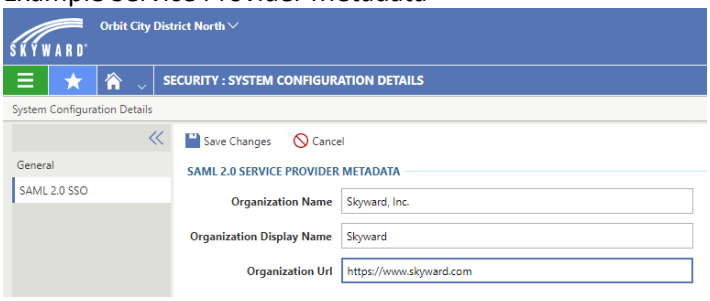
Step 1 – Configure the SAML Service Provider Metadata

Repeat this step once for each Qmlativ environment you are configuration for SSO.

1. **View Menu** -> Administrative Access -> Security -> System Configuration (under Settings) -> SAML 2.0 SSO

2. Enter the Organization Name, Organization Display Name, and Organization URL -> Save.

Example Service Provider Metadata



Step 2 – Create the SSO Authentication Method(s)

You can create multiple Authentication Methods in each Qmlativ environment. Common Examples of 3rd Party SSO Identity Providers (IdP) include but are not limited to Google, Office 365/Azure, or ClassLink. Repeat these steps for each IdP you wish to use for authentication.

1. **View Menu** -> Administrative Access -> Security -> Authentication Method (under Codes)

2. In the top browse, click 'Add Authentication Method'

3. If you are configuring Azure / Office 365 or Google, you can jump to the Authentication Method guidelines for your 3rd party IdP.

    1. Configure Azure / Office 365 as an Identity Provider
    2. Configure Google as an Identity Provider

4. For unlisted IdP's please continue with these steps.

    1. Name: This is the display text in the button that will be displayed to the users on the login screen
    2. Metadata URL (preferred): This is the URL to the metadata for the IdP that you are setting up. Azure / Office 365 provides a SAML URL, please see for details.
    3. Metadata: (optional / not recommended) This is for the raw metadata from the IdP, it should only be used in unique situations. Google SSO requires the use of Metadata, please see for details.
    4. NameID Format: Choose the NameID format that matches the NameID format used by your 3rd Party Identity provider. Consult your IdP vendor documentation for the format.
    5. Authentication Requests Signed (Y/N): Choose the signing Request option that matches your 3rd Party Identity provider. Consult your IdP vendor documentation for this setting.
    6. Want Assertion Requests Signed (Y/N): Choose the signing request option that matches your 3rd Party Identity provider. Consult your IdP vendor documentation for this setting.

5. The second screen of the workflow is mapping the nameidentifier attribute to the corresponding Skyward field. This defines the data that will be used for the NameID claim.

    1. Clicking 'Insert Field' will pop-up a tree browse screen to select the field.

        The tree browse is rooted on the User object, common NameID field choices are the Primary Email Address field (*User.Name.PrimaryNameEmail.EmailAddress)* or the User Name (*Username)* field.

6. Clicking 'Save' will add the Authentication Method and automatically set it to 'Enabled'

7. Next Step: Configure Authentication Role(s)

Configure Authentication Role(s)

Configuring the Authentication Roles enables the organization to set the security login credentials for their users. These roles contain the LDAP Provider information and the Single Sign-On Authentication Methods that are used.

Step 1 - Create the Authentication Role(s)

Authentication Roles determine the login methods a user can use, such as LDAP, SSO, or the local Skyward login. For every combination of login methods that users will be using, an associated Authentication Role must exist so it can be configured in the correct portal, role override, and user override. Authentication Roles can also be configured to be the interfaces users see when they sign into the Skyward software using their single sign-on authentication.

Typically, you would create a minimum of 3 Authentication Roles, for example:
Authentication Role 1: Skyward Only
Authentication Role 2: Skyward OR LDAP/SSO (whichever you are using)
Authentication Role 3: LDAP/SSO Only (whichever you are using)

1. Navigate to Administrative Access -> Security -> Authentication Role (under Features)
2. In the top browse, click 'Add Authentication Role'
3. The first screen of the workflow includes the following fields:
    1. Name: Unlike Authentication Method, this name will not be displayed to Users
    2. Display Text: This is the display text in the button that will be displayed to the users on the login screen, this is used for SSO Authentication methods.
    3. Allow Skyward Credentials: Checking this option allows the user's local skyward user and password to be used for this given Authentication Role.
    4. Icon: (optional) This is an icon that will be displayed beside the Display Text on the button on the login screen, this is used for SSO Authentication methods.
4. Save the configuration changes
5. Repeat these steps to create additional Authentication Roles that covers all your user's authentication scenarios.

Step 2 - Adding an SSO Authentication Method to Authentication Role(s)

If using SSO, this step connects the Authentication Method and Authentication Role. Skip this step if you are using LDAP and not SSO.

1. Navigate to Administrative Access -> Security -> Authentication Role (under Features)
2. Choose the Authentication Role that will include your SSO Authentication Method.
3. In the bottom browse, click the 'Add Authentication Role Method'.
4. Select the dropdown and pick the Authentication Method(s) that you would like to include for the Authentication Role. Repeat this step to add Multiple Authentication Roles.
5. Save the configuration changes

Step 3 - Adding an LDAP Provider to Authentication Role(s)

If using LDAP, connecting the LDAP Provider and Authentication Role together enables the user to use the authentication method. Skip this step if you are using SSO and not LDAP.

1. Navigate to Administrative Access -> Security -> Authentication Role (under Features)
2. Choose the Authentication Role that will include your LDAP Provider.
3. In the bottom browse, click 'Add Authentication Role LDAP Provider'
4. Select the dropdown and pick the LDAP Provider(s) that you would like to include for the Authentication Role. Repeat this step to add Multiple LDAP Providers.
5. Save the configuration changes

Step 4 - Authentication Override at the User Level

The next step is to configure at least one user that can log in with their Qmlativ password even if the LDAP Provider or SSO Authentication Method is not working. **This is an important first step that will prevent you from accidentally locking yourself out of the Qmlativ application.** The user-level authentication method and override options are visible on the security user profile.

1. **View Menu** -> Administrative Access -> Security -> User (Under Features)

2. Use the search to find user -> Open User (arrow) -> Choose Authentication Role Override that allows the Skyward Login -> Save

Step 5 - Configure Authentication Role(s) at the Portal/Security Role Level

Configuring the Authentication Roles at the Portal Level is required, and it enables the organization to set the security login credentials for their users by the portal.

1. **View Menu** -> Administrative Access -> Security -> Settings -> System Configuration

2. Scroll down to the Authentication roles and choose Authentication Roles as necessary for "Admin/Employee/Teacher/Family/Student/Activity" User types.

3. Optionally, enable the "Combine Authentication Roles" feature. When checked, indicates users with SSO login credentials have only one authentication role in effect when logging in.

4. Save the configuration changes.

Optionally, Authentication Role Overrides can be defined on Security Roles. This is found under the **View Menu** -> Administrative Access -> Security -> Security Role (Under Features) -> Open the Desired Security Role -> Choose the Authentication Role Override -> Save.

If an override is added to a Security Role or a User, the system will first check for the User value, then the Security Role value, and finally the Portal Level. Most users should have the authentication role configured at the Security Role or Portal Level.

Step 6 – Test the Authentication Role(s)

Note: The Qmlativ system updates the system cache every 60 seconds so you may need to wait up to 1 minute before testing Authentication Roles changes.

1. Navigate to your Qmlativ Login URL.

2. Test LDAP or Skyward logins by using the traditional username/password fields on the login screen.

3. The Qmlativ Login screen will also display the SSO Authentication roles that have been created. Test SSO Authentication using the SSO Authentication button(s).

If your Authentication Test succeeds, congrats!

If you are using SSO and want to create an SSO link on a website or within a portal continue to -> Creating an SSO Login Link

If your Authentication Testing fails review Troubleshooting Identity Provider Configuration(s).

Step 7 – Creating an SSO Login Link (Optional)

You can create a link on a website or portal that directs the users to the SSO login page.
Login Link:
https://[FQDN]/[EnvironmentName]STS/SSOAuthentication/CreateSAMLLoginRequest?authenticationmethodid=1

1. Substitute the [FQDN] with the Fully Qualified Domain Name from your Qmlativ login URL. Example: https://esdemo2.skyward.com/Student,
   FQDN = esdemo2.skyward.com

2. Substitute the [EnvironmentName] with the Environment Name from your Qmlativ login URL. Example: https://esdemo2.skyward.com/Student
   Environment Name = Student

3. Add the link text after the Environment Name
   Link Text =
   STS/SSOAuthentication/CreateSAMLLoginRequest?authenticationmethodid=

4. The Authentication Method number starts with 1. If you create a second authentication method it would be number 2, and so forth.

   Login Link Examples:
   https://esdemo2.skyward.com/StudentSTS/SSOAuthentication/CreateSAMLLoginRequest?authenticationmethodid=1

   https://esdemo2.skyward.com/StudentSTS/SSOAuthentication/CreateSAMLLoginRequest?authenticationmethodid=2

   https://esdemo2.skyward.com/StudentSTS/SSOAuthentication/CreateSAMLLoginRequest?authenticationmethodid=3

Configure Common 3rd Party Identity Provider(s)

Configure Google as an Identity Provider

1. Create the SAML App for Skyward in the Google Admin Console

Configuration of your Google SAML App within Google Admin is the responsibility of the District, Skyward IT Services can help as a billable consulting service. If you are interested in billable consulting services please submit an IT Services Service Call using the Support Center (Customer Login Required) or contact Tom Kellnhauser.

The Google link describing the steps to create a custom SAML application in Google Admin Console is found here: https://support.google.com/a/answer/6087519?hl=en

See the next step for information needed when creating the custom SAML App in your Google Admin

2. Determine your Assertion Consumer Service and Entity ID URL(s) for the Google SAML App. To determine your SAML URL(s) follow these instructions:

   Substitute the [FQDN] with the Fully Qualified Domain Name from your Qmlativ login URL.

   Example: If my Qmlativ URL is: https://esdemo2.skyward.com/Student, then my FQDN is: esdemo2.skyward.com

   Substitute the [EnvironmentName] with the Environment Name from your Qmlativ login URL.

   Example: If my Qmlativ URL is: https://esdemo2.skyward.com/Student, then my Environment Name is: Student

   1. Determine the Assertion Consumer Service (ACS) URL using your FQDN & EnvironmentName:

   https://[FQDN]/[EnvironmentName]STS/SSOAuthentication/AuthenticateSAMLResponse

   2. Determine the Entity ID URL using your FQDN & EnvironmentName:

   https://[FQDN]/[EnvironmentName]STS

3. Configure the Skyward SAML App in the Google Admin Console

   - ACS URL: Enter your Skyward Assertion Consumer Service URL
   - Entity ID: Enter your Entity ID URL
   - Start URL: Leave Blank
   - Certificate: Leave Default Google Certificate listed
   - Signed Response: Enable (Checkbox checked)
   - **Name ID**[1]: Basic Information / Primary Email
   - Name ID Format: EMAIL
   - Attribute Mapping: No attribute mappings are required

   [1]The **Name ID** determines the data that the IdP is expecting in the NameID claim. A common config is to match the Primary Email, which requires both systems to have the same email address entered for your SSO users.

4. Below the Certificate name, click **Manage Certificates** → Click **Download IDP Metadata** → **S**ave as an**.xml** file → Open the .XML file in a text editor (Notepad). You will need to copy and paste this information when creating the Qmlativ Authentication Method.

   Note: If Google changes their Metadata information, it will break the SSO authentication with Skyward until the new Metadata XML is updated in the Qmlativ Authentication method.

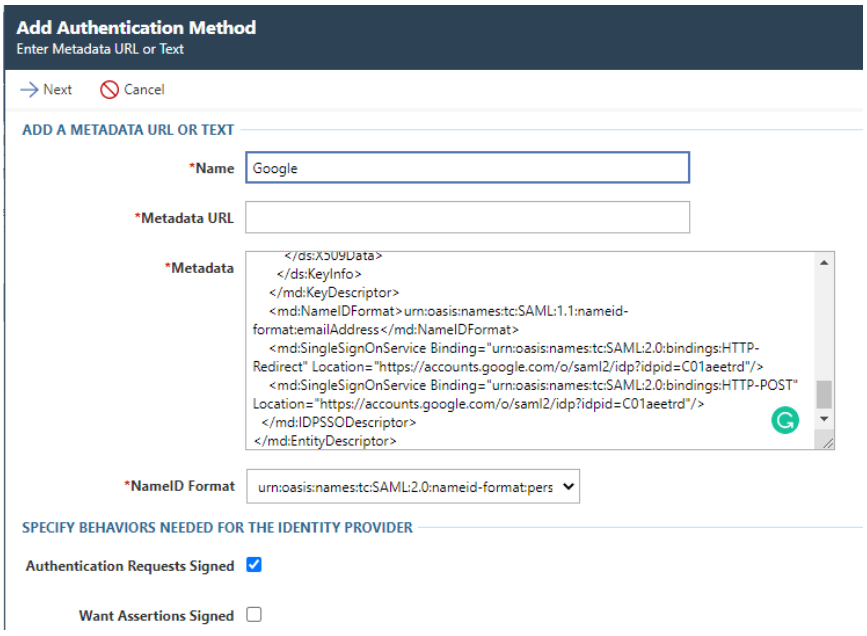
5. Next Step → Configure the Google Authentication Method Settings

Google Authentication Method Settings

1. **View Menu** --> Administrative Access -> Security -> Authentication Method (under Codes)

2. In the top browse, click the 'Add Authentication Method' and fill in the following information.
    1. Name: Enter a descriptive name, this name will be displayed to the users on the login screen
    2. Metadata URL: Leave blank, Google does not provide a Metadata URL.
    3. Metadata: Copy and Paste the Metadata XML from the Google Admin Console.
    4. NameID Format: Choose urn.oasis:names:tc:SAML:2.0:nameid-format:persistent
    5. Authentication Requests Signed (Y/N): Yes (checked)
    6. Want Assertion Requests Signed (Y/N): No (unchecked)
    7. Click Next

    Example Google Authentication Method



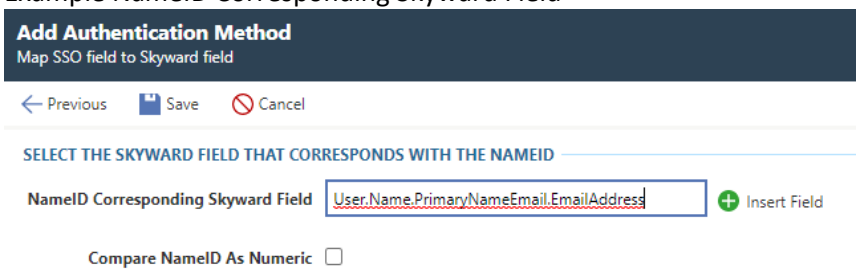
3. NameID Corresponding Skyward Field:

   The Name ID field you choose is important because it determines the NameID claim value (data) that Skyward uses for authentication. The most common Google configuration is to match the user's Email Address, which requires both systems to have the same Primary Email Address entered for your SSO users.

   1. If using the Primary Email field, then:
      1. Click Insert Field -> Browse to Name, Primary Name Email, choose Email Address -> Save
      2. Leave Compare NameID As Numeric blank -> Save

   2. If using Username field, then:
      1. -> Click Insert Field -> Choose Username -> Save
      2. Leave Compare NameID As Numeric blank -> Save

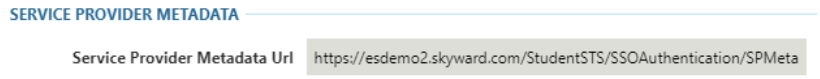
   Example NameID Corresponding Skyward Field



4. Click the blue arrow next to your new Authentication Method.

5. The Authentication Method screen allows you to modify the Authentication Method, and the Skyward Metadata URL for the Authentication Method can be copied from this screen.

   Example Skyward Metadata URL



6. Next Step: Configure Authentication Role(s)

Configure Azure / Office 365 as an Identity Provider

1. Create the SAML App for Skyward in the Azure Portal.

   Configuration of your SAML App within Azure Portal is the responsibility of the customer, Skyward IT Services can help as a billable consulting service. If you are interested in billable consulting services please submit an IT Services Service Call using the Support Center (Customer Login Required) or contact Tom Kellnhauser.

   The Microsoft link describing the steps to create a non-gallery SAML application in Azure Portal is found here: https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-single-sign-on-non-gallery-applications

2. Determine your SAML URL(s) for the Azure SAML App. To determine your SAML URL(s) follow these instructions:

   Substitute the [FQDN] with the Fully Qualified Domain Name from your Qmlativ login URL.

   Example: If my Qmlativ URL is: https://esdemo2.skyward.com/Student, then my FQDN is: esdemo2.skyward.com

   Substitute the [EnvironmentName] with the Environment Name from your Qmlativ login URL.

   Example: If my Qmlativ URL is: https://esdemo2.skyward.com/Student, then my Environment Name is: Student

   1. Determine the Entity ID using your FQDN & EnvironmentName, this is also your Sign-On URL.

      https://[FQDN]/[EnvironmentName]STS

   2. Determine both Assertion Consumer Service (ACS) Reply URL(s) using your FQDN & EnvironmentName:

      https://[FQDN]/[EnvironmentName]STS/SSOAuthentication/AuthenticateSAMLResponse
      https://[FQDN]/[EnvironmentName]STS/SSOAuthentication/AuthenticateMobileSAMLResponse

3. Configure the Skyward SAML App in the Azure Portal using the following Identity Provider settings.

   - **Basic SAML Configuration**
     - Entity ID: Enter your Entity ID URL
     - Reply URL (ACS URL): Enter both of your ACS Reply URL(s)
     - Sign-On URL: Enter your Sign-On URL (same as the Entity ID URL)
     - Relay State: Optional - Leave Blank
     - Logout URL: Leave the Default

   - **Configure User Attributes & Claims**
     - [1]Name: Email Address or Login Name
     - Unique User Identifier: Claim examples: Email Address, Login Name, onpremisesaccountname (matches your local Active Directory login name)
     - Choose Name Identifier format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistant

     [1]The **Name ID** determines the data that the IdP is expecting in the NameID claim. A common config is to match the Email Address, which requires both systems to have the same email address entered for your SSO users.

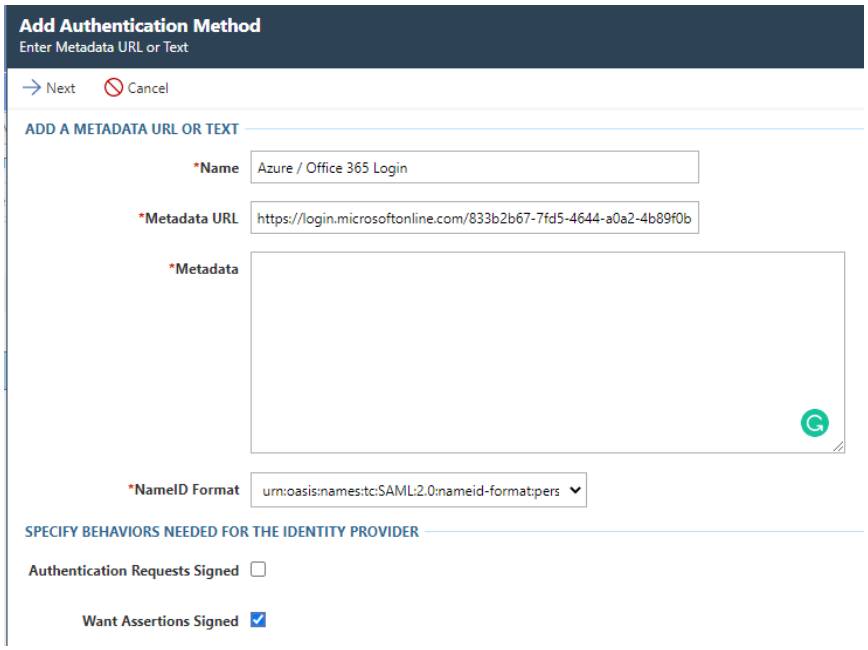
4. Next Step -> Configure the Azure / Office 365 Authentication Method Settings

Azure / Office 365 Authentication Method Settings

1. **View Menu** -> Administrative Access -> Security -> Authentication Method (under Codes)

2. In the top browse, click the 'Add Authentication Method' and fill in the following information.
    1. Name: Enter a descriptive name, this name will be displayed to the users on the login screen
    2. Metadata URL: Enter your Azure / Office 365 Metadata URL.
    3. Metadata: Leave Blank (Metadata URL preferred)
    4. NameID Format: Choose urn.oasis:names:tc:SAML:2.0:nameid-format:persistent
    5. Authentication Requests Signed (Y/N): No (unchecked)
    6. Want Assertion Requests Signed (Y/N): Yes (checked)
    7. Click Next

    Example Azure Authentication Method



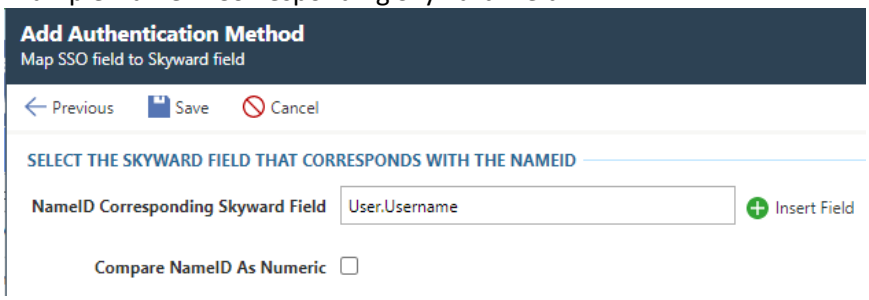
3. NameID Corresponding Skyward Field:

   The Name ID field you choose is important because it determines the NameID claim value (data) that Skyward uses for authentication. The most common Google configuration is to match the user's Email Address, which requires both systems to have the same Primary Email Address entered for your SSO users.

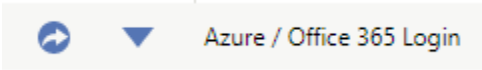
   1. If using the Primary Email field, then:
      1. Click Insert Field -> Browse to Name, Primary Name Email, choose Email Address -> Save
      2. Leave Compare NameID As Numeric blank -> Save

   2. If using Username field, then:
      1. -> Click Insert Field -> Choose Username -> Save
      2. Leave Compare NameID As Numeric blank -> Save

   Example NameID Corresponding Skyward Field

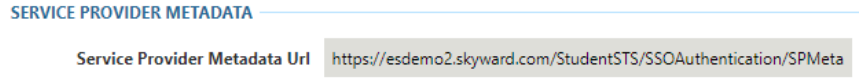


4. Click the blue arrow next to your new Authentication Method.



5. The Authentication Method screen allows you to modify the Authentication Method, and the Skyward Metadata URL for the Authentication Method can be copied from this screen.

   Example Skyward Metadata URL



6. Next Step: Configure Authentication Role(s)

Additional Information

Qmlativ Metadata URL

The Identity Provider may request the Metadata URL when creating a custom SAML App in a 3rd party portal.

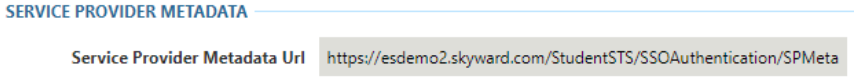
To locate the Skyward Service Provider Metadata URL follow these steps.

1. **View Menu** -> Administrative Access -> Security -> Authentication Method (under Codes)

2. Click the blue arrow next to your Authentication Method.

3. The Authentication Method has Metadata URL for the Authentication Method, it can be copied from this screen.

   Example Skyward Metadata URL



If the 3rd party does utilize a Metadata URL, you can use this information to determine the relevant Skyward Service Provider SSO URL(s)

Step 1: Substitute the [FQDN] section of the URL with the Fully Qualified Domain Name from your Qmlativ login URL. In the example URL: https://esdemo2.skyward.com/Student, the FQDN is equal to esdemo2.skyward.com.

Step 2: Substitute the [EnvironmentName] section of the URL with the Environment Name from your Qmlativ login URL. In the example URL https://esdemo2.skyward.com/Student, the Environment Name is equal to Student

Step 3: Identify your Entity ID, ACS, and Sign-On URL(s)

- Qmlativ Entity ID
  Example: https://[FQDN]/[EnvironmentName]STS

- Qmlativ Assertion Consumer Service Reply URL(s)
  https://[FQDN]/[EnvironmentName]STS/SSOAuthentication/AuthenticateSAMLResponse
  https://[FQDN]/[EnvironmentName]STS/SSOAuthentication/AuthenticateMobileSAMLResponse

- Qmlativ Sign-On URL:
  Example: https://[FQDN]/[EnvironmentName]STS

Troubleshooting Identity Provider Configuration(s)

The best way to diagnose configuration issues is to get a SAML Trace of the failure. To gather a SAML Trace using your Web Browser you can follow these steps.

1. Install a SAML trace extension in your web browser: The most useful information can be captured using a SAML trace extension added to your Web Browser, I use the SAML Chrome panel or the SAML-tracer for Chrome. There are other available if you have a preference or use a different web browser.
2. Hit F12 to display the developer tools in your browser, this will also allow you to see your SAML trace extension.
3. In the developer tools panel, locate the SAML tab extension you installed (example screenshot below).
4. Reproduce the SSO login issue before receiving an error message.
5. Locate the SAML in the SAML extension, select all and, copy the entire contents of each SAML entry to a text file(s). Repeat for each SAML entry.
6. Create an IT Services Service Call using Help Center and send the SAML trace text file(s) to Skyward. The SAML Trace will typically help us find the problem.

Chrome Browser SAML Chrome Panel example: