



Skyward Security – Best Practices

2019 User Group Conference

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



Security Configuration

Password Options

- Allow Employee/Secured users to change password
- Allow Guardian users to change password
- Allow Student users to change password
- Display the 'Forgot your Login/Password' link on the login page [?](#)
- Include IP Address In Email [?](#)
- Require reCAPTCHA when users retrieve a forgotten login/password [?](#)

I'm not a robot  [Test reCAPTCHA](#)

reCAPTCHA
Privacy - Terms

- Force Password Protection for Sky2Go
- Require strong passwords for Family/Student Access users
- Use Case-Sensitive Passwords
- Trust Application Domain Registry [?](#)
- Allow Skyward Support Accounts [?](#)

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

Use Case-Sensitive Passwords



Use Case-Sensitive Passwords

ALL users that log in using their Skyward password (not LDAP password) will be required to complete a "security update". This update will require users to enter their current passwords two more times to verify they are entering the correct case. If this option is enabled, a process will be added to the print queue to flip the "has case sensitive password" flag on all users to FALSE.

Are you sure you want to enable this option?



Important Notice

New security guidelines have been implemented. To ensure your password is recorded properly, please re-enter it twice on this screen.

Note, the case of your password is important. For example, if your password is "Tambourine" with a capital "T", you must always enter the password with a capital "T".

User Login

Login:

Enter Current Password:

Re-enter Current Password:

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

Strong Password Options

Number of Numeric Characters:

Number of Special Characters:

Minimum Password Length:

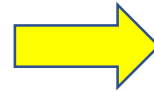
Number of Passwords Before Reuse: ?

Number of Days Until Password Expires: Override Days on Security Groups ?

Maximum Login Attempts Before Lock:

Email Account Lock Notifications: Yes

Email Lock Notifications To:



Insecure Password
Your password is insecure. Please enter a new password.

Name: **Avilezscr, Angela**
Login: **admin1**

New Password:

Confirm New Password:

Number of Numeric Characters Required:

Number of Special Characters Required:

Minimum Password Length:

Number of Passwords Before Reuse:

Name Used As: **SECURITY USER**

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



Automatic Log Out Options

Teachers/Substitutes:	<input type="text" value="60"/>	Minutes Idle	<input type="checkbox"/>
Family/Student Access:	<input type="text" value="15"/>	Minutes Idle	
All Other Users:	<input type="text" value="15"/>	Minutes Idle	

Skyward

These users are marked as a teacher or substitute in their staff records.

This also refers to any users in EA+ programs (i.e gradebook).

OK

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



Browser window: Add Security Group - PS\CA\SE\SG\WF - 27260 - 05.18.10.00.09-11.7 - Google Chrome
URL: https://esdemo1.skyward.com/scripts/wsisa.dll/WService=wsSky/sssgedit003.w?isPopup=true

Add Security Group

Security Group

System: Web Financial Management

Entity: 000 Entity (000)

* Group ID: Internal

* Group Description: Access to Sensitive Data

* Grant Security To: Internal Users Internal and External Users ?

* Group Status: Active

Asterisk (*) denotes a required field

Skyward

When a group is flagged as being for **Internal** users only, users outside of the local network will not get access from this group.

This is useful for limiting access to options such as Payroll from home.

OK

javascript:if (cbs('msoBtn1')) {closeMessage(false); cancelEvent();}

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

The screenshot shows the 'Internal IP Definitions' configuration page. At the top, it states: 'These addresses are automatically considered internal and don't need to be setup below: 10.*, 169.254.*, 172.16.* - 172.31.*, 192.168.*'. Below this, it says: 'Internal IP Ranges that do not fall within the automatic ranges should be added below. To add Descriptions to specific IP Ranges that are already included in the automatic ranges, add the ranges below as well. Descriptions can be useful to identify certain devices such as a True Time reader.' The main configuration area is titled 'Internal IP Configuration' and contains a form with the following fields: 'IP Low' (12 . 28 . 97 . 1), 'IP High' (12 . 28 . 97 . 254), and 'Description' (My Districts External IP Range (IScorp Hosted)). There are 'Save' and 'Back' buttons next to the form. On the right side of the page, there are 'Add', 'Edit', 'Delete', and 'Back' buttons. The browser address bar shows 'https://esdemo1.skyward.com/scripts/wsisadll/WSservice=wsSky/qipintedit000.w?isPopup=...'.

Internal IP Definitions

These addresses are **automatically** considered internal and don't need to be setup below:
10.*, 169.254.*, 172.16.* - 172.31.*, 192.168.*

Internal IP Ranges that do not fall within the automatic ranges should be added below. To add Descriptions to specific IP Ranges that are already included in the automatic ranges, add the ranges below as well. Descriptions can be useful to identify certain devices such as a True Time reader.

Internal IP Definitions

Internal IP Configuration

IP Low: 12 . 28 . 97 . 1
IP High: 12 . 28 . 97 . 254
Description: My Districts External IP Range (IScorp Hosted)

Save
Back

Add
Edit
Delete
Back

Additional IP Networks can be Defined (IP Based Restrictions)

SMS 2.0 TrueTime IP Restrictions

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



Log In Restriction Setup

This configuration allows the restriction of IP addresses from which users can log into True Time. If an employee does not log in from a device within the ranges set up below, the employee will not be able to add or edit any True Time transactions.

Use the [View/Select District Wide Timekeeping Rules](#) link to choose which timekeeping rules should be restricted to all district IP ranges. To restrict timekeeping rules to specific IP Ranges expand the details of the IP range and select which timekeeping rules are restricted to that specific IP Range. IP Ranges can also be selected from the IP Restrictions tab on the Timekeeping Rules configuration (WH\TT\PS\CF\TR).

Use IP Address Restriction in True Time

[View/Select District Wide Timekeeping Rules](#)

Views: General Filters: *Skyward Default

Low IP Address Value	High IP Address Value
There are no records to display; check your filter settings.	

Buttons: Add, Edit, Delete, Save, Back

Additional IP Networks can be defined (IP Based Restrictions)

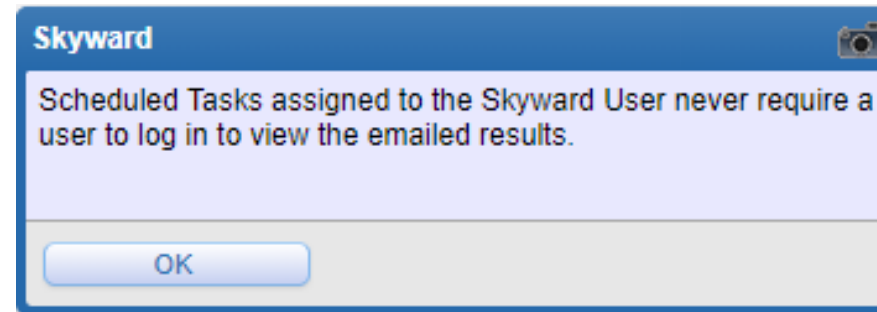
SMS 2.0 Scheduled Task Emails

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

Scheduled Tasks

All Users Can Schedule Tasks Only Users With Security Can Schedule Tasks (WS\PQ\ST, WH\PQ\ST, WF\PQ\ST, PS\SA\PQ\ST)

Do Not Require Users To Log In To View Results From Scheduled Task Emails [?](#)



Require Users to Login to View Scheduled Task Emails

Qmlativ Login Policies

Select  → Administrative Access → Security



*Days until Password Expires

*Failed Sign in Count Limit

Use Login Lock Retry Delay Minutes

Login Lock Retry Delay Minutes

Session Access Denied Limit

Define System Wide Login Policies

Qmlativ Automatic Logout Options

Select  → Administrative Access → Security



*Teacher/Activity Session Timeout (Seconds)	<input type="text" value="1200"/>
*Teacher/Activity Session Timeout Warning (Seconds)	<input type="text" value="900"/>
*Teacher/Activity Session Client Ping (Seconds)	<input type="text" value="60"/>
Teacher/Activity Missed Session Ping Count Limit	<input type="text" value="3"/>
*Admin Session Timeout (Seconds)	<input type="text" value="1200"/>
*Admin Session Timeout Warning (Seconds)	<input type="text" value="900"/>
*Admin Session Client Ping (Seconds)	<input type="text" value="60"/>
Admin Missed Session Ping Count Limit	<input type="text" value="3"/>
*Family/Student/Employee Session Timeout (Seconds)	<input type="text" value="1200"/>
*Family/Student/Employee Session Timeout Warning (Seconds)	<input type="text" value="900"/>
*Family/Student/Employee Session Client Ping (Seconds)	<input type="text" value="60"/>
Family Student Employee Missed Session Ping Count Limit	<input type="text" value="3"/>

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

Next Generation Firewalls

SONICWALL® Advanced Gateway Security Suite

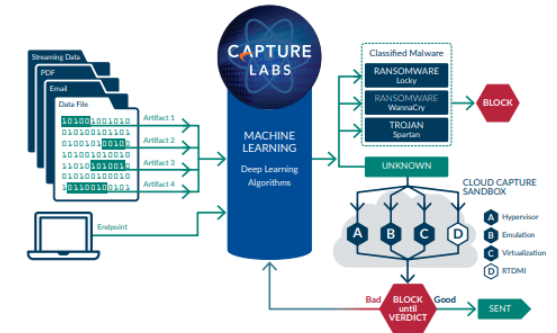
Deep Packet Inspection

- 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:

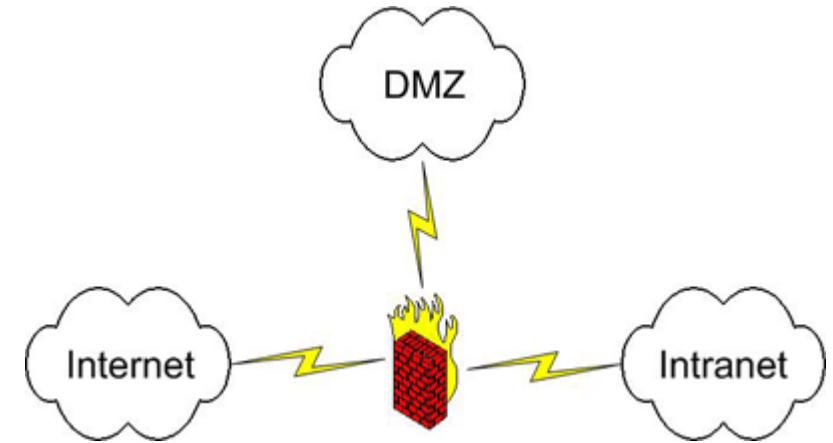
[SonicWALL's Capture Advanced Threat Protection \(ATP\) Service subscription](#)



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

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



Unitrends

Microsoft
GOLD CERTIFIED
Partner

PROGRESS
SOFTWARE

ISCORP
Integrated Systems Corporation

CISCO SYSTEMS

TEA
TEXAS EDUCATION AGENCY

symantec.

Hewlett Packard
Enterprise

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!