Skyward SMS 2.0
Email Launch Kit
Table of Contents

EMAIL CONFIGURATION – OVERVIEW ................................................................................................. 3

EMAIL SETUP FOR AN ON-PREMISE CUSTOMER ........................................................................... 4
   USE A DISTRICT OWNED SMTP SERVER .................................................................................. 5
   SETUP A VIRTUAL IIS SMTP SERVER ON AN ON-PREMISE SKYWARD SERVER ...................... 7

EMAIL SETUP FOR SECURE CLOUD COMPUTING (SCC) ISCORP CUSTOMERS .................................. 8
   WHAT IS AN SPF RECORD AND WHY IS IT REQUIRED? ............................................................. 11
   SPF RECORD EXAMPLES ........................................................................................................... 11
   USE A DISTRICT OWNED OR CLOUD PROVIDE SMTP SERVER ............................................ 12

EMAIL CONFIGURATION – ALL CUSTOMERS .................................................................................. 13
   EMAIL SERVER CONFIGURATION OPTIONS ............................................................................ 13
   MESSAGE HANDLING CONFIGURATION OPTIONS ................................................................ 14
   EMAIL SERVER CONFIGURATION: DEFAULT EMAIL CLIENT .................................................... 15

EMAIL TESTING AND TROUBLESHOOTING ................................................................................ 16
   EMAIL HISTORY ......................................................................................................................... 16
   ERROR EMAIL RETRY FEATURE ............................................................................................... 17
   EMAIL HISTORY CLEANUP ....................................................................................................... 18

USING CLOUD-BASED EMAIL SERVICES: GMAIL / OFFICE 365 .................................................. 19

EMAIL SERVER CONFIGURATION: TUTORIALS .......................................................................... 20
   INSTALL IIS SMTP MAIL SERVER ROLE ................................................................................ 20
   CONFIGURE IIS SMTP MAIL SERVER ROLE .......................................................................... 20
   MICROSOFT EXCHANGE CONFIGURATION ........................................................................... 20
   NOVELL GROUPWISE CONFIGURATION ............................................................................. 20

TROUBLESHOOTING EMAIL ........................................................................................................ 21
Email Configuration – Overview

Welcome to the SMS 2.0 Email Launch Kit. All customers can utilize email processing in the SMS 2.0 product suites regardless of their how the product is hosted. Skyward IT Services or the hosting provider is available for assistance to configure the Skyward system for email processing.

- The Skyward Business, Student Management and School Management product suites are identical in the way email is configured and processed.
- Skyward sends outbound emails and never receives inbound emails.
- The email server can be most third-party email systems that have a Simple Mail Transfer Protocol (SMTP) relay setup to allow Skyward to relay emails.
- When Skyward sends emails the Skyward system acts as an SMTP Email client.
- The Monolith CAS service is responsible for ‘sending’ the emails to the Email Server identified in the Skyward software. Only on-premise customers have access to Monolith and the CAS Service.
- Email History is a great tool for viewing the status, testing, and diagnosing email issues.

Quick Start links:
- Jump to: Email Setup for Secure Cloud Computing (SCC) ISCorp Customers
- Jump to: Email Setup for an On-Premise Customers

Contact Skyward if you need assistance by calling 1.800.236.0001 or creating an IT Services support request at Skyward Support Center
Email Setup for an On-Premise Customer

Skyward suggests the following email solutions:

- Use a District owned SMTP server for relaying the Skyward email onto recipients.
- If the district utilizes Office365, it is not supported because limitations imposed by Office365 cannot be fixed by Skyward. Mail delivery using Office365 will be sporadic and unreliable.
- If the district utilizes Gmail, it is supported as an email relay with the updated sending limitations allowed from a Google domain.
- Unlimited cloud-based services are available for a fee; example http://www.smtp.com) that can be used as the Email processing server in Skyward.
- If you do not have a district owned SMTP server or suitable Cloud Email Provider, you can setup a virtual IIS SMTP service on an on-premise server to use as the email processing server in Skyward.

Quick Start links:
- Jump to: Use a District Owned SMTP Server
- Jump to: Using Cloud-based email services: Gmail / Office 365
- Jump to: Setup a virtual IIS SMTP server on an on-premise Skyward server
Use a District Owned SMTP server

1. Use a District Owned SMTP server

On-premise customers that have their own SMTP Server will need to configure their Email (SMTP) Server security to accept inbound email from the Skyward CAS/Database server. The SMTP server will deliver the emails to the recipients.

2. Monolith Settings: Email Sending (On-Premise)

- Turn on Email processing in Monolith by editing the Monolith AppServer by starting Monolith, Control Center -> Configure …AppServers -> asxxxMon -> Edit -> Check Send Emails checkbox in CAS Connections area -> Save.
3. Monolith Settings: Email Sending Thread(s) (On-Premise)

- To speed up the sending of emails by the CAS you can increase the number of processing threads. Four (4) processing threads is typically enough. The Send Email checkbox must be checked for the Processing Threads: file to display.

4. Configure General Email Settings

Jump to: Email Configuration – All Customers.
Setup a virtual IIS SMTP server on an on-premise Skyward server

1. Setup a virtual IIS SMTP server on an on-premise Skyward server

   A common free solution is to install the IIS SMTP relay on any Windows server. The Email Relay Setup section of this launch kit includes Support Knowledgebase links that displays how to install the IIS SMTP relay. However, the IIS SMTP relay does not report to Skyward the status of any processed emails. To explain further, a Skyward email is created within the product, the CAS Service processes the email send, the Email History listing shows a successful send, but the IIS SMTP relay may not have been successful in its send process and this unsuccessful send does not get reported to the email in Email History listing.

   When using an SMTP relay, the SMTP server’s public address must be added to the Sender Policy Framework (SPF) configuration and you must create a reverse DNS entry. Failing to complete the SPF/DNS record setup properly will result in the Skyward emails being blocked or classified as spoofing or SPAM messages. Once an SMTP relay is configured, enter the ‘Email Server’ info in the Server Information Configuration page.
Email Setup for Secure Cloud Computing (SCC) ISCorp Customers

ISCorp and Skyward suggest the following email solutions:

- ISCorp Cloud Hosted customers that do not have their own Email server can utilize a free SMTP service provided by ISCorp.
- If preferred the district can use a District owned SMTP server.
- If the district utilizes Office365, it is not supported because limitations imposed by Office365 cannot be fixed by Skyward. Mail delivery using Office365 will be sporadic and unreliable.
- If the district utilizes Gmail, it is supported as an email relay with the updated sending limitations allowed from a Google domain.
- Unlimited cloud-based services are available for a fee; example http://www.smtp.com) that can be used as the Email processing server in Skyward.

Quick Start:
- Jump to: Use the ISCorp SMTP Server (Preferred)
- Jump to: Use a District Owned SMTP Server
1. **Use the ISCorp SMTP Server (Preferred)**

   ISCorp will provide the SMTP server for sending emails for the Secure Cloud Hosted (SCC) SMS 2.0 Student, Business, or School Management Suite(s). To ensure emails delivered by the ISCorp email server are not rejected or classified as Junk Mail / SPAM your district must create or modify your **Sender Policy Framework (SPF) Domain Name System (DNS)** record. SPF records are typically created and maintained by your **Internet Service Provider (ISP)**.

   Confused about SPF records? Read: [What is an SPF Record and why is it required?](#)

2. **Create or Modify your SPF Record**

   Please review the SPF information provided below if you are not familiar with this step. The IP addresses that should be added to your SPF record are:

   ISCorp Email source address - Mequon, WI - 66.195.143.26
   ISCorp Email source address - Dallas, TX - 8.12.72.20

   **Notes:**
   *Adding both ISCorp Email source addresses is recommended for Disaster Recovery purposes.*

   *If the Skyward Web URL starts “https://skyward.iscorp.com” Skyward is hosted in the Mequon, WI Datacenter and emails are processed from this Datacenter.*

   *If the Skyward Web URL starts “https://skyward10.iscorp.com” Skyward is hosted in the Dallas, TX Datacenter and emails are processed from this Datacenter.*
3. Create a support request

Once your SPF record is created submit a support request to Skyward or ISCorp to complete the SMS 2.0 email setup. ISCorp Support will verify the SPF record, configure your SMS 2.0 Email settings, and verify by sending a test email message.

Create a support request by calling 1.800.236.0001 or creating an IT Services support request at Skyward Support Center or at ISCorp Helpdesk.

Once ISCorp completes the setup, then move on to next step.

4. Configure General Email Settings

ISCorp will configure the SMTP Server Information in SMS 2.0, so do not change the SMTP server fields. There are additional Email configuration options available, please review all Email Configuration options as the next step.

Jump to: Email Configuration – All Customers.
What is an SPF Record and why is it required?

An SPF Record allows an email server that is receiving your email a way to verify the email was originated from your server. Without an SPF record email delivery from your SMS 2.0 system will be unreliable.

The SPF Record is typically hosted by your ISP and can contain references to multiple sites. Many ISPs have user friendly management interfaces that give the domain name owner the ability to manage their own SPF Record. When creating an SPF Record it is important to find out if you already have an SPF record or if you need to create a new one. A site can be checked for an existing SPF record using a tool like MX toolbox: https://mxtoolbox.com/spf.aspx

If you already have an SPF record, then it needs to be modified with any new information. Most DNS vendors do not allow the original SPF record to be modified, only overwritten, so it's important to check for an original SPF record, copy it, add to it, and then resubmit it to the ISP.

An SPF record is of the form: "v=spf1 mx a include: <DN> ~all" where DN is the Domain Name or outside facing IP of an email site (E.g., Exchange, SMTP, Gmail, Office365, etc.). In instances of multiple providers, it might look something like "v=spf1 mx a include: <DN> <DN> <DN>~all", where each <DN> is separated by spaces.

If you are unfamiliar with SPF Records the following websites and examples will help you.

**SPF Record Examples**

Example of simple Google Specific SPF record:
```
v=spf1 a:school.k12.state.us ip4:66.195.143.26 ip4:8.12.72.20
include:_spf.google.com ~all
```
Reference: https://support.google.com/a/answer/178723?hl=en&ref_topic=2759192

Example of Simple Office 365 SPF record:
```
v=spf1 a:school.k12.state.us ip4:66.195.143.26 ip4:8.12.72.20
include:spf.protection.outlook.com ~all
```

SPF Wizard to help with generating properly formatted records:
http://www.spfwizard.net/
Use a District owned or Cloud Provide SMTP server

ISCorp - SCC hosted customers that choose to use their own SMTP Server will need to configure their Email (SMTP) Server security to accept inbound email from the ISCorp external IP Address(s) to allow the emails to transfer.

1. Configure the District Owned SMTP Server

There are two options:

1. Configure the District Owned SMTP Server to Allow Email from ISCorp by allowing the IP Address using anonymous connections.

   **SCC-Hosted ISCorp customer adds:**
   - ISCorp Mequon, WI - 66.195.143.90
   - ISCorp Dallas, TX - 8.12.72.20

2. Configure Skyward to connect using SMTP authentication. The SMTP Username and Password will need be entered in the next step.

There are additional Email configuration options available, please review all Email Configuration options as the next step.

Quick Start:
- Jump to: Email Configuration – All Customers.
Email Configuration – All Customers

Email Setup is configured by navigating to Product Setup -> Skyward Contact Access -> District Setup -> Configuration -> Server Information Configuration.

Email Server Configuration Options

- **Email Server**: Enter the Email Server host name or IP address that Skyward will use to forward/relay the emails generated by Skyward software. The Email Server can be any third-party email system/service that has a Simple Mail Transfer Protocol (SMTP) relay setup to allow Skyward to relay emails. If you are using a Cloud Email provider also review the Gmail / Office 365 configuration.

- **Port**: Enter the Email Server Port used to connect to the SMTP server. The default SMTP port is 25.

- **User/Password**: If the Email server needs SMTP authentication, the username/password for the Email From address will be entered. If left blank, Skyward will attempt to make an anonymous SMTP connection to email server.

- **Enable SSL/TLS**: Enables Skyward as an SSL/TLS SMTP Client.

- **Email From**: Enter the preferred district Email From address. This address is used on automated email processes or when an email is sent from a non-district email address.

- **Do Not Reply Email**: The district should enter the preferred Do Not Reply Email address. This optional address is used for automated email processes.

- **Additional Email Domains**: This field allows you to specify additional email domains that will be considered as district email addresses and will be used by the Replies option on this screen.
  - Specify additional email domains as a list separating each by a comma schooldistrict1.edu,schooldistrict2.com,schooldistrict3.org
Message Handling Configuration Options

- **Allow Replies to District Emails**: When an email is sent from a district email address, the email’s From address will be the sender's email address. When an email is sent from a non-district email address, the From address will always be the Email From value and the Reply To address will always be the sender's email address.

- **Do Not Allow Replies to District Emails**: When an email is sent from a district email address, the From address and the Reply To address will be the Do Not Reply Email value, if configured, or else it will be the Email From.

- **Set the behavior of Emails sent to multiple recipients**: Choose either the Send Separate E-Mails to all TO Recipients or Send Single Email radio button.
  - **Send Single Email**: A single email will be sent to all recipients using the Blind Carbon Copy (BCC) email field. This prevents the recipients from viewing the email addresses of the other recipients.
  - **Send Separate E-mails to all TO Recipients**: One email will be generated for each recipient.

- **Suppress Email Footer**: Suppresses the default email footer. The default email footer contains district specific information.

- **Allow Users to Unsubscribe from Mass Emails**: If enabled a link will be added to the bottom of mass emails that will allow users to unsubscribe from the eligible emails. Users will be able to manage which emails they have unsubscribed from within their account screens.
  - This option will apply to the following email types:
    - Any email listed in Automated Emails
    - Family Access Progress Reports
    - Family Access Grading Notifications
    - Family Access Attendance Notifications
    - Family Access Food Service Low Balance Notifications

- **Send Notification Email if Emails Error**: Sends an email notification to the value entered in the Send To field that alerts Email Address recipient of email failures. Multiple Email addresses may be added, each separated by a comma. Please note that if the email server is misconfigured or not functioning correctly the email alerts may not be received.
Email Server Configuration: Default Email Client

The Skyward Internal Email Client feature is configured by navigating to Product Setup -> Skyward Contact Access -> District Setup -> Configuration -> Web Configuration.

- Make Email Links Open Skyward Email Program Instead of External Program
  - Always send a copy to sender for:  □ Employees  □ Secured Users  □ Teachers

When a Skyward user sends/opens an email the Skyward program uses either the workstation’s locally installed email client or the Skyward internal email ‘client’ program. If using a Web email client, you must enable the Skyward email ‘client’ program.
Email Testing and Troubleshooting

Email History

The Email History screen is viewed by navigating to System Administration -> System Administration -> Email History.

The Email History shows all the emails that were generated by the Skyward software. Also shown is the Status results of each email as it was processed by the Skyward software. The CAS Service is what processes the emails when sending to the Email Server. The five statuses are,

- **Unsent**: The email is waiting to be processed by Skyward. If emails are in Unsent status, restart the CAS Service.
- **Pending**: The email is in a ‘holding’ pattern as it moves from the Skyward system to the email system.
- **Sent**: The email processed successfully from the Skyward system to the Email server. Now it is up to the email server to relay/send the email to the end recipient.
- **Opt-Out**: The end user chose to Opt-out of receiving this email.
- **Error**: The email when processed by the Skyward system was not successful. Choose the arrow symbol to the left of the email to view the Error message/reason as to why the email ended in error.
Error Email Retry Feature

Skyward has added an email retry feature to the Skyward email system (CAS Service). This email retry service will allow the erred emails to be sent again later.

Erroneous emails will be retried after 2/4/8/24/48 hours in that sequence if the error from the email server contains one of the following error numbers. A total of 6 tries to send an Error email. The retry count will be listed in the Email History listing.

- 4.5.0 Mailbox Unavailable
- 5.5.1 User Not local or invalid address
- 5.4.5 Daily sending quota exceeded
- 4.7.0 Service not available
- 4.4.2 Message submission rate for this client has exceeded the configured limit (Common for Office 365
- Failure Sending Mail
Email History Cleanup

Emails processed from the SMS 2.0 database will remain in database indefinitely unless you purge them from the database. If a purge has never been run and you have been a customer for 15 years, then 15 years of emails remain in the database. Purge processes can be setup for all statuses of emails, Error, Pending, Sent and Unsent.

1. Navigate to PS\SA\SA\EH -> Choose Purge Emails button.
2. Select the ‘status type’ checkbox(es) to choose what emails to purge.
3. Select by date range and enter the date range desired or by date and enter the number of days to keep.
4. Click Run to purge the emails.

Some customers set By Day, run the task once and then set as a Scheduled Task to maintain xx of days of emails in the Email History listing.
Using Cloud-based email services: Gmail / Office 365

Many districts have moved to cloud email systems; Gmail or Office 365.

Office365 has not been proven as a reliable SMTP service for Skyward due to the vendors limitations. Skyward does not recommend using Office365 as an email relay service in Skyward. There are severe limitations imposed by Microsoft when using Office365.


Gmail can be a reliable SMTP service when properly configured. Please follow the links and settings listed below closely while configuring Gmail relay. If desired, Gmail customers can also apply G-Suite email security, advanced Gmail settings and comprehensive mail storage to outgoing messages.

2. Use this link to display the Google steps for configuring the Gmail SMTP Relay
   https://support.google.com/a/answer/2956491?hl=en. The Google SMTP Relay Allowed Senders should be set to “Only addresses in my domains”.

3. The public ip address(es) need to be added to the Gmail SMTP Relay configuration.
   SCC-Hosted ISCorp customer adds:
   - ISCorp Mequon, WI - 66.195.143.90
   - ISCorp Dallas, TX - 8.12.72.20

   On-Premise customer adds:
   - Skyward Server CAS public ip address (Typically the Database Server)

4. In the Skyward Email Server Configuration enter the Google SMTP server: smtp-relay.gmail.com and Port 587, and enable SSL/TLS. Do NOT enter a user or password in the Email Server Configuration section. If you enter a user and password to authenticate it will then limit the number of relaying emails by user instead of by domain and email delivery will be unreliable.

   There are additional Email configuration options available, please review all Email Configuration options as the next step.

Quick Start:
- Jump to: Email Configuration – All Customers.
**Email Server Configuration: Tutorials**

**Install IIS SMTP Mail Server Role**

How do I install the IIS SMTP Mail Server Role on W2019/2016/2012?

**Configure IIS SMTP Mail Server Role**

How do I configure the IIS SMTP Mail Server Role on W2019/2016/2012?

**Microsoft Exchange Configuration**

How do I configure Exchange 2013 for SMTP relay?

**Novell GroupWise Configuration**

How do I configure GroupWise for SMTP email relay?

How do I configure GroupWise to relay email for ISCorp?
Troubleshooting Email

- **Emails History:** The Email History listing can assist in determining what status the emails are in. Click “+” to the left of the email messages to view errors to aide in troubleshooting SMTP issues. The Email History Listing options available to Resend or send a Test Email.

- **Emails in Unsent Status:** If you host the Skyward servers and need to restart your Skyward Email System, start Windows Service. Locate the CAS Service (SkyStuCASv2, SkyFinCASv2, SkyCASv2) and stop/start the CAS Service.

- **Emails still in Unsent Status:** If the emails remain in Unsent status, stop the CAS service; Start Open Edge Explorer, stop/start the Monolith AppServer (asStuMon, asFinMon, asSkyMon), then start the CAS Service.

- **Emails are in Unsent status and for an ISCorp or Managed Site:** Please enter a Service Call for assistance to Skyward IT Services at 1.800.236.0001 or using Skyward Support Center.

- **Email in Sent status but end recipient did not receive the email:** You would want to review the logs of the SMTP Server to verify if the email arrived at the SMTP server.

- **Verify CAS AppServer Configuration in Monolith:** If emails are not attempting to send verify the CAS AppServer has the Send Emails checkbox checked in the Monolith Control Center and all AppServers are connected and active. If the CAS AppServer is not configured to send emails all emails in Email History will remain in an Unsent Status.

- **Email in Error Status:** Look at the reason for the Error status, if Unable to Relay is listed, then you need to review the section titled, Email Server Configuration: Tutorials. The email server is not accepting the emails from the Skyward CAS Service, so they are not being relayed onto the recipients.