Single Sign On Options

2019 User Group Conference
Agenda

• What is LDAP?
• What is SSO?
• SMS 2.0: LDAP Setup
• SMS 2.0: SSO Setup
• SMS 2.0: User Management
• Qmativ: LDAP Setup
• Qmativ: SSO Setup
• Qmativ: User Management
• Qmlativ: LDAP Setup
• Qmlativ: SSO Setup
• Qmlativ: User Management
What is LDAP?

LDAP (Lightweight Directory Access Protocol) 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 Novell’s eDirectory.

Skyward usernames match the Directory usernames.

Example: If the network login name is “jdoe” then the Skyward login name must also be “jdoe”.
Secure LDAP Protocols

Three secure LDAP Protocols are supported to ensure all usernames and passwords that are transmitted are encrypted and protected from hackers. LDAP requests are sent from the Web Servers to the LDAP Servers. For SMS 2.0 PaC users, LDAP requests are sent from the PaC Client to the LDAP Servers.

When using LDAPS or LDAP w/TLS the LDAP Server’s Certificate will need to be installed on the Web Servers and/or PaC Clients. Cloud hosted customers should send the SSL certificate to the hosting provider.

Secure Protocols include:
- LDAPS
- LDAP w/TLS
- Kerberos
What is Single Sign On?

**Single Sign On (SSO)** allows users to login to multiple related, yet independent, software systems using the same login and password.

Unlike LDAP, the property (or properties) used to match the login between systems can be selected as part of the SSO configuration.
SMS 2.0: LDAP Setup

Start Here ➔ SMS 2.0 SSO / LDAP Launch Kit
SMS 2.0: Add and Test Your LDAP Server(s)

Product Setup > Skyward Contact Access > Configuration > Single Sign-On Configuration
Enabling the **LDAP Groups** feature allows you to integrate the LDAP directory groups for Skyward user security. Users’ group memberships are read transparently from the LDAP directory during the user’s login process allowing you to manage group memberships exclusively from your LDAP Directory. Setup is required in the Skyward product to identify the LDAP groups that should be associated with the Skyward Security Groups.

LDAP Groups supports Active Directory Nested Groups.

In order to allow the use of Nested Groups the Member Filter needs to be updated to the following:
```
(&(objectClass=user)(MemberOf=1.2.840.113556.1.4.1941=%s))
```

If not using Nested Groups the Member Filter should be set to the following:
```
(&(objectClass=user)(MemberOf=%s))
```
SMS 2.0: Secure Token Service

• **SkySTS (Skyward Secure Token Service)** allows SMS 2.0 users to authenticate to a 3rd party **Identity Provider (IdP)**, and it allows SMS 2.0 to be an **Identity Provider (IdP)** for 3rd party systems.

• **SMS 2.0 to a remote IdP:** This means the SMS 2.0 users can log in using credentials from a 3rd party IdP, such as Office 365 (Azure) or ClassLink, using SAML 2.

• **SMS 2.0 as an IdP:** This means that users of the 3rd party system can login into the 3rd party system using their SMS 2.0 user/password using SAML 1, 2, or wsFed.

• In all scenarios the customer is responsible for configuring 3rd Relying Parties in SMS 2.0
SMS 2.0: Secure Token Service Setup

Start Here ➔ SMS 2.0 SkySTS Launch Kit
SMS 2.0: User Management

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

Many customers looking to implement LDAP or SSO face this challenge.

Good News! We have built several tools to help you!

• Automatically Generate Logins and Passwords
• User Import Tools
SMS 2.0: Username/Password Configuration Options

Product Setup > Skyward Contact Access > Security > Setup > Configuration
SMS 2.0: Employee/Secured Configuration Options

Product Setup > Skyward Contact Access > Security > Setup > Configuration > Employees/Secured Users
SMS 2.0: Students Configuration Options

Product Setup > Skyward Contact Access > Security > Setup > Configuration > Students
SMS 2.0: Guardians Configuration Options

Product Setup > Skyward Contact Access > Security > Setup > Configuration > Guardians
SMS 2.0: Mass Generate Employee/Secure Account Information

Product Setup > Skyward Contact Access > Security > Setup > Utilities > Mass Generate Account Information
SMS 2.0: Mass Generate Student Account Information

Student Management > Student Access > Setup > Utilities > Mass Generate Student Permissions/Passwords
SMS 2.0: Mass Generate Family Account Information

Student Management > Family Access > Setup > Utilities > Mass Generate Family Permissions/Passwords
SMS 2.0: Student Import Utility

Student Management > Student Access > Setup > Utilities > Mass Generate Student Permissions/Passwords
SMS 2.0: Staff Import

Student Management > Administration > SkyBuild > Staff Import Utility
Qmlativ: LDAP Setup

Start Here ➔ Qmlativ SSO / LDAP Launch Kit
Qmlativ: Configure User Authentication Override Codes

View Menu > Administrative Access > Security > User
Qmlativ: Add LDAP Providers

View Menu > Administrative Access > Security > LDAP Provider (under Features > Add LDAP Provider)
Qmlativ: Test LDAP Providers

View Menu > Administrative Access > Security > LDAP Provider (under Features > Run LDAP Provider Test
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.
Qmlativ: SSO Setup

Start Here ➔ Qmlativ SSO / LDAP Launch Kit
Qmlativ: Single Sign On

SSO (Single Sign On) relies on a 3rd party Identity Provider (IdP) to authenticate Qmlativ users by means of security tokens provided by SAML.

Mobile App SSO support is also available.

Active Directory Federated Services Identity Provider Support is planned for 2019.
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.

• Configure Username Structure
• User Import
Qmlativ: Configure Username Structure for Students

View Menu → Administrative Access → Student → System Configuration (Under Settings) → Security
User Creation

![Username Creation Interface]

- **Auto Generate Security User Type**: Required and Editable
- **Allow Student Access**: Not selected
- **Example Student**: Not specified

![Username Structure Interface]

- **Search Rank**: View Skyward Default
- **Rank**: N - Student Number
- **Part Type**: L - Leading Characters

- **Character Number Limit**: Not specified
- **Character Type Limit**: Not specified
- **Text**: Not specified
- **Group Truncation Order**: Not specified
- **Character Limit Group**: Not specified
- **Character Limit Group Max Length**: Not specified
Qmlativ: Configure Username Structure for Guardians

View Menu → Administrative Access → Family → System Configuration (Under Settings) → Security User Creation
Qmlativ: Configure Username Structure for Staff

View Menu → Administrative Access → Staff → System Configuration (Under Settings) → Security User Creation

### USERNAME CREATION

**Auto Generate Security User Type**
- R - Required on Staff Add

**Staff**
- Armstrong
- Jason

**USERNAME STRUCTURE**

<table>
<thead>
<tr>
<th>Rank</th>
<th>Part Type</th>
<th>Character Number Limit</th>
<th>Character Type Limit</th>
<th>Text</th>
<th>Group Truncation Order</th>
<th>Character Limit Group</th>
<th>Character Limit Group Max Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>K - Name Key</td>
<td>12</td>
<td>T - Trailing Characters</td>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Qmlativ: Configure Username Structure for Employees

View Menu → Administrative Access → Employee → System Configuration (Under Settings) → Security User Creation
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 security 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 would use this import.
Qmlativ: User 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.
Thank you for attending!