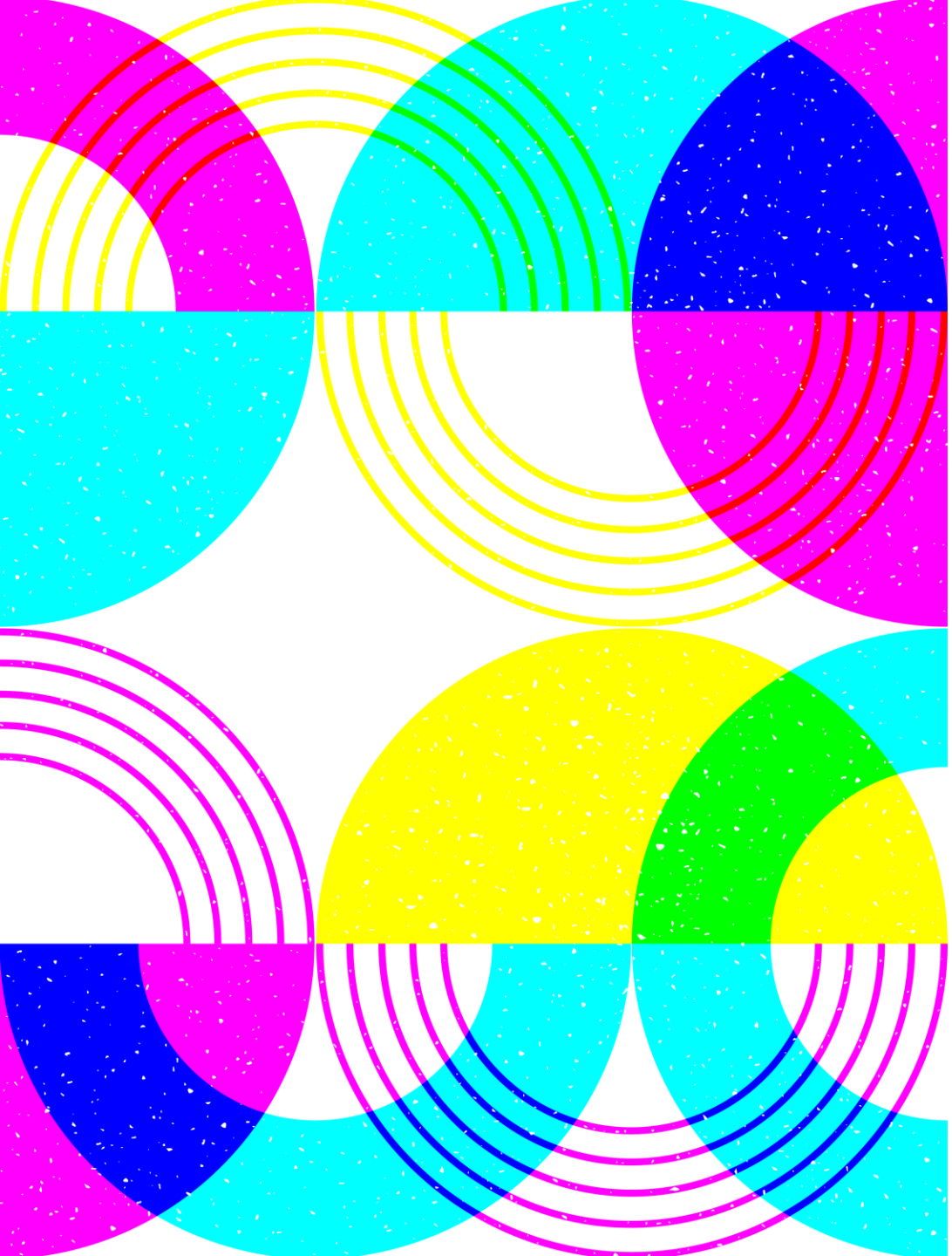


follow us on social!

#skyicon



SKYWARD®

iCON

Implementing SSO & MFA in Qmlativ and SMS 2.0

Mike Bianco – VP of Information Security

Agenda

- Multi Factor Authentication
- Single Sign On
- Skyward using an Identity Provider
- Skyward as an Identity Provider
- Skyward User Management Tools

Multi Factor Authentication

- What is Multi-Factor Authentication?
- Why use Multi-Factor Authentication?
- Verification Methods
- Authenticator Apps
- Experiences with MFA

Multi Factor Authentication

What is Multi Factor Authentication?

Multi-Factor Authentication (**MFA**) is a security system that verifies a user's identity by requiring multiple credentials. Another commonly used term is **2 Factor Authentication** (**2FA**).



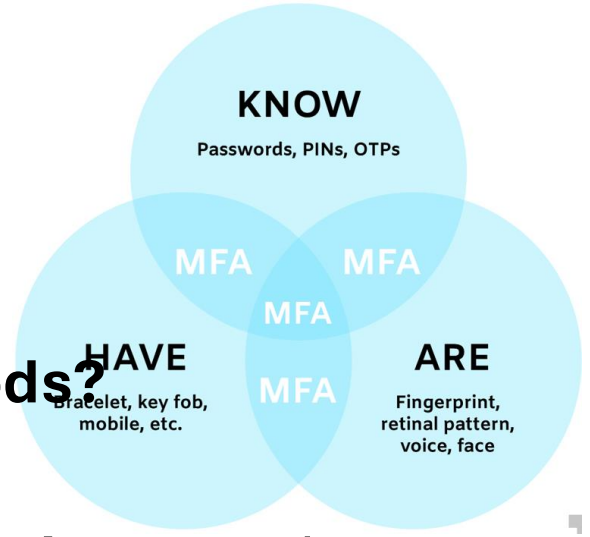
Multi Factor Authentication

Why use Multi Factor Authentication?

While not entirely fool proof, **security experts** agree **Multi-factor authentication has evolved as the single most effective control to protect an organization against remote attacks** and when implemented correctly, can prevent most threat actors from easily gaining an initial foothold into your organization, even if credentials become compromised.



Multi Factor Authentication



What are Multi Factor Authentication Verification Methods?

The most common verification methods are **something you know** and **something you have** along with **who/what you are.**

*Something that you already **know***. The most common method is a *password*. Other examples include PINs, answers to security questions, and one-time passwords (OTP).

*Something that you physically **have***. This category may include fobs, key cards, smartphones, or USB devices.

*Who or what you **are***. This category involves anything that is a unique identifier of your physical being (e.g., biometrics).

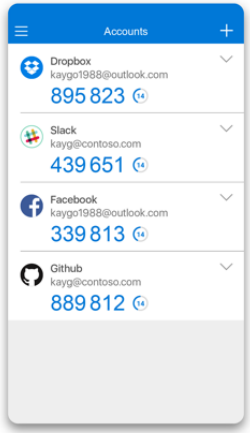
Authenticator Apps

An **Authenticator App** generates a passcode every 30 seconds. The passcode can be used as a login factor for accessing an account. An **Authenticator App** can be installed on a smartphone, Windows, Mac, or ChromeOS device.

Any service that supports the standard **one-time password (OTP)** 2FA approach will work with all the apps below, including most mainstream websites and services.

Common Authenticator Apps

- Google Authenticator
- LastPass Authenticator
- Microsoft Authenticator



Our Experiences Implementing MFA



Ensure you have your leadership on board.

Rollout by groups; start with a pilot group to ensure success. After that prioritize the groups by the **Highest Risk** employees (those that work with the most sensitive data / financials)

Be aware that MFA issues can cross boundaries into the Human Resources realm; employees may not want to use a personal cell phone.

Be prepared with Alternative MFA options: Phone Call w/Audio Code, Email, OTP Device (Key Fob)

What challenges has your district experienced rolling out MFA?

Single Sign On

What is Single Sign On?

- Single Sign On allows Skyward users to **authenticate** into Skyward using a username and password from a 3rd party **Identity Provider**.
- Common examples of Identity Providers are Google, Microsoft Entra ID (Azure), ClassLink, Clever, DUO, etc.
- SSO works with your Identity Providers' **Multi Factor Authentication**
- SMS 2.0 SSO uses the **SAML 2.0 protocol**

SMS 2.0

- Multi Factor Authentication (MFA)
- SMS 2.0 using an Identity Provider
- SMS 2.0 as an Identity Provider
- User Management Tools

SMS 2.0 Native MFA

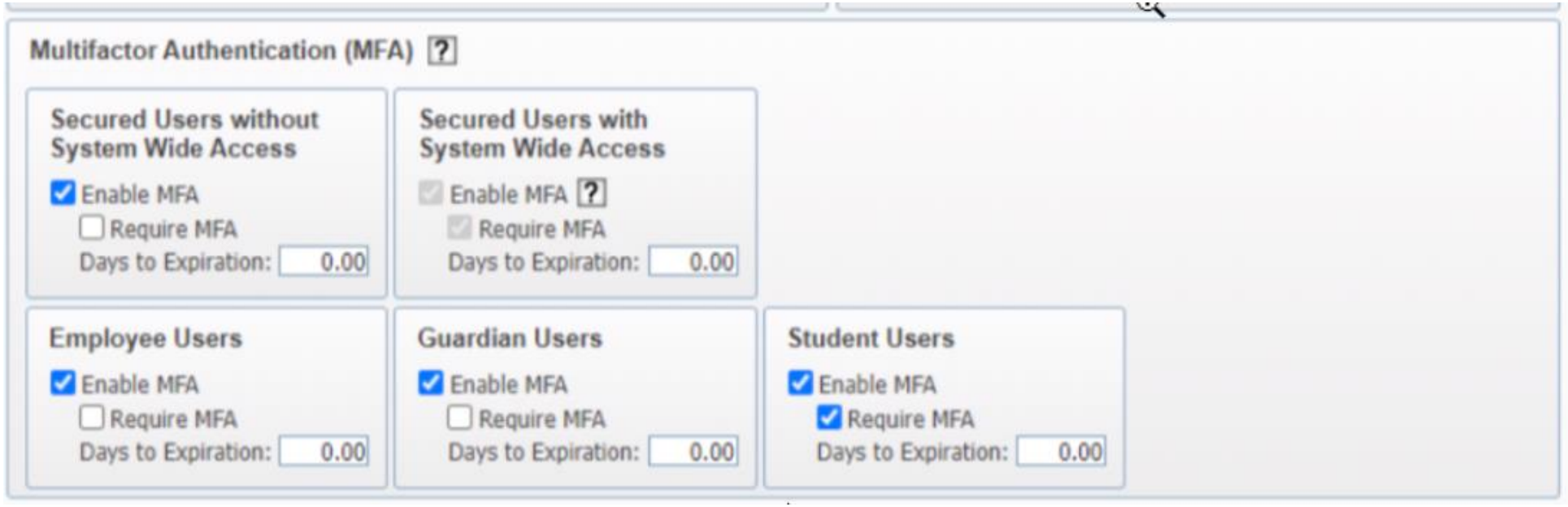


Mandatory MFA
All System Wide Users
Business & Human Resources Users:
- Web Human Resources & Setup Security Groups
- Web Financial Management & Setup Security Groups

Note: SSO logins do not require Native MFA

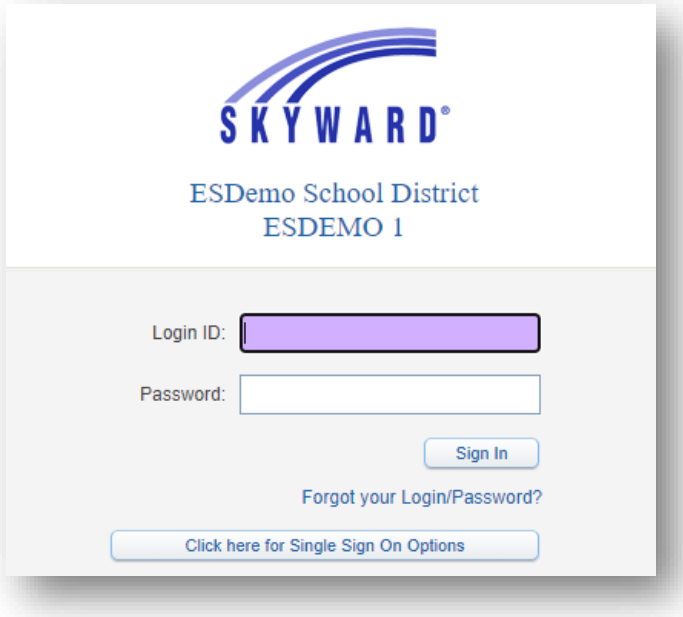
MFA Available (District Decision)
Employee Access, Guardians, Teachers, and Students

SMS 2.0 Native MFA



SMS 2.0 Native MFA Launch Kit:
https://support.skyward.com/DeptDocs/Corporate/IT%20Services/Public%20Website/Technical%20Information/administration/SMS%202.0%20Native%20MFA%20Launch%20Kit.pdf

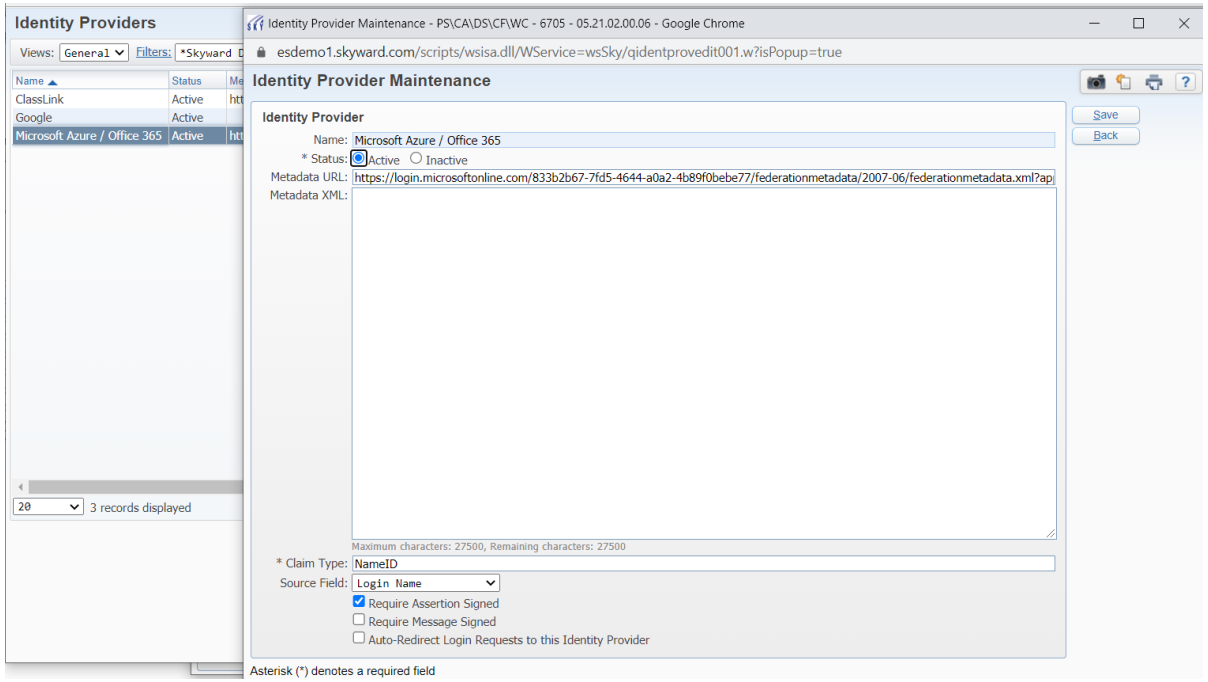
SMS 2.0 MFA with SSO



SMS 2.0 supports MFA using 3rd party Identity Providers. These include popular IdP's like Google® Apps, Microsoft® Entra ID (Azure) / Office 365, ClassLink, Duo, and many more.

SMS 2.0 using an Identity Provider

1. SMS 2.0: Install SkySTS
2. SMS 2.0: Create Identity Provider
3. 3rd Party: Create SAML App
4. Test



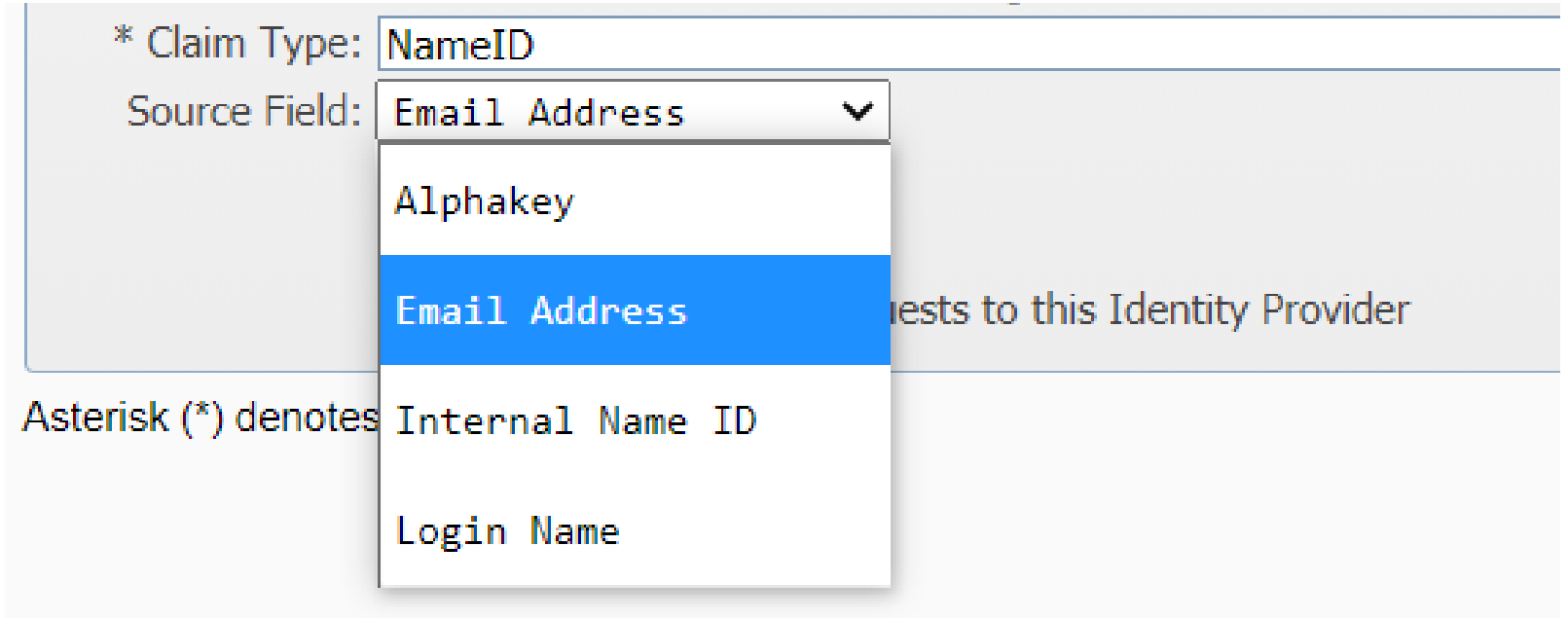
Menu Path:

Product Setup -> Skyward Contact Access -> District Setup -> Configuration -> Web Configuration -> Identity Provider Configuration

What is the NameID Claim?

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

Choose Source field:



SMS 2.0 as an Identity Provider

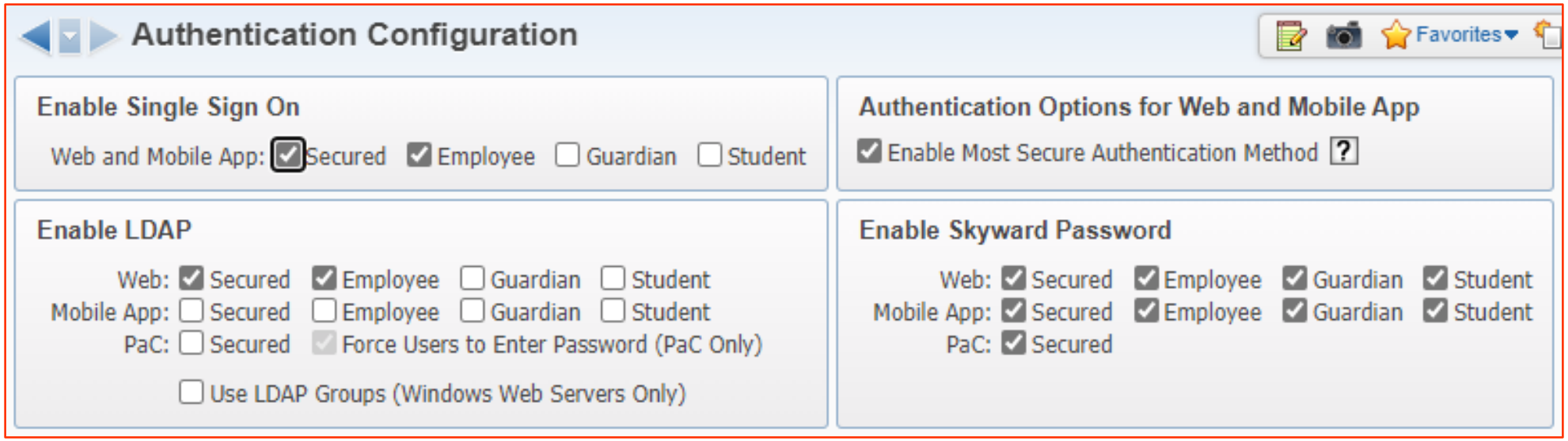
SMS 2.0 can also be the Identity Provider for 3rd Parties.

Links can be created in SMS 2.0 that provide a seamless login to the 3rd Party product.

Useful for 3rd Party products that require Parent logins.

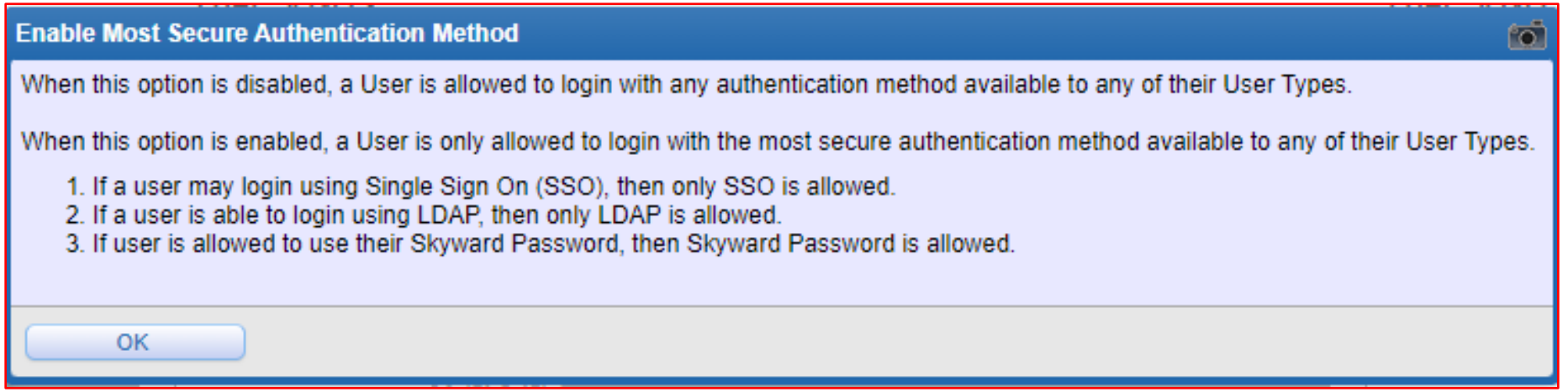
Examples: Registration Gateway (SRC Solutions), School Pay, MiLearn (Michigan), etc.

Enhanced Single Sign-On Configuration

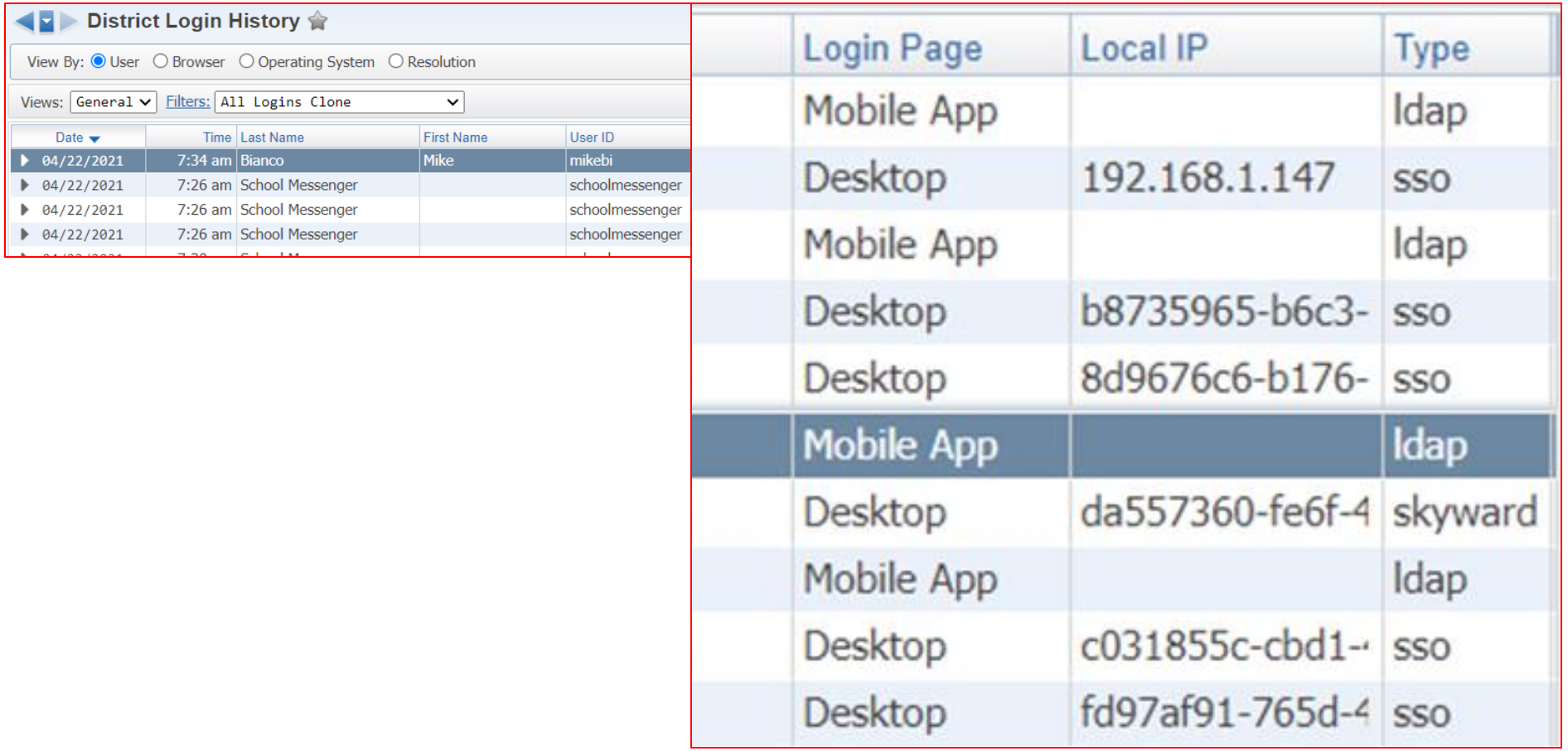


Enhanced Single Sign-On Configuration

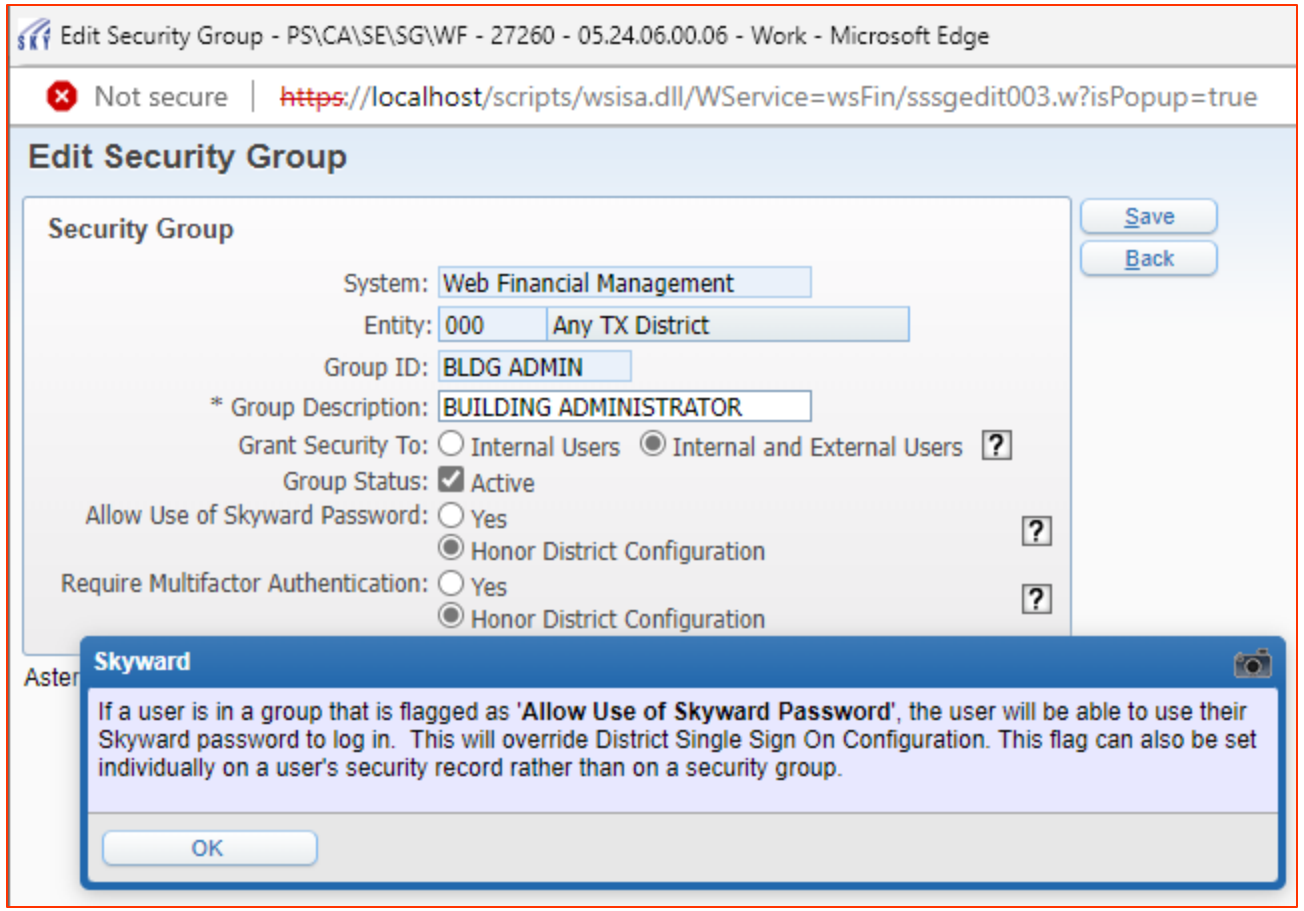




District Login History Enhancements

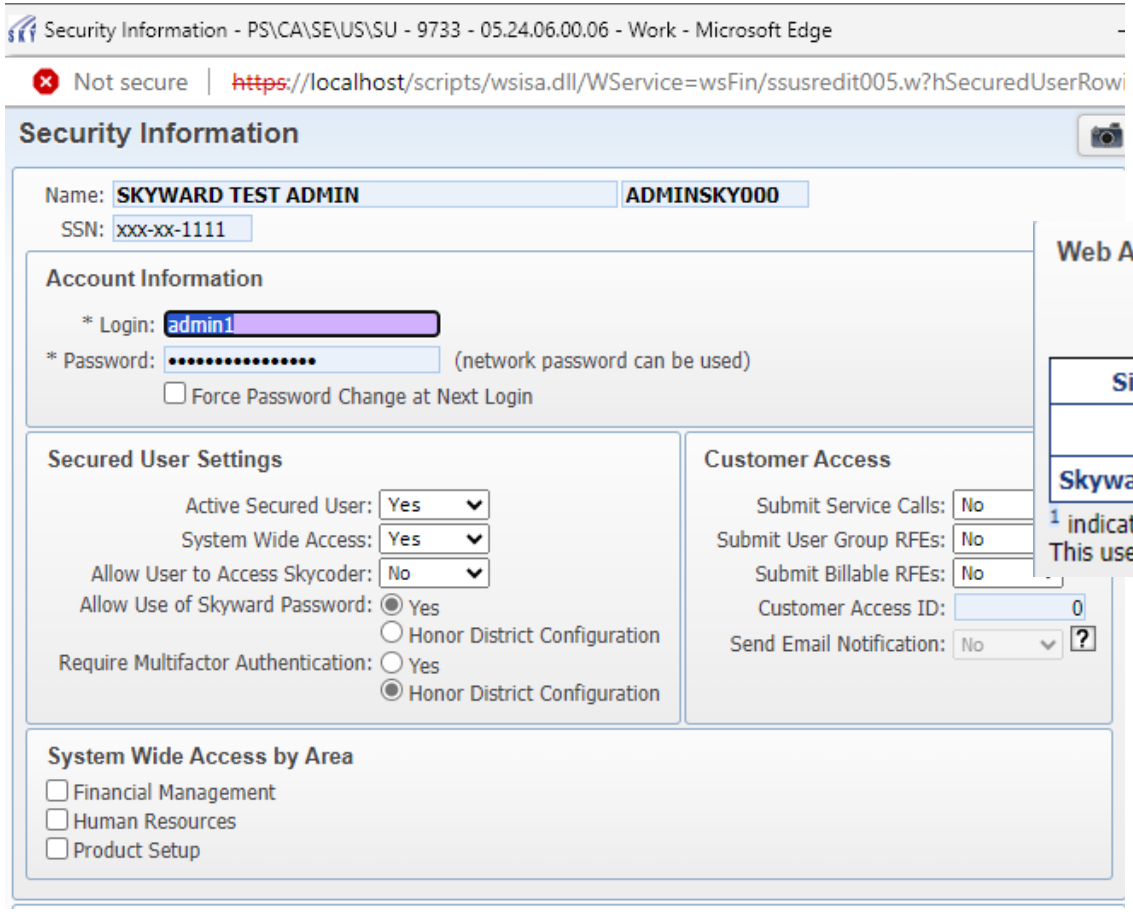


Single Sign-On Enhancements



Security Groups

Single Sign-On Enhancements



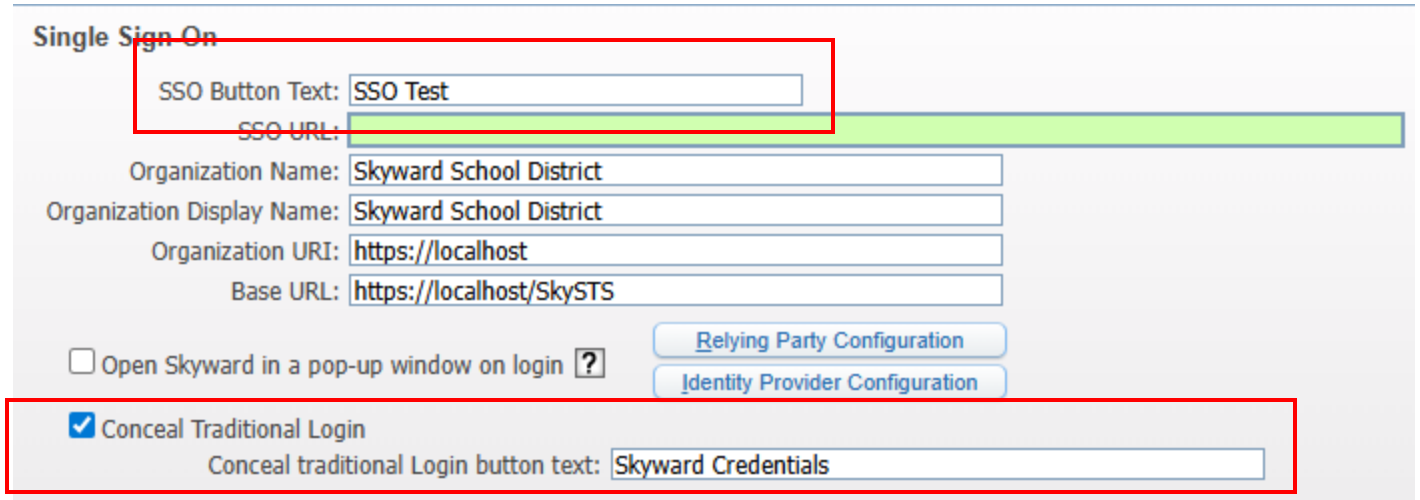
Web Authentication Methods

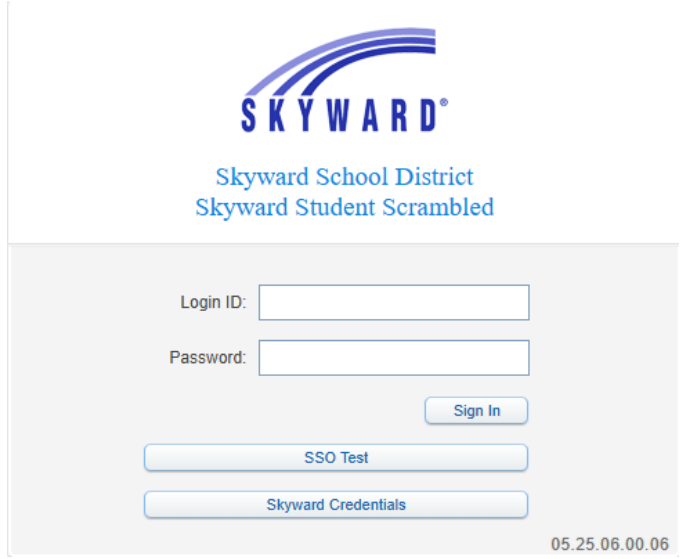
	Secured User Active w/ Security	Employee User Active
Single Sign On Allowed	Yes	Yes
LDAP Allowed	Yes[1]	Yes[1]
Skyward Password Allowed	Yes	Yes

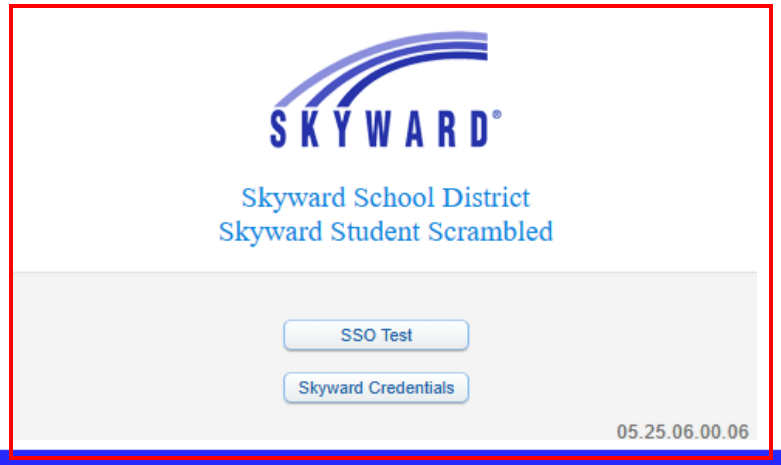
[1] indicates user must use a more secure authentication method.
This user may use their Skyward Password because of a User Override.

Users

Single Sign-On Enhancements

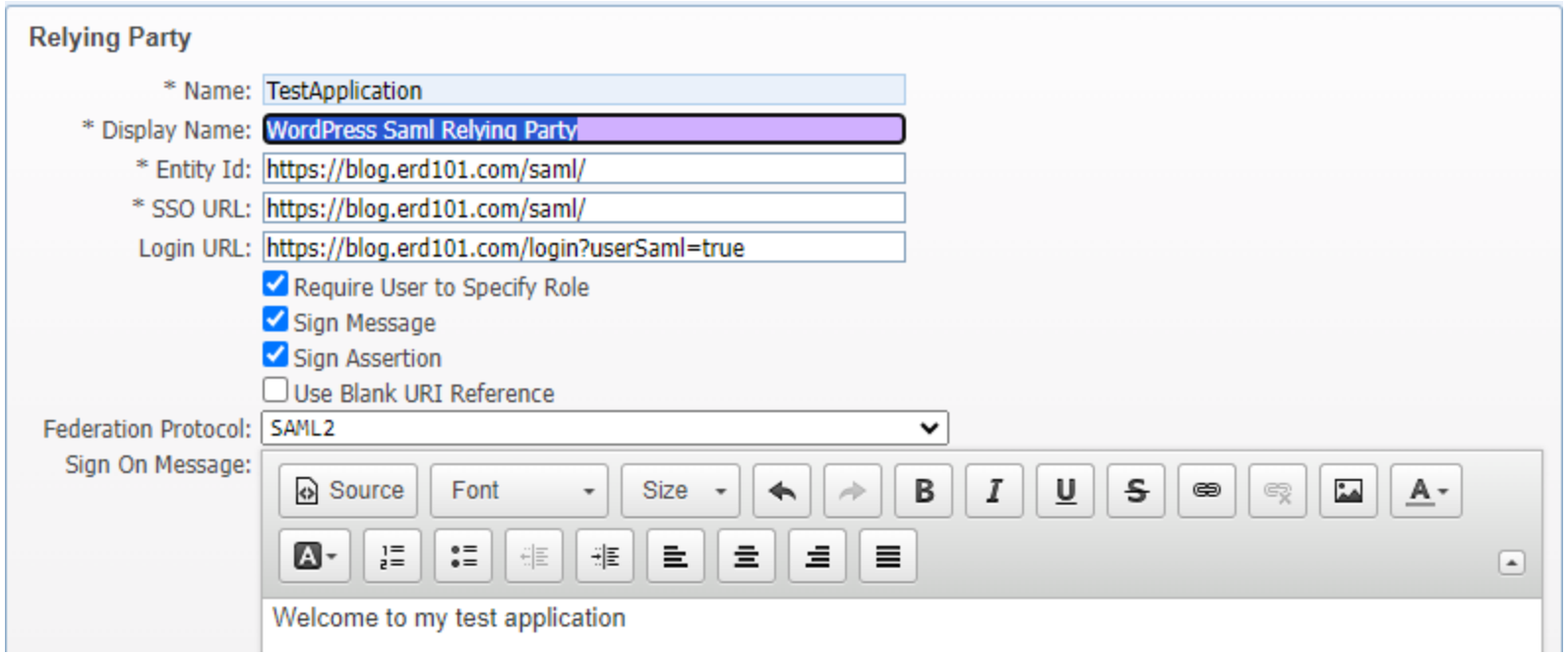






Logon Page

SMS 2.0 as an Identity Provider





SMS 2.0 User Management Tools

SMS 2.0 has several tools that assist you with User Management.

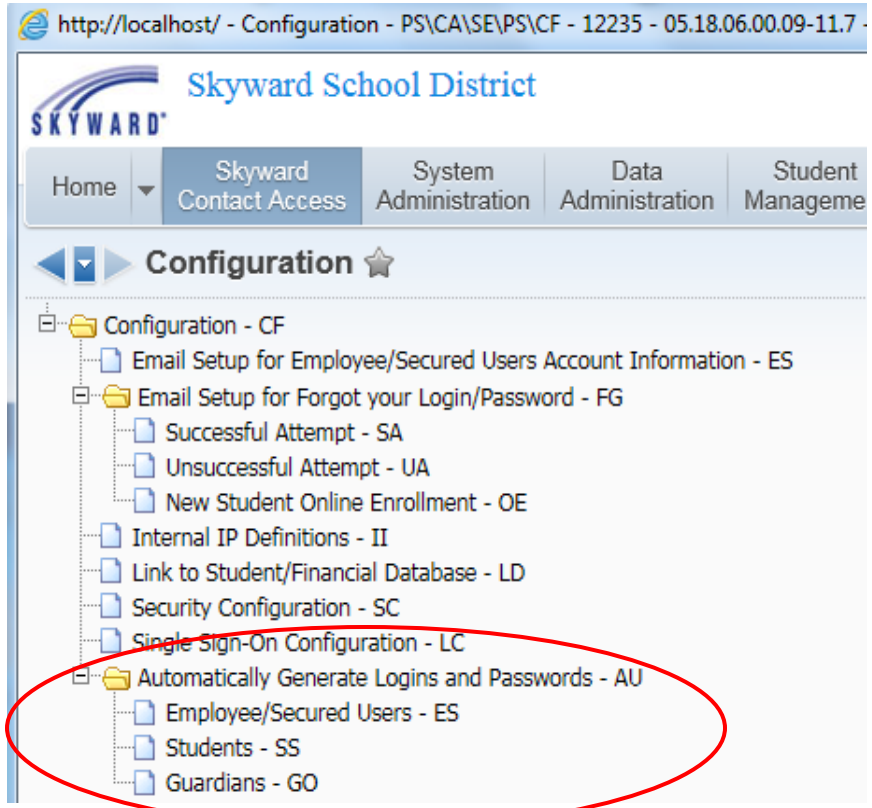
The following tutorials have the details on how to mass change the SMS 2.0 logins or email addresses.

How do I set up Students Auto Username Generation?
https://support.skyward.com/DeptDocs/Corporate/Documentation/Public%20Website/Tutorials/FQ/PS_CA_SE_PS_CF_1062348_100_T.pdf

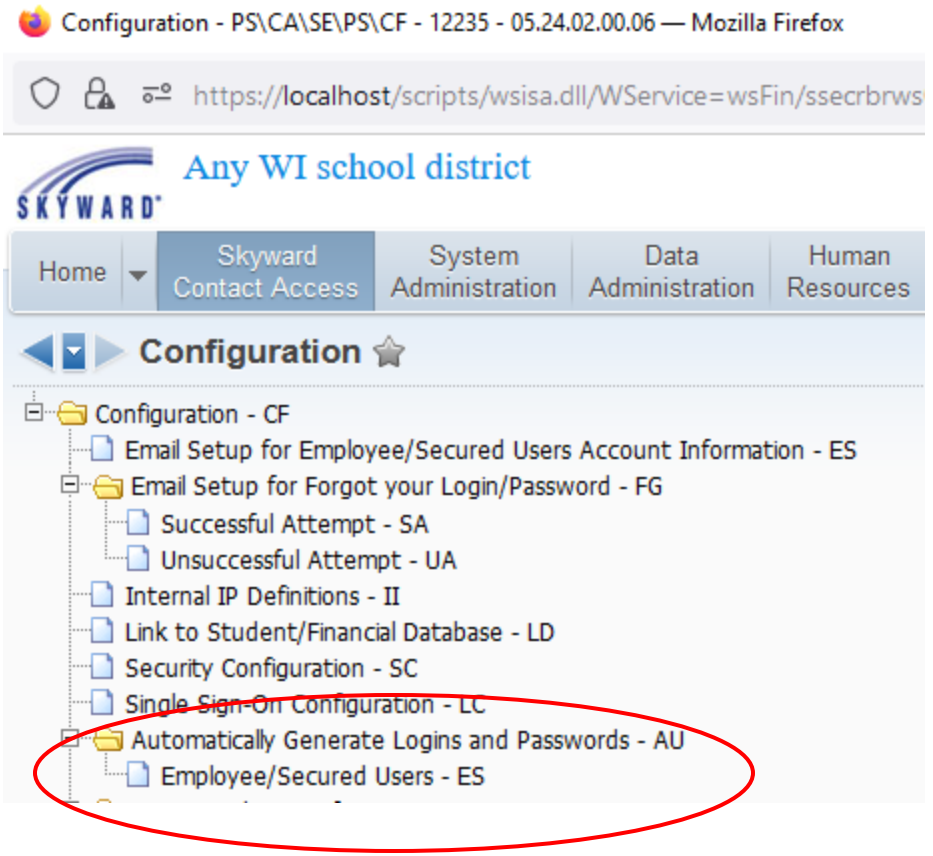
How do I set up Employees/Secured Users Auto Username Generation?
https://support.skyward.com/DeptDocs/Corporate/Documentation/Public%20Website/Tutorials/FQ/PS_CA_SE_PS_CF_AU_ES_1112165_100_T.pdf

Username/Password Configuration

Student

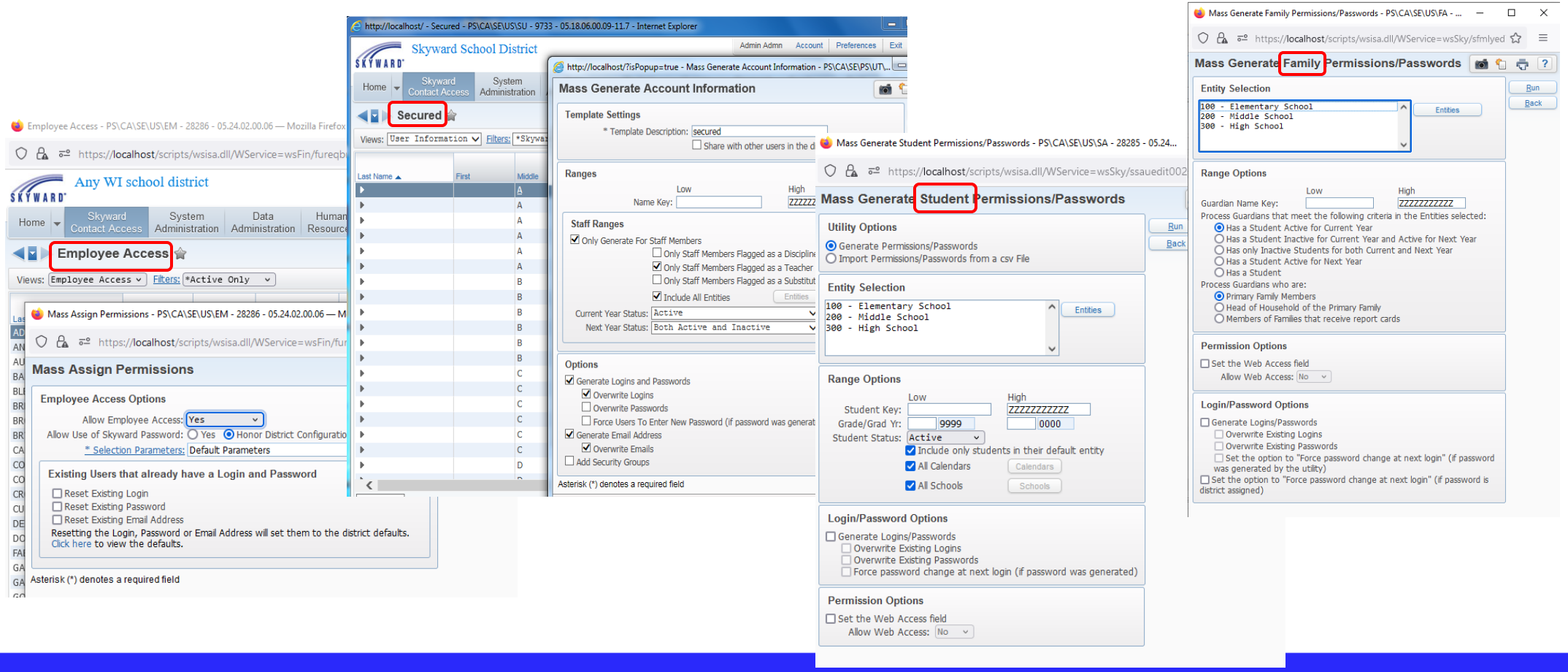


Business



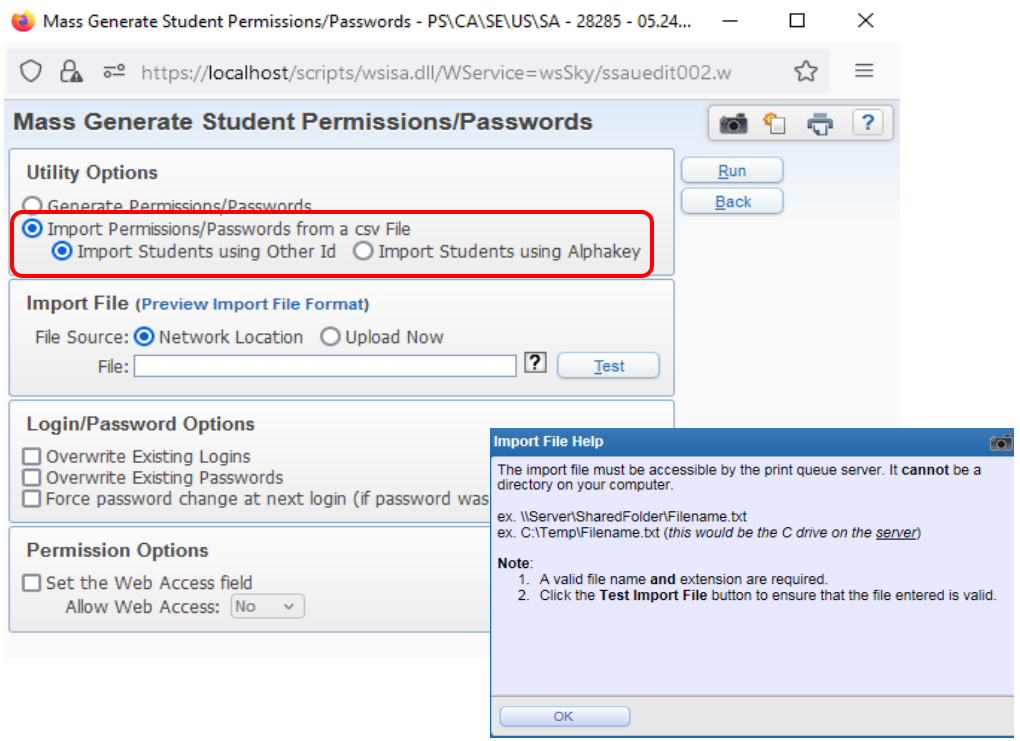
Mass Assign Permissions

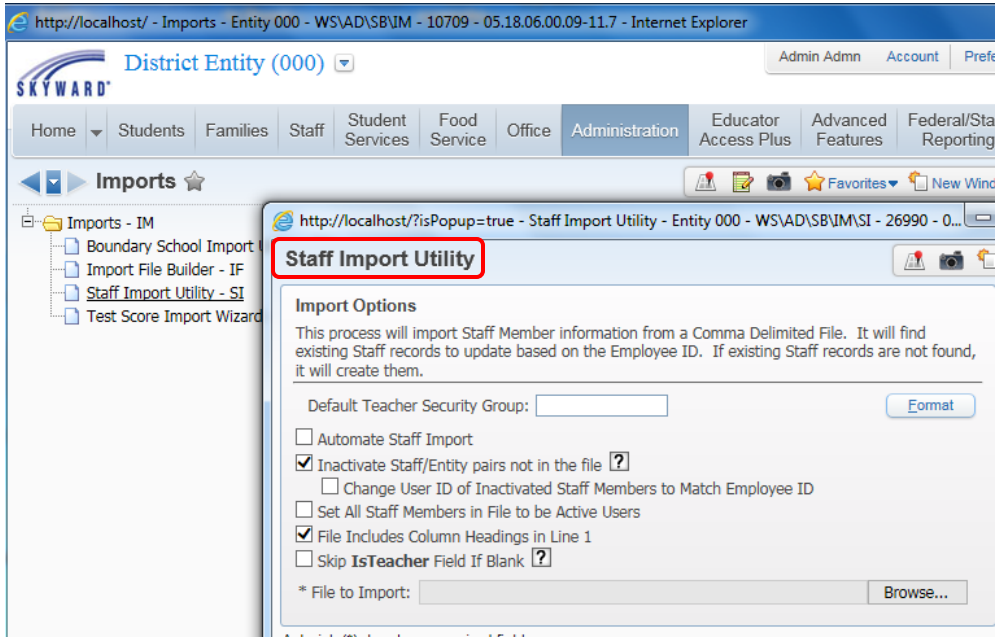
Employees/Secured/Students/Guardians Users



Students / Staff

Import

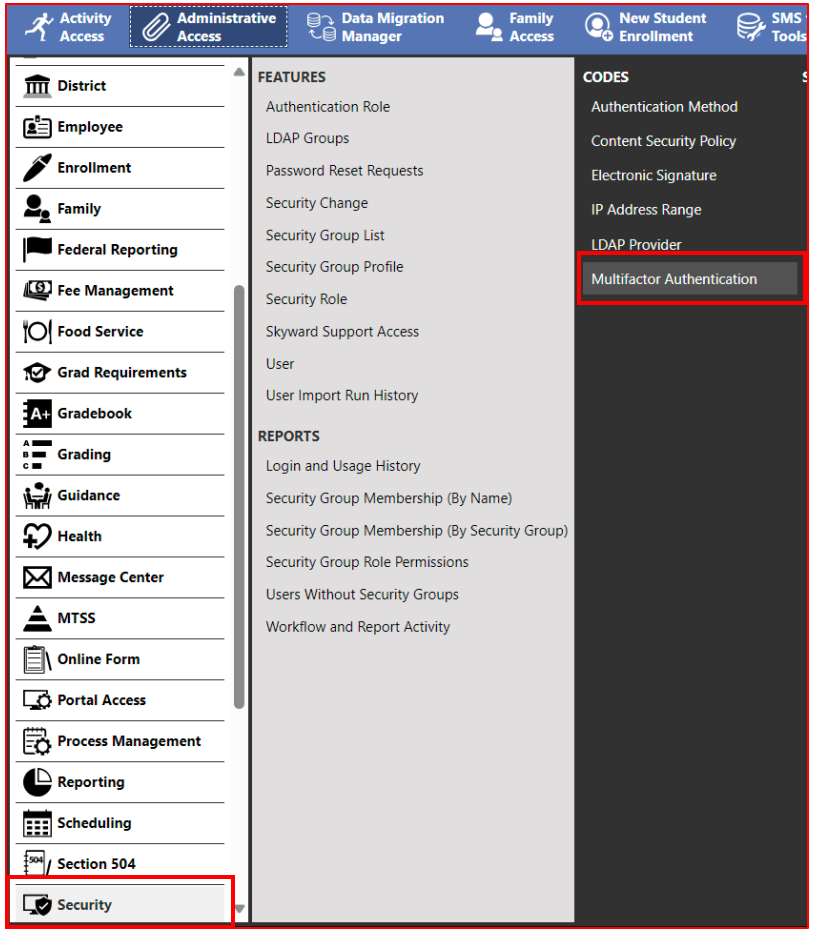




Qmlativ

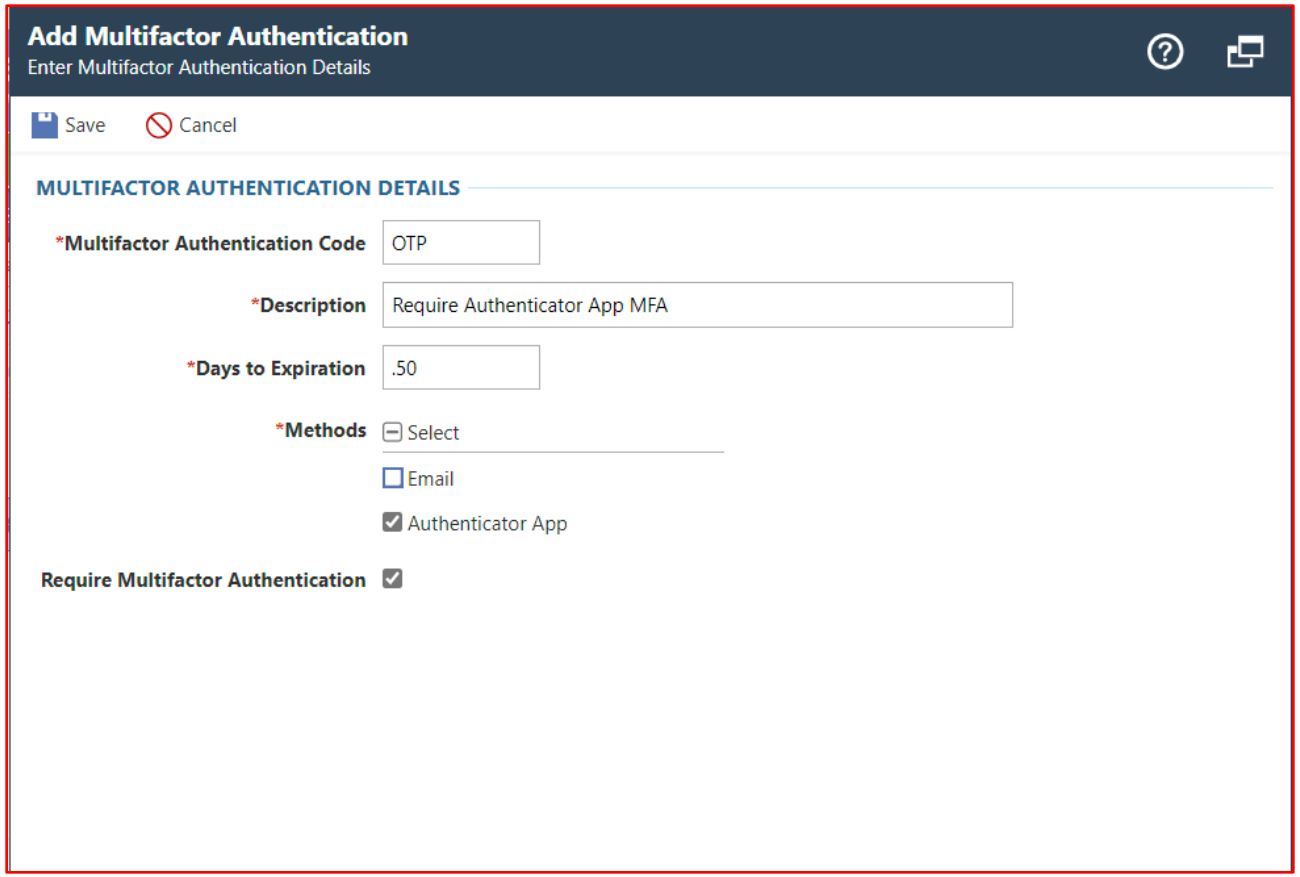
- Multi Factor Authentication (MFA)
- Qmlativ using an Identity Provider (SSO)
- Qmlativ as an Identity Provider
- User Management Tools

Qmlativ Native Multi Factor Authentication



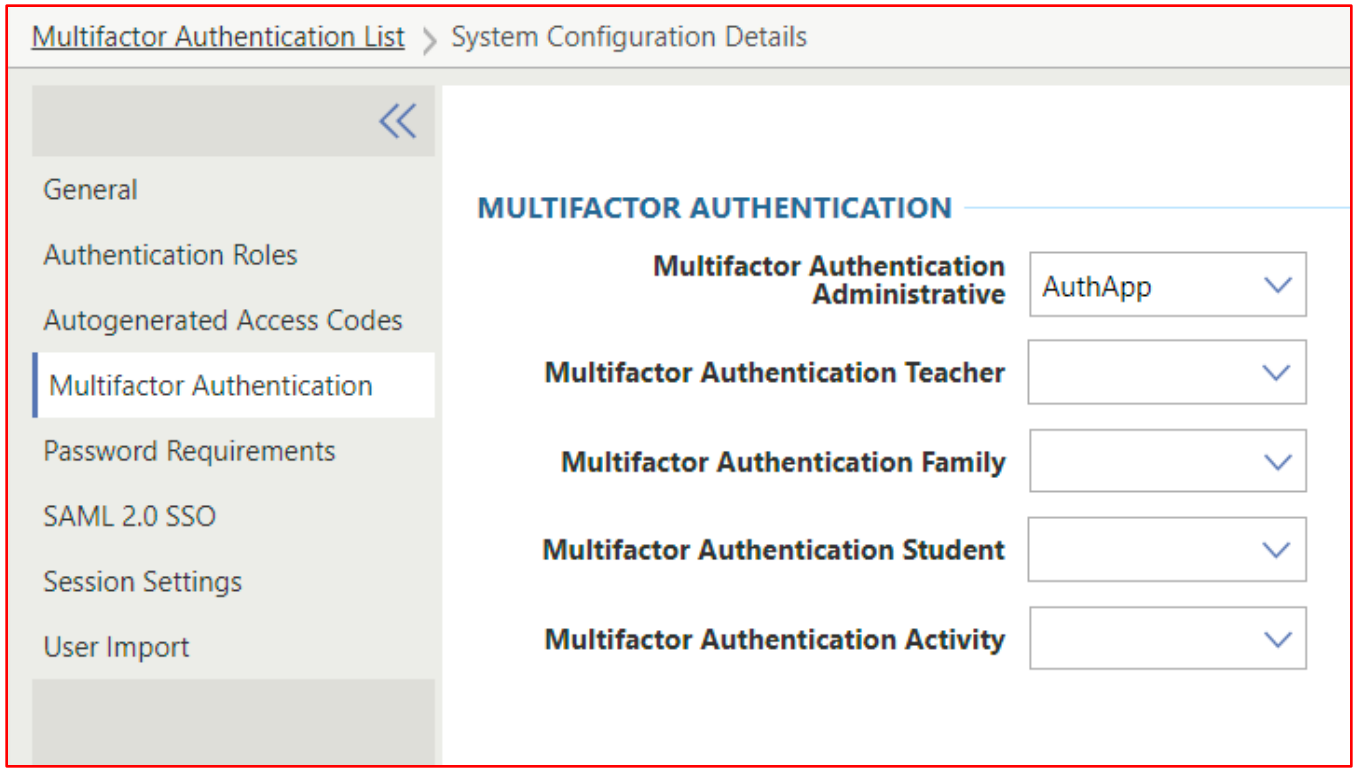
1. Qmlativ: Add Authentication Code(s)
2. Qmlativ: Assign Authentication Code(s)
3. Test

Add MFA Authentication Code(s)



- **View Menu** -> Administrative Access -> Security -> Codes -> Multifactor Authentication
- Days to Expiration is optional and supports partial days > ".5" is equal to 12 hours.
- Authenticator App Recommended
- Email is NOT Recommended

Assign MFA Authentication Code(s)

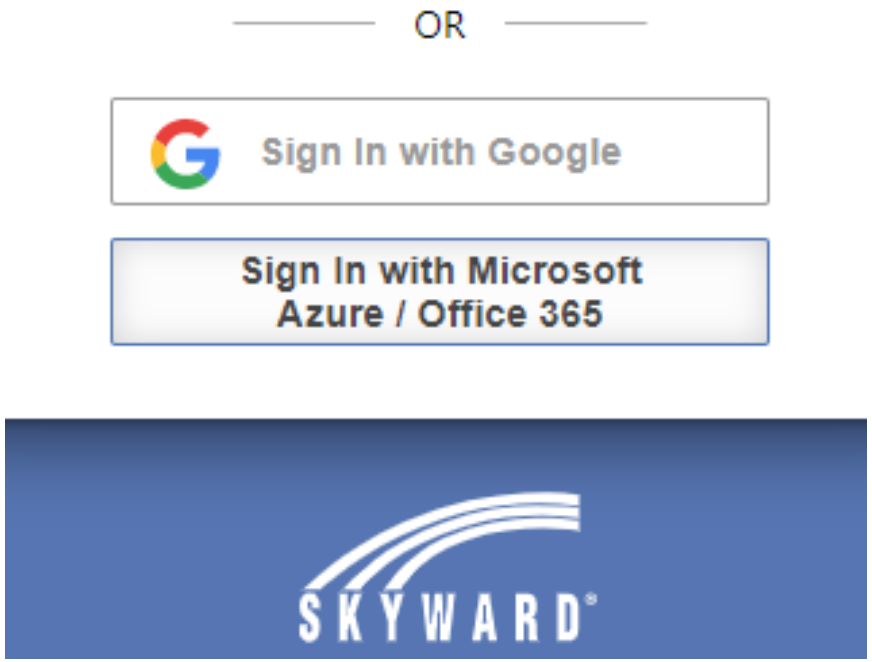


- **View Menu** -> Administrative Access -> Security -> System, Security Role, or User
- Flexible Design – MFA can be assigned at the System, Security Role, or User Level

Define: Single Sign-On

- Single Sign On allows Skyward users to **authenticate** into Skyward using a username and password from a 3rd party **Identity Provider**.
- Common examples of Identity Providers are Google, Microsoft Entra ID (Azure), ClassLink, Clever, DUO, and many more.
- SSO works with your Identity Provider's **Multi Factor Authentication**
- Qmlativ SSO uses the **SAML 2.0 protocol**

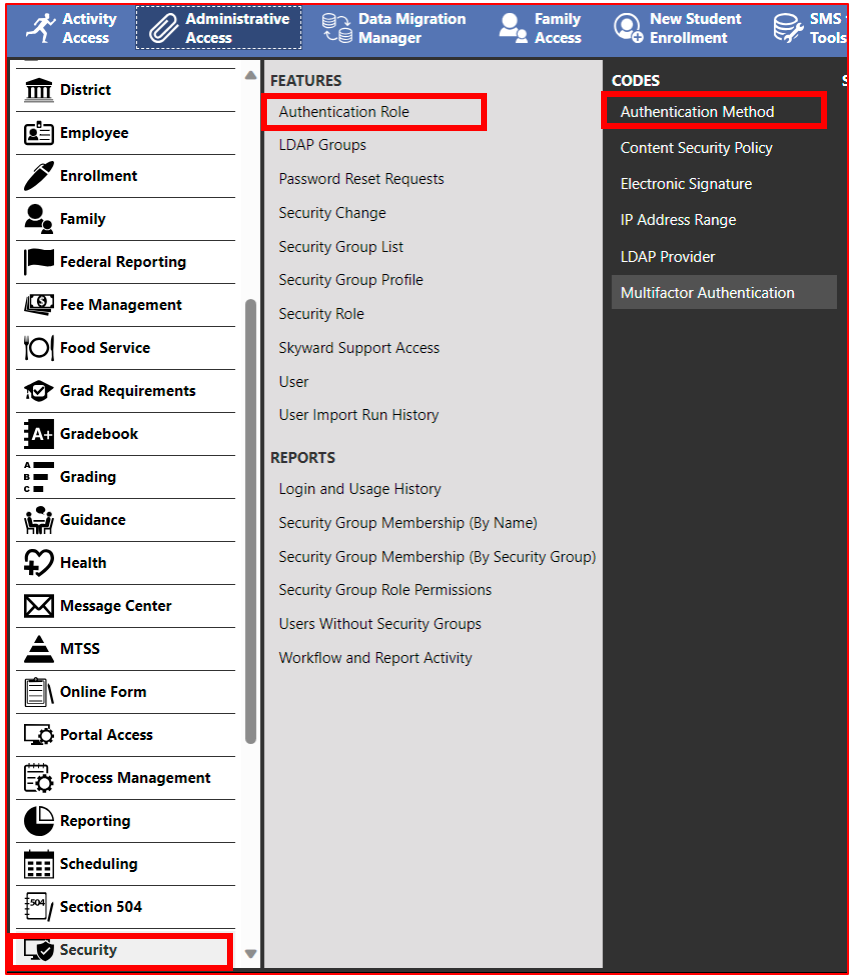
Qmlativ MFA with SSO



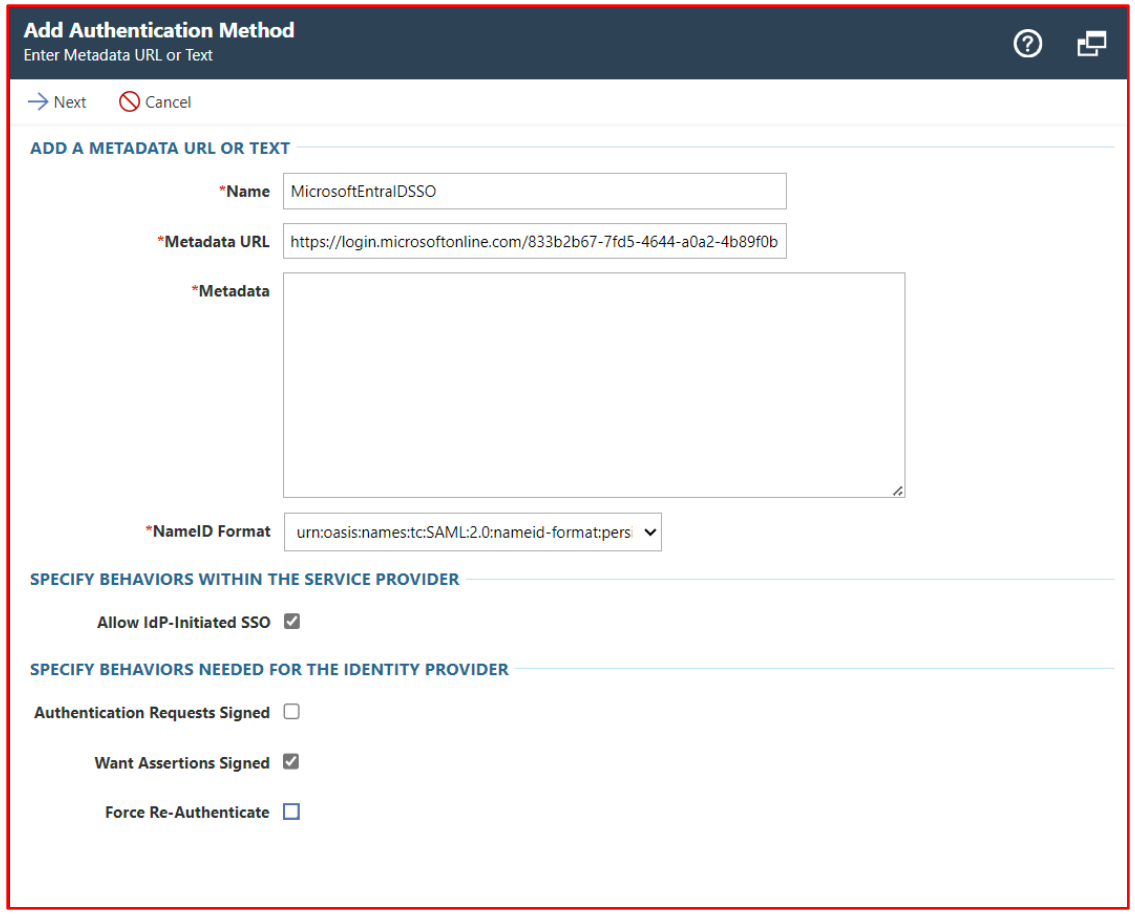
Qmlativ supports MFA using third-party Identity Providers. These include popular IdPs like Google® Apps, Microsoft® Entra ID (Azure) / Office 365, ClassLink, Duo, and many more.

Qmlativ using an Identity Provider

1. Qmlativ: Create Authentication Method(s)
2. Qmlativ: Create Authentication Role(s)
3. Qmlativ: Assign Authentication Role(s)
4. 3rd Party: Create SAML App
5. Test



Add Authentication Method(s)

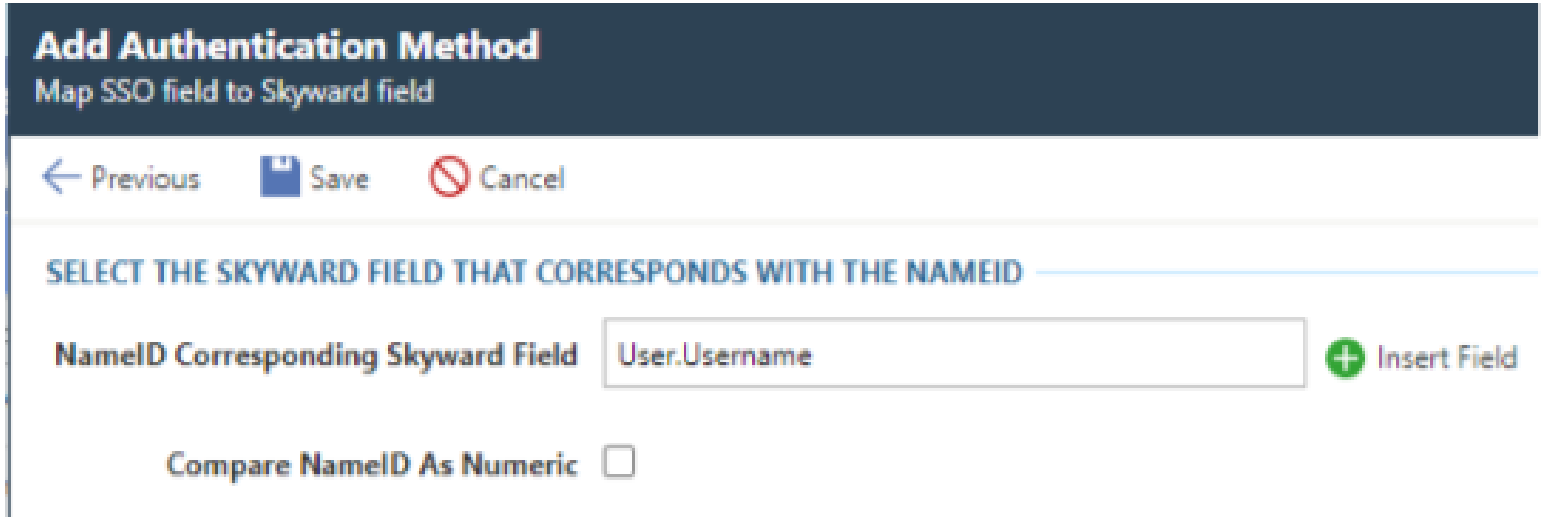


- SSO Launch Kit will reference common IDP settings
- IDP providers will be configured in Skyward.
- You will work between the provider SAML app and Skyward Authentication Method with settings.
- Authentication Method and SAML App Configuration is what allows the ‘connection’ for authentication.

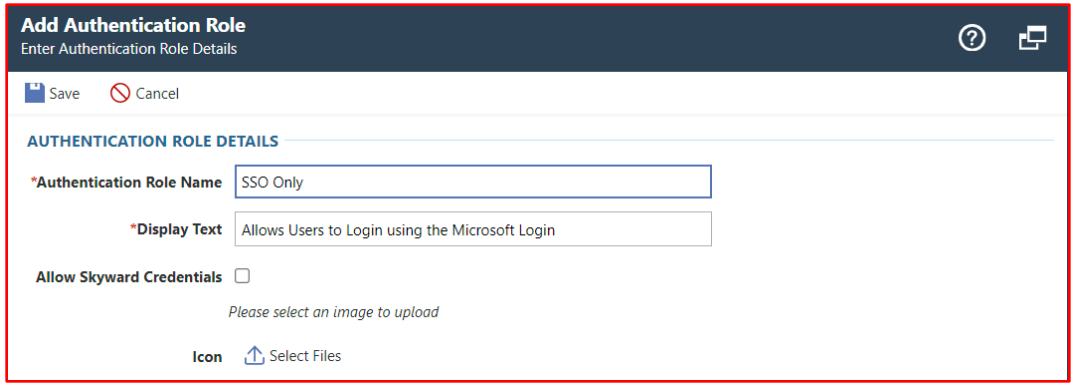
What is the NameID Claim?

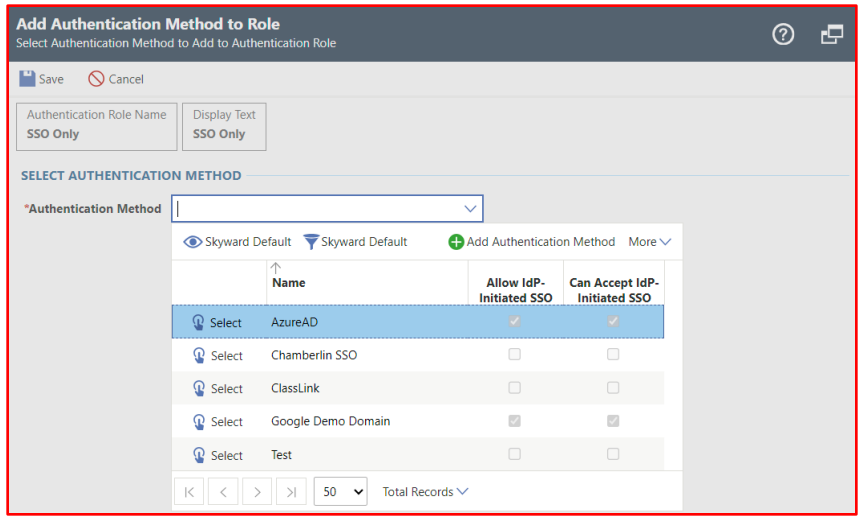
The **NameID Skyward Field** determines the data that the IdP is expecting in the NameID claim. A common config is to match the Email Address or Username, which requires both systems to have the same email address or Username (Login Name) entered for your SSO users.

MAP SSO field to Skyward field:



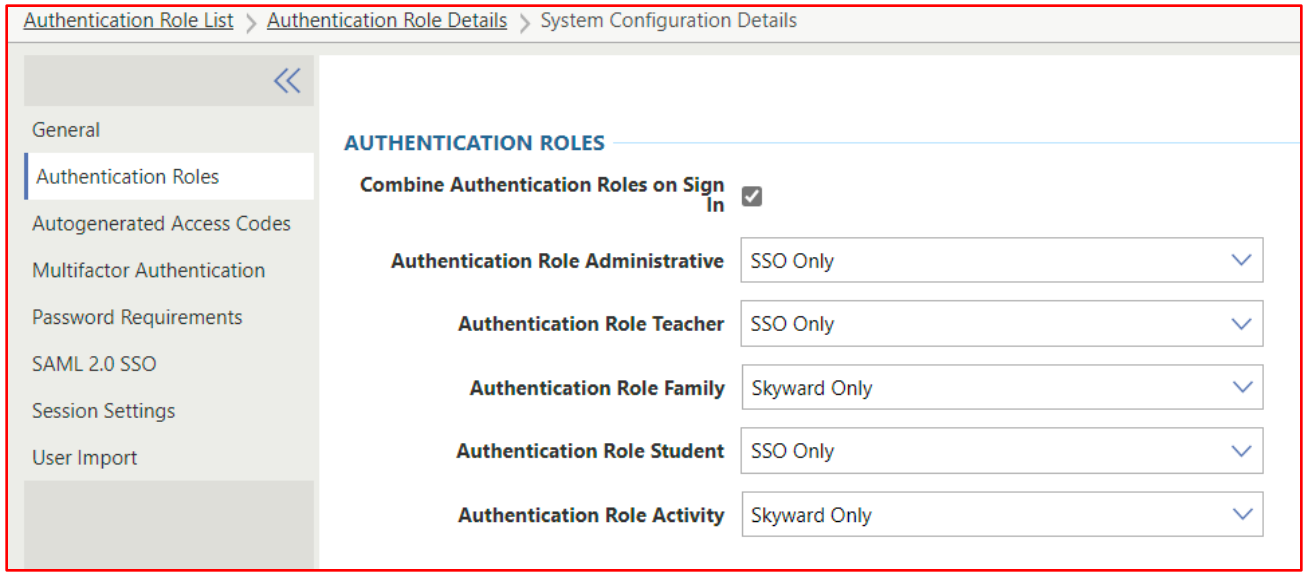
Add Authentication Roles





- **View Menu** -> Administrative Access -> Security -> Codes -> Authentication Role
- Best Practice: Create multiple Authentication Roles, one for each Authentication Role possibility and combination.
- Add Authentication Method(s) to your Authentication Roles

Assign Authentication Roles



- **View Menu** -> Administrative Access -> Security -> System, Security Role, or User
- Flexible Design – Authentication Role(s) can be assigned at the System, Security Role, or User Level

Allow IdP-Initiated SSO

- Check the box for Allow IdP-Initiated SSO but there are no authentication methods configured to allow IdP-initiated SSOs, a warning displays that indicates an IdP-initiated SSO is less secure than an SP-initiated SSO.

- Check the box for Allow IdP-Initiated SSO and an authentication method exists that allows IdP-initiated SSOs, a warning displays that lists the authentication methods that will resume accepting IdP-initiated SSO attempts.

- Did not check the box for Allow IdP-Initiated SSO and an authentication method exists that allows IdP-initiated SSOs, a warning displays that lists the authentication methods that will no longer accept IdP-initiated SSO attempts.

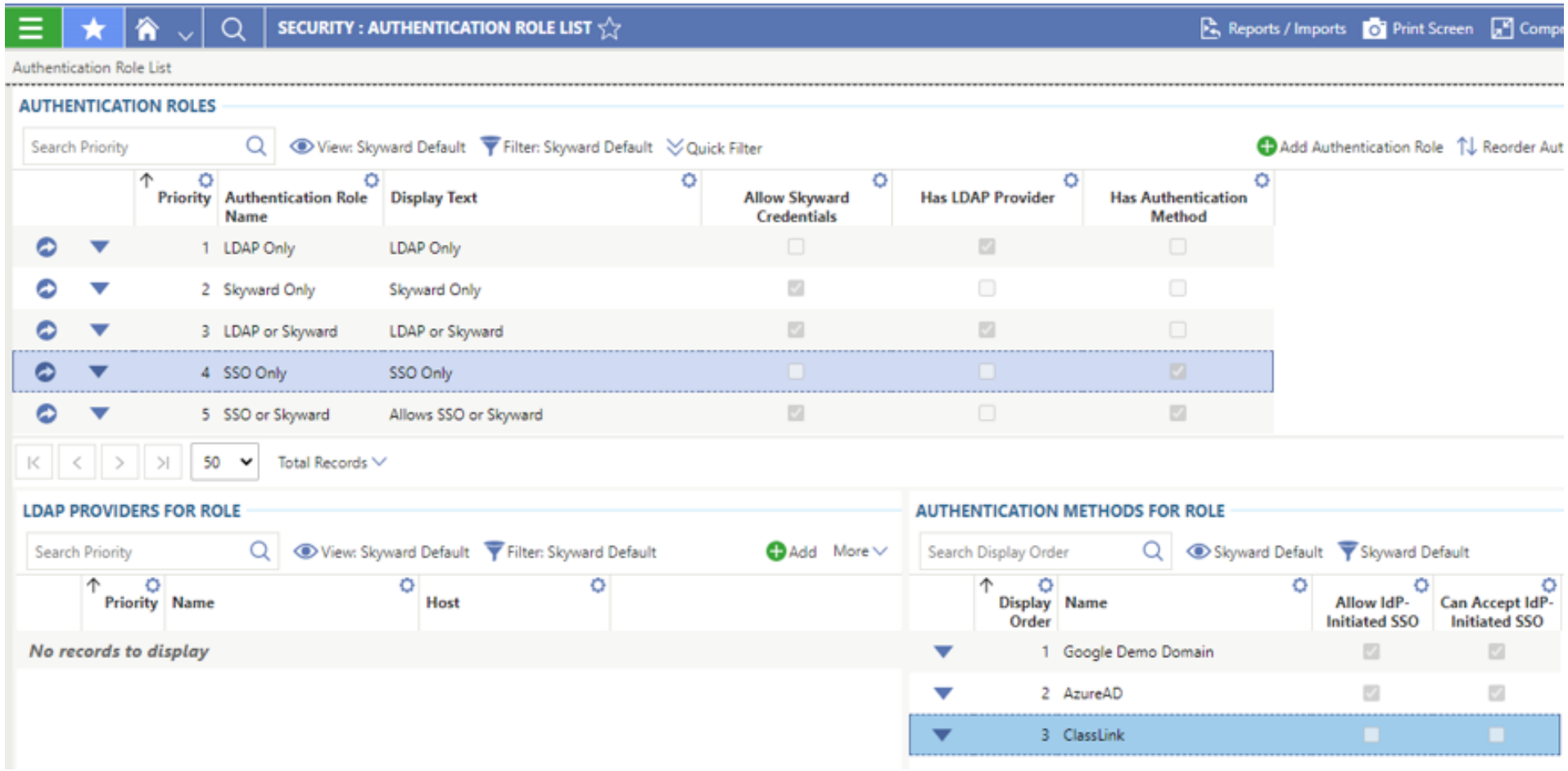
System Configuration in Security



Authentication Method

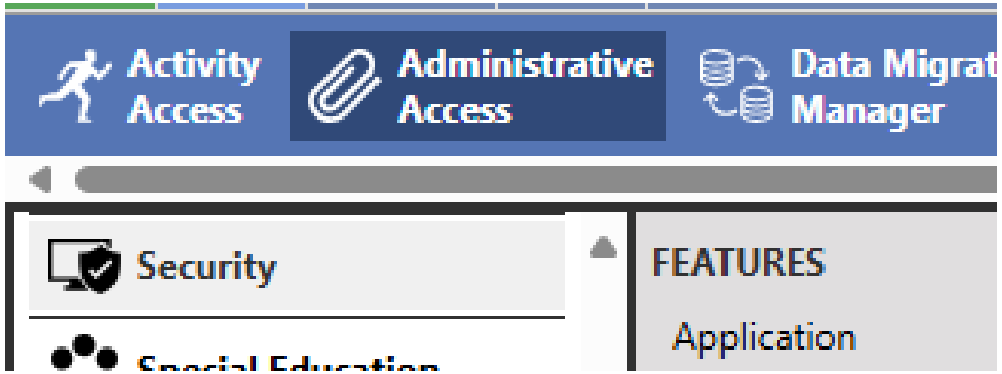


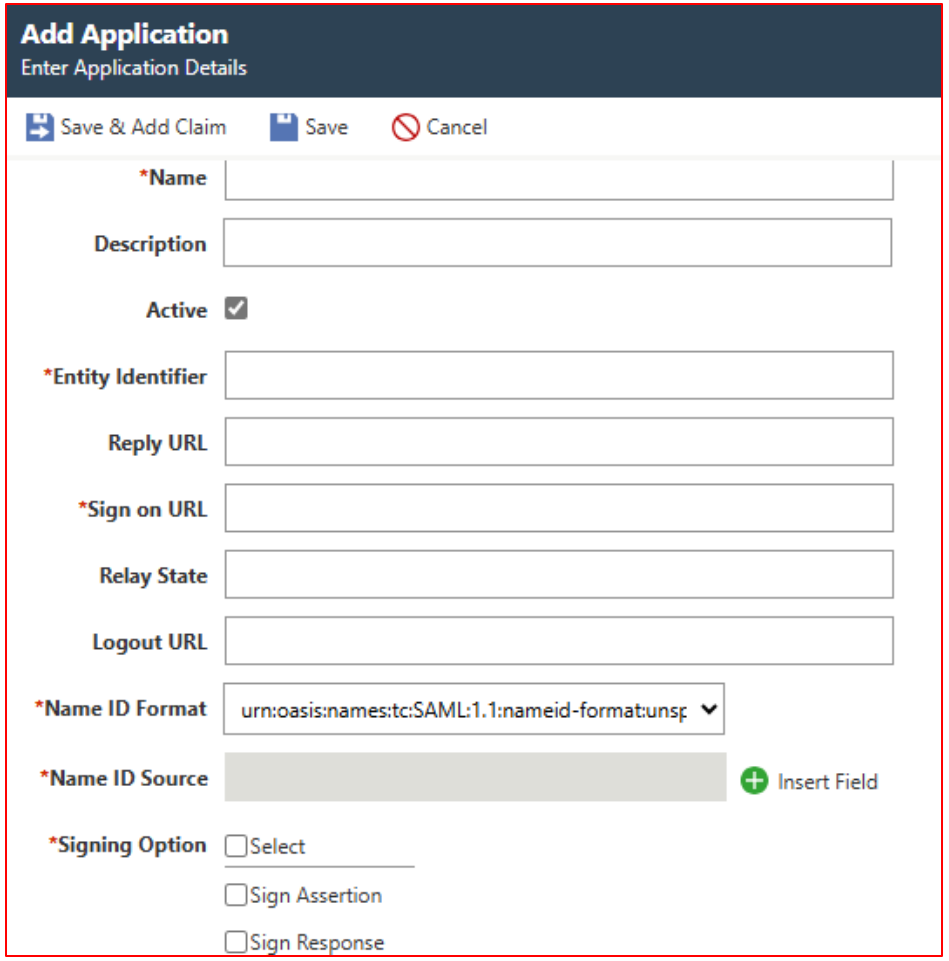
Allow IdP-Initiated SSO



Qmlativ as an Identity Provider

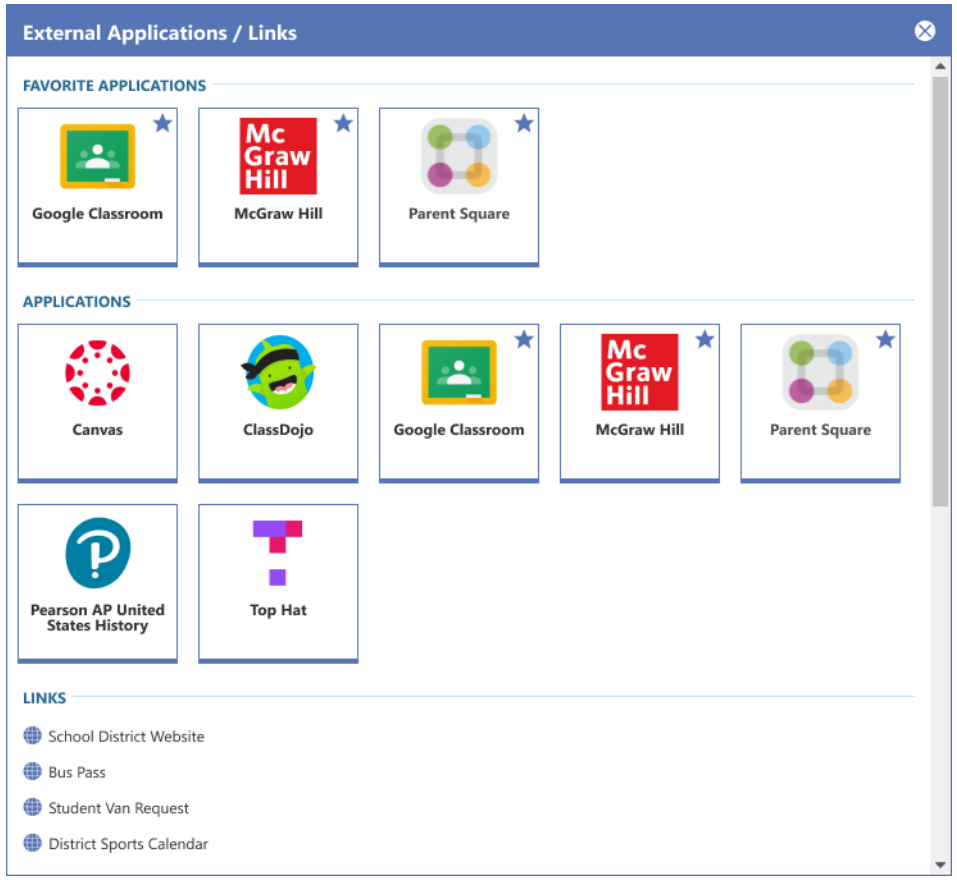
Qmlativ can be an Identity Provider (IdP) for 3rd party systems, such as your School Payment or Learning Management System. This means that users of the 3rd party system can log in to the 3rd party system using their Qmlativ username/password using SAML 2.





Application Collections

- Districts can create Applications and Application Collections to distribute links to SSO enabled applications to end users.
- Administrative Access / Security / Features / Application & Application Collections



Qmlativ User Management Tools

Qmlativ has several tools that assist User Management.

New Users: **Configure Username / Email Structure by User Type**

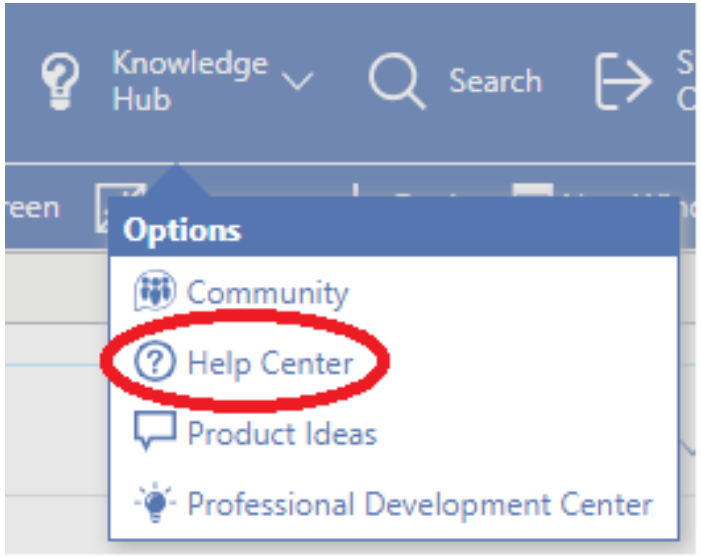
- Students
- Family
- Staff
- Employee

New / Modify Users: **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.

Qmlativ User Import

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



PROGRESS SOFTWARE

ISCorp Integrated Systems Corporation

Microsoft Authorized Education Partner

KnowBe4 Human error. Conquered.

aruba a Hewlett Packard Enterprise company

Skyward's IT experts have the latest knowledge on industry trends and developments to help keep your network running smoothly.

Extreme networks

FORTINET

CyberNut

Mitel

Verkada

TEA Texas Education Agency

APC by Schneider Electric

SONICWALL

BARRACUDA NETWORKS

GeoTrust powered by digicert

veeam

Lightspeed Systems | Partners

TOOLS4EVER IDENTITY GOVERNANCE & ADMINISTRATION

Hewlett Packard Enterprise

NETWORK CONSULTING

- Resilient Wired Network Infrastructure
- Complete Wireless Network Solutions
- Virtual Server Design and Support
- Storage Area Network Solutions
- IP Telephony Solutions

SUPPLEMENTAL IT STAFFING

- Onsite and Remote IT Support
- Network Assurance Services

ASSESSMENT SERVICES

- Network / Security
- Disaster Recovery
- Secure Cloud Computing

SKYWARD OPTIMIZATION

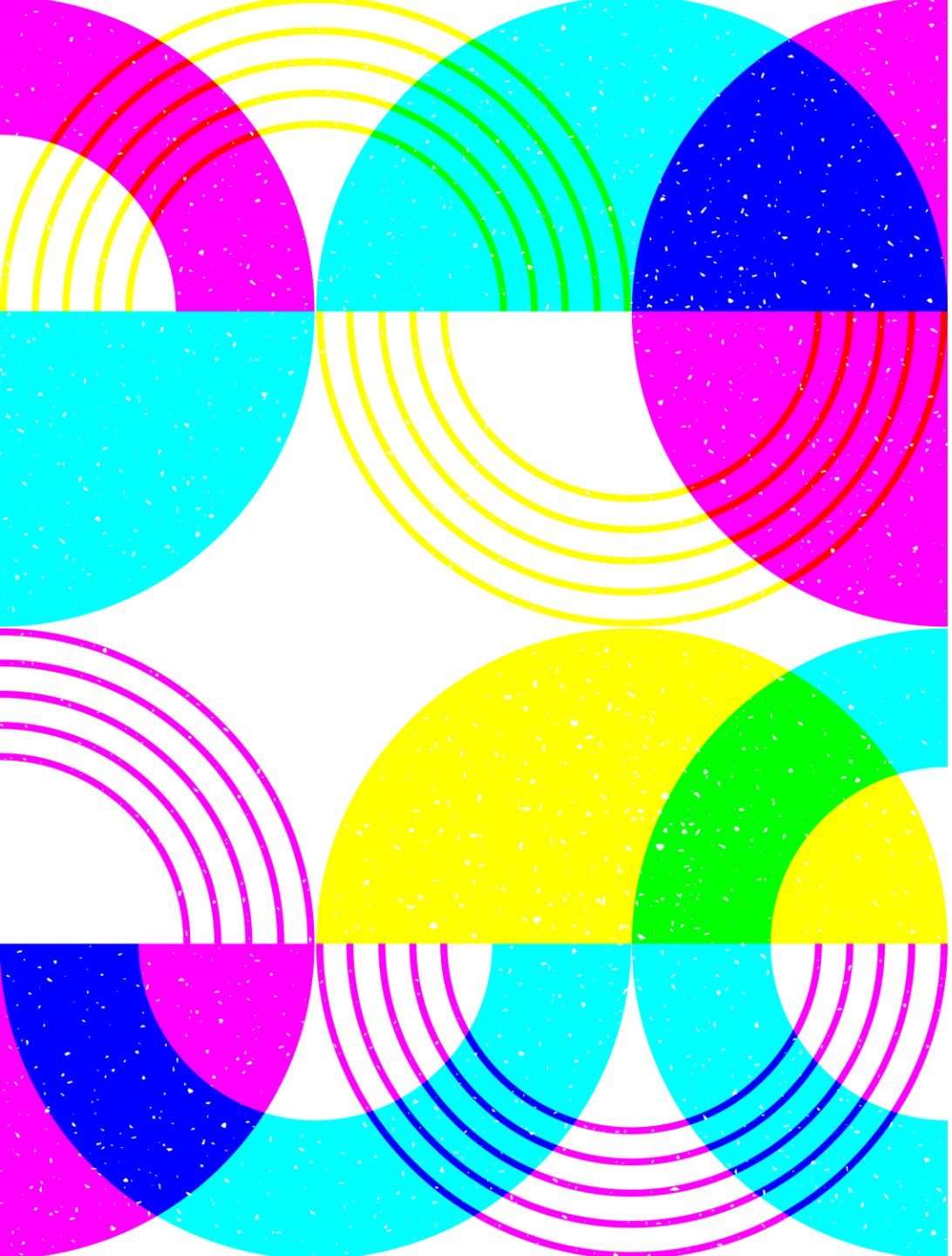
- Managed Services
- Database Tune-ups
- Remote Update Services
- System Admin Training

NETWORK SECURITY SOLUTIONS

- Intrusion Detection, Prevention, and Next Generation Firewalls
- Email Filtering, Archiving, and Security Solutions
- Internet Filtering and Monitoring Solutions
- On-Staff Security Experts

DISASTER RECOVERY SERVICES

- Skyward Disaster Recovery from ISCorp
- Onsite Data Center Disaster Recovery Solutions



SKYWARD®

iCON

thank you!