

Contents

Introduction	1
Sendio User Roles	1
Documentation	1
Conventions in the Manual.....	2
SECTION 1: Concepts and Definitions	3
SECTION 2: Logging in to Sendio	5
SECTION 3: Sendio User and Administrator UI	6
User UI	6
Adding Administrative Rights to a User Account.....	7
Administrative UI	8
Message Icons.....	9
Virus	9
Bad IP Reputation	9
Mailing List.....	9
Spam	9
Attachment	10
SECTION 4: System Pages.....	11
System > Options	11
Integrity Services.....	12
Response Control	14
Deliver Status Notifications (DSN)	16
Message Journaling.....	16
System > Inbound Control	18
General.....	18
Attachment Control	19
Address Validation	19
Sender IP Address	20
Anti-Virus	20
Zero-Hour	21
Spam	21
Bulk	21

Anti-Spoofing	21
DKIM Inbound	22
SPF	22
DMARC	23
System > Outbound Control	24
General.....	24
Attachment Control	24
Address Validation	24
Anti-Virus	25
DKIM Outbound	25
System > Contacts.....	26
Creating a New Contact	26
Updating a System Contact.....	28
Changing the View of the Contacts Page	28
Contact Search	28
Import System Contacts.....	28
Export All Contacts.....	29
System > Exemptions	29
Create Server Recon (Silverlisting) Exemption.....	30
Create SPF Exemption.....	30
Create DKIM Exemption.....	31
Create DKIM Exemption.....	31
Create Spam Exemption.....	32
System > SSL.....	33
SECTION 5: Global Views Pages	35
SECTION 6: Domains	37
Creating A New Domain.....	37
Domain Level Configuration	38
Domain Contacts.....	39
DKIM Signing	39
Steps to enable DKIM signing	40
SECTION 7: Accounts Page	41

SECTION 8: Addresses Page	43
SECTION 9: Logs	44
SECTION 10: Queue Summary	45
Clicking on Accept or Drop icon in Queue Summary Email	46
Accept Button	47
Drop Button	47
Clicking on Message from Queue Summary Email	47
Message View	48
History	48
Original	48
Accept	49
Add Sender	49
Drop	49
Drop Sender	50
Delete	50
SECTION 11: DKIM Primer	51
SECTION 12: Messaging Interaction	53
SECTION 13: System Email Messages	55
Maintenance Release Notifications	55
SECTION 14: SAV Messages	59

Introduction

The decision to incorporate Sendio into your communications environment is going to dramatically reduce the administrative overhead of managing email security and result in very happy end users who receive all their legitimate email and no junk.

Sendio User Roles

Conceptually, there are two “classes” of Sendio users:

- End-users (simply called **Users** in this manual) are individuals whose email inboxes are protected by Sendio. For each protected email account, there is a corresponding “account” on Sendio that is accessible via a Web interface. The Sendio **User** web interface is described in the *Sendio User Guide*.
- **Administrators** are individuals that install, configure, and maintain Sendio systems. When an **Administrator** logs in to the Sendio Web interface, they have an additional functionality that allows them to access the system administrative configuration features.

Documentation

Documentation for Sendio is organized into several different manuals and guides. These are summarized below. These can all be accessed on the Sendio website: <https://sendio.com/support/documentation-and-support-tools/>

Administration Manual

This Document. It describes the functionality of all Sendio features and discusses configuration options and trade-offs. Intended for Administrators.

User Guide

Describes the features and functionality of the Sendio web interface for the End-user. Intended for Users.

Backup & Restore Guide

A checklist of activities to support the implementation of Sendio in any network. It is focused on network details, Corporate Policy considerations and End-user notification. Intended for Administrators.

Quick Start Guide – Sendio Hosted

A checklist of activities to incorporate and configure Sendio’s hosted solution into your corporate email infrastructure. It covers firewall settings, directory services and routing options. Intended for Administrators.

Sendio and Office 365 Integration

Configuration guide to enable email routing to and from Office 365 with Sendio. Intended for Administrators.

Azure Active Directory Setup in Sendio

Configuration guide to connect Sendio with your Azure Active Directory for account creation and user password authentication. Intended for Administrators.

Email Continuity Administration Manual

Configuration guide to configure and user Sendio's Email Continuity feature in the event of an email system outage. Intended for Administrators.

Exchange Smart Host Configuration

Configuration guide to enable routing of inbound and outbound email from Microsoft Exchange. Intended for Administrators.

Conventions in the Manual

Note: A Note is information that deserves special consideration.

Troubleshooting Tip: A Troubleshooting Tip provides information that has been known to help solve various problems.

Warning: A Warning identifies information that could lead to unintended consequences if not properly considered.

Menu Commands

Sendio's web interface has menu commands that you follow to change display pages, open dialog boxes and initiate certain actions. Primary menu commands (or paths through the interface) are shown in **bold** type in the format **Admin > System > Outbound Control**. This example would mean:

- the Admin UI
- the System button
- the Outbound Control button

The options in drop down menus, such as *Accept Contacts only*, are shown in *italics*.

Sendio Terminology

Words that have special meaning within the context of Sendio operations are shown in *italics*, such as *Accept-List*, *Pending*, *etc...*

SECTION 1: Concepts and Definitions

Before diving into all the details involved in administering Sendio, it will be useful to first review several concepts and definitions that the reader of this manual is presumed to understand.

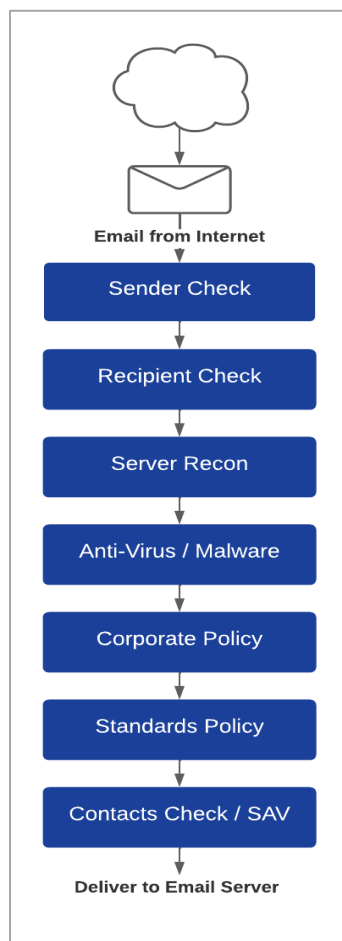
Platform

Sendio's system is running in a high-security implementation of the Linux operating system. Sendio has developed many message processing "services" that run on the system. Many of these services are administratively configurable. Sendio is available in a hosted service, virtual server edition, and a physical appliance application. Everything in this manual applies to all system options.

Message Flow

Sendio is installed "logically" between the internet and the mail server. The corporate MX (mail exchange) record in DNS is set to point to Sendio, causing all email from the internet to be routed to Sendio. Sendio receives the messages, processing them through a series of email integrity services, eliminating unwanted messages, and forwarding the clean email to the email server(s) for delivery to the end-users.

- **Warning:** Sendio does not have its own internal firewall. The physical or virtual appliance should be installed "behind" the organization's firewall. Any system directly accessible from the internet has the potential of being compromised. It is assumed that your organization employs "best practices" to protect Sendio from external attack. Sendio's hosted solution is serviced via a Tier 3 data center, with highly redundant hardware, power, and internet bandwidth.



Workflow

Sendio is a sophisticated system that implements a highly configurable workflow engine. The Administrator can configure a specific policy and system behavior for each stage of the workflow.

- **Sender Check:** the system does a series of tests using the Domain Name Service (DNS) and other mechanisms to identify and classify the original sender of the message.
- **Recipient Check:** the system verifies that the intended recipient(s) of a message have accounts on the target email server.
- **Server Recon:** the system uses a series of low-level SMTP tests to determine the validity of the sending email server.
- **Anti-Virus / "Malware":** the system scans all messages to ensure that they do not contain viruses, trojans, bots or other "malware".
- **Corporate Policy:** the system implements policies for handling large messages, those with "untrusted" attachments, or with an excessive number of recipients.
- **Standards Policy:** messages are checked against industry standards for sender authentication, such as DKIM and SPF.
- **Contacts Check / SAV:** messages are checked against both System and individual User *Accept Lists*, *Hold Lists* and *Drop Lists*, and may be processed using the Sender Address Verification (SAV).

Service Availability

Sendio Administrators must decide how to balance the need for security against the desire for maximum productivity. Specifically, there are several configuration options that specify how the Sendio workflow should respond if one of the email integrity services becomes unavailable for a period.

For example, if the anti-virus scanning services for inbound messages becomes unavailable, should email keep flowing or should it be halted until the service is restored? Since the risks associated with virus infections are high, this might be a prudent choice. In contrast, it may be quite acceptable to maintain email flow if the Zero-Hour checking for outbound messages becomes unavailable for a period.

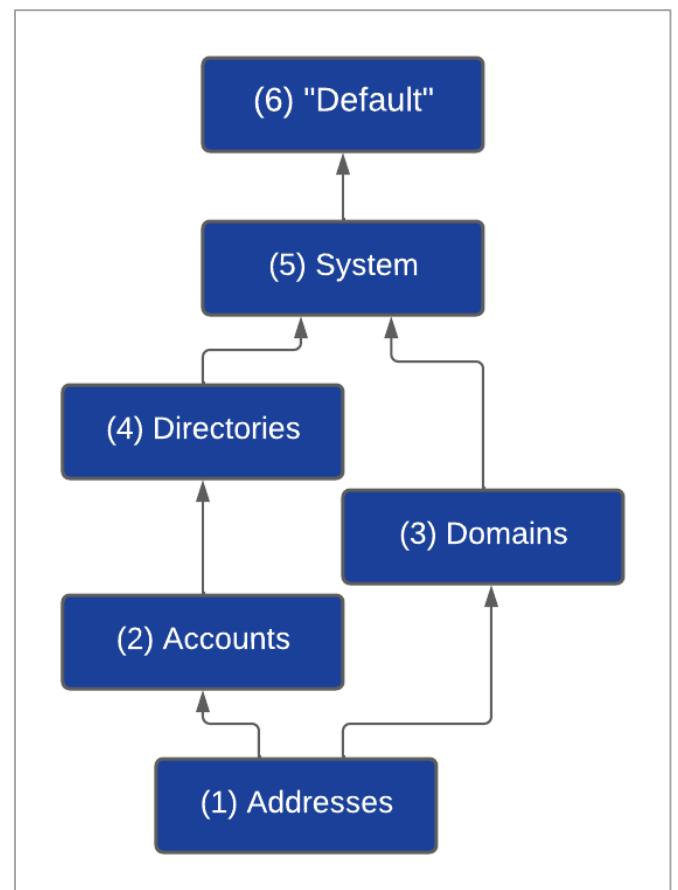
Relationships, Ownerships, and “Default” Settings

Sendio maintains a database of the email inboxes that are protected and the relationship between the various addresses, domains and directories that comprise the email environment. The diagram below shows a high-level representation of these relationships. It also includes a “default” level that holds the default settings for options.

The arrows in the diagram indicate “ownership”, meaning that **Addresses** are “owned” by both **Accounts** and **Domains**. **Accounts** are owned by **Directories**, and both **Domains** and **Directories** are owned by the **System**.

All mail operations which make a decision based on an option setting in Sendio look up the setting for the recipient of the message currently being delivered. If no setting exists at the **Address** level, then the setting is inherited from the related “owning” level, in numerical order as shown. If no setting is supplied at the **System** level, then the default settings are used.

Once a **Domain** is created, it must have one or more **Directories** assigned. If an email server manages a domain that is not configured in Sendio, email sent to an address in that domain will not be processed by Sendio.



SECTION 2: Logging in to Sendio

During the installation process, a DNS Host record (A) that “names” the Sendio server is recommended.

EXAMPLE: sendio.example.com

Using a Web browser, connecting to Sendio would use this name.

EXAMPLE: http://sendio.example.com

A Sendio login screen will be displayed. The default requires an email address and network password, typically the same as your email account login.

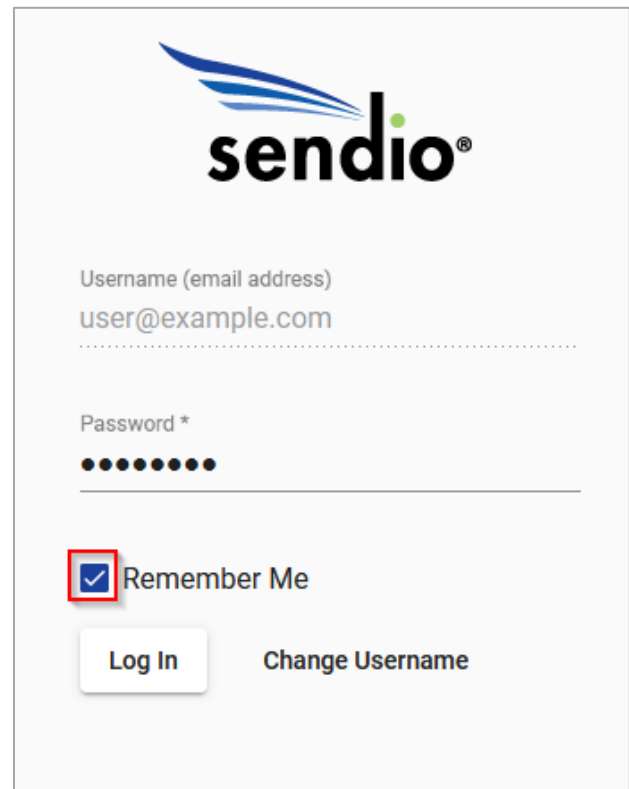
If the *Allow Remember Me on Login* option on the **Admin > System > Options** page (described in Section 5) has been *Enabled*, then the login screen will include a *Remember Me* check box. If checked, the *Remember Me* option causes Sendio to “remember” the email address authentication for a configurable period, so that this login step is skipped in the future.

Troubleshooting tip: If the web interface login fails, investigate the following possibilities:

- The login account used to synchronize password has changed.
- Sendio has lost communication with the directory server and is therefore unable to validate the directory password.
- The directory synchronization process has not yet occurred.
- Changes have been made to the **Directory** (eg a CN has been renamed).
- The Azure AD token/secret may have expired.

In any case, you may use the *sysconfig* administrative login and access the functions of the server. The login format for this user is *sysconfig@esp* and the password is the previously set *sysconfig* password. As the **Administrator** you may have also set up a local password for any Sendio **Account** which can be used in this scenario (Azure Active Directory sync does not allow setting local passwords in Sendio). If you suspect that Sendio has lost communications with the directory services, you may also use the *sysconfig* interface to ping the directory server.

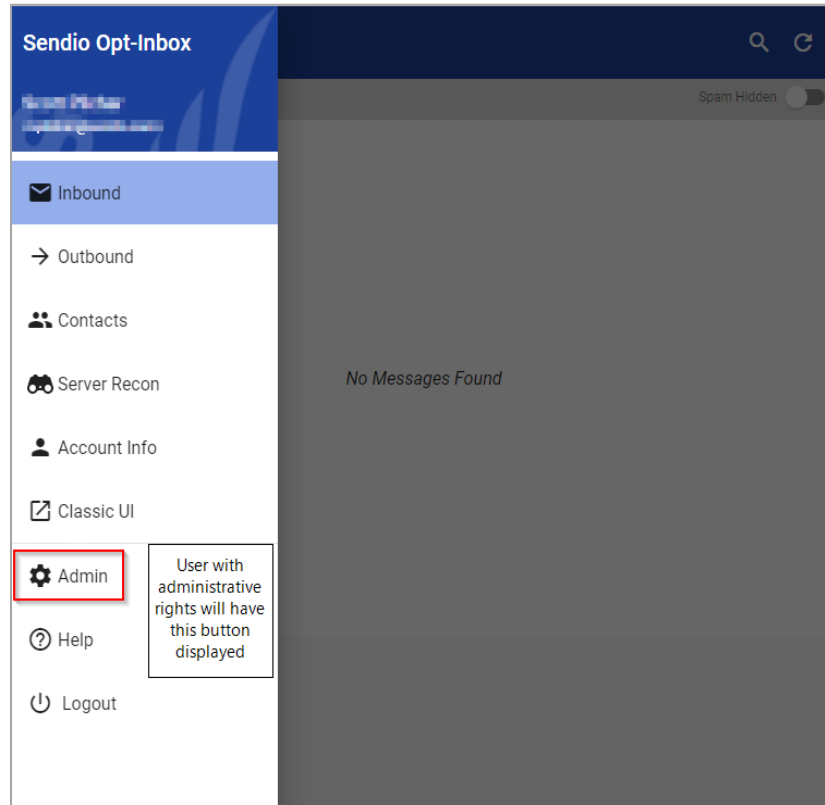
You may also navigate to the **Directories** menu option on the **Admin UI** and synchronize the directory, which will verify communications and also confirm that the addresses you been synchronized to Sendio. Navigate to the **Addresses** menu option to verify that the original email address that was attempted during login appears on this list.

The image shows a web-based login interface for Sendio. At the top is the Sendio logo, which consists of a stylized blue wing above the word "sendio" in a bold, black, sans-serif font. Below the logo, there are two input fields. The first is labeled "Username (email address)" and contains the text "user@example.com". The second is labeled "Password *" and is filled with ten black dots. Below the password field is a checkbox that is checked, with the label "Remember Me" to its right. At the bottom of the form are two buttons: "Log In" and "Change Username".

SECTION 3: Sendio User and Administrator UI

There are two different navigation User Interfaces, one for **Users** and an expanded one for **Administrators**. Users with administrative privileges will have an Admin button on their screen which will allow them to switch to the Administrator view. Users without administrative rights will not see the Admin button.

User UI



Inbound will show the user their inbound message queue.

Outbound will show the outbound message queue.

Contacts will show a list of the user's contacts.

Server Recon will show any messages waiting to complete the server recon test

Account Info will show details of the user's account in Sendio

Classic UI will switch to a Flash required view of the Sendio UI

Admin will switch the user to the Admin UI (if present)

Help will connect the user to the Sendio website for additional information

Logout will log the user out of their Sendio queue

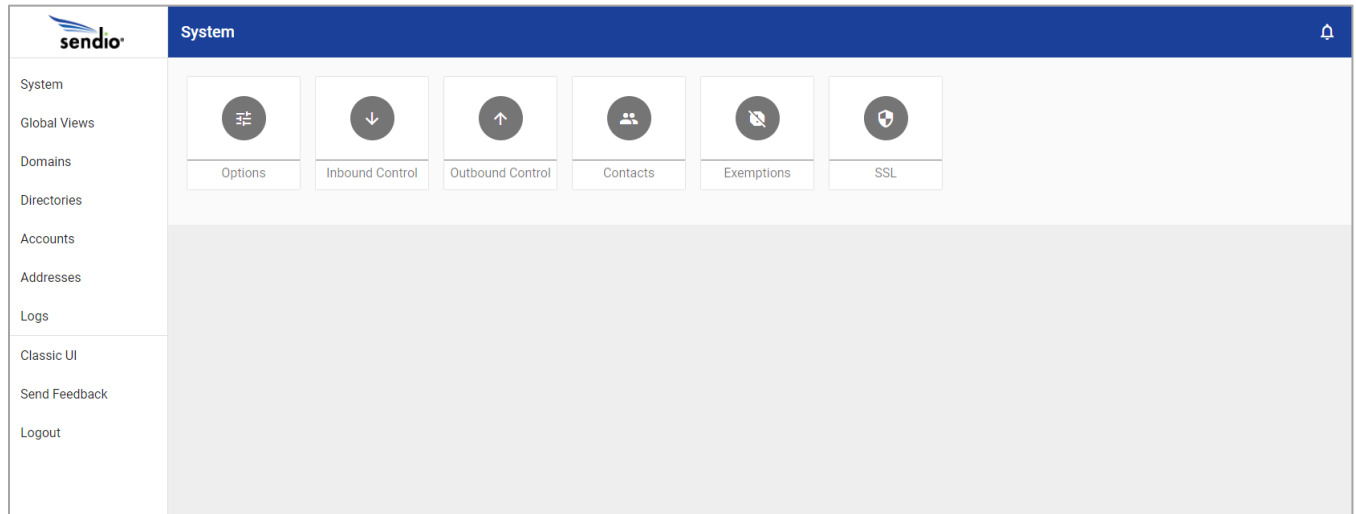
Adding Administrative Rights to a User Account

To add administrative rights to a user account that will allow them to access the Sendio Admin UI with their own credentials:

1. Using the Sendio SSH (PuTTY) interface, navigate to the Directory Management section.
2. Arrow over to "Press enter or Type Entry". Enter the user's last name and press Enter.
3. Select the appropriate user with the space bar. Tab to highlight Select and press Enter.
4. Move to "Grant Full Admin Access", and then press Enter.
5. Save your settings.
6. Repeat for additional Administrators.



Administrative UI



The Administrative UI is a group of buttons that allow the **Administrator** to access distinct parts of the Sendio system.

System is a group of pages that allow the **Administrator** to configure system-wide options for Sendio.

Global Views gives the **Administrator** access to both the Inbound and Outbound message queues for all user accounts in Sendio.

Domains is a list of email domains that are handled by Sendio.

Directories is where the directory services connection (Active Directory, Azure AD, LDAP) is specified.

Accounts is the list of all user accounts in Sendio. The **Administrator** can access any information about any user account (Options, Addresses, Contacts, Message Queues).

Addresses displays a cross references of email addresses and their associated account. Address options can be managed.

Logs provides real-time interface to the SMTP, SMTPS, MTA, SAV, HTTP, HTTPS, FTP, Passthrough and AutoAccept logs in Sendio. There is an export function from any of these logs.

Send Feedback is a form that will allow the **Administrator** to provide feedback or feature requests to Sendio.

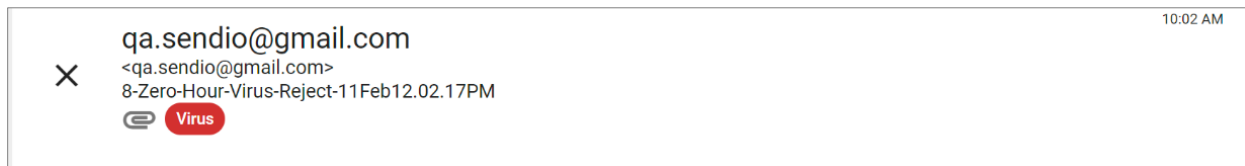
Logout will log the **Administrator** out of the Sendio UI.

Message Icons

In the Sendio UI, there are various icons that you will see in the queue. These provide the user or Administrator with information as to policies that have been applied to the email. These icons are the result of policies set by the Administrator for Sendio filtering.

Virus

If an email is tagged as virus infected, virus suspected, or the anti-virus service is unavailable, a red oval with “Virus” will be shown with the email.



Bad IP Reputation

If a sender's IP Reputation is tagged as high risk for sending spam, a gray oval with “IP Rep” will be shown with the email.



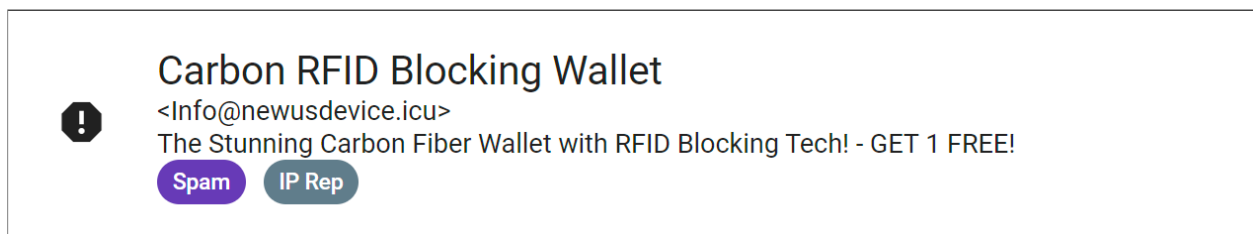
Mailing List

If an email contains a List Header, an additional header included in a message that transmits a unique mailing list identifier, a blue oval with “List” will be shown with the email.



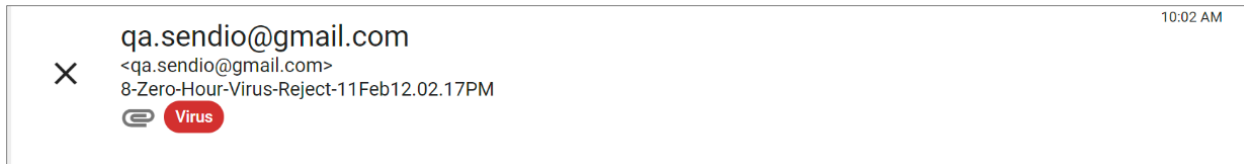
Spam

Any email that is tagged as Spam will show a purple oval with “Spam”.



Attachment

If an email has an attachment, you will see the “paper clip” icon.

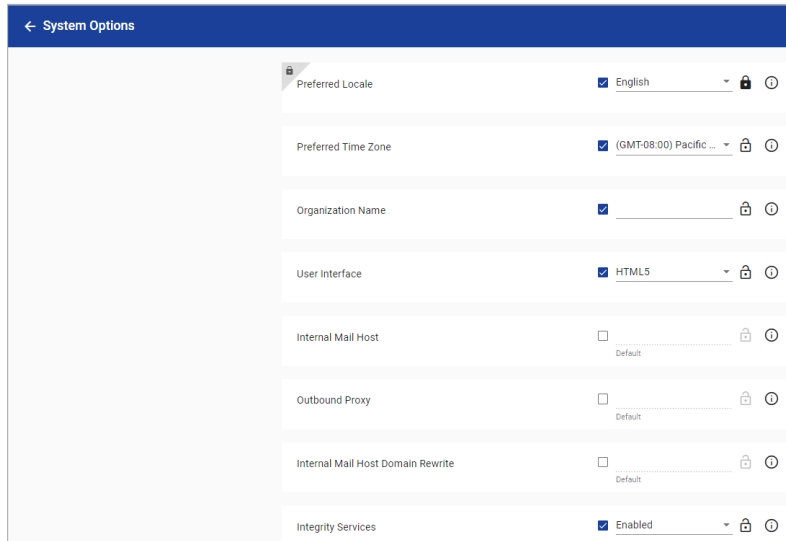


The rest of the page left blank intentionally.

SECTION 4: System Pages

The System pages on the Admin UI provides access to the majority of Sendio configuration functions. These functions are divided into six areas: Options, Inbound Control, Outbound Control, Contacts, Exemptions and SSL.

System > Options



Option	Value	Lock	Refresh
Preferred Locale	English	Yes	Yes
Preferred Time Zone	(GMT-08:00) Pacific ...	Yes	Yes
Organization Name		Yes	Yes
User Interface	HTML5	Yes	Yes
Internal Mail Host	Default	Yes	Yes
Outbound Proxy	Default	Yes	Yes
Internal Mail Host Domain Rewrite	Default	Yes	Yes
Integrity Services	Enabled	Yes	Yes

The **Admin > System > Options** page displays a list of options for Sendio that can be set at the **System** level. Many of these options can also be set at the **Domains, Accounts and Addresses** levels as appropriate (described in later sections).

The following sections describe each of the options.

Preferred Locale: The preferred locale for choosing display language and formats. Currently, only English (United States) is available.

Preferred Time Zone: Indicates the time zone for date and time display in the web UI. It does not affect timestamps in email, which use the Sendio server's internal time zone setting (set in sysconfig).

Organization Name: The name of the organization Sendio is serving. The value typed directly into the value box. This is also the name of the organization that is included in the SAV message that is sent out from Sendio.

User Interface: HTML5 is the default UI.

Internal Mail Host: (Default: No Setting) The IP address, machine name, or Office 365 URL of the Internal Mail Transport Authority (MTA) to which accepted messages will be delivered. Sendio must have port 25 (SMTP) connectivity to the server that is indicated in this option value. If Sendio is in a DMZ or in a geographically disparate location from the email server, the firewall must be configured to allow this traffic to pass. At the **Domains** level, this value can be set to allow mail for different domains to pass to different mail servers. This can also be set at the **Accounts** and **Addresses** level if necessary.

Note: If a machine name is used, it must have a DNS MX or A record resolvable by Sendio to one or more IP addresses.

Outbound Proxy: (Default: No Setting) In the event that there is an outbound proxy between Sendio and the internet for outbound mail, Sendio can be configured to send mail through that proxy by entering the IP address or hostname in this field.

Internal Mail Host Domain Rewrite: (Default: No Setting) If set, this value rewrites the domain n of the recipient address before sending the message to the internal mail server. This option is rarely used.

Integrity Services

Integrity Services is the combination of Server Recon (Silverlisting), Sender Address Verification (SAV) and Contact Checking. Integrity Services, as well as each individual component, can be configured at the **System, Domain, Account** and **Address** level.

When Integrity Services are disabled, messages are not stored locally and, therefore, are not displayed in the message queue UI. The one exception to this rule occurs if the message is determined to have a virus. In this case, the held or rejected message will be displayed in the user's message queue.

Messages that bypass Integrity Services are displayed in a different log than normal messages. This log can be viewed by clicking the "Passthrough Log" butt in the **Logs** tab of the web UI.

Note: *Accounts/Users with Integrity Services disabled are unable to receive the daily queue summary notifications.*

Integrity Services: (Default: Enabled) Indicates whether or not the Integrity Services option is enabled. Disabling Integrity Services disables all sub-options as well.

SilverListing: (Default: Enabled) Indicates whether or not the SilverListing (Server Recon) process is enabled. Please see the Server Recon section later in this document for more information.

SilverListing Spoof Protection: (Default: Enabled) Indicates whether or not the SilverListing (Server Recon) process is applied to messages which are received from email addresses in a Contact list but from an IP which has not previously passed the SilverList test. Please see the Server Recon section later in this document for more information.

SilverListing Service Outage: (Default: Allow Message) Indicates what to do with messages in the event the SilverListing service is unavailable. Options are Allow Message or Defer Message.

Contact Checking: (Default: Enabled) Indicates whether or not the Contact Checking process is enabled. If Contact Checking is disabled, the Sender Address Verification (SAV) will be disabled as well.

Sender Address Verification (SAV): (Default: Enabled) Indicates whether or not the Sender Address Verification (SAV) process is enabled for non-Bulk messages

Note: *If you are evaluating Sendio, you may choose to set this value to Disabled and Unlocked. Then, at the **Accounts** level, several users can be selected to evaluate the functionality by setting this value to Enabled.*

Send SAV for Bulk Messages: (Default: Disabled) Indicates whether or not the Sender Address Verification (SAV) process is enabled for Bulk messages.

Send SAV Acknowledgements: (Default: Enabled) Indicates whether or not the Sender Address Verification (SAV) process will send an acknowledgement email to the original sender once they complete the SAV process.

When No Contact Matches: (Default: Hold Message) Instructs Sendio how to respond to non-Bulk messages which do not match a Contact.

When No Contact Match for Bulk Message: (Default: Hold Message) Instructs Sendio how to respond to Bulk messages which do not match a Contact.

Queue Summary: (Default: Disabled) Indicates whether Queue Summary emails are sent to Users and Groups. There are three options available:

- Enabled: Users and Groups
- Enabled: Users Only
- Disabled

The “Enabled: Users Only” setting allows a single setting to disable Queue Summaries for all distribution group Accounts on the system. To enable the Queue Summary for specific groups only, go to Accounts, select the specific account, and then select “Enabled: Users and Groups” in the Options tab for the account. For more information, see Section __: Queue Summary.

*Note: The **Queue Summary** and **Queue Summary Allow User Subscribe/Unsubscribe** setting behave as follows: If you want the users to receive Queue Summaries, you must enable **Queue Summary** and set the **Queue Summary User Subscribed** field to “Yes”.*

Queue Summary Deliver Target: (Default: 8:00) Specifies the target time by which all Queue Summary messages are to be delivered to users on a particular day, in 24-hour format. See Section __: Queue Summary for more details.

Queue Summary #2 (OPTIONAL) Delivery Target: (Default: Disabled) Specifies the target time, in 24-hour format of an optional second Queue Summary. The time for the second Queue Summary should be at least 5 hours later than the first Queue Summary delivery target.

Queue Summary Web Interface URL: (Default: No Setting) Specifies the URL used in the Queue Summary email that is sent to users. The URL can be preceded by http (unsecure, port 80) or https (secure, port 443)(recommended). The URL must be followed by a trailing forward slash “/”. If the URL is available only internally, then users who attempt to click an **Accept** link from outside the firewall will receive an error message. A DNS entry for external and internal access should be made available.

Queue Summary Show Pending Bulk: (Default: Disabled) Indicates whether or not the Queue Summary will contain a Pending Bulk section.

Queue Summary Automatic Login: (Default: Disabled) If enabled, the user can follow a link in the Queue Summary email to automatically log in a (non-admin) user without entering their password.

Queue Summary Allow User Sub/Unsub: (Default: Enabled) Allows users to subscribe and unsubscribe themselves from the Queue Summary mailings. Changing setting to Disabled will force the System Enabled/Disabled setting on the user account.

Queue Summary User Subscribed: Yes or No, is the user subscribed to receive Queue Summaries?

Continuity Inbox: (Default: Disabled) Once enabled, Sendio no longer attempts delivery of inbound email to your mail server. If this option is grayed out with no Enabled/Disabled options, they you have not purchased the Continuity License. Contact Sendio Sales for licensing information.

Pending Queue Lifetime: (Default: 2 weeks) The Pending Queue, also known as the Message Queue, is where messages are kept until they are verified through the SAV process or discarded. The value can be set for as little as one day or as long as four weeks. If this value is changed, the expiration dates of messages currently in the system are not modified.

Note: *For high message volume environments, best performance is achieved by keeping the Pending Queue Lifetime as low as business requirements will allow.*

Response Control

Verification Request Template: (Default: Standard Request (English)) This option can be modified to change between English, Spanish and combination templates. See Section __: SAV Messages for more information.

Verification Acknowledgement Template: (Default: Standard Request (English)) This option can be modified to change between English, Spanish and combination templates.

Bounce Template: (Default: Standard Bounce (English)) In the situation where Sendio receives an SAV Response to a message that has been deleted either manually or through the aging process, a bounce message will be generated.

Attach Original to Verification Request: (Default: Attach Message Headers Only) Indicates whether or not to attach a copy of the ORIGINAL MESSAGE BEING VERIFIED to the verification request message. Can be set to attach the entire original message, only the headers, or no attachment. Attaching the entire message is strongly discouraged as it may cause other servers to mistake an SAV Request for spam messages.

Attach Original to Verification Acknowledgement: (Default: Attach Message Headers Only) Indicates whether or not to attach a copy of the ORIGINAL VERIFIED MESSAGE to the verification acknowledgement message. Can be set to attach the entire original message, only the headers, or no attachment.

Attach Original to Bounce: (Default: Attach Message Headers Only) Indicates whether or not to attach a copy of the ORIGINAL MESSAGE BEING BOUNCED to the bounce message. Can be set to attach the entire original message, only the headers, or no attachment. Attaching the entire message is strongly discouraged as it may cause other servers to mistake the bounce message for spam messages.

24h System Sender Response Limit: (Default: 50) Defines the maximum number of system messages (NDR, DNS, SAV) Sendio will generate to any particular email address in a 24 hour period. Options from 1 to 5000 using the slide bar.

24h Per User Sender Response Limit: (Default: 1) Defines the maximum number of system messages from a given Sendio user to any particular address in a 24 hour period. Options from 1 to 50 using the slide bar.

Add Senders to Drop List: (Default: Enabled) Defines whether a user add senders to drop list for incoming messages.

Allow Dropping Message Groups: (Default: Disabled) This feature allows users to drop all pending messages for an entire day in their queue with one click. Can be enabled at the System or Account level.

Allow User Message Preview: (Default: Enabled) This option allows the **Administrator** to block the view of the message content via the Sendio web UI. The message can be viewed in the user's Mail Client but not via the Sendio web UI.

Allow User Rejected Message View: (Default: Enabled) This option allows users to see rejected emails in their queue. Users will need to change the default view from Pending to Rejected to see the list of rejected messages in their queue.

Allow Admin Message Preview: (Default: Enabled) Blocks the administrative view of the message content via the web UI. The message can be viewed at the user's Mail Client, but not via the Sendio web UI.

Incoming Proxies: (Default: Disabled) Indicates whether an organization's incoming mail is first received by a proxy before reaching Sendio. If there is a proxy, the value should be set to Enabled.

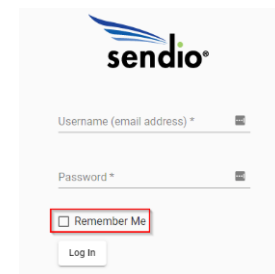
Note: *In some cases, firewalls can be configured to be mail proxies.*

Sender Proxy Analysis: (Default: Enabled) Sendio can determine the IP address of the remote sending server (prior to local proxies) by inspecting the headers of the message. This is required for proper function of SPF and IP-specific Contacts but has a small performance overhead. If the network has an active proxy and SPF checking is desired, the value should be set to Enabled

Proxy Identifiers: (Default: empty) The IP addresses and/or hostnames of all mail proxies should be listed in comma separated format.

Allow Remember Me on Login: (Default: Disabled) Enables the display of Remember Me check box in the web UI login screen. Selecting Remember Me instructs the web UI to remember the user's email address and password for the duration specified by the **Remember Me Duration** option.

Remember Me Duration: (Default: 2 weeks) Specifies how long the system should wait before requiring re-authorization of login credentials if a user checks the Remember Me box on the login screen. Options from 1 day to 4 weeks



Account Password Caching: (Default: Disabled) Should password caching be enabled for Accounts?

NOTE: Password Caching does not work if using Azure Active Directory

Bounce Undeliverable Outbound Messages After: (Default: 1 Day) Defines how long should temporarily undeliverable outbound messages be retried before giving up and sending a non-deliver report. Options from 2 hours to 1 week.

Bounce Undeliverable Inbound Messages After: (Default: 1 Day) Defines how long should temporarily undeliverable inbound messages be retried before giving up and sending a non-deliver report. Options from 2 hours to 1 week.

Deliver Status Notifications (DSN)

To internal Senders

Initial DSN After: (Default: No DSN Sent) Defines the minimum time the system will wait before sending a Delivery Status Notification (DSN) to an internal sender. Can enable with options from 5 minutes to 1 day.

Minimum Time Between DSNs: (Disabled unless **Initial DNS After** is enabled) Options from 1 hour to 2 days.

To External Senders

Initial DSN After: (Default: No DSN Sent) Defines the minimum time the system will wait before sending a Deliver Status Notification (DSN) to an internal sender. Can enable with settings from 5 minutes to 1 day.

Minimum Time Between DSNs: (Disabled unless **Initial DNS After** is enabled) Options from 1 hour to 2 days.

Message Journaling

Message Journaling allows for copies of messages to be delivered to an external email archiving or journaling solution. Based on the way Sendio processes messages, Journaling includes all inbound messages that have passed the SilverList test. Message Journaling only works for inbound messages.

Message Journaling: (Default: Disabled) Defines if Sendio will Journal all inbound messages to an archival host or mailbox.

Journaling Host: (Default: No setting) IP address or hostname of an archival host. If a hostname, a DNS A or MX record must exist for it. May be blank if a Journaling Mailbox is specified (then Journaling Host is just the domain of the Journaling Mailbox).

Journaling Failsafe Mailbox: (Default: No setting) A mailbox for journaling any messages rejected by the primary journaling host/mailbox. It may happen that the journaling system returns a permanent failure when asked to journal a message, or it may return temporary failures (deferrals) for an unacceptable time. When this happens, the message will be journaled to the Failsafe Mailbox.

Journaling Timeout: (Default: 1 day) The maximum time we will attempt to send to the primary Journaling Host or Mailbox before giving up and trying the Failsafe Mailbox. Options from 1 hour to 2 weeks.

Journaling Queue Limit: (Default: 10,000) The number of messages that will be held in the Journaling queue before Sendio begins deferring messages.

Journaling Queue Alert Threshold: (Default: 1,000) The number of messages that will be held in the Journaling queue before Sendio begins notifying the Sendio administrator. Email notifications will be sent to either the email address(s) specified at Sendio Console Interface > System Configuration > Alert Addresses or accounts that have been configured with Sendio administrator access at Sendio Console Interface > Directory Management > Modify User Access.

Journaling Queue Alert Interval: (Default: 1 hour) The interval at which Journaling Queue Alert Threshold message are sent to Administrators. Options form 10 minutes to 4 hours.

List Message Auto-accept: (Default: Disabled) List Message Auto Accept applies additional logic to list (i.e., newsletter) messages. By enabling this option Sendio will attempt to determine which list messages are valid and automatically accept them.

Add Contact on Auto-Accept: (Default: Disabled) If a list message is accepted via the List Message Auto Accept option, should an Account Contact be automatically created for the sending email address.

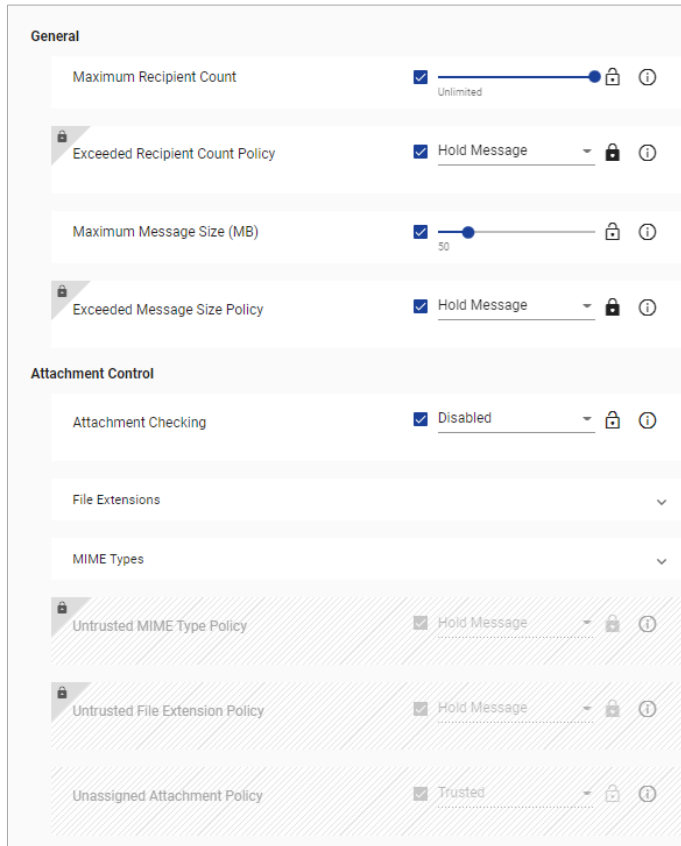
GUI Inactivity Timeout: (Default: 20 minutes) If a user leaves their web browser open to the Sendio web interface, after how long will the session timeout. Options from 10 minutes to 4 hours.

Note: Remember to click the **Save** button at the bottom of the Options screen if any changes are made to any options or else the changes will be lost when you exit.

System > Inbound Control

The System > Inbound Control page displays a list of options that specify how Sendio should process inbound messages. These options are grouped by related functions

The groups are:



- General
- Attachment Control
- Address Validation
- Sender IP Address
- Anti-Virus
- Zero-Hour
- Spam
- Bulk
- Anti-Spoofing
- DKIM Inbound
- SPF
- DMARC

General

Maximum Recipient Count: (Default: Unlimited) Specifies the combined number of addresses that are allowed to be in the 'To:', 'CC:' and 'BCC:' fields in an inbound message.

Exceeded Recipient Count Policy: (Default: Hold) Allows the Administrator to determine the disposition of a message that violates the maximum value set in the option above. Choices for this value are Hold and Reject.

Maximum Message Size (MB): (Default: Unlimited) Messages can be limited by the size of the message. This includes the attachment. This value is indicated in megabytes from 1 to 50.

Exceeded Message Size Policy: (Default: Hold) Allows the Administrator to determine the disposition of a message that violates the maximum value set in the option above. Choices for this value are Hold and Reject.

Attachment Control

Attachment Control specifies how attachments to messages are to be handled by Sendio.

Attachment Checking: (Default: Disabled) Should Sendio selectively block inbound message with associated file types? If Enabled, Administrators will have to configure Trusted/Untrusted file extensions and MIME types. If Enabled, Untrusted file extensions and MIME type policies will need to be configured.

File Extensions: If Attachment Checking is Enabled, Administrators will select which file extensions will be Trusted (accepted) or Untrusted (Held or Rejected based on policy setting). There is a default list, but Administrators can add additional file extensions if needed.

MIME Types: If Attachment Checking is Enabled, Administrators will select which MIME types will be Trusted (accepted) or Untrusted (Held or Rejected based on policy setting). There is a default list, but Administrators can add additional MIME types if needed.

Untrusted MIME Type Policy: What should be done with messages that are denied for failing MIME type policy checking? Options are to Hold or Reject the message.

Untrusted File Extension Policy: What should be done with messages that are denied for failing file extension policy checking? Options are to Hold or Reject the message.

Unassigned Attachment Policy: Default action on inbound messages with Unassigned file extension or MIME types? Options are to treat them as Trusted (Accept) or Untrusted (policy previously configured will be applied to the message).

Address Validation

The Address Validation group includes three options that are part of the basic email integrity workflow described in the beginning of this manual.

Unknown Recipient Address: (Default: Reject) Indicates what should be done with messages that have unknown recipients. If the value is set to Reject (recommended), then messages with invalid recipient addresses are dropped by Sendio and will not tax the MTA and IT infrastructure with unnecessary traffic. If the value is set to Allow, then unrecognized email is sent to the MTA. There are many potential side effects of this configuration, including allowing spam to pass through to retired email addresses that still exist on the MTA.

Sender's Domain Lacks MX: (Default: Defer) Indicates what to do with messages that don't have a DNS MX record for the sending address domain. Options for this option are Allow, Defer and Reject.

Sender Domain Lookup Error: (Default: Defer) Indicates what to do with messages where a DNS returns an error when looking up the sending address domain. Options for this option are Allow and Defer.

Sender IP Address

Sendio always attempts to determine the IP address of the sender of a message. This information is used by several services, including SPF checking and Contact checking. If there is a proxy system in front of Sendio, proxy addresses must be specified via the Admin > System > Options > Proxy Identifiers option or else the Sender IP Address will not be determined properly.

Sender IP Address Unknown: (Default: Allow) Specifies the action Sendio is to take if the Sender IP Address cannot be determined for a message. Other options are Hold and Reject. If the Sender IP Address cannot be determined, all Services that rely on this information will be bypassed by Sendio workflow.

Sender IP Address Bad Reputation: (Default: Hold) Specifies the action Sendio is to take if the Sender IP Address Reputation indicates a 90% or higher likelihood of being spam. This will show as a

IP Reputation Service Outage: (Default: Allow) Specifies the action Sendio is to take if the Sender IP Address Bad Reputation is not functioning or running.

NOTE: *The IP address of a message “sender” in this context can be a confusing concept. Frequently, a message sent from an email client passes through several intermediate email handling systems before it reaches the edge of your (receiving) network. Typically, Sendio is the initial receiving system, unless there is a proxy in front. In either case, the “sender” of the message from the perspective of Sendio workflow is the IP address of the last external system the email message passed through before it was received by Sendio (or the proxy).*

Anti-Virus

Sendio includes comprehensive anti-virus protection licensed from Sophos that utilizes traditional signature-based detection, Behavioral Genotype Protection, and Live Protection. Behavioral Genotype Protection test samples against continuously validated behavioral rule sets to provide immediate zero-day protection against emerging threats. This advanced feature enhances detection accuracy and reduces false positives. Additionally, Live Protection enables real-time lookups and access to up-to-the-minute threat intelligence to improve existing detections, find new malware patterns, and target emerging threat vectors. Together, these features provide a robust defense against malware, viruses, and other evolving email-based threats.

Virus Infected: (Default: Reject) Inbound messages that have been determined to have a virus should be rejected. An SMTP 550 message rejection will be sent to the sender indicating that the message was not accepted due to a virus in the content. It is **STRONGLY RECOMMENDED** that this value be set to Reject unless there is an anti-virus mechanism elsewhere in the messaging stream. .

Virus Suspected: (Default: Allow) The action for Inbound messages that are suspected to have a virus in the payload defaults to Allow, indicating that the message will be sent through to the next point in the messaging stream. .

Virus Unscannable: (Default: Allow) The action for Inbound messages that are “unscannable” defaults to Allow, indicating that the message will be sent through to the next point in the workflow. An unscannable message is one that is encrypted, or password protected. .

Anti-Virus Service Outage: (Default: Defer) If the anti-virus service is unavailable for a period, incoming messages can either be deferred until the protection resumes or can be forwarded on without anti-virus scanning.

Zero-Hour

Zero-Hour: (Default: Reject) The action for Inbound messages that have been scanned and determined to have a Zero-Hour infection should be set to Reject. Zero-Hour infections are those viruses that are in the early hours of dissemination prior to the virus signature databases being updated.

Zero-Hour Service Outage: (Default: Defer) If the Zero-Hour anti-virus service is unavailable for a period, messages can either be deferred until the protection resumes or can be forwarded on without scanning.

Spam

Confirmed Spam: (Default: Hold) The action for Inbound messages that have been scanned and confirmed to have spam content. Setting this policy to Hold Message will cause Sendio to apply an Admin Hold on a confirmed spam message. This Admin Hold will hold the message for Admin review even if an Accept contact exists for the sender and prevent users from releasing the message themselves. Setting this policy to Allow Message will allow users to release messages that have been classified as spam themselves.

Bulk

Sendio uses the “bulk tags” to classify certain messages in the Inbound Pending Queue and displays them in a secondary Show Bulk view, since they are often deemed to be “less desirable”.

Bulk Tagging Service Outage: (Default: Allow) Specifies how Sendio should process messages if the Bulk Tagging Service is unavailable for a period.

Anti-Spoofing

Multiple MIME FROM addresses: (Default: No setting) What should be done for an email with multiple addresses in the FROM header? Normally, only a single address is used in the FROM header, however, a common attack vector used for impersonation is to place multiple addresses in the FROM header of an email with the first address being a known contact. Having multiple addresses in the FROM header is valid but not normally used in practice. Consequently, legitimate mail may inadvertently be held for admin review via an Admin Hold if this policy is set to Hold.

DKIM Inbound

At the System level, the Administrator specifies whether DKIM is going to be used overall, for either inbound or outbound messages, or both. Actual configuration of DKIM options is done at the Domain level.

DKIM Signature Checking: (Default: Enabled) DomainKeys Identified Mail provides a mechanism for verifying the authenticity of an email. In a DKIM email header, there will be a signature associated only with the domain or subdomain of the sender. The Administrator may enable DKIM Signature Checking which will verify this signature and place an indication of the status of the check in the header of the email.

DKIM Signature Bad: (Default: Allow) If a DKIM signature is determined to be bad because of the check, the administrator may configure Sendio to Reject, Hold or Allow the message. The default value for this option is Allow, which will send the message through to the next step in the workflow even though the DKIM checking has failed.

DKIM Signature Lookup Error: (Default: Allow) DKIM is dependent on DNS access. If there is an issue with accessing the DKIM (TXT) record via DNS, this option will dictate the action to be performed. The default is to Allow the message through if the DKIM process cannot be performed.

SPF

Sender Policy Framework is a Microsoft-led standard for email anti-spoofing. For further information on SPF, please consult www.open-spf.org. The implementation of an SPF record is highly recommended.

SPF Checking: (Default: Disabled) Indicates whether or not Sendio will examine the SPF (Sender Policy Framework) record of an incoming message domain. If the value Enable is chosen, then there are several subordinate actions that can be taken based on the level of SPF failure ('fail', 'softfail', 'temperror' or 'permerror'). The actions based on the level of SPF failure span Allow, Hold, Defer and Reject.

SPF 'fail': (Default: Allow) The sending email server is not authorized to send messages for the domain in question. Available options are Allow, Hold and Reject. This generally means the SPF record is followed by a -ALL.

SPF 'softfail': (Default: Allow) The sending email server is not authorized to send messages for the domain in question, but the domain owner has not explicitly restricted other servers from sending messages for the domain in question. Setting this value to Hold will allow you to review the message manually in more detail before deciding how to proceed. This generally means the SPF record is followed by a ~ALL.

SPF 'temperror': (Default: Allow) A temporary error occurred during the SPF check. As such a determination of the SPF records could not be made. Setting this value to Defer will cause Sendio to retry the SPF check when message delivery is retried by the sending server.

SPF 'permerror': (Default: Allow) A permanent error occurred during the SPF check. This is very likely due to an incorrect SPF record for the sending domain. Options are Allow and Reject.

NOTE: *If you have an active proxy in front of Sendio, then INBOUND PROXIES on the Admin > System > Options page MUST be specified. Sendio can perform SPF checking behind a proxy by setting these additional Proxy Options.*

NOTE: *If desired, specific sending domains can be exempted from Sendio. For more information, see the System > SPF Exemption section of this Admin Guide.*

DMARC

DMARC Authentication: (Default: Enabled) Indicates whether Sendio will check for and apply the DMARC (Domain-based Message Authentication, Reporting, and Conformance) record/policy of a domain to analyze sender authenticity. This verification ensures that the sender is properly authenticated to send emails on behalf of the domain specified in the From header.

DMARC Failure: (Default: Enabled) A sender failed to comply with the DMARC authentication requirements specified by the domain in the From header. Setting this policy to Apply DMARC Policy will apply the action specified in the DMARC record of the sending domain. Setting this policy to Hold will apply an Admin Hold to all messages that do fail DMARC verification.

DMARC Temperror: (Default: Enabled) During DMARC processing a temporary error occurred. Setting policy to Defer Message will cause the message to be retried at a later time. Setting policy to Allow Message will Allow the message through despite the temporary processing error.

General

Maximum Destination Count: (Default: Unlimited) Specifies the combined number of addresses that are allowed to be in the 'To:', 'CC:' and 'BCC:' fields in an outbound message.

Maximum Message Size (MB): (Default: Unlimited) Specifies the maximum allowable size, including attachments, for an out-going message.

Attachment Control

Attachment Checking: (Default: Disabled) Specifies whether there is to be policy checking for attachments to out-going messages. If enabled, an Administrator must use the button to open the definition page and specify which attachment types are allowed to go out and which are prohibited from being sent. Refer to the Attachment Control discussion in the Admin > System > Inbound Control section for details.

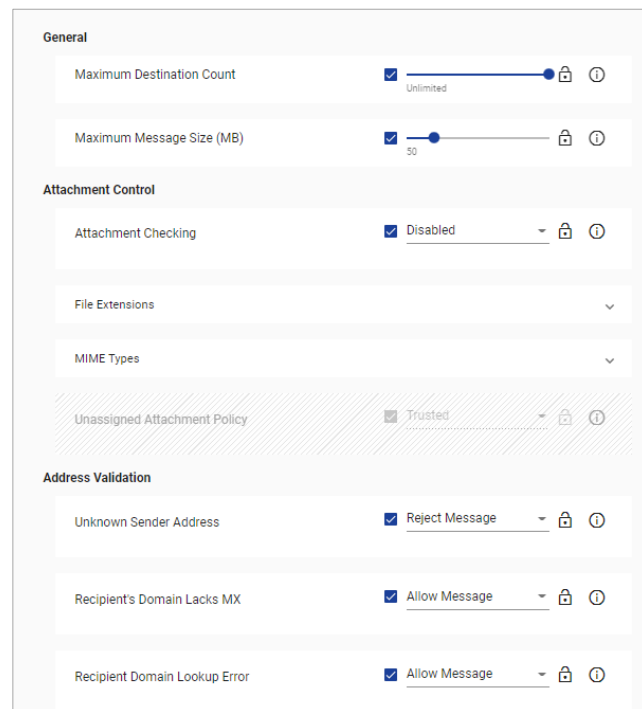
Unassigned Attachment Policy: (Default: Trusted) If Attachment Checking is Enabled, and some attachment types are left in the Unassigned category, this option specifies whether Unassigned types are Trusted or Untrusted.

Address Validation

Unknown Sender Address: (Default: Reject) Specifies the policy that Sendio should follow if an out-going message is received from the internal email server with an unknown sender's address. This could be a sign of a compromised email server.

Recipient's Domain Lacks MX: (Default: Defer) Specifies the policy that Sendio should follow if an out-going message includes a recipient whose domain does not have an MX record. In a Microsoft Exchange environment, it is recommended to set this option to Allow due to the way Exchange utilizes Queues when sending email.

Recipient Domain Lookup Error: (Default: Defer) Specifies the policy that Sendio should follow if the target domain for out-going message cannot be verified via DNS. In a Microsoft Exchange environment it is recommended to set this option to Allow due to the way Exchange utilizes Queues when sending email.



Anti-Virus

The Anti-Virus and Zero-Hour options specify the actions to take if an out-going message is found to contain a virus or potential virus, and what policies to follow if either the Anti-Virus or Zero-Hour services are unavoidable. Refer to the Anti-Virus and Zero-Hour section in the **Admin > System > Inbound Control** section for details.

DKIM Outbound

DKIM Signing: (Default: Disabled) Specifies whether Sendio is to sign out-going messages with DKIM certificates. The specific configuration of DKIM options is done at the **Domain** level, accessed via the **Domains** tab on the Admin navigation menu.

***Note:** The configuration options on the Admin > System > Outbound Control page mirror many of the corresponding options on the Admin > System > Inbound Control page previously described. The Outbound Control establishes criteria to minimize the potential of sending out a compromised message that could harm a recipient's environment. As with Inbound Controls, options are organized into groups.*

The rest of this page left blank

System > Contacts

The Contacts page displays a list of system-wide contacts. These addresses represent individuals or organizations whose emails are to be either Accepted, Dropped or Held on a system-wide basis when they are received by Sendio



System	Global Views	Domains	Directories	Accounts	Addresses	Logs	Classic UI	Send Feedback	Logout
System	Global Views	Domains	Directories	Accounts	Addresses	Logs	Classic UI	Send Feedback	Logout

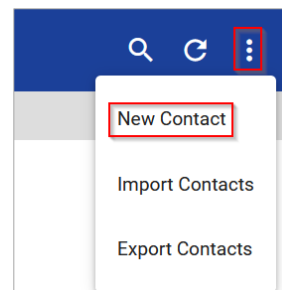
Note: It is suggested that System contacts be compiled and imported into Sendio prior to full deployment to reduce the initial number of **Sender Address Verification (SAV)** messages to known contacts.

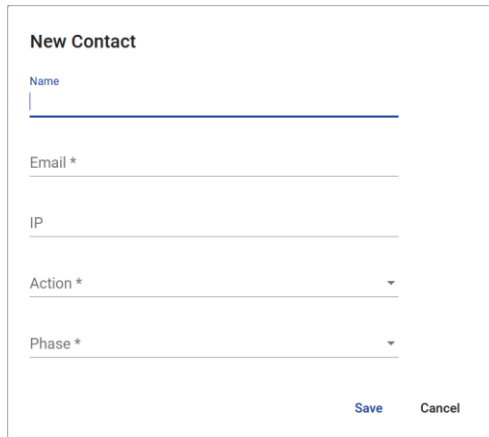
Each contact on the list has a color icon next to it to identify what type of contact it is; Accept, Drop or Hold.

1. An **Accept** contact is indicated by a blue “thumbs up” icon, messages from this sender are to be accepted and delivered to the destination inbox.
2. A **Drop** contact is indicated by a red “thumbs down” icon, messages from this sender are to be dropped and not delivered to the destination inbox.
3. A **Hold** contact is indicated by a yellow “pause” icon, messages from this sender are to be held in a user’s Pending Queue and either manually released to the inbox or allowed to “age out” of the queue.

Creating a New Contact

To enter a new contact, click the upper right corner of the screen. In the pop-up window, select New Contact.





Name: This field is for display purposes only.

Email (required): Specifies the email address for the contact. One or more wildcards (*) may be used at any point in the email address. Example is [*@domainname.com](#).

IP: Allows you to put in a specific IP address or CIDR range from which the corresponding email address must originate. You can also use a wildcard (*) indicating that this contact's email can come from any IP address. Only one IP address or CIDR range per contact.

Action (required): The Action field has three options on the

drop-down; Accept, Drop or Hold.

Note: Drop Contacts should only be created in cases where messages are reaching your inboxes from a well-known unwanted source. Excessive use of Drop Contacts can adversely affect system performance.

Phase (required): A System Contact also has a Phase indication which is available on the drop-down menu. Your options are **pre-user** or **post-user**. The phase of a contact indicates the order in which the contact is checked against the **System**, **Domain**, and **User** contact Lists.

The order of checking contacts is:

1. System pre-user
2. Domain pre-user
3. User
4. Domain post-user
5. System post-user

The phase of **pre-user** will prevent **Users** from overriding a **System** contact, while **post-user** allows them to customize their own contact list.

Example: A contact with a phase of **post-user** will be checked after the contact is checked against the **User** contact list. A contact with a phase of **pre-user** will be checked against the **System** contact list prior to a **User** contact list.

If a contact is on multiple Contact Lists with conflicting workflow definitions (e.g., on both an Accept-List and a Drop-List), the order of priority is that the Accept Lists are checked first, then the Hold-Lists, and then the Drop-Lists.

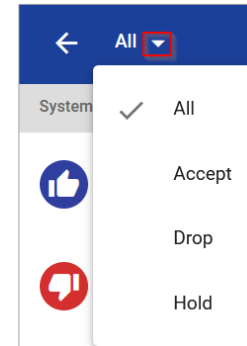
Note: By default, when a new Domain is added to Sendio, a **Drop Contact** entry for that domain is added to the System contact list with a post-user phase. The reason for this is that only your mail server should generate messages from your domain. If a message from the internet is coming into your organization from your domain, then some type of "spoofing" is probably occurring and the message would be rejected.

Updating a System Contact

To change any of the information in an existing contact, simply click on the contact in the contact list and the contact will open. You can edit any of the fields as needed, then click **Save** to update the contact.

Changing the View of the Contacts Page

To view specific types of contacts, you can change the view of the page. By default, the Contacts page opens to **All** contacts. To change to view specific types of contacts, click the arrow at the top of the screen and select which types of contacts you wish to see.



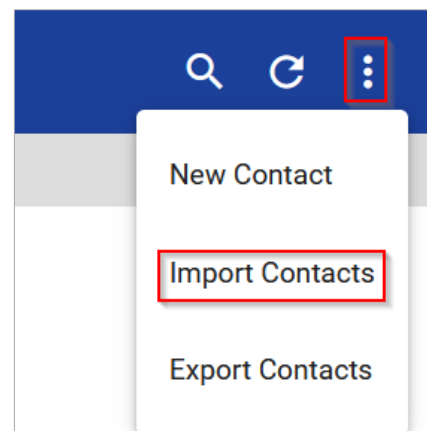
Contact Search

To do a custom search of System Contacts, click on the “magnifying glass” icon at the right of the menu bar to open a search space where you can enter search parameters to search your System Contacts. A portion of the name or email address can be entered for your search.



Import System Contacts

To import a group of System Contacts, click the upper right corner of the screen and select Import Contacts.



Browse... No file selected. **1**

Default phase of unspecified imported contacts:

- ☐ pre-user **2**
- ☒ post-user

Import **3** Cancel

File formats accepted:

- CSV exports from Outlook/Outlook Express (An example minimum import file can be found [here](#).)
- vCard 2.1 & vCard 3.0 exports

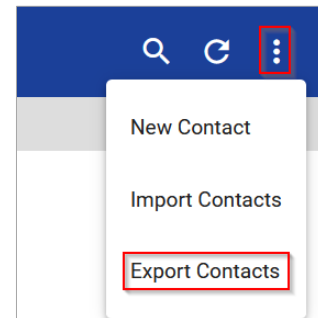
In the next Window, you will select the file to import, choose the phase, and finally upload a list of contacts into your System Contact list.

1. Browse and find the CSV file you created of your contacts.
2. Select the phase of the contacts, post-user is the default.
3. Click Import to import your contacts.

Note: We recommend clicking on the example link to review the formatting needed to upload contacts.

Export All Contacts

To export your entire list of System Contacts into a CSV file, click on the upper right corner of the screen and select Export Contacts. This will begin a download of your System Contacts.

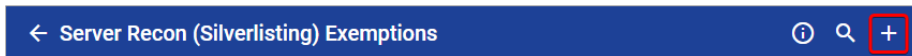


System > Exemptions

Sendio gives you the ability to add exemptions for **Server Recon (Silverlisting)**, **SPF**, **DKIM**, **DMARC**, and **Spam**. This allows you to enter address patterns and IP addresses of specific senders that you want to exempt from **Server Recon**, **SPF**, **DKIM**, **DMARC**, and **Spam** policies you have configured in **System > Inbound Control**. The most common use of these exemptions is to avoid situations where a sending domain that your organization trusts have a misconfigured SPF, DKIM, or DMARC record that causes incoming emails to be held due to the SPF, DKIM, or DMARC check failing. Or if a domain does not respond correctly to the Server Recon deferral, an exemption will allow those emails to be received by Sendio.

← Exemptions	
Name	Description
Server Recon (Silverlisting)	Exemptions to Server Recon (Silverlisting)
SPF	Exemptions to the Inbound Control SPF policy
DKIM	Exemptions to the Inbound Control DKIM policy
DMARC	Exemptions to the Inbound Control DMARC policy
Spam	Exemptions to the Inbound Control Spam policy

Create Server Recon (Silverlisting) Exemption

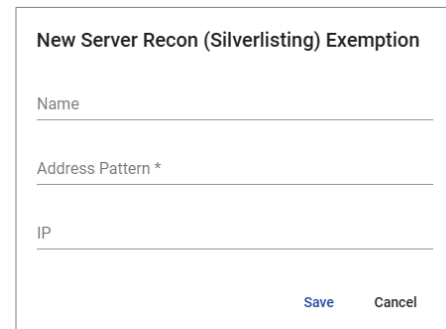


Click on **Server Recon (Silverlisting)** on the Exemptions screen. This will open the **Server Recon Exemptions** screen. Click on the “+” sign to create a new exemption.

In the new window, create your exemption.

Name: For display purposes only

Address Pattern (required): Enter the email address or domain that you want to exempt from the Server Recon test. A full email address or wildcard such as *@microsoft.com can be used here. This pattern is matched against the envelope sender email address used in the SMTP conversation.



IP: Enter the specific IP address or CIDR range or use a wildcard “*” for any IP address for the address pattern.

Click **Save** to add this exemption to your Sendio system.

Create SPF Exemption

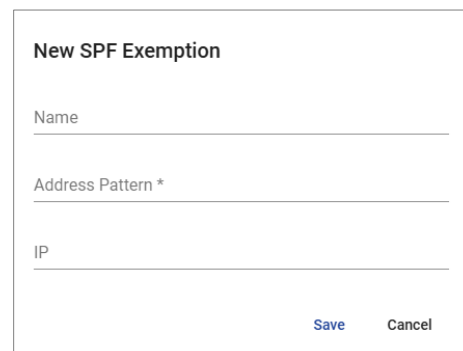


Click on **SPF** on the Exemptions screen. This will open the **SPF Exemptions** screen. Click on the “+” sign to create a new exemption.

In the new window, create your exemption.

Name: For display purposes only

Address Pattern (required): Enter the email address or domain that you want to exempt from the Server Recon test. A full email address or wildcard such as *@microsoft.com can be used here. This pattern is matched against the envelope sender email address used in the SMTP conversation.



IP: Enter the specific IP address or CIDR range or use a wildcard “*” for any IP address for the address pattern.

Click **Save** to add the exemption to your Sendio system.

Create DKIM Exemption



Click on **DKIM** on the Exemptions screen. This will open the **DKIM Exemptions** screen. Click on the “+” sign to create a new exemption.

In the new window, create your exemption.

Name: For display purposes only

Address Pattern (required): Enter the email address or domain that you want to exempt from the Server Recon test. A full email address or wildcard such as *@microsoft.com can be used here. This pattern is matched against the From header address of a message.

IP: Enter the specific IP address or CIDR range or use a wildcard “*” for any IP address for the address pattern.

Click **Save** to add the exemption to your Sendio system.

New DKIM Exemption

Name

Address Pattern *

IP

Save Cancel

Create DKIM Exemption



Click on **DMARC** on the Exemptions screen. This will open the **DMARC Exemptions** screen. Click on the “+” sign to create a new exemption.

In the new window, create your exemption.

Name: For display purposes only

Address Pattern (required): Enter the email address or domain that you want to exempt from the Server Recon test. A full email address or wildcard such as *@microsoft.com can be used here. This pattern is matched against the From header address of a message.

IP: Enter the specific IP address or CIDR range or use a wildcard “*” for any IP address for the address pattern.

Click **Save** to add the exemption to your Sendio system.

New DMARC Exemption

Name

Address Pattern *

IP

Save Cancel

Create Spam Exemption

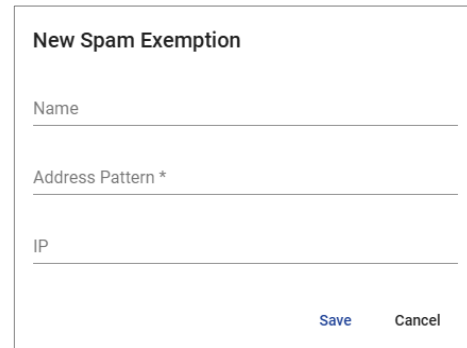


Click on **Spam** on the Exemptions screen. This will open the **Spam Exemptions** screen. Click on the “+” sign to create a new exemption.

In the new window, create your exemption.

Name: For display purposes only

Address Pattern (required): Enter the email address or domain that you want to exempt from the Server Recon test. A full email address or wildcard such as *@microsoft.com can be used here. This pattern is matched against the envelope sender email address used in the SMTP conversation.



The form is titled "New Spam Exemption". It contains three input fields: "Name", "Address Pattern *" (with an asterisk indicating it is required), and "IP". At the bottom right of the form are two buttons: "Save" and "Cancel".

IP: Enter the specific IP address or CIDR range or use a wildcard “*” for any IP address for the address pattern.

Click **Save** to add the exemption to your Sendio system.

It is recommended that user access to the Sendio web UI be made over an SSL connection. The SSL certificate can be a Sendio (Default) or can be specified via the Options on the **System > SSL** page.

<div>Certificate Name Default (Sendio, Inc.)</div> <div>HTTPS/SSL access only No</div> <div>Organization Info Fully Qualified Domain Name esp.yourdomain.com Country US State or Province California Locality Name Newport Beach Organization Name Your Company Organization Unit Name IT Contact Email Address webmaster@yourdomain.com <div><div>Save</div><div>Undo</div></div></div>	<div>Actions Download Certificate Signing Request (CSR) with Organization Info <div>Download</div> Download Private Key <div>Download</div> Download Self Signed Certificate <div>Download</div> Upload Signed Certificate <div>Choose File</div> No file chosen <div>Upload</div></div>
---	---

Certificate Name: (Default, Sendio, Inc.) Specifies the name of the SSL certificate to use for secure access to the Sendio web UI. There are three options shown in the drop-down list: Default (Sendio, Inc.), Self Signed and Signed by Trusted Authority.

Note: *Self Signed and Signed by Trusted Authority certificate name should only be selected once a certificate has already been uploaded.*

HTTPS/SSL access only: (Default: No) Specifies whether users must utilize an SSL connection to access the Sendio web interface. If enabled, access will not be possible without https://.

Organization Info: Will be filled out based on the configuration of your Sendio System. Administrators can edit the Organization information as needed, click **Save** after any changes.

The certificate request process requires that you provide the Certificate Authority (CA) with a Certificate Signing Request (CSR). This is completed in the Actions section.

Actions:

Download the Certificate Signing Request (CSR) with Organization Info to send to your Certificate Authority (CA).

- A CSR is generated with the Sendio web server software and contains both the public key portion of your web server's key pair and the Distinguished Name, which is derived from the organizational information requested. The generation of a CSR also includes the generation of a server key pair. It is strongly recommended that you back up the key pair. The key pair cannot be recovered if lost
- Submit the key for signature
- Upload the signed certificate

Once the certificate has been uploaded, select **Signed by Trusted Authority** from the Certificate Name drop-down menu.

Note: *SSL certificates that require an intermediate certificate or a certificate chain may require the assistance of Sendio Support. An example of this would be GoDaddy.com certificates.*

SECTION 5: Global Views Pages

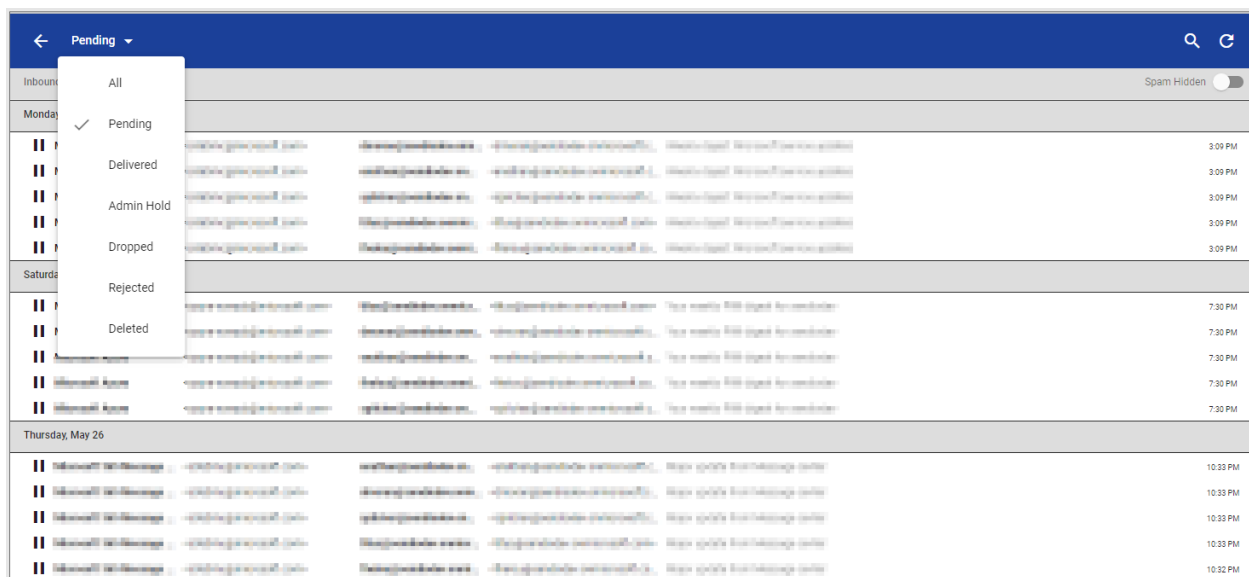
The **Global Views** pages give Administrators a facility to see an aggregate view of various message queues for all users. Many Administrators find a Global View of all Held messages to be particularly useful. Most held messages will be a result of a specific policy that has been enabled on the **Admin > System > Inbound Control** and **Outbound Control** pages.

A Global View displays a list of messages across all accounts that Sendio recognizes. In this way, the Administrator can view messages with specific characteristics across all accounts. The view can assist in determining the effectiveness of a policy or potentially the requirements of an additional policy.

Because **Global Views** function performs comprehensive queries across the entire Sendio database, it can have significant impact on system performance. When the **Global Views** button on the Admin menu is selected, the UI first displays an Alert to remind the Administrator about this potential impact. If the Administrator chooses to proceed, they then choose which queue they want to see, Inbound or Outbound. Once selected, the message queue will open.

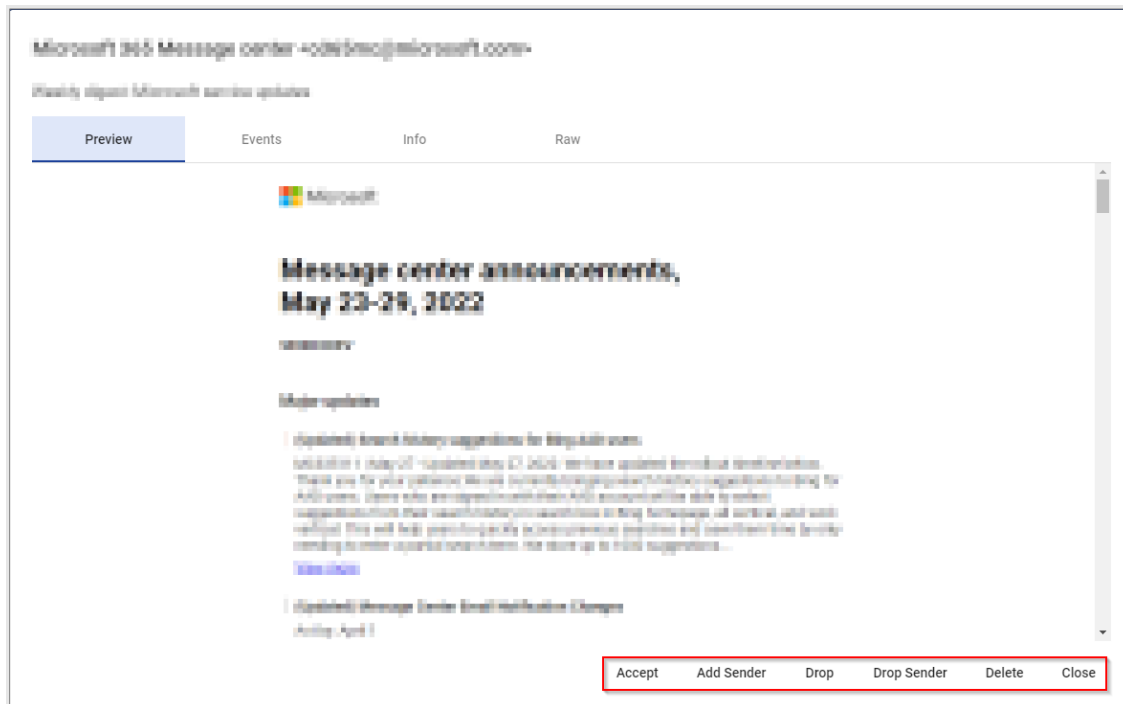
CAUTION

Global Views is a powerful administrative tool that allows you to see lists of messages across the message queues of all users. Please be advised that the data processing required to generate these views is resource intensive and may temporarily disrupt system mail flow. For this reason, use of this tool is not recommended during peak mail flow hours.

[View Inbound](#)
[View Outbound](#)


The page always opens with the Pending view selected. By clicking on the arrow, Administrators can change which messages they see in the queue; All, Pending, Delivered, Admin Hold, Rejected, Deleted (For Sendio system administrators only). Once the preferred view is selected, the corresponding messages are displayed.

Once the Administrator finds the message needed, clicking on it will give the Administrator options to process the message. When the Administrator clicks Add Sender to accept the message, a contact for the sender will be created in the user's contact list so that all further email will be accepted.



The rest of the page left blank

SECTION 6: Domains

Sendio can provide email integrity service to one or multiple domains simultaneously on a single instance.

Example: A customer owns four companies, each with their own IT infrastructure and email system.

- franks-flowers.com
- franks-fish.com
- franks-farm-feed.com
- franks-furniture.com

Sendio can receive all the email for all four businesses, process the messages through the email integrity workflow (with specific policies if desired), and then forward the legitimate messages on to the appropriate email system at the correct company.

Domains are managed by selecting **Domains** in the Admin UI. When the **Domains** page opens, the display will show all the currently configured domains.

Domains +	
Name	Addr
franks-flowers.com	4
franks-fish.com	6
franks-farm-feed.com	29

Creating A New Domain

Clicking on the “+” sign on the Domains page displays the New Domain window.

New Domain

Domain Name *

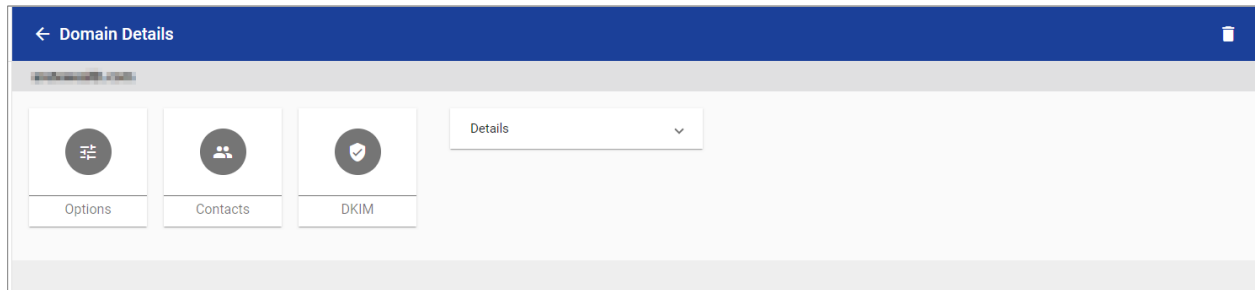
☒ Create anti-spoofing drop contact for this domain.

Add Cancel

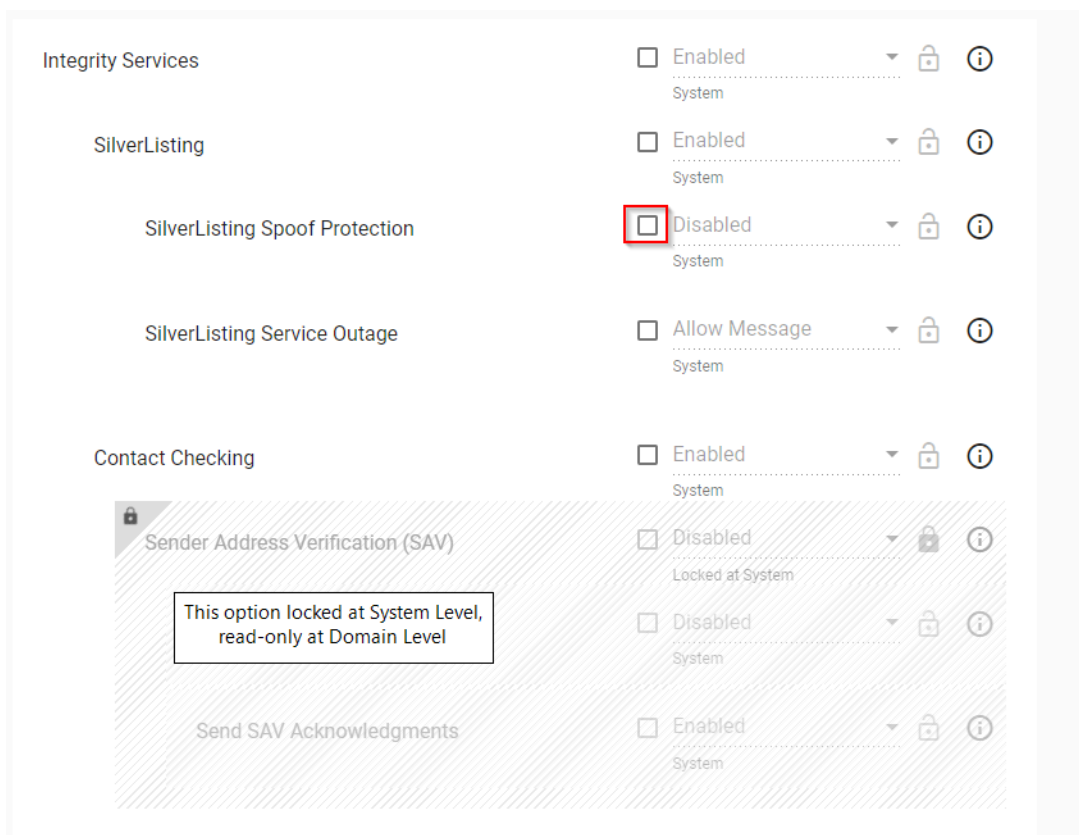
The administrator will add the domain name (FQDN) in the **Domain Name** field. By default, Sendio will create a System anti-spoofing drop contact for that domain in the System Contact list. If the administrator chooses not to have this contact created by default, they can uncheck the box before clicking the **Add** button to add the domain to Sendio.

Domain Level Configuration

Many of the options described in **Admin > System > Options** pages of this manual can be modified at the **Domain** level.



When a new **Domain** is created, it “inherits” the configuration settings from the **System** level. If an option is “locked” at the **System** level, the option is “read-only” at the **Domain** level. Except for DKIM, the options for the **Domain** are equivalent to the options on the **Admin > System > Options** page. DKIM is described later in this section. Clicking on the check box next to an option that is not “grayed-out” allows the Administrator to change the setting for that option. It can be locked here so that it cannot be overridden at the **Address** level.



Domain Contacts

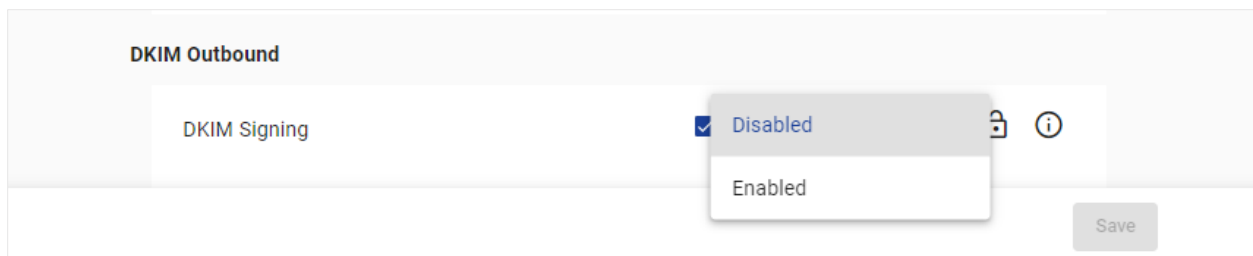
In a multiple domain Sendio environment, an administrator can create Domain Contacts that are specific to each domain on the system and will not be applied to other domains configured in the system. Like System Contacts on a single domain instance, these Domain Contacts will apply to all email addresses in that specific domain configured in the system.

DKIM Signing

DKIM lets senders verify authorship and origination of their email messages using cryptographic digital signatures. Records are published in DNS records to allow recipient mail servers to verify an email's authenticity and origin.

Sendio has the capability to “sign” outbound mail. Sendio can be configured to use **DKIM** to sign all outgoing mail, or DKIM signing can be restricted to a domain.

DKIM signing is disabled by default and is enabled in **System > Outbound Control > DKIM Outbound**



Sendio provides a default setting which can be used for DKIM signing selector, or administrators can create new selectors as needed. Once the selector is chosen (**default** used for this example) click on **Show Instructions** which will give you the necessary entry to add to your DNS record. Clicking **New** will allow administrators to create new/multiple selectors.

← Domain DKIM Settings		
acmecorp.com		
Name	Revoked	Modified
default		12/5/2022, 11:41:02AM
<div> <div>New</div> <div>Show Instructions</div> </div>		

Example of the default selector instructions.

; If you're managing DKIM selectors yourself, insert the following

; TXT records into the BIND zone configuration of acmecorp.com.

```
default._domainkey.acmecorp.com. 600 IN TXT "v=DKIM1; k=rsa;  
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDMEB02j3ene5uugNwA1vE/QXKzN3BTUFVtTfDqvKo8rxSqJhnu6iuWHJ/I  
ogOyB73GADyHbRq4HyTD8JaD2I0Ik8ZE3bbPySuMZ0fLwJtk8jktMVADk3pFY1BdnC6OzFd232QLttPrjyYNQx02DxKgSB0gJeXE/785  
74CvQYNCwIDAQAB"
```

Steps to enable DKIM signing

1. On the **Domain > DKIM page**, select the default selector or create a new one as needed.
2. Click on **Show Instructions** which will provide you with the instructions which opens a new tab with the DNS entry that will be required to add to the DNS record of the domain.
3. Create DNS entry with the public side of the DKIM key shown above which will be used to match the private key that Sendio is signing. Note the entry on the third line in the example matches the DNS name that is given when the Selector is created. The above record specifically is for use in a BIND configuration file. When using a web UI the name of the DNS TXT record would be *default._domainkey.acmecorp.com* and the value will be the quoted value above beginning with *v=DKIM1; K=rsa; ...* without the quotes.
4. Allow for a few minutes for the new DNS records to propagate before proceeding on to step 5.
5. **Domain > Options > DKIM Prefix**, use to add a subdomain to your DKIM DNS record if needed.
6. Choose the selector the domain should sign with in **Domain > Options > DKIM Selector**.

When these steps have been completed, outgoing mail will be signed with the generated key (private side) which is required to match the public side of the key in the DNS record.

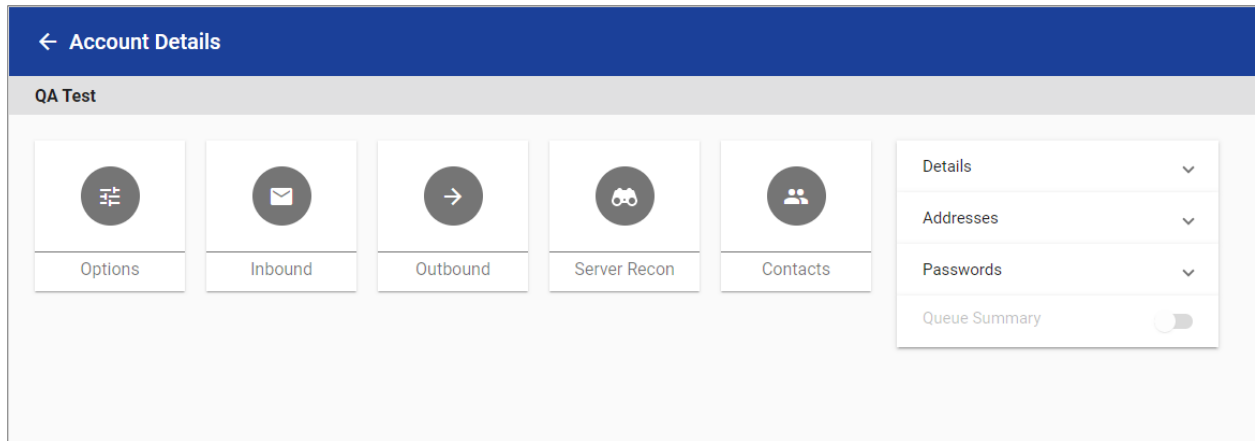
SECTION 7: Accounts Page

The Accounts page in the Sendio Admin UI displays a table of the accounts that are being managed by Sendio.

Accounts Search			
Name	Addresses	Dir DN	Added
deferafter	deferaftercptto@clippership.com, deferafterdata@clippership.com	uid=deferafter,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA Test	qatest@clippership.com	uid=qatest,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA Test2	qatest2@clippership.com	uid=qatest2,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA Test3	qatest3@clippership.com	uid=qatest3,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA Test4	qatest4@clippership.com	uid=qatest4,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA Test5	qatest5@clippership.com	uid=qatest5,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA Test6	qatest6@clippership.com	uid=qatest6,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA User1	qauser1@qasendio.com	uid=qauser1,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA User2	qauser2@qasendio.com	uid=qauser2,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
QA User3	qauser3@qasendio.com	uid=qauser3,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM
rejectafter	rejectafterdata@clippership.com, rejectaftercptto@clippership.com	uid=rejectafter,ou=people,dc=sendio-local	9/14/2022, 12:43:58 PM
System Administrator	sysadmin@icebox, sysadmin@esp	cn=sysadmin,dc=esp-local	9/13/2022, 4:29:41 PM
System Configurator	sysconfig@icebox, sysconfig@esp	cn=sysconfig,dc=esp-local	9/13/2022, 4:29:41 PM
Test User	testentry@clippership.com, testentry3@clippership.com, test@clippership.com, newtest@clippership.com	uid=test,ou=people,dc=sendio-local	9/14/2022, 12:43:57 PM

Clicking on an Account record opens a view of that account's details. The default Account Details page shows links to the account's Options, Inbound Message Queue, Outbound Message Queue, Server Recon held emails, and Contacts. You can also view the Details of the account's directory settings, all email addresses associated with the account, and the option to reset passwords.

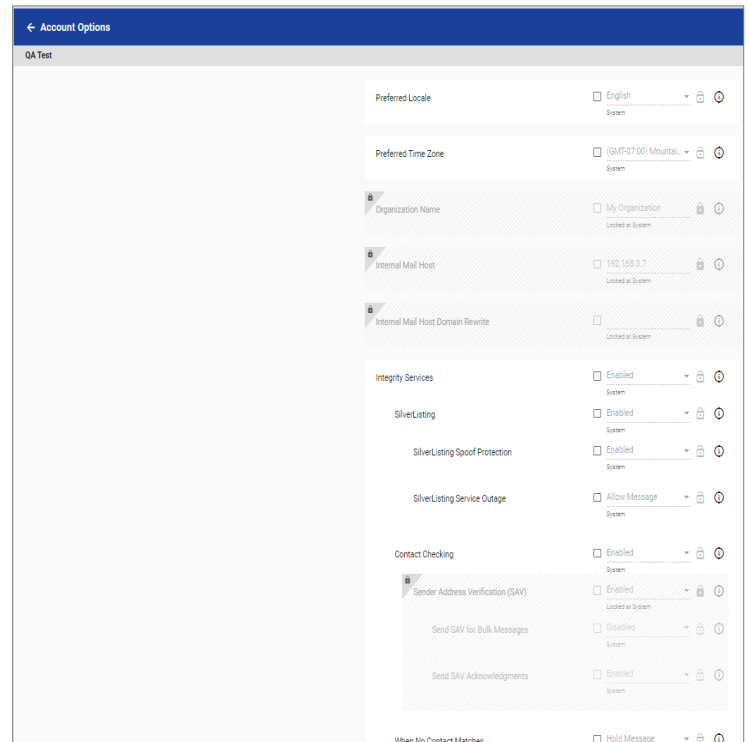
Primary email address is the address where system messages and the Queue Summary (if enabled) will be sent. If the address that is designated as the primary address is removed from the Active Directory, then the next synchronization will remove the primary designation and the system will promote the first address in the list as primary.



The Account **Options** page allows administrators to configure, for this individual account, the options previously described for the System > Options and the System > Domains > Options pages.

The setting Queue Summary Custom Recipient Address List is only available in the Account > Options, it is not available at the System level. With this setting, the Administrator can specify and alternate email address(es) to receive the Queue Summary for this account. Two common cases for this are monitoring of the account by an administrative assistant, or for large distribution groups, the queue summary can be sent to a specific list of members for account management.

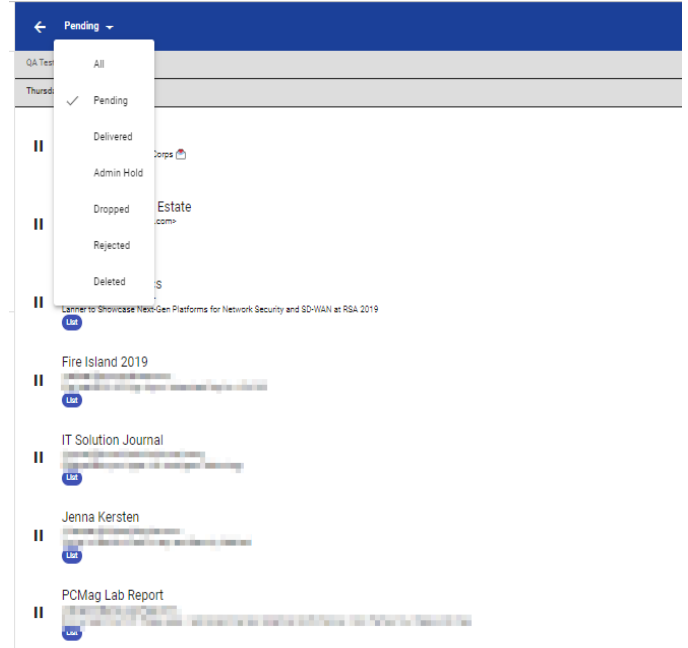
Any email address entered in this field must be present in the Addresses section of the Sendio interface and cannot be sent to external addresses.



The **Inbound** and **Outbound** pages allow the administrator to view the account's message queues and perform all the actions that a User can do. The default view is Pending messages but can be changed to any of the views available.

The **Server Recon** page allows administrators to see the status of all IP addresses that are being processed for the account.

The account **Contacts** page allows administrators to see all the contacts associated with this account. This is the same view the user would see on the User > Contacts page. The default view is All contacts, but can be changed to only view Accept, Drop, or Hold contacts as needed.



SECTION 8: Addresses Page

The **Addresses** page in the Sendio Admin UI lists the addresses that are recognized by Sendio as valid recipient addresses. Every **User** or **Account** has at least one email address associated with it, and some have multiple addresses.

This page will show administrators all email addresses created by the directory sync, the domain the address belongs to (for systems with multiple Domains, the Account Name that contains the address, and the Date it was added to Sendio.

Addresses			
Address	Domain	Account	Added
defectdata@clippership.com	clippership.com	defectdata	9/14/2022, 12:43:58 PM
defectdata@clippership.com	clippership.com	defectdata	9/14/2022, 12:43:57 PM
newtest@clippership.com	clippership.com	Test User	9/14/2022, 12:43:57 PM
qatest@clippership.com	clippership.com	QA Test	9/14/2022, 12:43:57 PM
qatest2@clippership.com	clippership.com	QA Test2	9/14/2022, 12:43:57 PM
qatest3@clippership.com	clippership.com	QA Test3	9/14/2022, 12:43:57 PM
qatest4@clippership.com	clippership.com	QA Test4	9/14/2022, 12:43:57 PM
qatest5@clippership.com	clippership.com	QA Test5	9/14/2022, 12:43:57 PM
qatest6@clippership.com	clippership.com	QA Test6	9/14/2022, 12:43:57 PM
rejectdata@clippership.com	clippership.com	rejectdata	9/14/2022, 12:43:58 PM
rejectdata@clippership.com	clippership.com	rejectdata	9/14/2022, 12:43:58 PM
test@clippership.com	clippership.com	Test User	9/14/2022, 12:43:57 PM
testentry@clippership.com	clippership.com	Test User	9/14/2022, 12:43:57 PM
testentry3@clippership.com	clippership.com	Test User	9/14/2022, 12:43:57 PM
sysadmin@esp	esp	System Administrator	9/13/2022, 4:29:41 PM
sysconfig@esp	esp	System Configurator	9/13/2022, 4:29:41 PM
sysadmin@icebox	icebox	System Administrator	9/13/2022, 4:29:41 PM
sysconfig@icebox	icebox	System Configurator	9/13/2022, 4:29:41 PM
qauser1@qasendio.com	qasendio.com	QA User1	9/14/2022, 12:43:57 PM
qauser2@qasendio.com	qasendio.com	QA User2	9/14/2022, 12:43:57 PM
qauser3@qasendio.com	qasendio.com	QA User3	9/14/2022, 12:43:57 PM

The Administrator can check the Address Details and Options by clicking on an email address. Details will show the Administrator the account full name, the date created, and the date modified if applicable. Clicking on **Options** will show any address specific settings made to this address.

← Address Options

Organization Name

☐

System

Internal Mail Host

☐

Default

Internal Mail Host Domain Rewrite

☐

Default

Integrity Services

☐

Enabled

System

SilverListing

☐

Enabled

System

SilverListing Spoof Protection

☐

Enabled

System

SilverListing Service Outage

☐

Allow Message

System

SECTION 9: Logs

Sendio maintains 9 log files that track all message transactions and workflow processes. These logs can be viewed on the **Admin > Logs** page.

44

© 2024 Sendio Technologies. All rights reserved.

Rev 1.1.0

- SMTP: The **incoming** SMTP transactions through Sendio
- SMTPS: The secure SMTP transactions between Sendio and remote servers
- MTA: The **outbound** SMTP transactions with mail servers
- HTTP: Users who are accessing the system via the GUI
- HTTPS: Users who are accessing the system via the GUI
- FTP: The FTP transactions between Sendio and internal hosts
- Passthrough: The messages that are not processed using Integrity Services
- AutoAccept: The messages that are processed using the List-Message Auto-Accept option

Logs	
Name	Description
SMTP	Incoming mail
SMTPS	Incoming mail via SMTPS
MTA	Mail to internal mail server / Outbound mail
SAV	SAV statistics
HTTP	Web UI requests
HTTPS	Secure Web UI requests
FTP	FTP requests
Passthrough	Messages passed through without analysis
AutoAccept	Messages automatically accepted

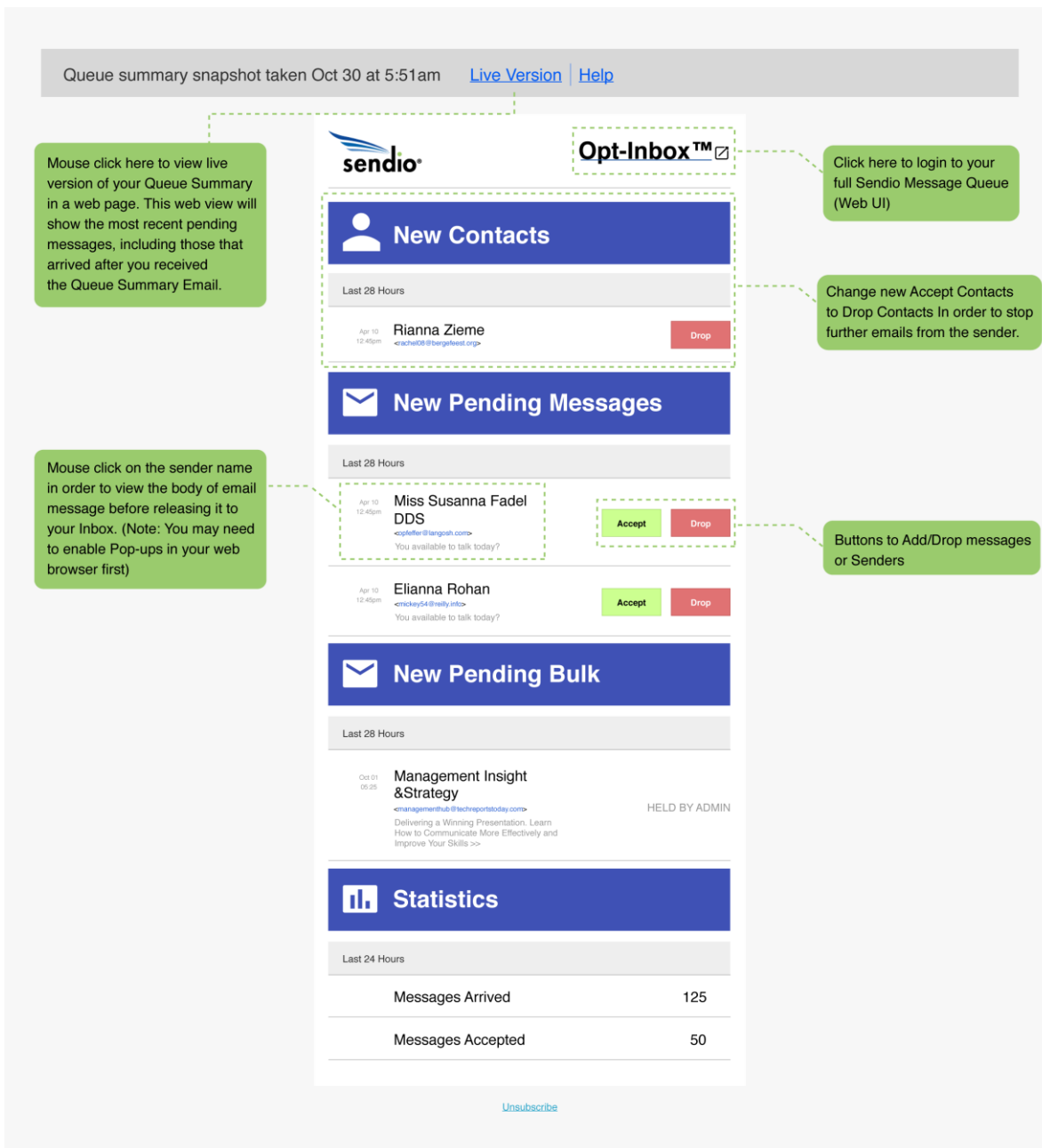
The logs can be exported to a text (.txt) file. The specific log page allows the administrator to stop/start the view of the log. Logs of the previous 24 hours, last 3 days or last week can be exported by clicking on the respective links. Alternatively, a custom timeframe can be defined by the administrator.



SECTION 10: Queue Summary

Your Sendio system has a powerful tool called the Queue Summary which is emailed daily to show you new Contacts added to your Contact List and additions to your Pending Messages queue. If properly

configured, you can also log in to your Sendio message queue directly from the queue summary without the need of entering your password to utilize the full functionality of your Sendio system.



Queue summary snapshot taken Oct 30 at 5:51am [Live Version](#) | [Help](#)

sendio Opt-Inbox™

New Contacts

Last 28 Hours

Apr 10 12:45pm **Rianna Zieme** <richard88@bargainland.org> [Drop](#)

New Pending Messages

Last 28 Hours

Apr 10 12:45pm **Miss Susanna Fadel DDS** <csiemer@hangsh.com> "You available to talk today?" [Accept](#) [Drop](#)

Apr 10 12:45pm **Elianna Rohan** <mickey54@reilly.info> "You available to talk today?" [Accept](#) [Drop](#)

New Pending Bulk

Last 28 Hours

Oct 01 08:28 **Management Insight & Strategy** <managementhub@techreportstoday.com> **HELD BY ADMIN**
Delivering a Winning Presentation. Learn How to Communicate More Effectively and Improve Your Skills >>

Statistics

Last 24 Hours

Messages Arrived	125
Messages Accepted	50

[Unsubscribe](#)

Callouts:

- Mouse click here to view live version of your Queue Summary in a web page. This web view will show the most recent pending messages, including those that arrived after you received the Queue Summary Email.
- Click here to login to your full Sendio Message Queue (Web UI)
- Change new Accept Contacts to Drop Contacts In order to stop further emails from the sender.
- Buttons to Add/Drop messages or Senders
- Mouse click on the sender name in order to view the body of email message before releasing it to your Inbox. (Note: You may need to enable Pop-ups in your web browser first)

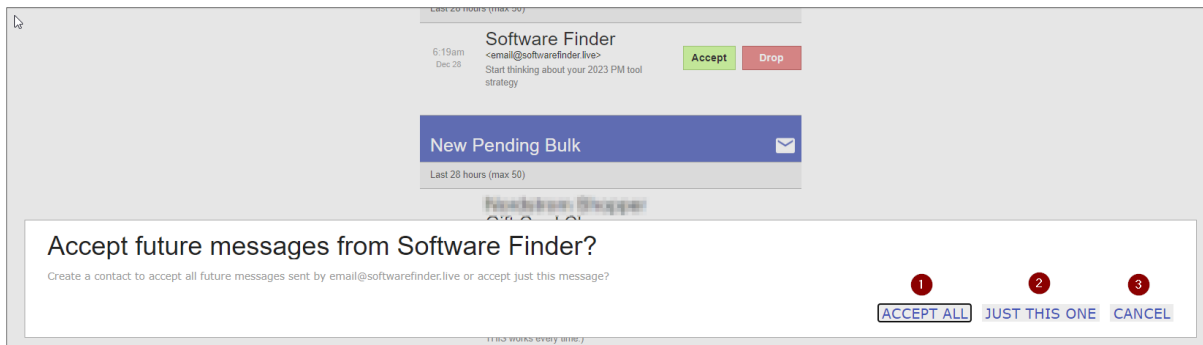
Clicking on Accept or Drop icon in Queue Summary Email

If you click on the Accept or Drop button in the Queue Summary email, you will be redirected to a web browser window for additional information. If you don't see anything in the browser window, be sure to allow popups from your Sendio system.

Accept Button

When you click on the Accept button in the Queue Summary email, a new browser window will open and allow you the following options.

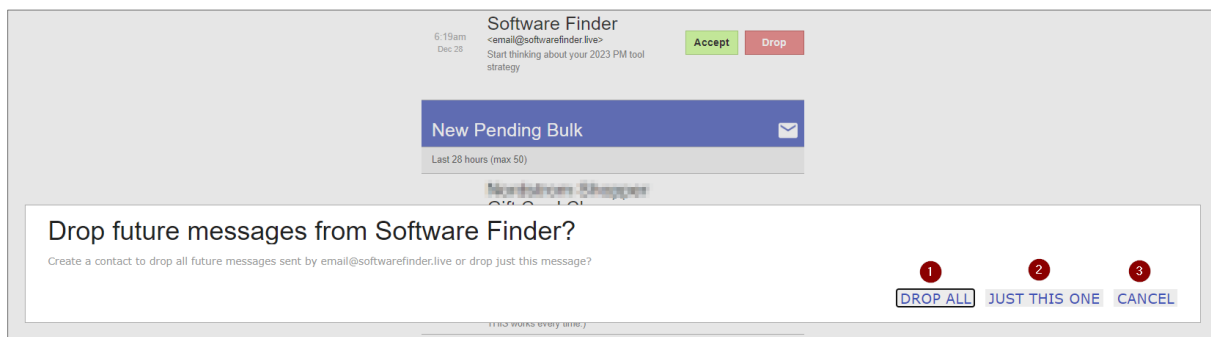
1. **Accept All** – Will accept and deliver all pending messages from the sender and add an *Accept Contact* to the user list to deliver any future messages from this sender.
2. **Just This Once** – Will accept the message and deliver without adding an *Accept Contact* to the user list.
3. **Cancel** – Will close the options window without taking any action on the message and the user can see their full queue.



Drop Button

When you click on the Drop button in the Queue Summary email, a new browser window will open and allow you the following options.

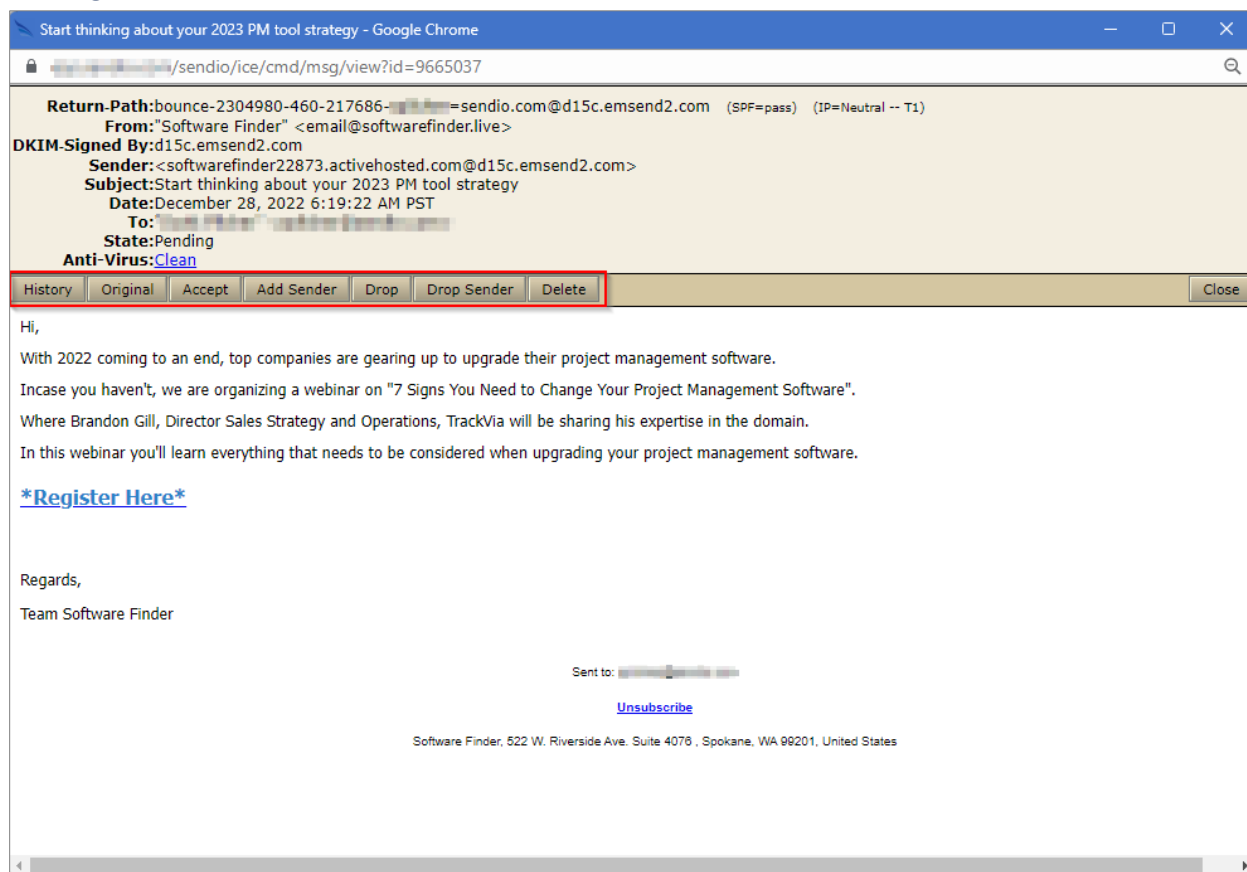
1. **Drop All** – Will drop all pending messages from the sender and add a drop contact to the user list to drop any future messages from this sender.
2. **Just This Once** – Will drop the message without adding a drop contact to the user list.
3. **Cancel** – Will close the options window without taking any action on the message and the user can see their full queue.



Clicking on Message from Queue Summary Email

If you click on the Message in the Queue Summary email, you will be redirected to a web browser window so that you can preview the message and take actions to Accept, Drop or Delete the email.

Message View



The menu bar highlighted in the red box gives the user many options from the Message View window.

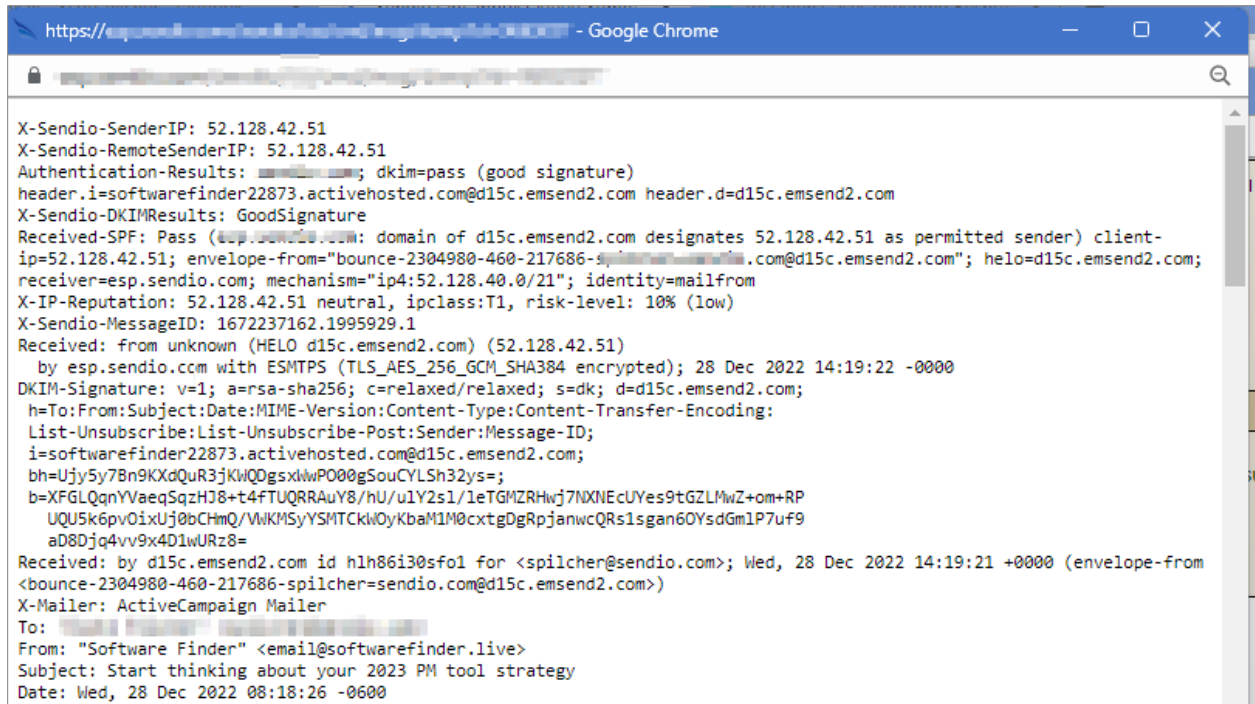
History

Will show the user everything that Sendio has done with the message.

Date & Time	Event	Event Detail
12/28/22 6:19 AM	Pending	No contact match, holding, no SAV sent (Mailing list message, has List-Unsubscribe header)
12/28/22 6:19 AM	Antivirus	No threats found.
12/28/22 6:19 AM	ZeroHourScan	No threats detected
12/28/22 6:19 AM	SilverListing	Sending IP passed test on Nov 30
12/28/22 6:19 AM	Received	delivery id is 1672237162.1995929.1.0

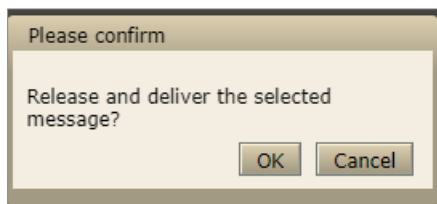
Original

Will show you the raw email with headers in a new window.



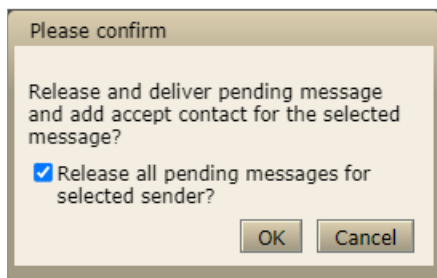
Accept

Accept the message without adding a contact to the user contact list.



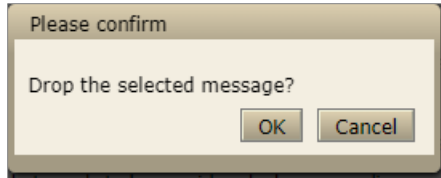
Add Sender

Accept the message and add an accept contact to the user contact list.



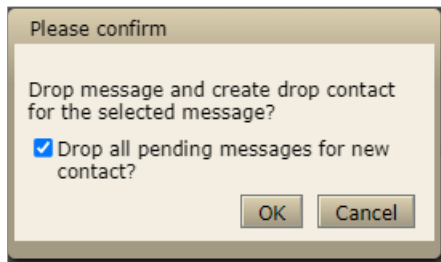
Drop

Drop the message without adding a drop contact to the user contact list.



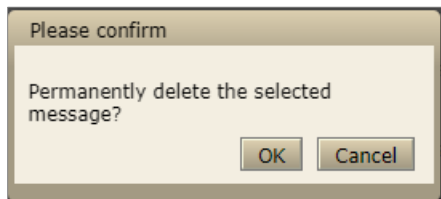
Drop Sender

Drop the message and add a drop contact to the user contact list.



Delete

Delete this message from the user queue.



SECTION 11: DKIM Primer

Per the DKIM.org website:

DKIM attaches a new domain name identifier to a message and uses cryptographic techniques to validate authorization for its presence. The identifier is independent of any other identifier in the message, such as the author's From: field.

The first version of DKIM synthesized and enhanced Yahoo!'s DomainKeys and Cisco's Identified Internet Mail specifications. It was the result of a year-long collaboration among numerous industry players, during 2005, to develop an open-standard e-mail authentication specification. Participants included Alt-N Technologies, AOL, Brandenburg InternetWorking, Cisco, EarthLink, IBM, Microsoft, PGP Corporation, Sendmail, StrongMail Systems, Tumbleweed, VeriSign and Yahoo!. The team produced the initial specification and several implementations. It then submitted the work to the IETF for further enhancement and formal standardization.

DomainKeys Identified Mail (DKIM) lets an organization take responsibility for a message that is in transit. The organization is a handler of the message, either as its originator or as an intermediary. Their reputation is the basis for evaluating whether to trust the message for further handling, such as delivery. Technically DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication. The identity is independent of other email identities, such as the author's From: field.

DKIM is not an anti-spam technology. It is a concept that is being rapidly adopted to prevent the spoofing of Internet Mail. The benefit to the DKIM design is that it avoids overloading the "main" TXT record for a domain (e.g., sendio.ca.com). If this domain wanted to use both DKIM and SPF (and maybe other TXT records for other purposes), then it may end up with too many TXT records returned to the query for the domain and the "right" record may not reach the requestor. DKIM is a cryptographic, signature-based type of email authentication. It is a combination of Yahoo's DomainKeys (DK) and Cisco's Identified Internet Mail.

DKIM requires a sender's MTAs or edge devices to generate "public/private key pairs" and then publish the public keys into their DNS records. The matching private keys are stored in a sender's outbound email servers, and when those servers send out email, the private keys are used to generate message specific "signatures" that are added in additional embedded email headers.

ISPs that authenticate using DKIM look up the public key in DNS and then can verify that the signature was generated by the matching private key. This ensures that an authorized sender actually sent the message, and that the message headers and contents were not altered in any way during the transmission from the original sender to the recipient.

The DKIM authentication process involves checking the integrity of the message using the public key included in the email signature header, in addition to verifying whether the public key used to sign the message is authorized to use the sender's email address. This step currently involves utilizing the DNS record of the sending domain. The authorization records in the DNS contain information about the

binding between a specific key and email address. Using a US Postal Service analogy, DKIM is like verifying a unique signature, which is valid regardless of the envelope or letterhead it is written on.

One of DKIM's advantages over an earlier version of the same technology is that it supports digital signatures by authorized third parties. This permits a legitimate sender of email newsletters, for example, to outsource the bulk mailing. It should also make it easier to maintain a legitimate signature when the email passes through several forwarders before arriving at its destination. Also, because of the way DKIM works, recipients can verify whether an email has been altered during transmission.

So DKIM's impact on phishing might be immediate, because it verifies that emails come from where they say they come from. For spam, however, it will probably take somewhat longer, because there's nothing to prevent a spammer from getting a key and sending out verified email. The spammer then has to build a reputation as a spammer unless there is a sender verification process such as that integrated into Sendio.

The rest of the page left blank

SECTION 12: Messaging Interaction

A few options that are used by Sendio may affect the interaction with the other components of your messaging environment.

Attachment Size: The default attachment size incoming to Sendio is 50 Megabytes. This size should be made larger or consistent with the message size on the MTA.

Timeout Values: Certain timeout values associates with the SMTP conversation can be modified if necessary.

System Response: The system response value e.g., sendio.<yourdomain>.com can be modified if necessary.

There are several SMTP compliant error messages that are associated with Sendio. If an error message is received because of an email, it is possible to compare this error against the list below to discover if the message came from Sendio or from another point in the messaging infrastructure.

No error -- continue:

235 ok, go ahead (#2.0.0)

Temporary errors which cause a deferral:

421 out of memory (#4.3.0)

421 unable to figure out my IP addresses (#4.3.0)

421 unable to read controls (#4.3.0)

451 qmail-spp failure: %ERRDETAIL1%: %ERRDETAIL2% (#4.3.0)

451 qqt failure (#4.3.0)

451 timeout (#4.4.2)

451 sorry, your envelope sender domain must exist (#4.1.8)

451 DNS lookup for your envelope sender domain failed (#4.1.8)

451 temporary error looking up your envelope sender domain (#4.1.8)

451 mailbox temporarily unavailable (#4.2.1)

454 oops, child won't start and I can't auth (#4.3.0)

454 oops, problem with child and I can't auth (#4.3.0)

454 oops, unable to open pipe and I can't auth (#4.3.0)

454 oops, unable to write pipe and I can't auth (#4.3.0)

Permanent errors which cause a rejection:

500 Your email was rejected because it contains the %VIRNAME% virus

501 auth exchange canceled (#5.0.0)

501 malformed auth input (#5.5.4)

501 Syntax error in options or argument. Illegal domain name SENDERDOMAIN% (#5.1.7)

501 Syntax error in options or argument (#5.1.7)

501 syntax error in options or argument (#5.1.3)

502 unimplemented (#5.5.1)

503 auth not available (#5.3.3)

503 MAIL first (#5.5.1)

503 no auth during mail transaction (#5.5.0)

503 RCPT first (#5.5.1)

503 you're already authenticated (#5.5.0)

504 auth type unimplemented (#5.5.1)

535 authentication failed (#5.7.1)

550 wrong address for responding to an address verification request. Your address has not been verified. Please see text of verification request message for instructions. (#5.7.1)

550 mailbox unavailable (#5.1.2)

550 mailbox unavailable (#5.1.1)

552 sorry, that message size exceeds my databytes limit (#5.3.4)

553 sorry, that domain isn't in my list of allowed rcpthosts (#5.7.1)

553 sorry, your envelope sender is in my badmailfrom list (#5.7.1)

554 too many hops, this message is looping (#5.4.6)

555 syntax error (#5.5.4)

SECTION 13: System Email Messages

Sendio generates a variety of alert and informational messages that are sent as emails to Users and Administrators.

Maintenance Release Notifications

There are four messages that Administrators may receive regarding new Maintenance Release software updates.

- Notification that a Maintenance Release is scheduled for Automatic Installation (1)
- Notification that a Maintenance Release is scheduled for Automatic Installation when no Alert Addresses have been specified in the system console (2)
- Notification that a Maintenance Release has been downloaded to Sendio and is available for manual installation (3)
- Notification that a Maintenance Release has been successfully automatically installed (4)
- Notification that Push Backup Failed (5)
- Journaling Queue Alert Notification (6)

Notice Date: 2022-11-14 12:23.

This automated notification is to inform you that your Sendio [node1.sendio.test] has finished downloading a new Maintenance Release that is ready to be installed.

Current Sendio Version: Sendio 9 (9.4.0)
Maintenance Release Version: Sendio 9 (9.4.0)
Automatic Update Scheduled: Sun Nov 20, 01:00 AM PST

For details about this update, visit <http://www.sendio.com/software-release-history>.

You have Automatic Updates enabled (recommended). If you take no further action, Sendio 9 (9.4.0) will be installed at your next scheduled update time on Sun Nov 20, 01:00 AM PST. Sendio updates normally take 5 minutes or less to complete and do not lead to any loss of messages or any noticeable disruption of email flow.

If you want it to be installed at a different time, you may:

- o Manually install at any time before the scheduled time
- o Configure a different automatic update time
- o Temporarily disable automatic updates

To manually install this Maintenance Release:

1. Access the console interface using a keyboard and monitor connected to the unit or using an SSH network connection.
2. Log into the console by specifying username "sysconfig" and the appropriate password (nothing will appear on screen when the password is entered).
3. Navigate to "Sendio Update" on the left side of console interface and press Enter.
4. Navigate to the "Apply Maintenance Release" button and press Enter.

To configure a different Automatic Update time or temporarily disable Automatic Updates:

1. Access the console interface using a keyboard and monitor connected to the unit or using an SSH network connection.
2. Log into the console by specifying username "sysconfig" and the appropriate password (nothing will appear on screen when the password is entered).
3. Navigate to "Backup/Maintenance" on the left side of console interface and press Enter.
4. Navigate to the "System Automatic Update" section and use the "Add" and "Delete" buttons to change the schedule.
5. Navigate to the "Save" button at the bottom of the "System Automatic Update" section after making changes and press Enter.

(1) Maintenance Release Scheduled for Automatic Installation

=====

NOTICE

=====

You received this message because no 'Alert Addresses' have been specified via the Console Interface.

You can set this value by going to the System Configuration tab.

Notice Date: 2022-11-14 12:31,

This automated notification is to inform you that your Sendio [node1.sendio.test] has finished downloading a new Maintenance Release that is ready to be installed.

Current Sendio Version: Sendio 9 (9.4.0)

Maintenance Release Version: Sendio 9 (9.4.0)

Automatic Update Scheduled: Sun Nov 20, 01:00 AM PST

For details about this update, visit <http://www.sendio.com/software-release-history>.

You have Automatic Updates enabled (recommended). If you take no further action, Sendio 9 (9.4.0) will be installed at your next scheduled update time on Sun Nov 20, 01:00 AM PST. Sendio updates normally take 5 minutes or less to complete and do not lead to any loss of messages or any noticeable disruption of email flow.

If you want it to be installed at a different time, you may:

- o Manually install at any time before the scheduled time
- o Configure a different automatic update time
- o Temporarily disable automatic updates

To manually install this Maintenance Release:

1. Access the console interface using a keyboard and monitor connected to the unit or using an SSH network connection.
2. Log into the console by specifying username "sysconfig" and the appropriate password (nothing will appear on screen when the password is entered).
3. Navigate to "Sendio Update" on the left side of console interface and press Enter.
4. Navigate to the "Apply Maintenance Release" button and press Enter.

To configure a different Automatic Update time or temporarily disable Automatic Updates:

1. Access the console interface using a keyboard and monitor connected to the unit or using an SSH network connection.
2. Log into the console by specifying username "sysconfig" and the appropriate password (nothing will appear on screen when the password is entered).
3. Navigate to "Backup/Maintenance" on the left side of console interface and press Enter.
4. Navigate to the "System Automatic Update" section and use the "Add" and "Delete" buttons to change the schedule.
5. Navigate to the "Save" button at the bottom of the "System Automatic Update" section after making changes and press Enter.

(2) Maintenance Release Scheduled for Automatic Installation, No Alert Addresses Specified

Notice Date: 2022-11-14 12:23,

This automated notification is to inform you that your Sendio [node1.sendio.test] has finished downloading a new Maintenance Release that is ready to be installed.

Current Sendio Version: Sendio 9 (9.4.0)
Maintenance Release Version: Sendio 9 (9.4.0)
Automatic Update Scheduled: Sun Nov 20, 01:00 AM PST

For details about this update, visit <http://www.sendio.com/software-release-history>.

You have Automatic Updates enabled (recommended). If you take no further action, Sendio 9 (9.4.0) will be installed at your next scheduled update time on Sun Nov 20, 01:00 AM PST. Sendio updates normally take 5 minutes or less to complete and do not lead to any loss of messages or any noticeable disruption of email flow.

If you want it to be installed at a different time, you may:

- o Manually install at any time before the scheduled time
- o Configure a different automatic update time
- o Temporarily disable automatic updates

To manually install this Maintenance Release:

1. Access the console interface using a keyboard and monitor connected to the unit or using an SSH network connection.
2. Log into the console by specifying username "sysconfig" and the appropriate password (nothing will appear on screen when the password is entered).
3. Navigate to "Sendio Update" on the left side of console interface and press Enter.
4. Navigate to the "Apply Maintenance Release" button and press Enter.

To configure a different Automatic Update time or temporarily disable Automatic Updates:

1. Access the console interface using a keyboard and monitor connected to the unit or using an SSH network connection.
2. Log into the console by specifying username "sysconfig" and the appropriate password (nothing will appear on screen when the password is entered).
3. Navigate to "Backup/Maintenance" on the left side of console interface and press Enter.
4. Navigate to the "System Automatic Update" section and use the "Add" and "Delete" buttons to change the schedule.
5. Navigate to the "Save" button at the bottom of the "System Automatic Update" section after making changes and press Enter.

(3) Maintenance Release Available for Manual Installation

At 2022-11-14 12:41:48 Sendio [node1.sendio.test] successfully updated to software version Sendio 9 (9.4.0).

(4) Maintenance Release Successfully Installed Automatically

Domain: QA.vibx.SENDIO.net
Serial Number: QAtest
Sendio ESP Version: Sendio ESP v5 (10.0507.0)

Could not mount remote backup

(5) Push Backup Failed

Notice Date: Mon, 20 Apr 2009 14:59:00 -0700 (PDT)

Current Journaling Queue Size: 1010
Journaling Queue Alert Threshold: 1000
Journaling Queue Limit: 10000

Dear Sendio Admin,

Your Sendio message journaling queue has exceeded the configured alert threshold of 1000 messages. This usually indicates that the archival system(s) being journaled to are either not reachable or are not able to journal messages as quickly as messages are arriving.

PLEASE CONFIRM THAT YOUR ARCHIVAL SYSTEM(S) ARE REACHABLE BY THE SENDIO Sendio DEVICE AND FUNCTIONING PROPERLY.

You will continue to get alerts as long as the condition persists. You have configured a minimum alert interval of 60 minutes, so the next alert will not be sent before Mon, 20 Apr 2009 15:59:00 -0700 (PDT).

If necessary, Message Journaling options can be configured in the Options tab of the System page in Sendio Admin GUI.

Recent Journaling Queue Size History:

	queued messages
== 2009-04-20 ==	
14:59:00	1010
14:58:00	905

(6) Journaling Queue Alert Notification

SECTION 14: SAV Messages

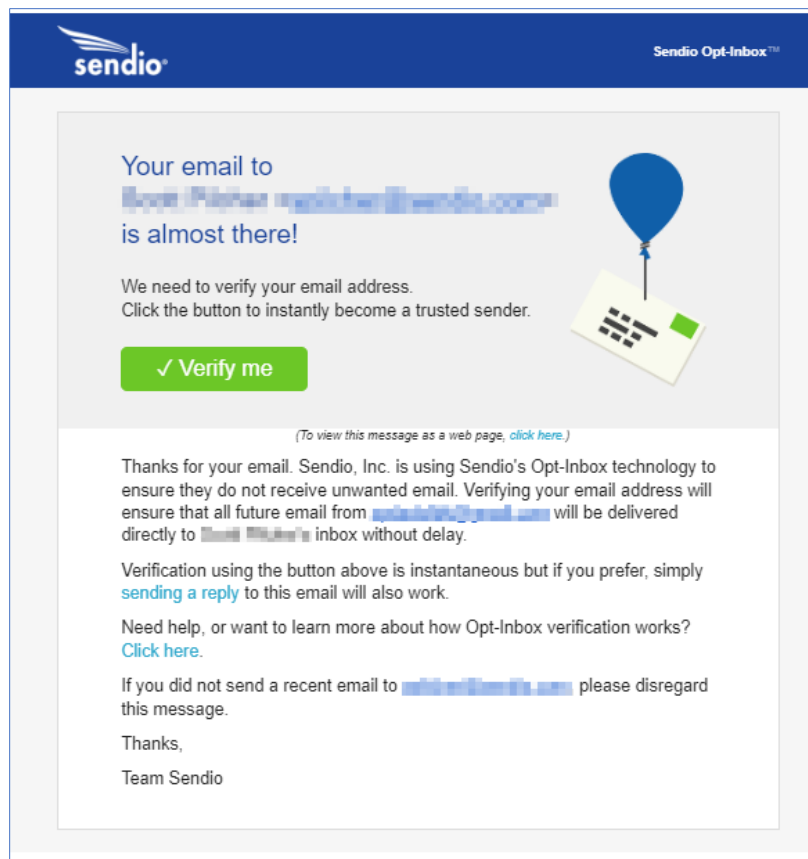
Part of Sendio email integrity workflow is the Sender Address Verification (SAV). Sendio generates SAV messages when an email is received from a sender that is not on a Contact list. These messages are based on templates which have dynamic fields that are filled in when a specific message is generated by Sendio.

There are two templates that are used as part of the Sender Address Verification process:


- SAV Request: the message that is sent to “challenge” an unknown email sender to verify they are human
- SAV Acknowledgement: the message that thanks a now “known” email sender for completing the verification process

These templates are available in various formats;

- Standard HTML Request (English)
- Brief Request (English) or (Spanish & English) *Examples shown below*
- Detailed Request (Spanish & English) or (Spanish) *Examples shown below*



SAV Verification request email



Your message has been delivered,
and your address has been verified
with **Sendio Opt-Inbox**

What is Sendio Opt-Inbox?

Bolster Your Existing Email Security

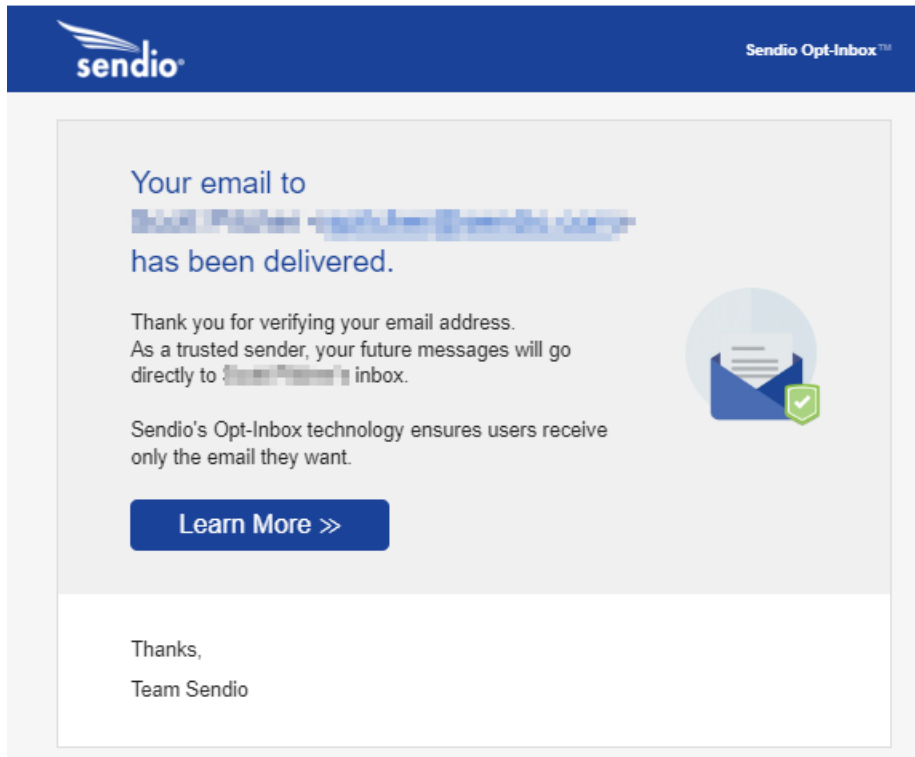
Despite being protected by advanced email security systems, many inboxes continue to be inundated with countless security-cleared messages comprised of persistent sales pitches and marketing communications, distribution lists and bulk sources.

Identifying and separating harmful messages from nuisance and potentially desired ones is increasingly difficult for many email security solutions. This can become particularly troublesome for executives and professionals who simply cannot afford to overlook an important email. Discovering a desired message in their cluttered quarantine queue (known as a false positive) is simply unacceptable.

Sendio's Opt-Inbox is a proprietary sender management process, acting on messages having already cleared email security, which would otherwise be released into a user's inbox, ensuring that recipients only receive messages from desirable sources, whether from individuals or subscriptions, leaving the new yet undecided sources to the recipient's discretion in a queue separate from the usually messy quarantine queue.

[Learn More About Opt-Inbox](#)[Request Product Information](#)

Web page that opens once the Verify process is completed.



Email confirmation received once SAV process has been successfully completed

SAV RESPONSE MESSAGES

Brief Request (English)

Action Required - Press REPLY and SEND

Inbox

12:43 PM (0 minutes ago)

Thank you for your e-mail. In order for your original message to be delivered, please join my e-mail network.

It's easy: just reply to this message.

By pressing REPLY and then SEND, you will be added to my list of trusted contacts and all your future e-mails will be delivered directly to my inbox. For more information on how this process works, please visit the link below.

Thank you,

This clean inbox powered by Sendio

<http://www.sendio.com/authentication-about>

Brief Request (Spanish & English)

Spanish > English View translated message

Always translate: Spanish

Gracias por su mensaje electrónico. Para poder entregar su mensaje original, por favor únase a mi red privada.

Es fácil: Sólo responda este mensaje.

Con oprimir RESPONDER y después ENVIAR, usted será agregado a mi lista de contactos de confianza y de ahí en adelante, toda su correspondencia será directamente entregada a mi correo personal. Para más información sobre como trabaja este proceso, por favor visite la página directamente abajo.

Gracias,

Este buzón se mantiene limpio a través de Sendio

<http://www.sendio.com/authentication-about>

Thank you for your e-mail. In order for your original message to be delivered, please join my e-mail network.

It's easy: just reply to this message.

By pressing REPLY and then SEND, you will be added to my list of trusted contacts and all your future e-mails will be delivered directly to my inbox. For more information on how this process works, please visit the link below.

Thank you,

This clean inbox powered by Sendio

<http://www.sendio.com/authentication-about>

Detailed Request (Spanish & English)

Un mensaje de "[REDACTED]"

Al parecer este mensaje es el primero que usted me envía desde que implementamos el Sistema de Verificación de Dirección del Remitente (SAV).

Su mensaje es importante para mí, y como me imagino que usted también lucha contra el SPAM como yo, le cuento que hemos implementado SAV, un poderoso sistema de verificación de quien envía correos electrónicos, para asegurarme de no recibir correos electrónicos indeseados.

Por favor, solo responda a este mensaje al presionar la opción Responder y luego Envía. Con esto se confirma su dirección. Haciendo solo esto sus futuros mensajes ya serán automáticamente aceptados al ser reconocido y entraran directamente a mi casilla de correos.

Cuando responda a este mensaje, asegúrese de que la dirección a la cual esta contestando sea:

[verify-1672170427.1921607.1.0.4e113f77-\[REDACTED\]@verify.sendio.com](mailto:verify-1672170427.1921607.1.0.4e113f77-[REDACTED]@verify.sendio.com)

Si usted no responde a este pedido de verificación de dirección durante 2 weeks, o si su respuesta no es enviada a la dirección indicada arriba, su mensaje original nunca será despachado.

Muchas Gracias!

[REDACTED]

Este buzón se mantiene limpio a través de Sendio

<http://www.sendio.com/authentication-about>

Message from "[REDACTED]"

I recognize from your email address that this is the first message I have received from you since Sendio, Inc. began using Sender Address Verification (SAV).

Your message is very important to me. Like you, we are very concerned with stopping the proliferation of spam. We have implemented Sender Address Verification (SAV) to ensure that we do not receive unwanted email and to give you the assurance that your messages to me have no chance of being filtered into a bulk mail folder.

By pressing REPLY and SEND to this message your original message will be delivered to the top of my Inbox. You need only do this once and all future emails will be recognized and delivered directly to me.

When replying to this email, please make sure that the following email address appears in the To: field of the reply:

[verify-1672170427.1921607.1.0.4e113f77-\[REDACTED\]@verify.sendio.com](mailto:verify-1672170427.1921607.1.0.4e113f77-[REDACTED]@verify.sendio.com)

If you are unable to respond to this authentication request within 2 weeks, or if your reply is not sent to the correct email address (as indicated above), your message may not be delivered.

Thank you!

[REDACTED]

This clean inbox powered by Sendio

<http://www.sendio.com/authentication-about>

[Message body removed.]

Detailed Request (Spanish)

Un mensaje de "[REDACTED]"

Al parecer este mensaje es el primero que usted me envía desde que implementamos el Sistema de Verificación de Dirección del Remitente (SAV).

Su mensaje es importante para mí, y como me imagino que usted también lucha contra el SPAM como yo, le cuento que hemos implementado SAV, un poderoso sistema de verificación de quien envía correos electrónicos, para asegurarme de no recibir correos electrónicos indeseados.

Por favor, solo responda a este mensaje al presionar la opción Responder y luego Envía. Con esto se confirma su dirección. Haciendo solo esto sus futuros mensajes ya serán automáticamente aceptados al ser reconocido y entraran directamente a mi casilla de correos.

Cuando responda a este mensaje, asegúrese de que la dirección a la cual esta contestando sea:

[verify-1672171004.1922445.1.0.d3491d03-\[REDACTED\]@verify.sendio.com](mailto:verify-1672171004.1922445.1.0.d3491d03-[REDACTED]@verify.sendio.com)

Si usted no responde a este pedido de verificación de dirección durante 2 weeks, o si su respuesta no es enviada a la dirección indicada arriba, su mensaje original nunca será despachado.

Muchas Gracias!

[REDACTED]

Este buzón se mantiene limpio a través de Sendio

<http://www.sendio.com/authentication-about>
