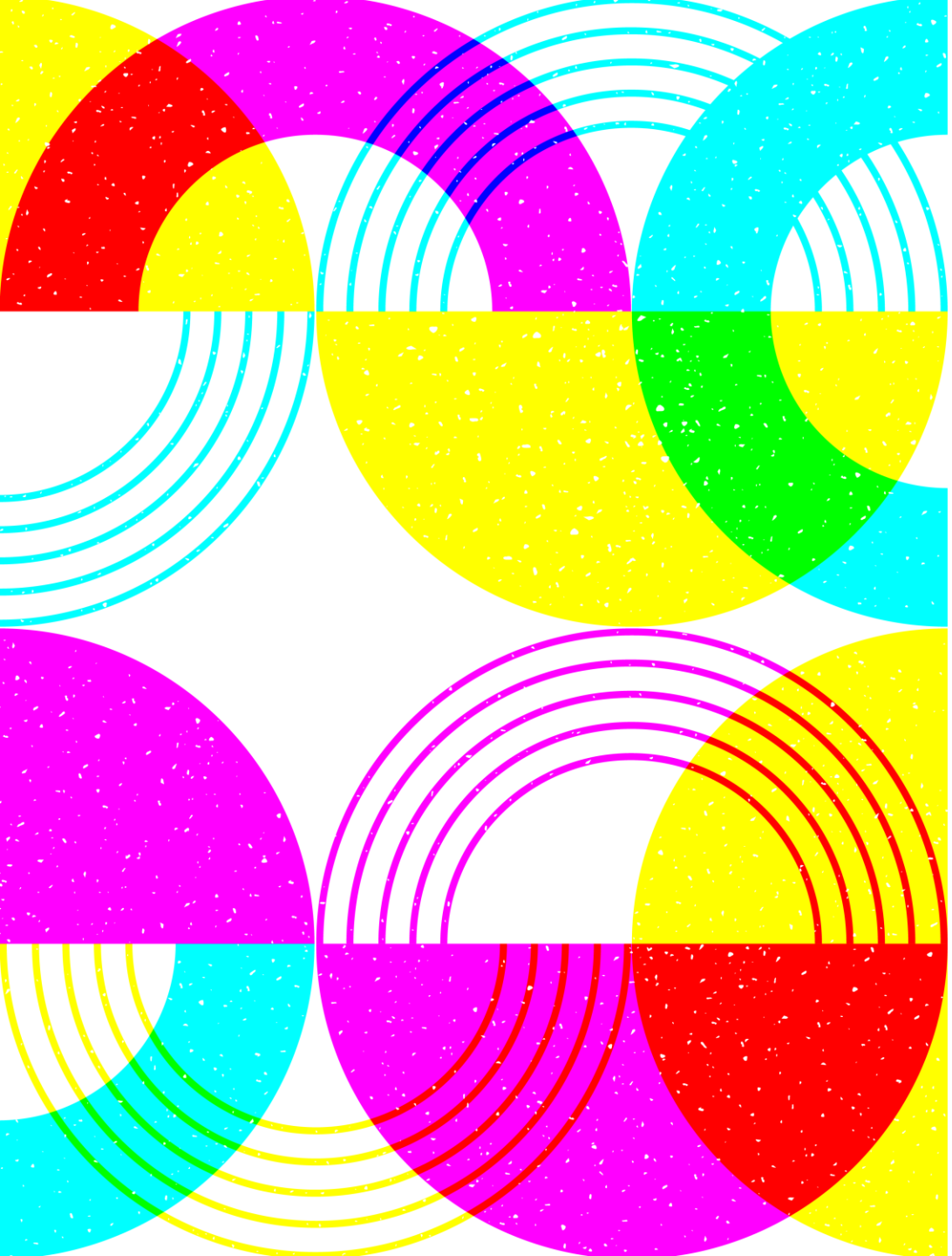


follow us on social!

#skyicon



SKYWARD®

iCON

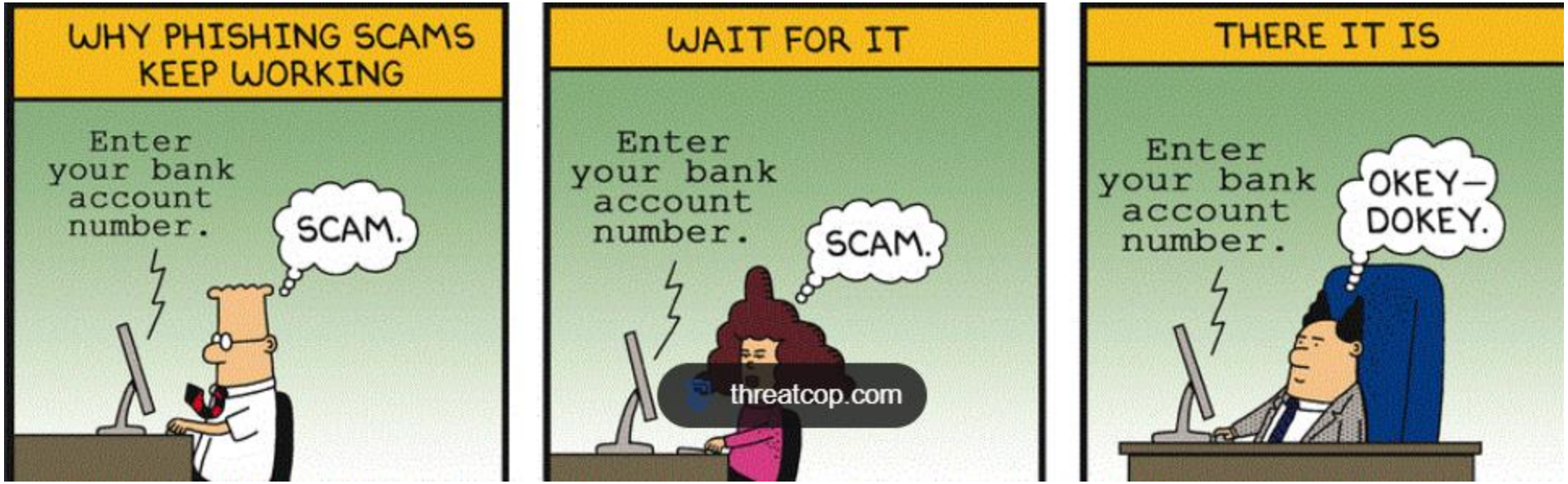
Minimize Risk - Maximize Protection - Skyward Security Essentials

Mike Bianco – VP of Information Security

Minimize Risk - Maximize Protection - Skyward Security Essentials

- Security Awareness Training
- Foundational Security in Skyward
- Secure Authentication
- SMS 2.0 Security Features
- Qmlativ Security Features

Why Security Awareness Training?



Security Awareness Training

Security Awareness Training is all about teaching your **colleagues** and **employees** to understand the **risks** and **threats** around the ever-evolving **cyber world**.

Employees must be fully **aware** of the **consequences** of failing to **protect** the **organization** from outside **attackers**.

91% of **cyberattacks** begin with a **spear phishing email** according to research from security software firm Trend Micro.



Security Awareness Training

Baseline Testing
Use simulated phishing to baseline assess the Phish-prone™ percentage of your users.

Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

Phish Your Users
Best-in-class, fully automated simulated phishing attacks, hundreds of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both training and phishing, ready for management. Show the great ROI!



Securing Data At Rest

Data At Rest is data that is stored on a hard drive, laptop, flash drive, or archived/stored in some other way.

An effective method of Securing Data At Rest is by encrypting the data.

Data at rest includes your Skyward OpenEdge or SQL database(s) and the backup of the database(s).

Securing Data At Rest

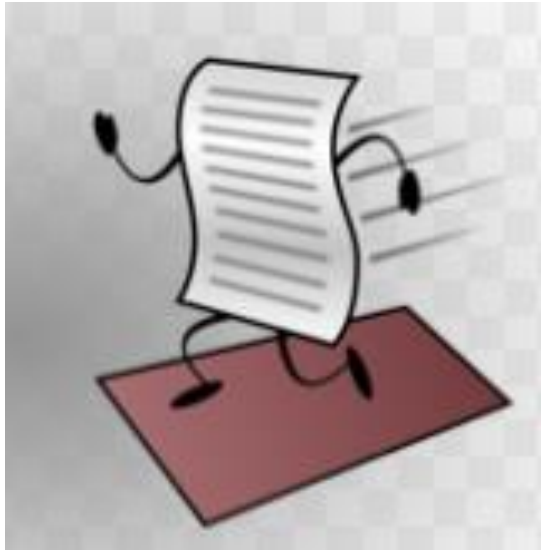


Transparent Data Encryption (TDE) for Database(s)

- SMS 2.0: Progress® OpenEdge
  - One Time Implementation cost / Training
  - Licensed product (Annual License Fee)

- Qmlativ: Microsoft® SQL TDE
  - One Time Implementation Cost / Training
  - TDE is included with SQL Licensing

Securing Data In Transit



Data in transit, or data in motion, is data actively moving from one location to another such as across the internet or through a private network.

An effective method of Securing Data In Transit is by encrypting the data while it is in motion.

QuickSSL Premium SSL Certificates



- Security: Origanization Validated, up to 256-bit encryption, 2048-bit root
- Assurance: $500K USD warranty, GeoTrust dynamic True Site Seal Trustmark
- Convenience: most certificates issued in minutes, 1 year validity option
- Cost-effective: unlimited server licenses, unlimited free reissues for certificate lifetime
- Universality: support for more than 99% of browsers and most mobile device browsers
- **Available from Skyward IT Services**, purchase includes Installation

Transport Layer Security (TLS)

TLS is the foundation of a secure connection and TLS is evolving as new threats emerge

- TLS 1.0/1.1, SSL 2/3 are no longer considered secure.
- TLS 1.2 is mainstream and supported by Skyward
- TLS 1.3 adoption is accelerating rapidly and is now widely supported across modern browsers, CDNs, and major cloud platforms.
- TLS 1.3 is not supported on Windows Server 2019 or older OS

Transport Layer Security (TLS)

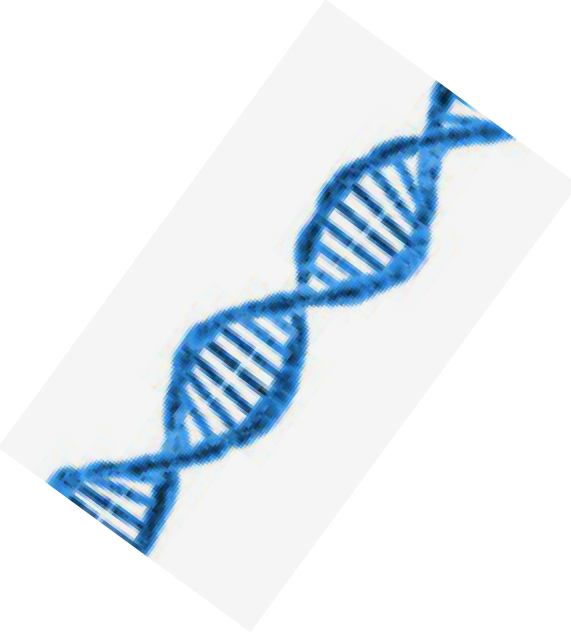
- Both the application and the Server OS controls what versions of TLS are supported.
  - We recommend on-premises customers review their Windows Server TLS settings.
- IIS Crypto tool can be used to change Windows settings (server reboot required to implement changes
- Each customer should review their 3rd party integrations TLS support before making changes
- Free 3rd Party Verification tools example: SSL Labs SSL Server Test

https://www.nartac.com/Products/IISCrypto/Download
https://www.ssllabs.com/ssltest/

Securing Data in Transit

Skyward supports the following encryption protocols to ensure all data is encrypted while it's being sent across the network.

- All Web Portals (HTTPS) - Required
- Secure FTP (SFTP/ SSH) – Required
- ExComm SIF / Ed-Fi (HTTPS) – Required
- LDAP (LDAPS/TLS/Kerberos) – Required
- Single Sign On (HTTPS) - Required
- SMTP Email (TLS) – Optional



Secure HTTP

- Secure HTTP (aka HTTPS) prevents data from being read by eavesdroppers as it's sent across the "wire".
- If packets are captured on the "wire" the data cannot be read because it is encrypted.
- What Skyward products use HTTPS?
  - All Skyward Web Applications
  - Single Sign On
  - ExComm SIF / Ed-Fi
  - eCommerce
  - Payment Integrations (Ex. RevTrak)
- HTTPS is the industry standard for Securing Web Applications

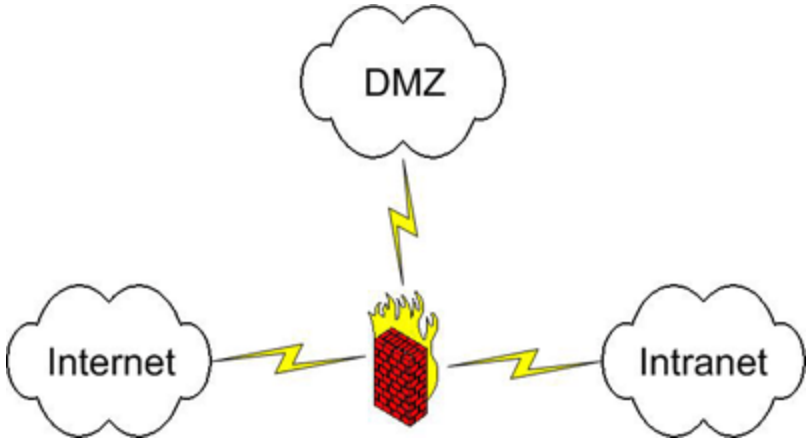
Secure LDAP

- LDAP Offers multiple Encrypted Protocols
  - (LDAPS, LDAP w/TLS, Kerberos)
- Encryption prevents Users & Passwords from being read by eavesdroppers.
- Both SMS 2.0 & Qmlativ require Secure LDAP

Secure Email (SMTP)

- SMTP Offers an Encrypted Protocol (TLS)
- Encryption prevents message from being read by eavesdroppers.
- Use the Email Launch Kit to verify the use of a Secure Email configuration
  - SMS 2.0 Email Launch Kit
  - Qmlativ Email Launch Kit

DMZ Web Server Design



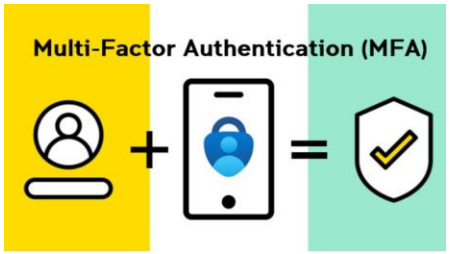
- Optimal Design for Security
- Reduces Internet facing Attack Surface

SMS 2.0: Firewall Friendly DMZ Web Server Support

Qmlativ: Firewall Friendly DMZ Web Server Support

Multi Factor Authentication

Why use ……..



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.

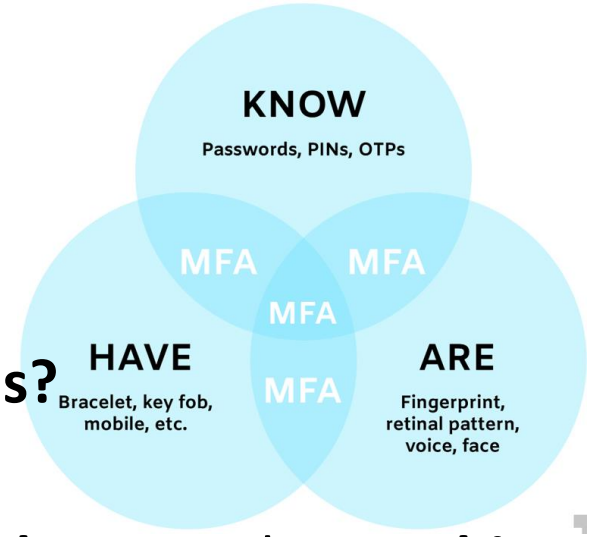
Multi Factor Authentication

What is ……

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). The most common factors are **something you know** and **something you have.**



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).

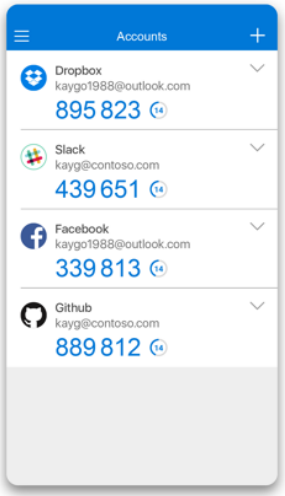
Authenticator Apps

An **authenticator app** is usually installed on a smartphone and generates a passcode every 30 seconds. The passcode can be used as login factor for accessing an account.

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

Common Authenticator Apps

- Google Authenticator
- LastPass Authenticator
- Microsoft Authenticator
- Many others..





SMS 2.0

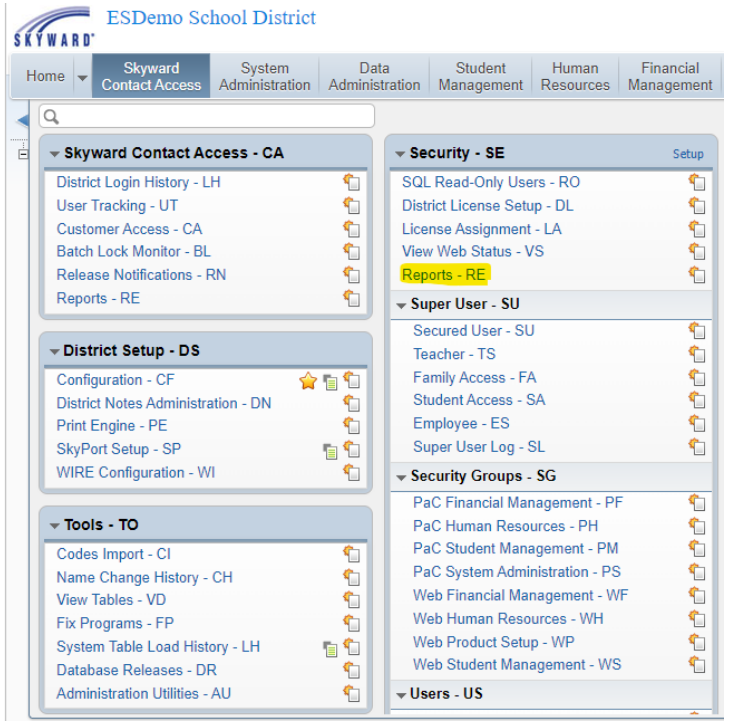
SMS 2.0 PaC Program Server

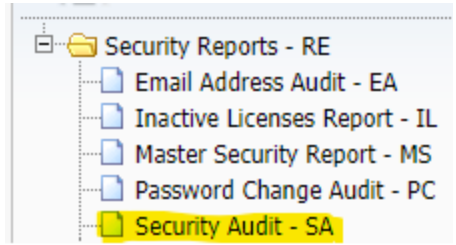


- Use a Separate server for PaC Programs
- Use an existing Network File Server
- Install Monolith DAS Role for Program Updates
- Programs Share on a Database server = Infections from infected PaC Clients.
- Ransomware infections on the Database Server causes downtime and heartburn.

SMS 2.0 Security Audit Report

Product Setup → Skyward Contact Access → Security → Reports → Security Audit





- **System Settings**
  - Mobile Enabled
- **SMTP Settings**
  - SMTP Server
- **Authentication Settings**
  - Single Sign On Configuration
    - By User Type
    - Web/Mobile App/PaC
  - LDAP Server

- **Password Settings**
  - Minimum Password Length
- **Session Settings**
  - Session Idle Time Logout
- **Security Alert Notification Status**
  - Account Locked
  - New Login Device
  - Password Changed
- **Security Groups**
  - Security IDs
- **User Info**
  - # of System Wide Users
  - # of Active/Inactive/Other Users
- **Attachment Upload Settings**
  - Blocked File Extensions
    - Recommended
    - Configured

SMS 2.0 Self Service Password Resets

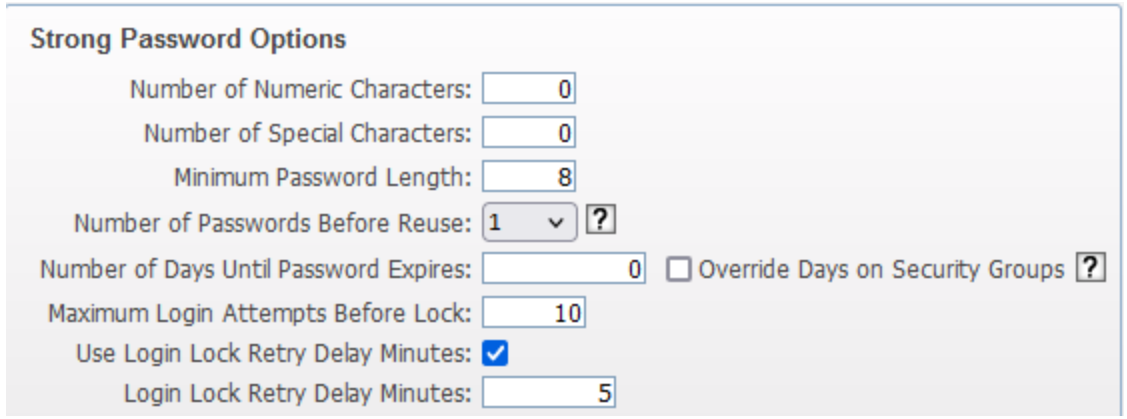
Product Setup → Contact Access → Security → Setup → Configuration → Security Configuration

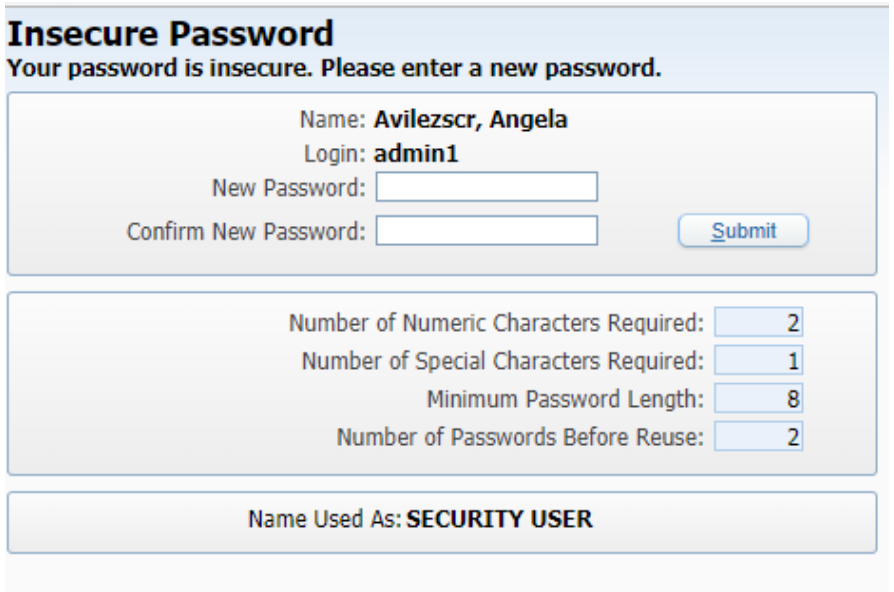


If using Self Service Password resets, Include the IP Address in the Email and require reCAPTCHA.

SMS 2.0 Strong Password Options

Product Setup → Contact Access → Security → Setup → Configuration → Security Configuration



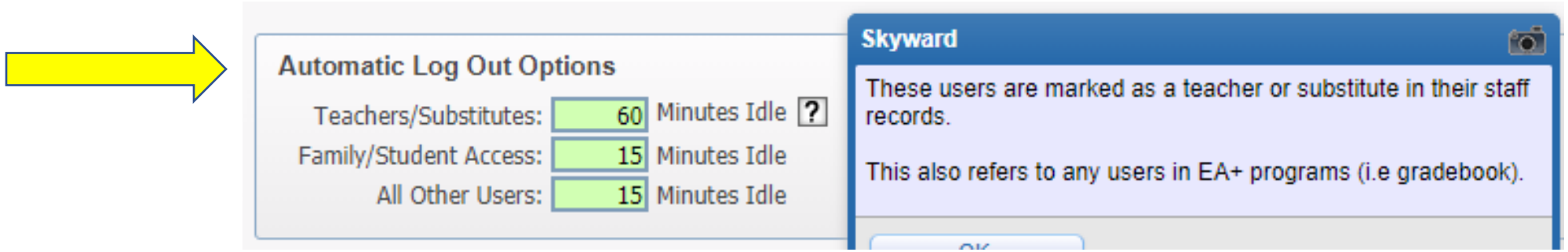


- Minimum Password Length is 8; range is 8 - 64
- Number of Passwords Before Reuse is 1; range is 1 - 15
- Maximum Login Attempts Before Lock is set to 10; range is 1 - 255
- Use Login Lock Retry Delay Minutes is set to 5; range is 5 - 32767

Users that do not meet the password requirements will be prompted to enter a new stronger password.

SMS 2.0 Automatic Logout Options

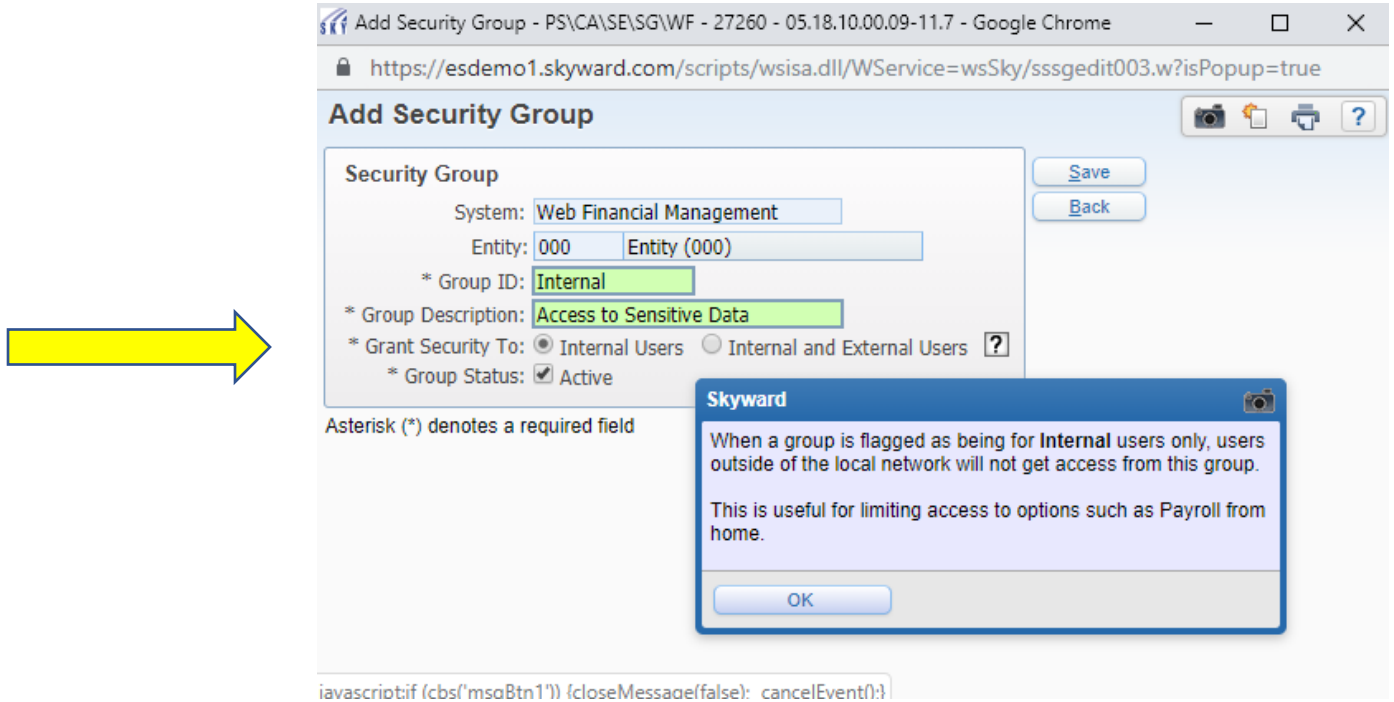
Product Setup → Contact Access → District Setup → Configuration → Web Configuration



Idle Users will get a warning prior to being Automatically Logged out.

SMS 2.0 Security Group IP Restrictions

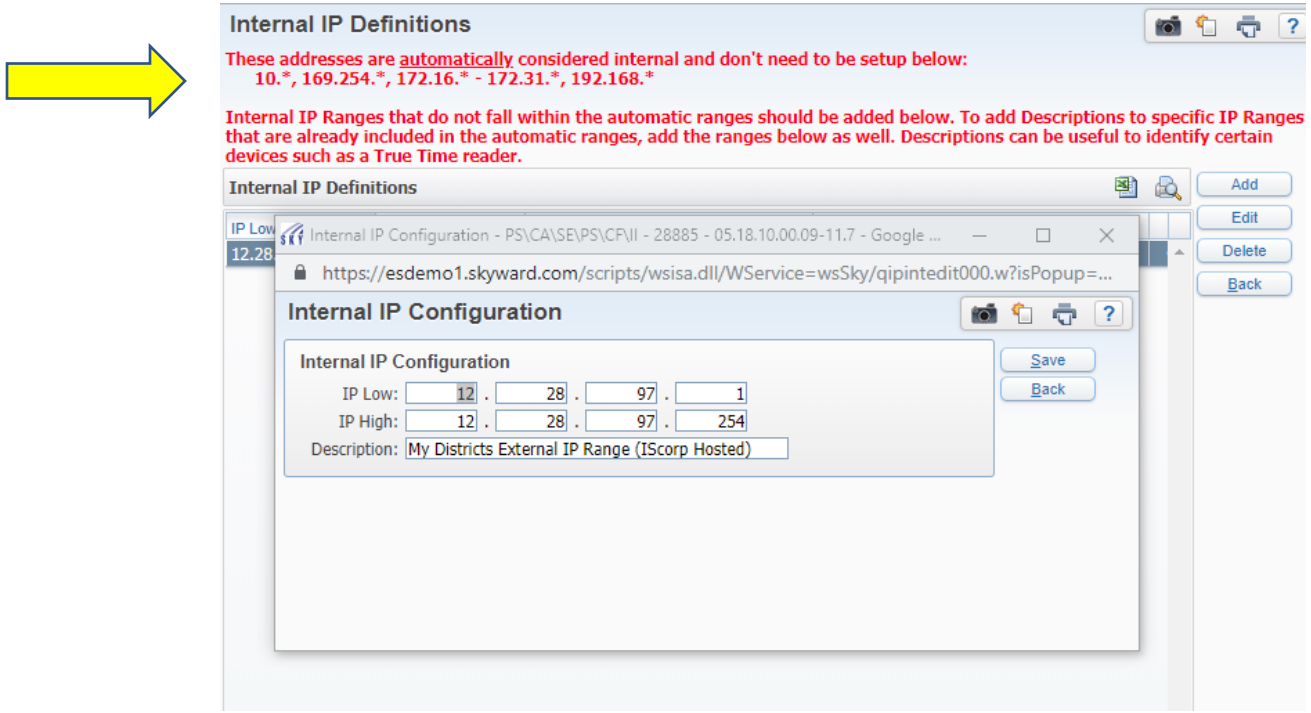
Product Setup → Contact Access → Security Groups



Security Groups can be restricted to Internal Users (IP Based Restrictions)

SMS 2.0 Security Group IP Restrictions

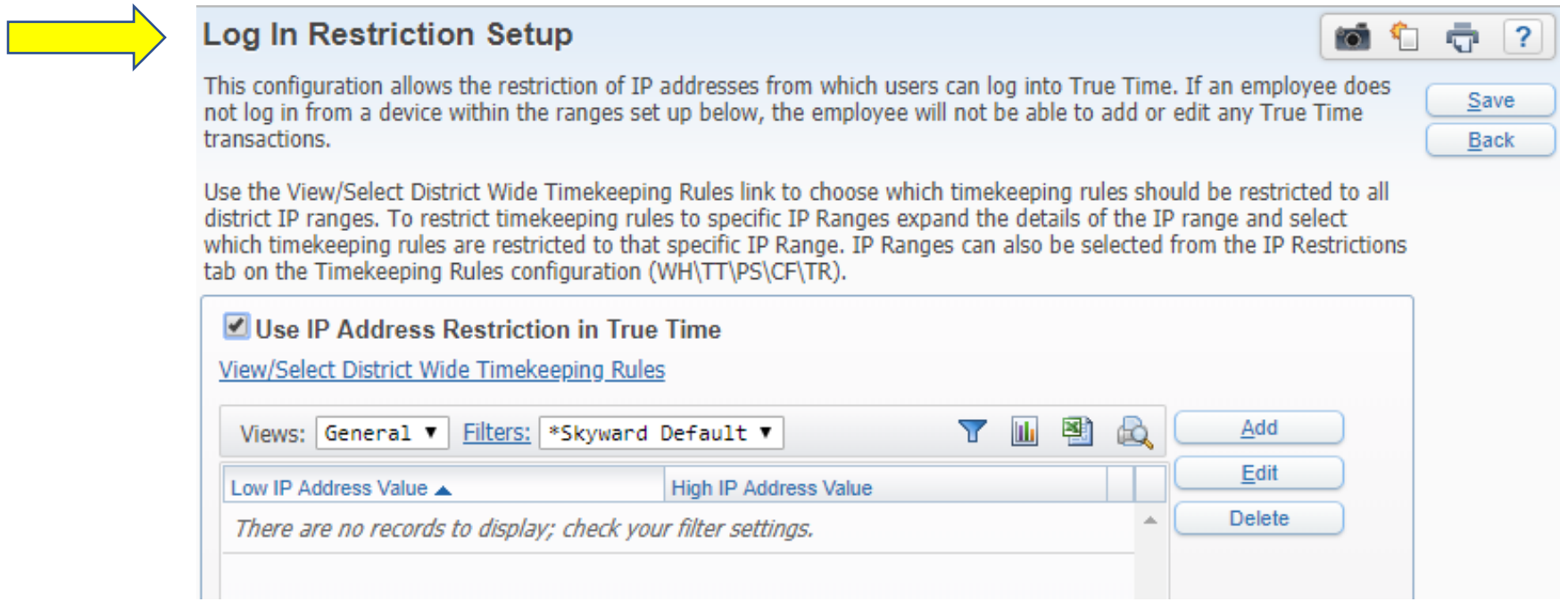
Product Setup → Contact Access → Security → Setup → Configuration → Internal IP Definitions



Additional IP Networks can be Defined (IP Based Restrictions)

SMS 2.0 TrueTime IP Restrictions

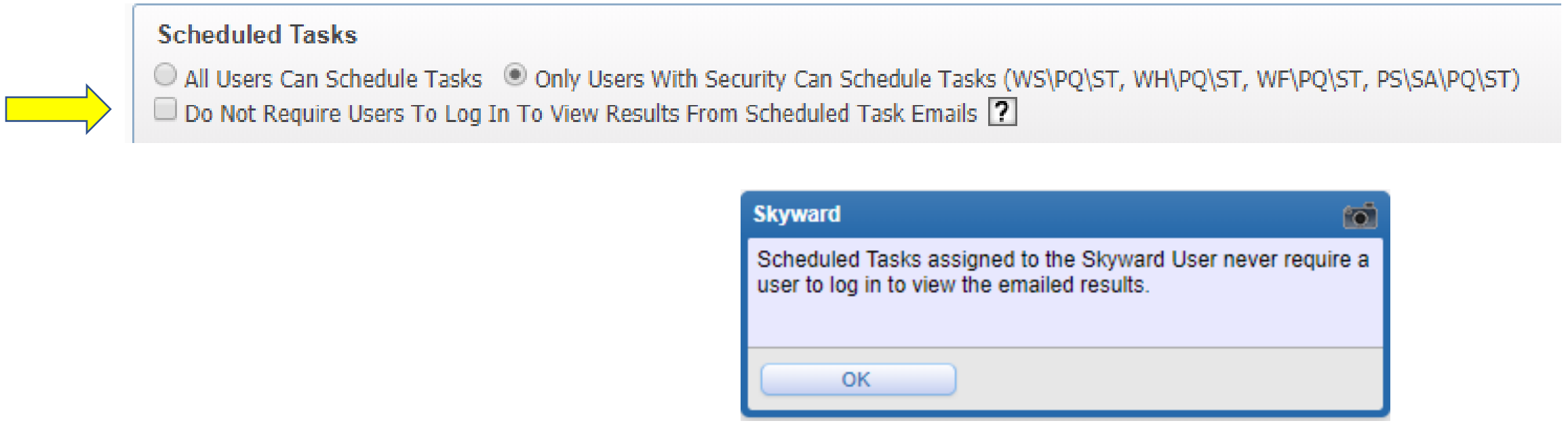
Product Setup → Human Resources → TrueTime → Configuration → Login Restriction Setup



Additional IP Networks can be defined (IP Based Restrictions)

SMS 2.0 Scheduled Task Emails

Product Setup → System Admin → District Print Queue→ Report Configuration

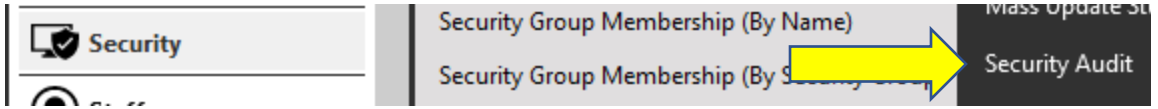


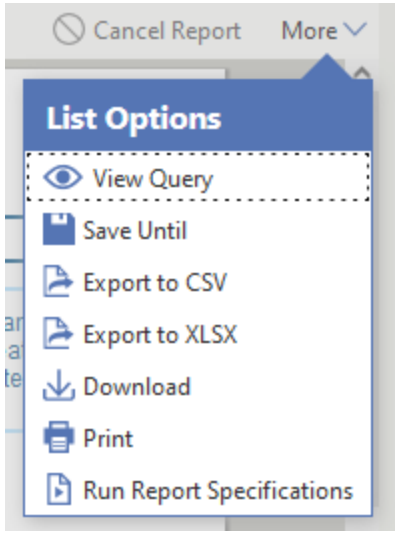
Require Users to Login to View Scheduled Task Emails


Qmlativ

Qmlativ Security Audit Report

Select ☰ → Administrative Access → Security → Utilities: Security Audit

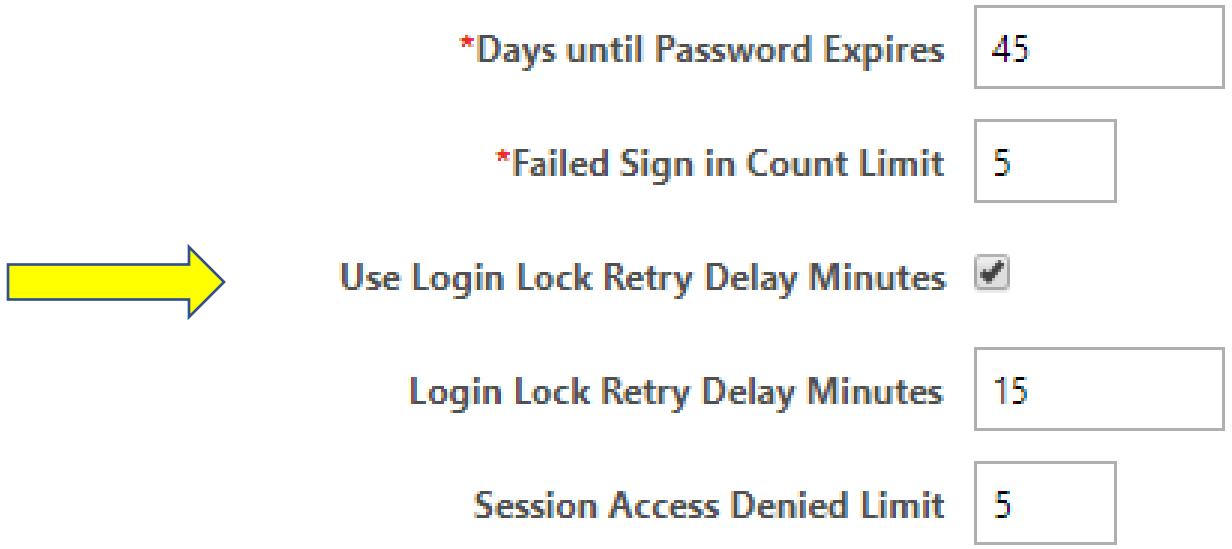




- **System Settings**
  - Mobile Enabled
  - SMTP Settings
    - SMTP Server
- **Authentication Settings**
  - Authenticate Roles
  - LDAP Providers)
  - Authentication Method(s)
  - MFA Code(s)
- **Password Settings**
  - Minimum Password Length
- **Session Settings**
  - Session Idle Time
  - Session Disconnected Time
- **Security Groups**
  - Security Group Codes
- **User Info**
  - Number of Super Users
  - Number of Active/Inactive Users

Qmlativ Login Policies

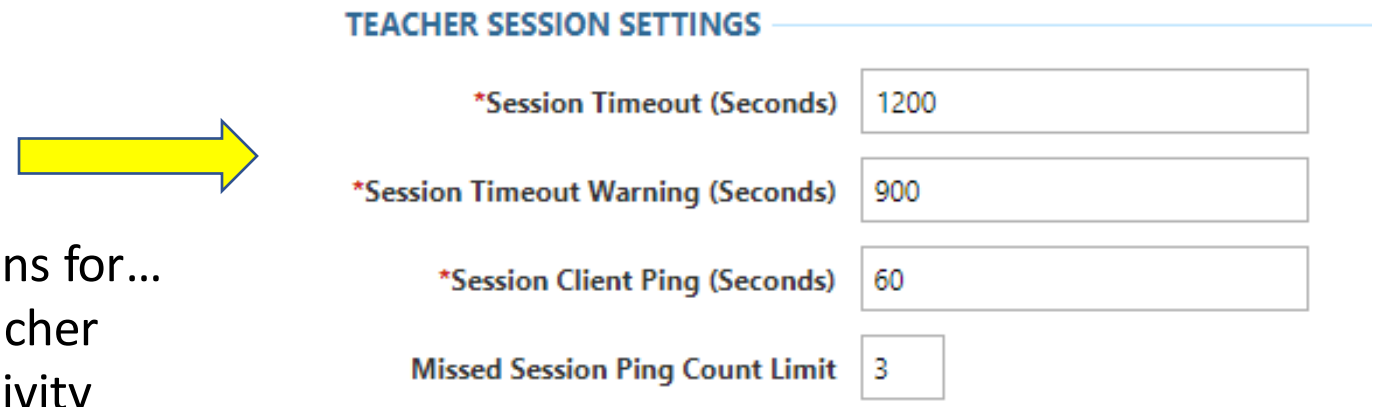
Select ☰→ Administrative Access → Security → Settings: System Configuration → General



Define System Wide Login Policies

Qmlativ Automatic Logout Options

Select ☰ → Administrative Access → Security → Settings: System Configuration → Session Settings



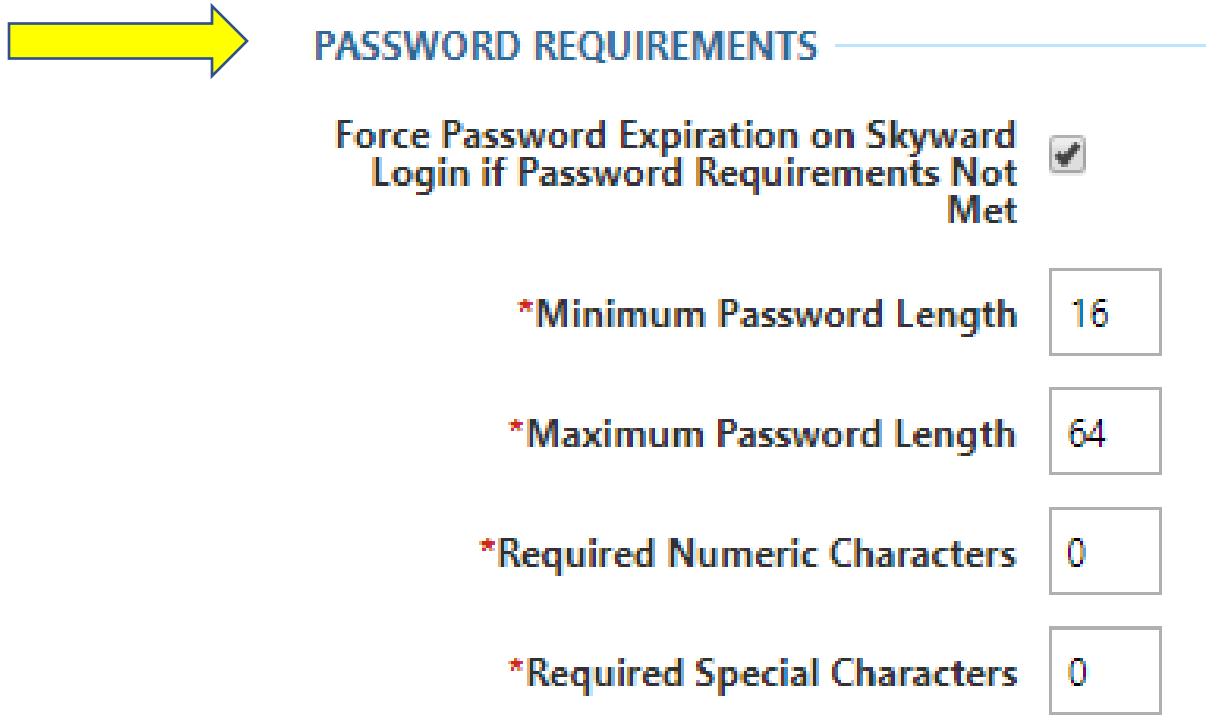
Sections for…

- Teacher
- Activity
- Admin
- Student Services
- Student
- Family

Idle Users will get a warning prior to being Automatically Logged out.

Qmlativ Strong Password Requirements

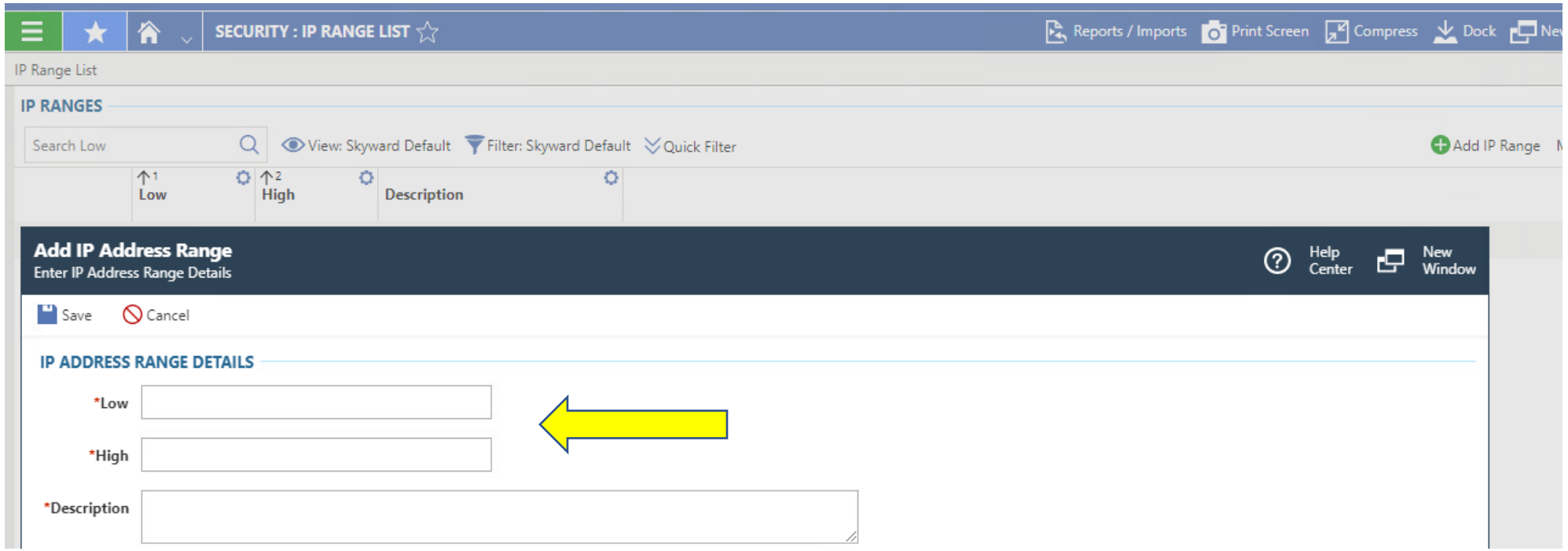
Select ☰ → Administrative Access → Security → Settings: System Configuration → Password Requirements



Consider requiring longer “pass phrases” instead of complex passwords.
Pass phrases are harder to crack and are easier for users to remember.
Example Pass Phrase: Today is going to be a great day!

Qmlativ IP Range Definitions

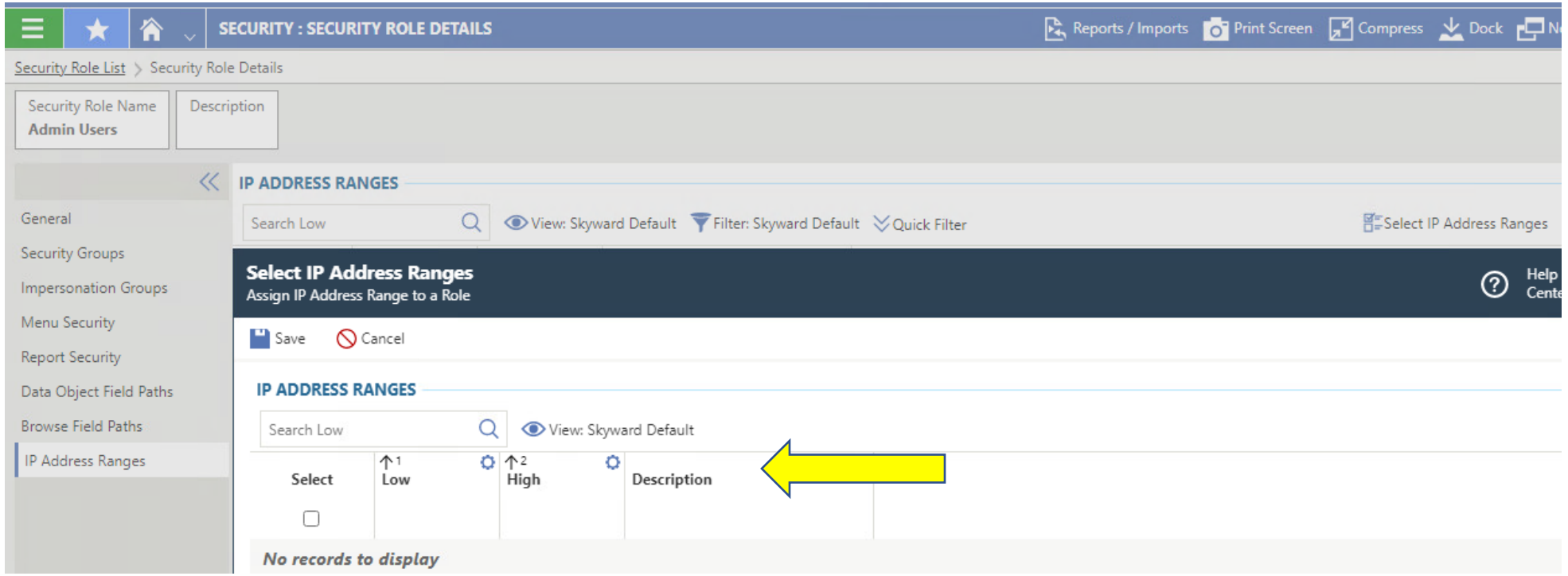
Select ☰ → Administrative Access → Security → Codes: IP Address Range



Non-routable addresses will also need to be entered; they are not assumed.

Qmlativ Security Roles

Select ☰ → Administrative Access → Security → Features: Security Role → Edit Security Role Name → IP Address Changes



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

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

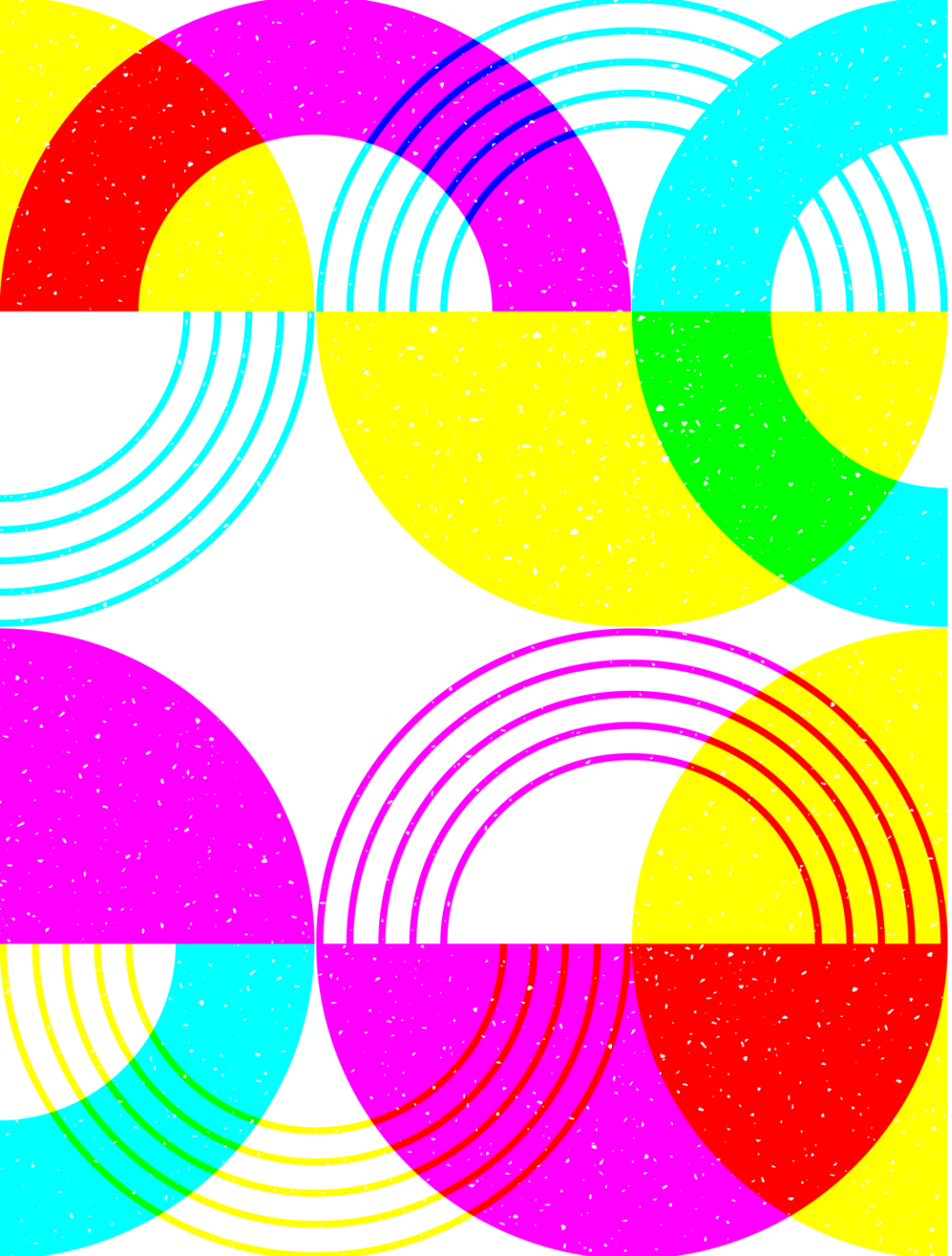
- Managed Services
- Database Tune-ups
- Remote Update Services
- System Admin Training

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!