Skyward Security – Best Practices

2019 User Group Conference

SKYWARD

Agenda

- Securing Data in Transit
- Best Security Practices
  - SMS 2.0
  - Qmlativ
- Network Considerations

Securing Data in Transit

Skyward supports the following encryption protocols to ensure all data is encrypted during data transfers

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

Transport Layer Security (TLS)

- Skyward fully supports TLS 1.1 / 1.2.
- TLS 1.0, SSL 2/3 are no longer considered secure.
- Windows Server OS controls what versions of TLS are available.
  - We recommend on-premises customers review their Windows Server TLS settings.
- IIS Crypto tool can be used to change 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

QuickSSL Premium SSL Certificates

- Security: domain control validation, up to 256-bit encryption, 2048-bit root
- Assurance: $500K USD warranty, GeoTrust dynamic True Site Seal Trustmark
- Convenience: most certificates issued in minutes, 1-2 year validity options
- 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

Secure LDAP

- LDAP Offers multiple Encrypted Protocols
  - (LDAPS, LDAP w/TLS, Kerberos)

- Encryption prevents Users & Passwords from being read by eavesdroppers.

- Verify that you are using a Secure LDAP configuration.

  - SMS 2.0 SSO / LDAP Launch Kit

  - Qmlativ SSO / LDAP Launch Kit

Secure Email (SMTP)

- SMTP Offers an Encrypted Protocol (TLS)
- Encryption prevents message from being read by eavesdroppers.
- Verify that you are using a Secure Email configuration.

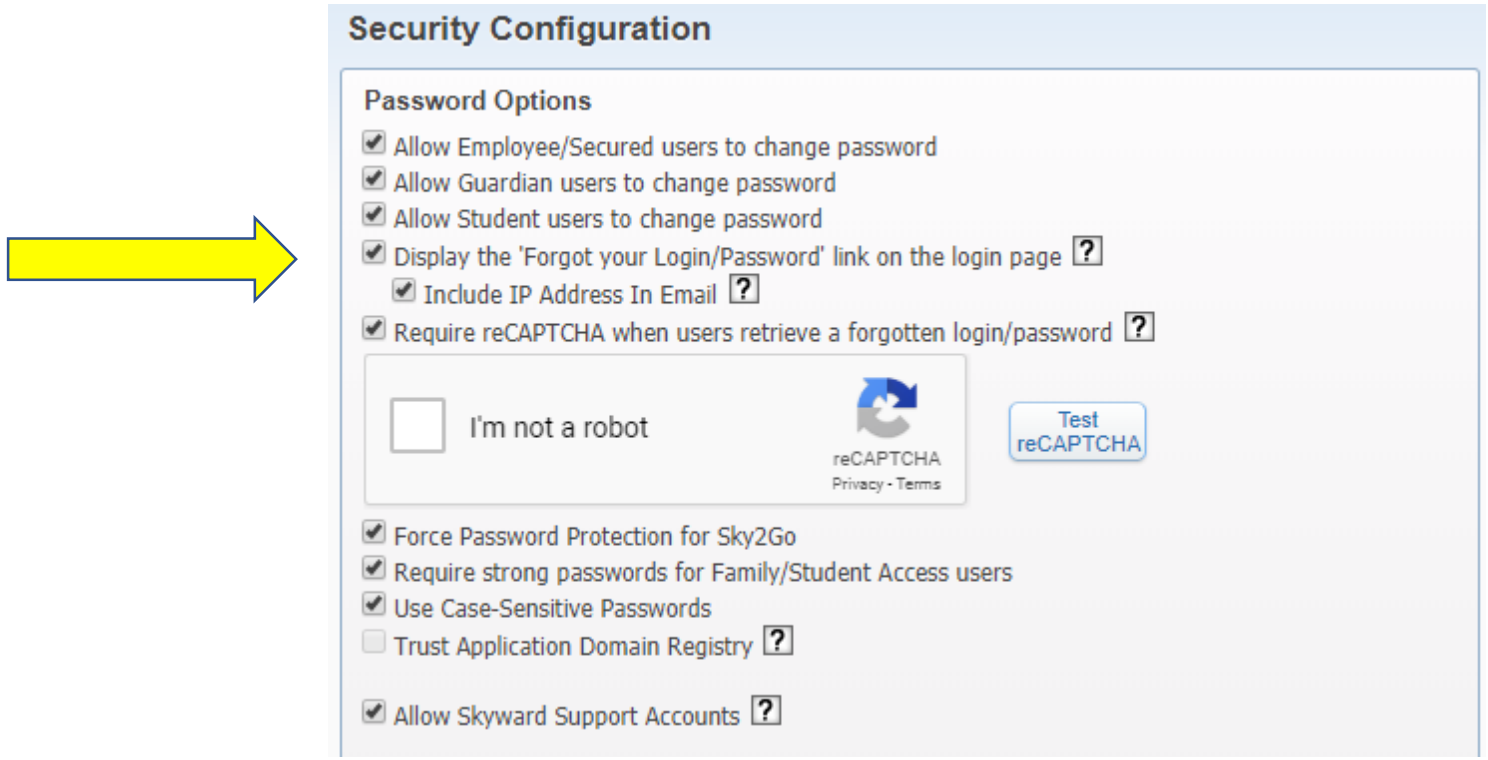
  - SMS 2.0 Email Launch Kit
  - Qmlativ Email Launch Kit

SMS 2.0 PaC Program Servers

- 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 Self Service Password Resets

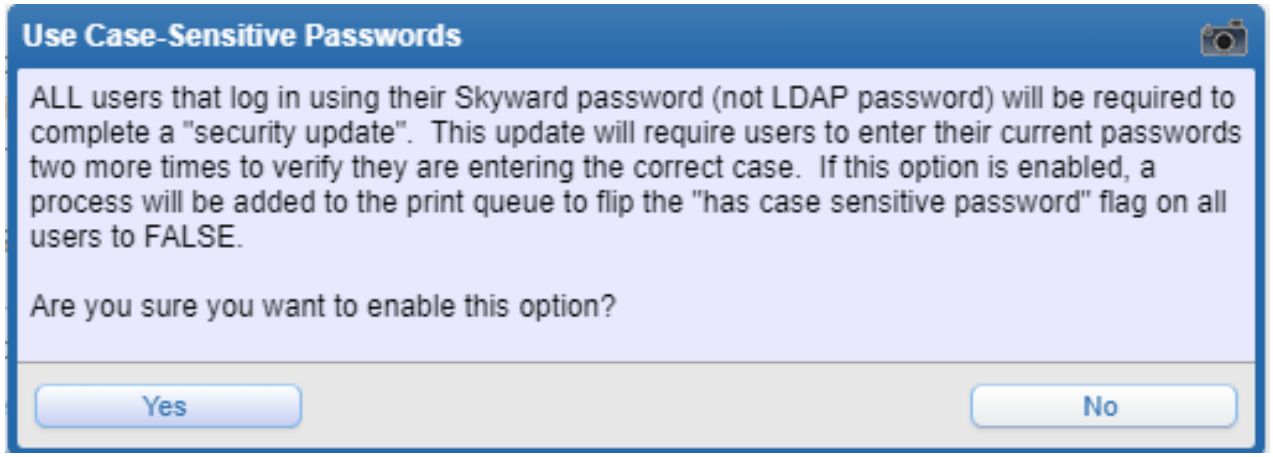
Product Setup → Contact Access → Security → Setup → Configuration → Security Configuration

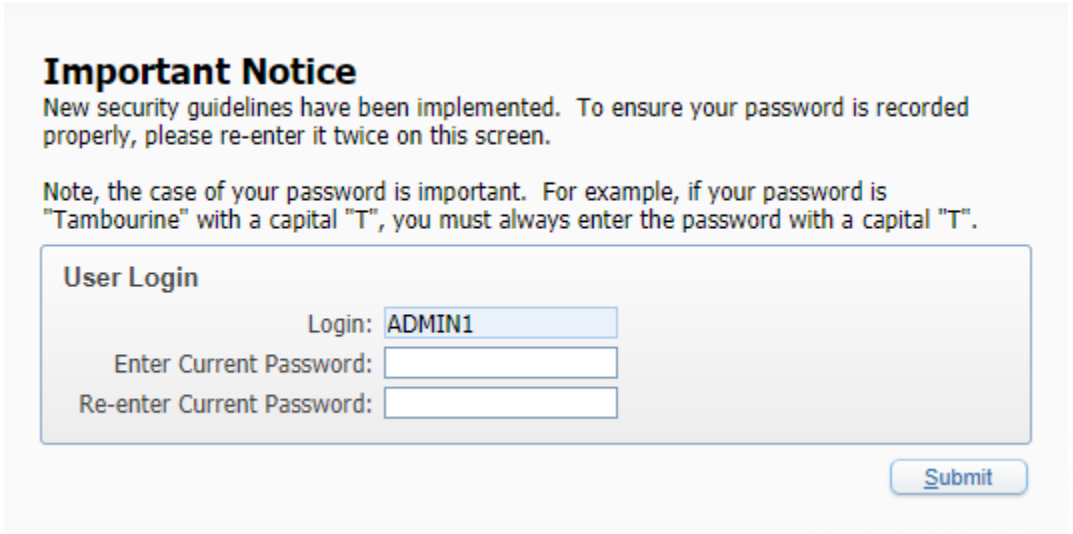


If using Self Service Password resets, Include the IP Address in the Email and require reCAPTCHA.

SMS 2.0 Use Case-Sensitive Passwords

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

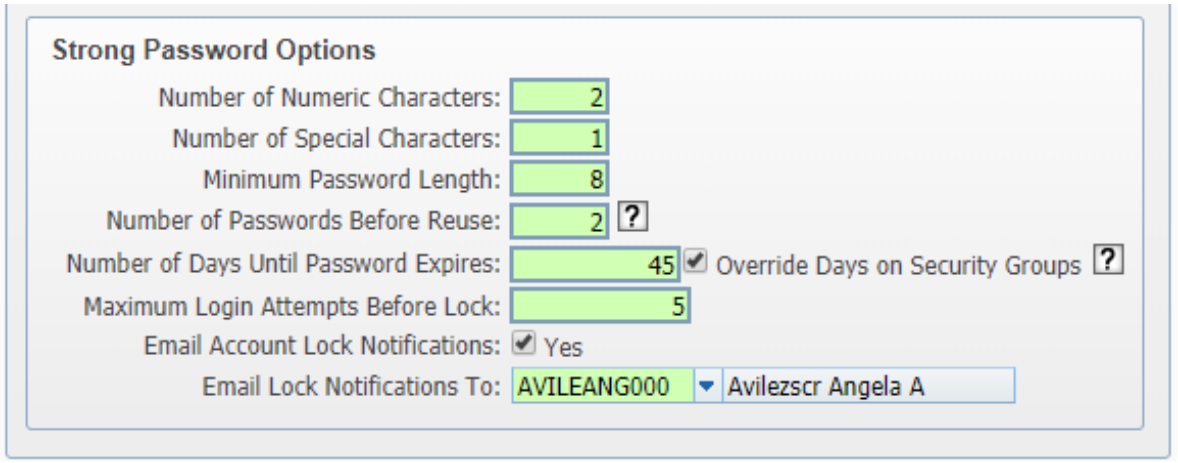


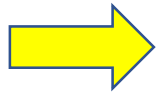


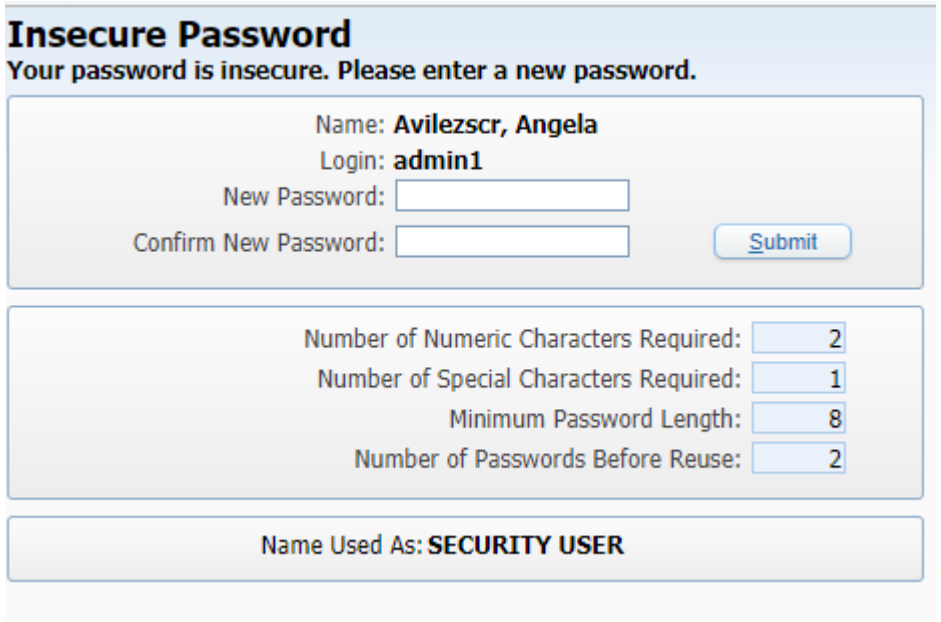
Yes – on their next login users will be prompted to enter password twice to create new case-sensitive password.

SMS 2.0 Strong Password Options

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



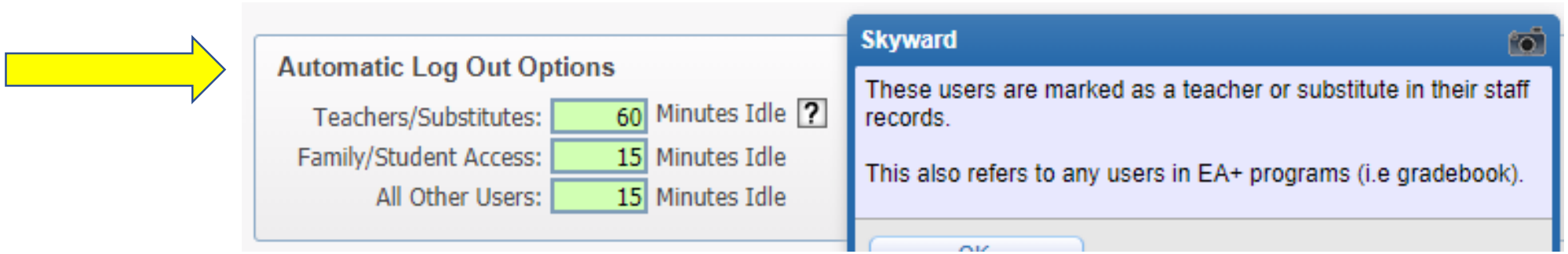




Users that do not meet the password requirements will be prompted to enter a new stronger password twice.

SMS 2.0 Automatic Logout Options

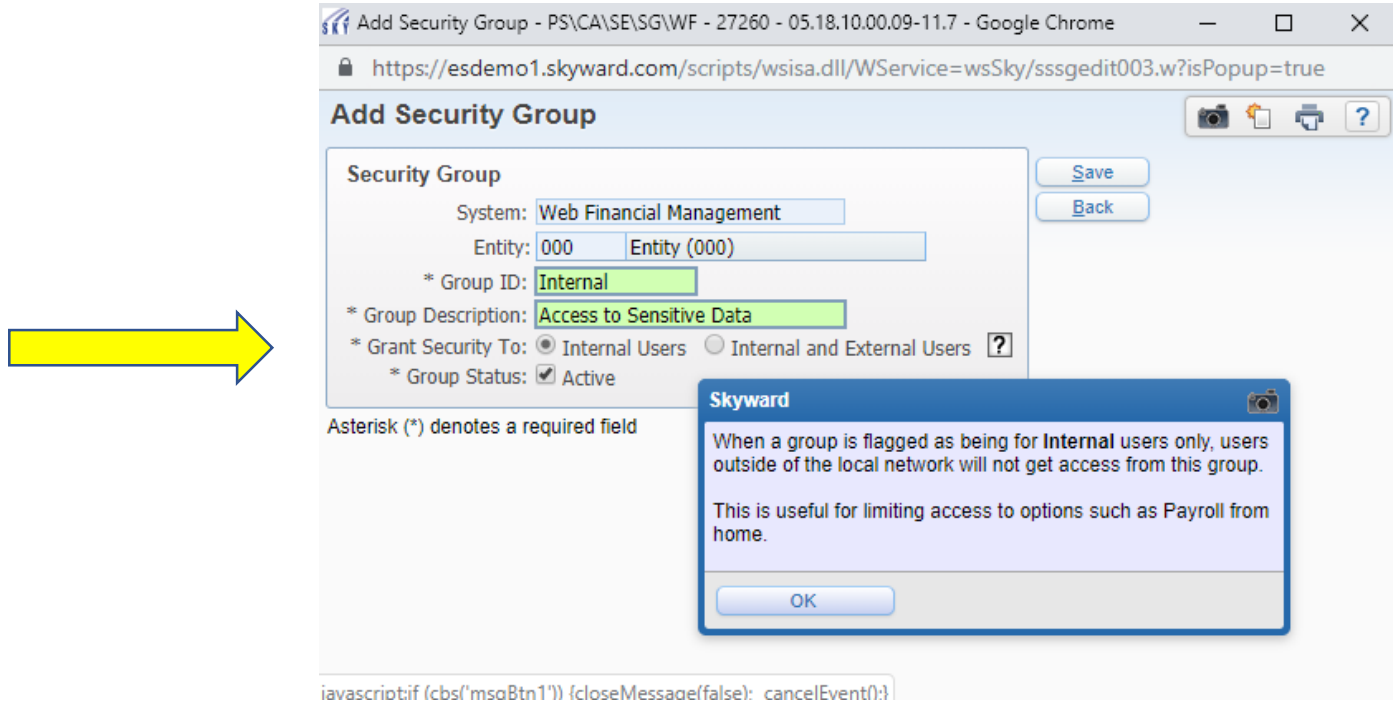
Product Setup → Contact Access → District Setup → Configuration → Web Configuration



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

SMS 2.0 Security Group IP Restrictions

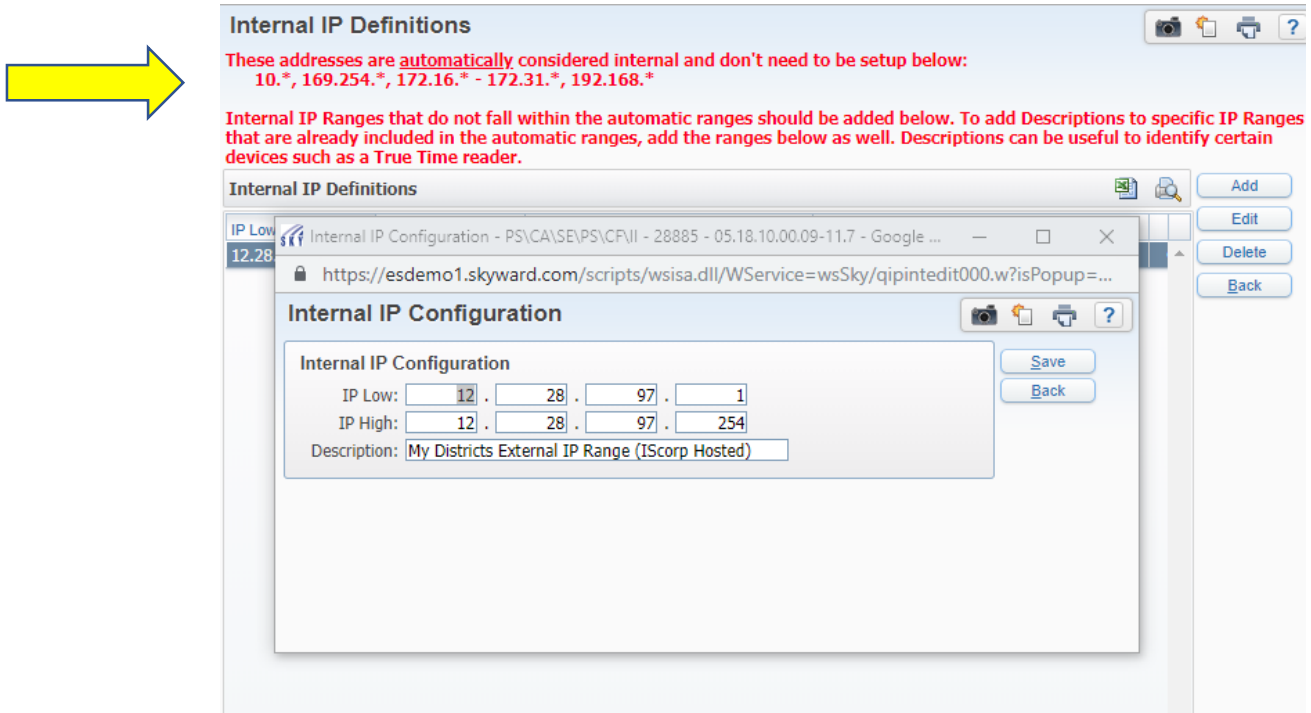
Product Setup → Contact Access → Security Groups



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

SMS 2.0 Security Group IP Restrictions

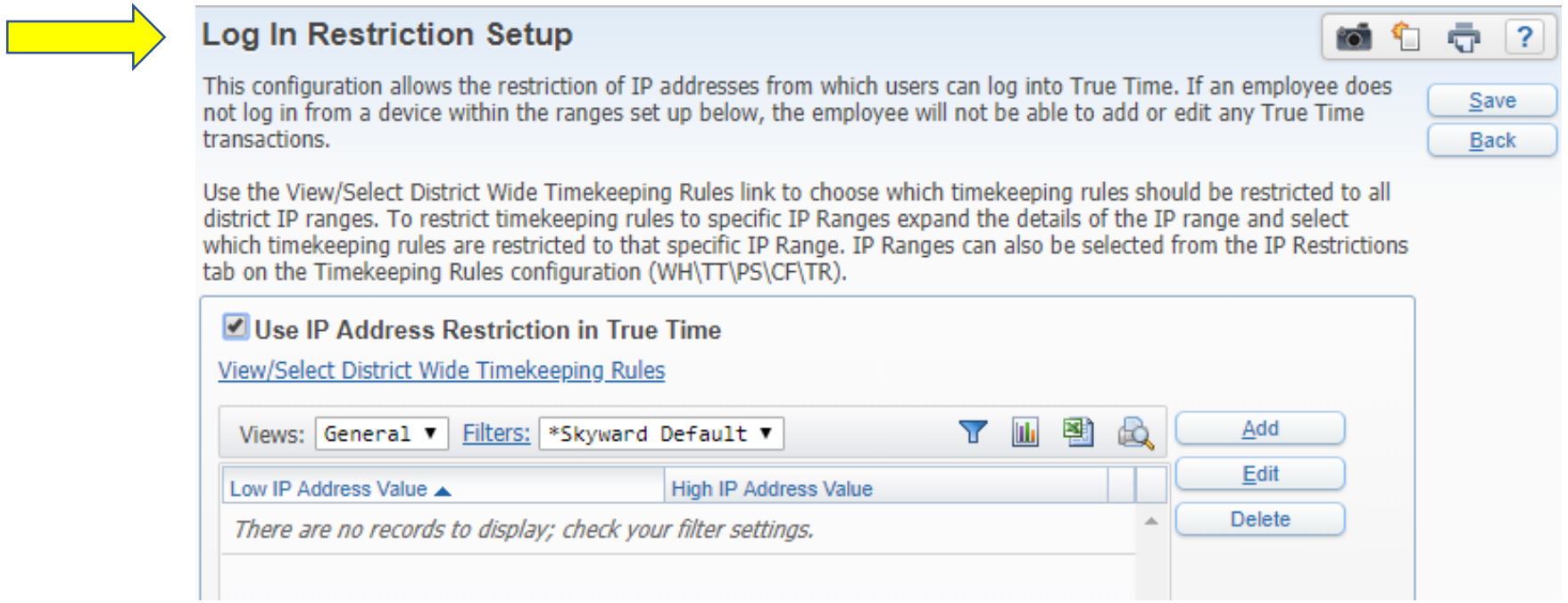
Product Setup → Contact Access → Security → Setup → Configuration → Internal IP Definitions



Additional IP Networks can be Defined (IP Based Restrictions)

SMS 2.0 TrueTime IP Restrictions

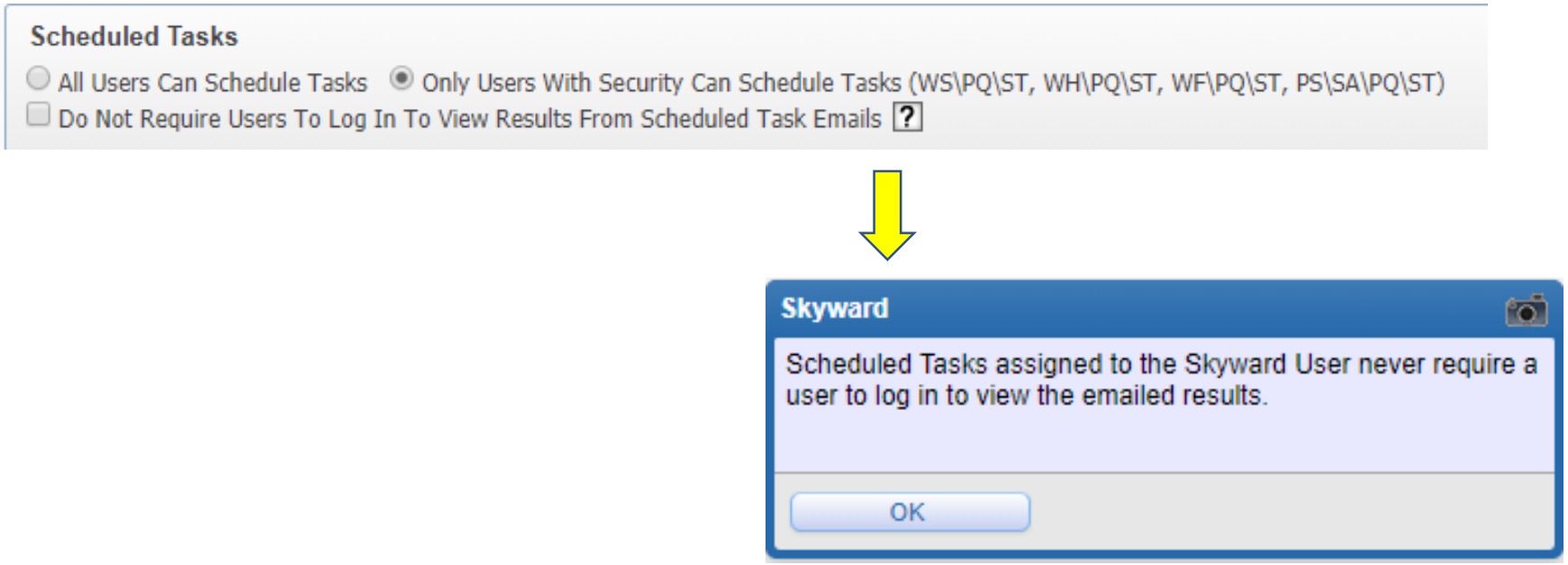
Product Setup → Human Resources → TrueTime → Configuration → Login Restriction Setup



Additional IP Networks can be defined (IP Based Restrictions)

SMS 2.0 Scheduled Task Emails

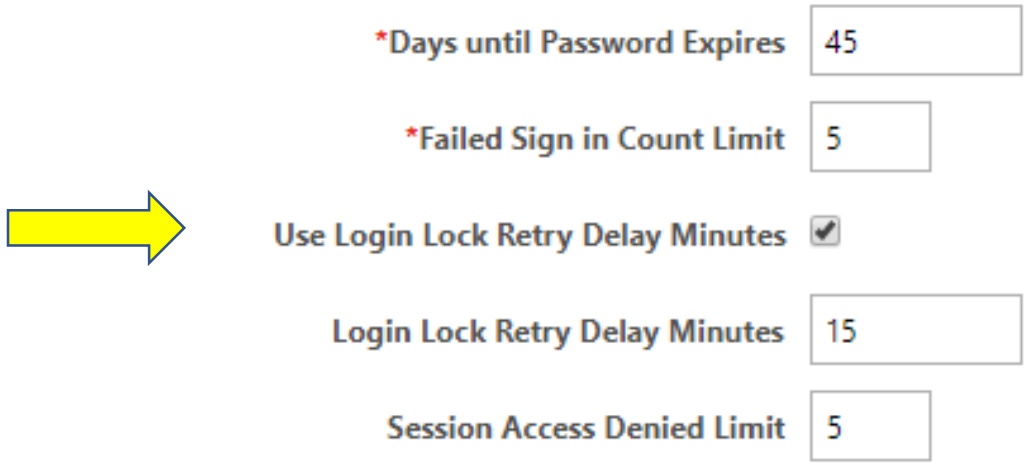
Product Setup → System Admin → District Print Queue→ Report Configuration



Require Users to Login to View Scheduled Task Emails

Qmlativ Login Policies

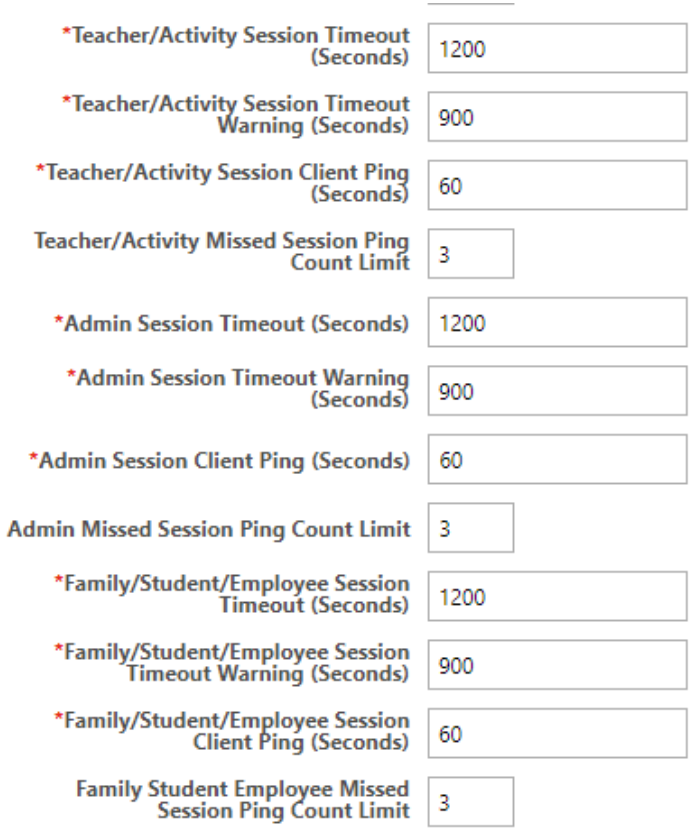
Select ☰ → Administrative Access → Security



Define System Wide Login Policies

Qmlativ Automatic Logout Options

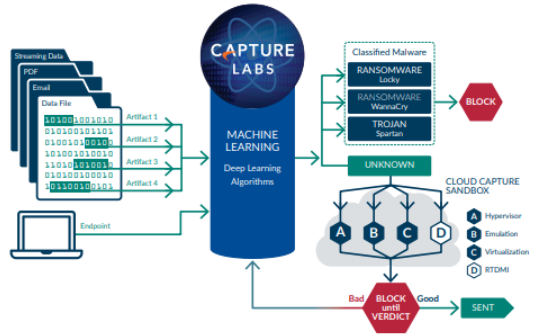
Select ☰ → Administrative Access → Security



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

Next Generation Firewalls

SONICWALL Advanced Gateway Security Suite



A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway

Deep Packet Inspection

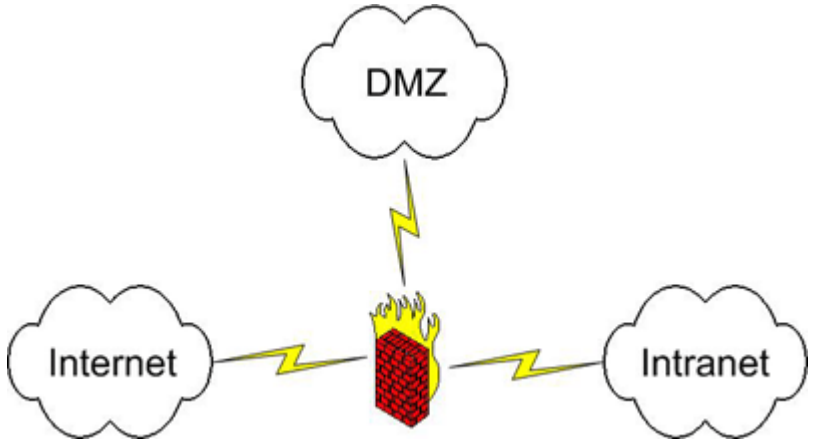
- Scans against multiple application types and protocols
- Protects against internal and external attacks and application vulnerabilities
- Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service subscription
- Content Filtering Service subscription
- 24x7 Support subscription

IDS and IPS - ……..

- IPS systems have advantages over intrusion detection systems (IDS)
- IPS is designed to sit inline with traffic flows and prevent attacks in real-time.
- IDS/IPS solutions have the ability to look at (decode) layer 7 protocols like HTTP, FTP, and SMTP.

- Discover and stop zero-day and other unknown attacks using**:**
  SonicWALL's Capture Advanced Threat Protection (ATP) Service subscription

DMZ Web Server Design



- Optimal Design for Security
- Reduces Internet facing Attack Surface
- SMS 2.0: Firewall Friendly DMZ Web Server Support
  - Use WebSpeed Messenger instead of Broker

Qmlativ: Firewall Friendly DMZ Web Server Support


Microsoft
GOLD CERTIFIED
Partner
PROGRESS
SOFTWARE
Unitrends
ISCorp
Integrated Systems Corporation
Cisco Systems
TEA
Texas Education Agency
Hewlett Packard
Enterprise
symantec.
SKYWARD
IT Services
SONICWALL
propalms
terminal services edition
GeoTrust
vmware
BARRACUDA
NETWORKS
MICRO FOCUS
Novell.
arcserve
VEEAM
Lightspeed Systems
Partners
TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

Thank you for attending!