sendio®
The eMail Integrity Company

Sendio® Email System Protection

Administration Manual

Sendio version 5.0 & 6.0

Sendio, Inc. ▪ 4911 Birch, Suite 150 ▪ Newport Beach, CA 92660 USA ▪ +1.949.274.4375 ▪ www.sendio.com

Comments, corrections and suggestions regarding this document should be sent to:

support @ sendio.com

Table of Contents

INTRODUCTION

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

SENDIO USER ROLES

Conceptually, there are two "classes" of Sendio users:

- End-users (called simply **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 "slider" button that allows them to access the system administrative configuration features.

DOCUMENTATION

Documentation for Sendio is organized into a number of different manuals and guides. These are summarized below.

Administration Manual

THIS DOCUMENT. It describes the functionality of all Sendio features, and discusses configuration options and trade-offs. Intended for Administrators.

Backup & Restore Guide

Describes the processes for copying important data files from Sendio to a backup environment, and the processes for restoring backed-up data to Sendio in the event of a system failure. Intended for Administrators.

Deployment 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.

Installation Guide

A detailed description of the configuration that must be done in order to install Sendio on your network. It encompasses firewall modifications, IP address assignments and mail server administration. It also addresses server hardware installation. Intended for Administrators.

Quick Start Guide

An abbreviated 15-step process for complete Sendio installation and mail routing. Comprehensive installation details are found in the Installation Guide. Intended for Administrators.

User Guide

Describes in vivid detail the User experience in the Sendio web interface. It is appropriate to post this tutorial (in .PDF format) on a company intranet for User reference. Intended for Users.

User Quick Start Guide

Designed to be an easy reference for the most commonly used functions of the User interface on an Sendio. Intended for Users.

CONVENTIONS IN THIS 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.

Data that is typed into a field in the GUI is identified `using this Courier font`.

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 menu
- the System button
- the Outbound Control tabbed page

The options on 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*, *Established* or *Waiting*.

SECTION 1: CONCEPTS AND DEFINITIONS

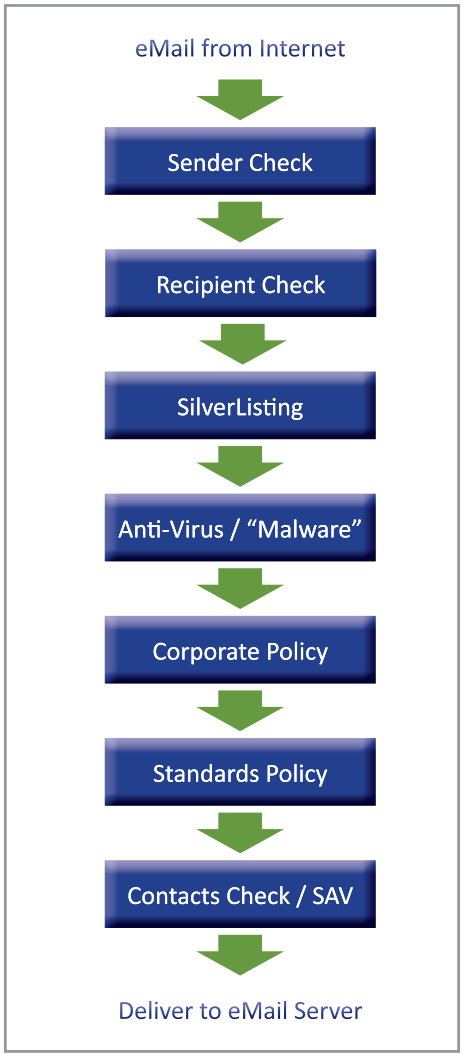
Before diving in to all of the details involved in administering Sendio it will be useful to first review a number of concepts and definitions that the reader of this manual is presumed to understand.

Platform

Sendio is a custom-built server appliance running a high-security implementation of the Linux operating system. Sendio has developed a large number of email message processing "services" that run on the system. Many of these services are administratively configurable. Sendio is also available as a hosted service. Everything in this manual applies to both the appliance and hosted version - there are no differences.

Message Flow

Sendio is installed "logically" between the Internet and one or more email servers (e.g. MS Exchange or Lotus Notes). 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 the unwanted messages, and forwarding the clean email to the email server(s) for delivery to end-users.



[1] Sendio High-Level Workflow Model

WARNING: It is recommended that the Sendio appliance be installed "behind" the organization's firewall. Sendio does have its own internal firewall. However, 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.

Workflow

Sendio is a sophisticated system that implements a highly configurable workflow engine. A high-level model of the workflow is shown in Figure [1]. The Administrator can configure specific policy and system behavior for each stage in 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 a message
- **Recipient Check:** the system verifies that the intended recipients of a message have accounts on the target email server
- **SilverListing:** 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 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 a number of configuration options that specify how the Sendio workflow should respond if one of the email integrity services becomes unavailable for a period of time.

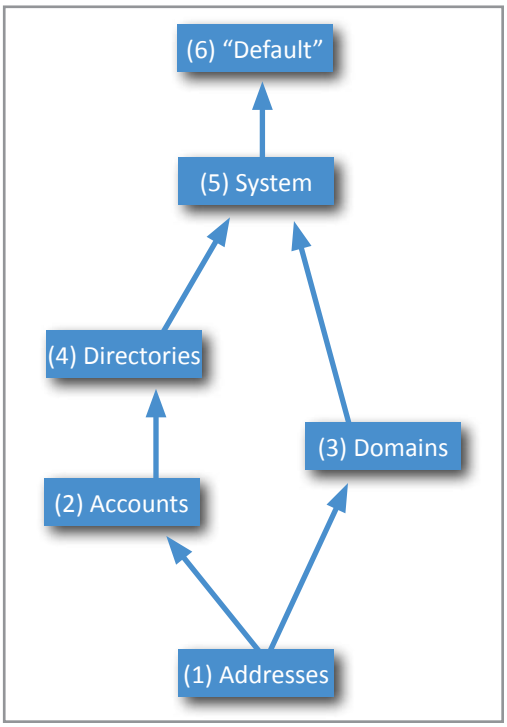
For example, if the anti-virus scanning service for inbound messages becomes unavailable, should email keep flowing or should it be halted until the service is restored. Since the risks associated with virus infections are high, this might be a prudent choice. In contrast, it may be quite acceptable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

Relationships, Ownership and "Default" Settings

Sendio maintains a database of the email inboxes that are protected and the relationships 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 a option setting in Sendio look up the setting for the recipient of the message currently being delivered. If no setting exists at the Addresses 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 Sendio installation process, a DNS Host record (A) that "names" the Sendio server is recommended.

EXAMPLE sendio.firstfederal.com

Using a Web browser, connect to Sendio with this name.

EXAMPLE http://sendio.firstfederal.com

NOTE: The Sendio web interface currently supports only the Microsoft Internet Explorer v7 (or later), Firefox v1.5 (or later) and Safari 3.1.2 (or later) browsers. Others may work but are not supported.

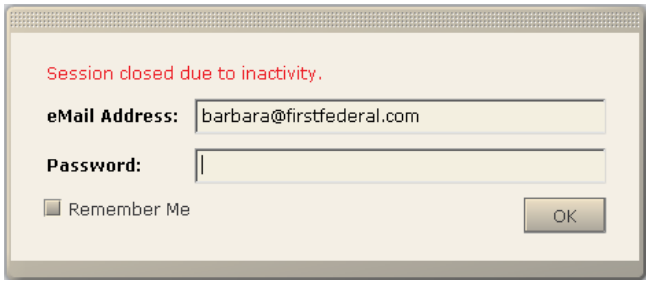
[2] Sendio Default Login Window

A Sendio login screen will be displayed, in one of two versions. The default requires an email address and network password, typically the same as your email account login, as shown in Figure [2].

[3] Sendio Login Window w/ 'Remember Me' Check Box

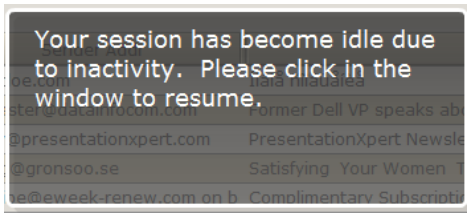
If the *Allow Remember Me on Login* option on the **Admin > System > Options** page (described in *Section 5*) has been *Enabled*, then the login screen will include a *Remember Me* check box (Figure [3]).

The *Remember Me* option causes Sendio to "remember" the email address authentication for a configurable period of time, so that this login step is skipped in the future.



[4] Expired Login (No 'Remember Me')

Sendio will automatically terminate a connection from the interface after 20 minutes of inactivity, requiring either a re-login or a session restart depending on whether the *Remember Me* option has been selected. (Figures [4] & [5]) The *GUI Inactivity Timeout* can be configured on the **Admin > System > Options** page to a value of 10 minutes, 20 minutes (default), 30 minutes or 1, 2, 3, or 4 hours.



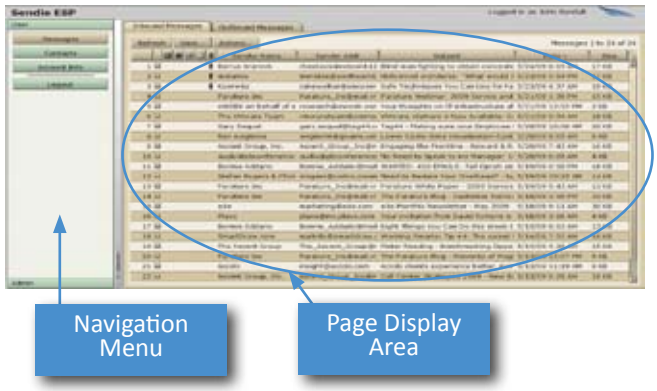
[5] Inactive Session Notice ('Remember Me')

TROUBLESHOOTING TIP: In the event that 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)

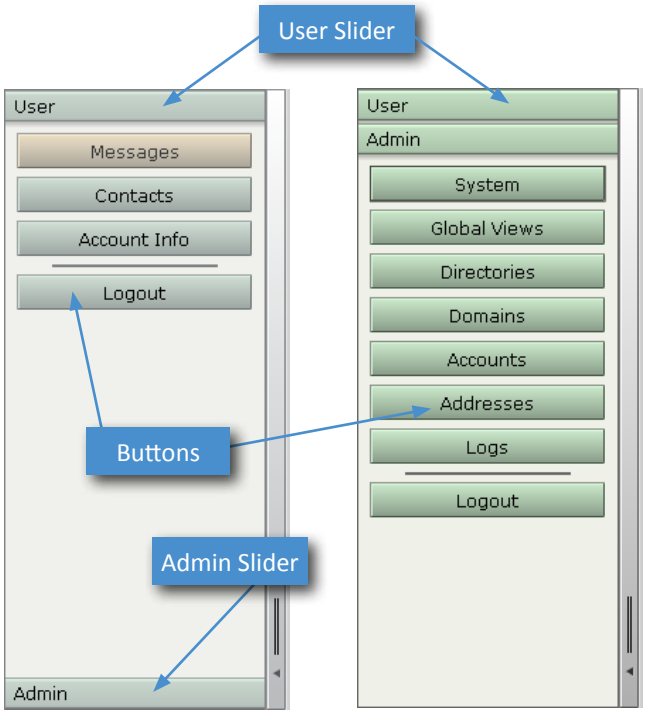
In any case, you may use the *sysconfig* administrative login and access the functions of the server. The format of this user is **`sysconfig@icebox`** and the password is the previously set *sysconfig* password. As the **Administrator**, you may have also set up a local password for any Sendio **Account** which can also be used in this scenario. If you suspect that Sendio has lost communications with the directory services, you may use the *sysconfig* interface to ping the directory server. You may also navigate to the Directories menu option on the **Admin** menu and synchronize the directory, which will verify communications and also confirm that the addresses have 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.

SECTION 3: SENDIO INTERFACE CONCEPTS



[6] Web GUI Layout

The Sendio web interface is composed of a navigation menu (left side) and a page display area (right side), shown in Figure [6].

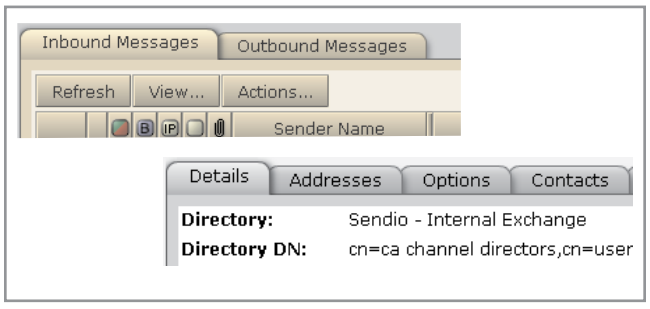


[7] User and Admin Navigation Menus

Two different navigation menus, one for **Users** and an expanded one for **Administrators**, are comprised of navigation buttons as shown in Figure [7].

Users with administrative privileges (i.e. **Administrators**) have an Admin "slider" at the bottom of their **User** navigation menu (left example above). Clicking on the Admin slider causes the **Admin** menu to "slide" up and display as shown in the right example above. Clicking on the User slider at the top of the **Admin** navigation menu makes the **Admin** menu slide away to reveal the **User** menu again. Users without administrative privileges will not have the Admin slider.

NOTE: The **User** menu and its functions are described in the *Sendio User Guide.*



[8] Examples of Pages with Tabs

PAGE DISPLAYS

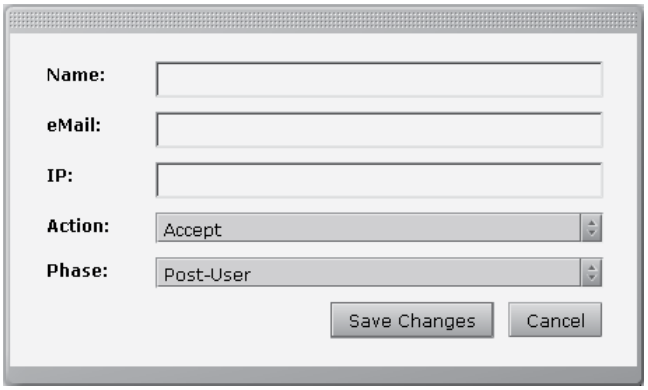
Clicking on different navigation menu buttons causes different Sendio information and configuration pages to be displayed. Some pages show information in tables and others in list format (described in more detail below).

Some pages are actually multiple pages separated into "tabs". Examples of tabbed pages are shown in Figure [8].

Pages include various control buttons that modify the display or change information, as shown in Figure [9].

[9] Examples of Control Buttons

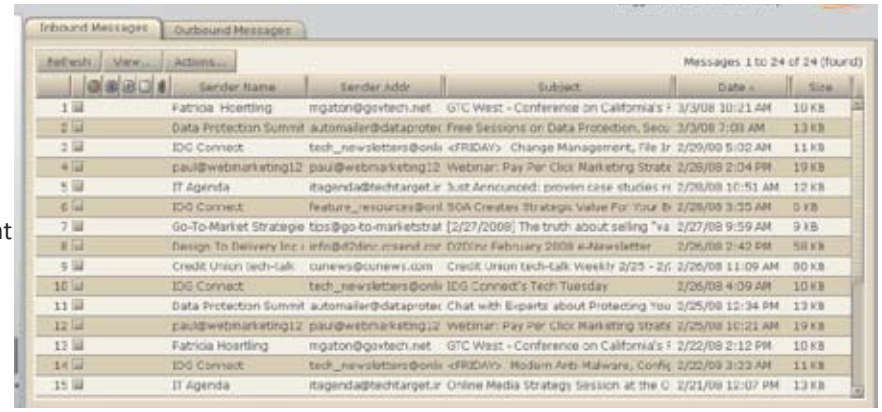
Some control buttons cause additional pages (or "windows") to "pop up" on top of primary pages, as shown in Figure [10].



[10] Example Pop-up Window

Table-Oriented Controls

Many pages display information in tables, such as the **Inbound Messages** and **Outbound Messages** pages. [11]



[11] Example of a Page Showing a Table

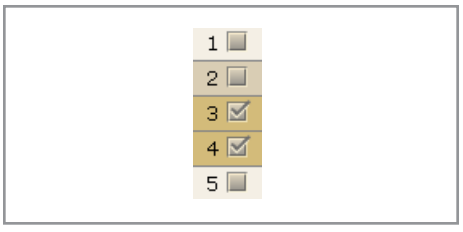
The number of records displayed in a table page is 50. If the table contains more than 50 records,  controls are displayed in the upper right of the page that allow you to jump between pages.

The  button causes a page to be reloaded in the browser.

The  button opens a pop-up window that lets you create a new record.

The  button opens either a drop-down list or a pop-up window of alternate criteria for viewing the displayed table.

The  button opens a drop-down list of actions that can be performed to modify the information in the table. Specific records can be modified individually or in a batch by "checking" the box(es) next to the record number(s). [12]



[12] Check boxes

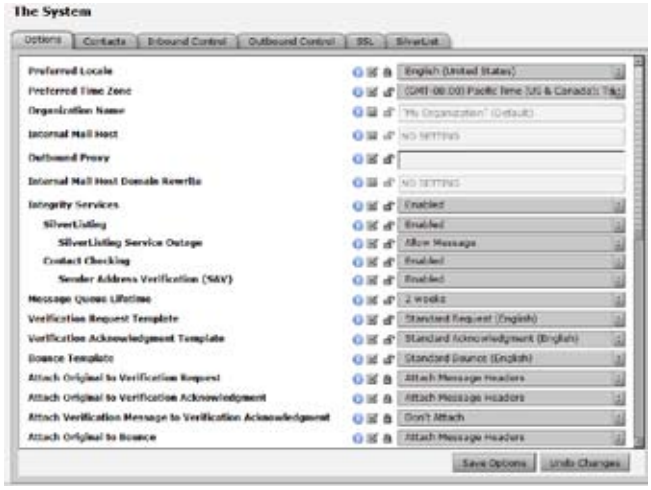
NOTE: Holding the Shift key and clicking lets you select a contiguous range of records. Holding the Ctrl key lets you select individual records as a group (but don't Ctrl-Click on the check boxes).

Subject	Date ▲
Credit Union tech-talk Weekly 3/3 - 3/7	3/4/08 11:21 AM
GTC West - Conference on California's F	3/3/08 10:21 AM
Free Sessions on Data Protection, Secu	3/3/08 7:08 AM
<FRIDAY> Change Management, File Ir	2/29/08 5:02 AM
Webinar: Pay Per Click Marketing Strate	2/28/08 2:04 PM
Just Announced: proven case studies re	2/28/08 10:51 AM

[13] Table Records Sorted by Date

Subject ▲	Date
Webinar: Pay Per Click Marketing Strate	2/28/08 2:04 PM
Webinar: Pay Per Click Marketing Strate	2/25/08 10:21 AM
Webinar Reminder: Leverage Channel F	2/21/08 8:22 AM
SOA Creates Strategic Value For Your Bı	2/28/08 3:55 AM
Show Your Commitment to Intellectual F	2/20/08 9:02 AM
Research Insider: The Fuel for Influence	2/21/08 9:29 AM

[14] Table Records Sorted by Subject



[15] Example of a Page Showing a List of Options

Clicking on a table column title or icon causes the table to resort the records in either ascending or descending order

List-Oriented Controls

Many pages display configuration options in lists, such as the **Admin > System > Options** tab. [15]

Most options can be configured at the **System** level, meaning the top administrative level for Sendio, thereby defining behavior for the overall system. Many options can also be modified at the **Domain** and **Account** (User) level, providing levels of customizability for sub-groups of users. Some options are configured at only the **Domain** level (e.g. DKIM Prefix).

This permissions architecture allows an **Administrator** to tailor Sendio email integrity functionality to their specific environment and user community.

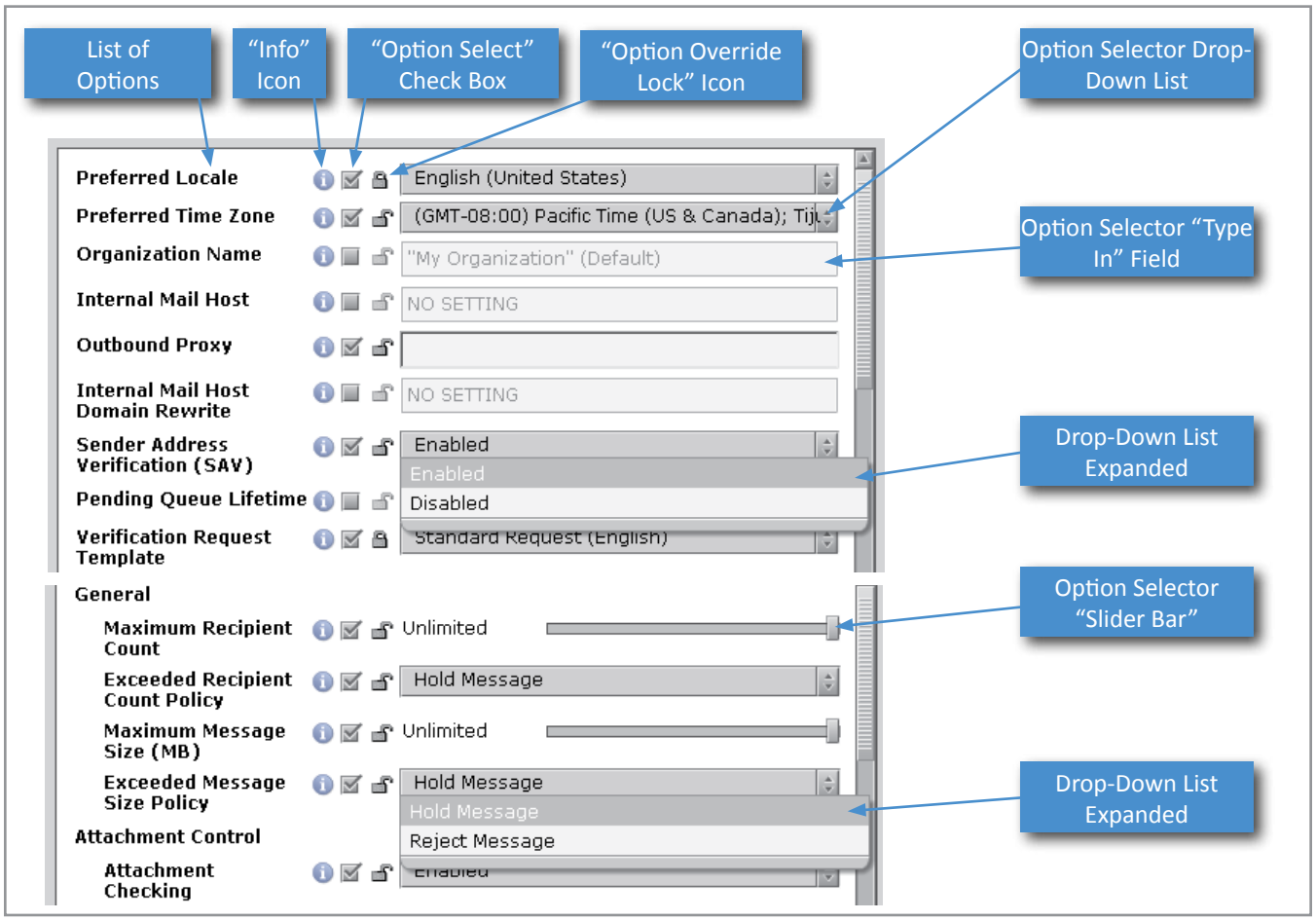
All configuration options share some common GUI controls, such as the *Help* icon, the *Option Select* icon and the *Option Override Lock* icon. Depending on the nature of the range of values for a option, different value selection controls are used.

Clicking on the *Info* icon for a configuration option causes *Information* text for the option to be displayed, consisting of a brief description, the inherited value of the option, the timestamp for when the option was last set, and the username of the **Administrator** who made the last setting. This *Information* text can also be displayed by clicking on the option name in the list.

The *Option Select* check box identifies whether the option is configured at a particular level in the hierarchy. If the box is not checked, the value display is "grayed out" and shows the value inherited from a higher level in the hierarchy, with the name of the level from which the value is inherited in parentheses. If the box is checked, a value can be specified or chosen from the available options.

If the *Option Override Lock* icon is "unlocked" , then the value set for the option can be reconfigured by the **Administrator** at a lower level in the hierarchy. If the icon is "locked" then the value cannot be checked and changed at a lower level.

You can change the *Option Override Lock* icon state back and forth from "locked" to "unlocked" by clicking on the icon.



[16] List-Oriented Controls

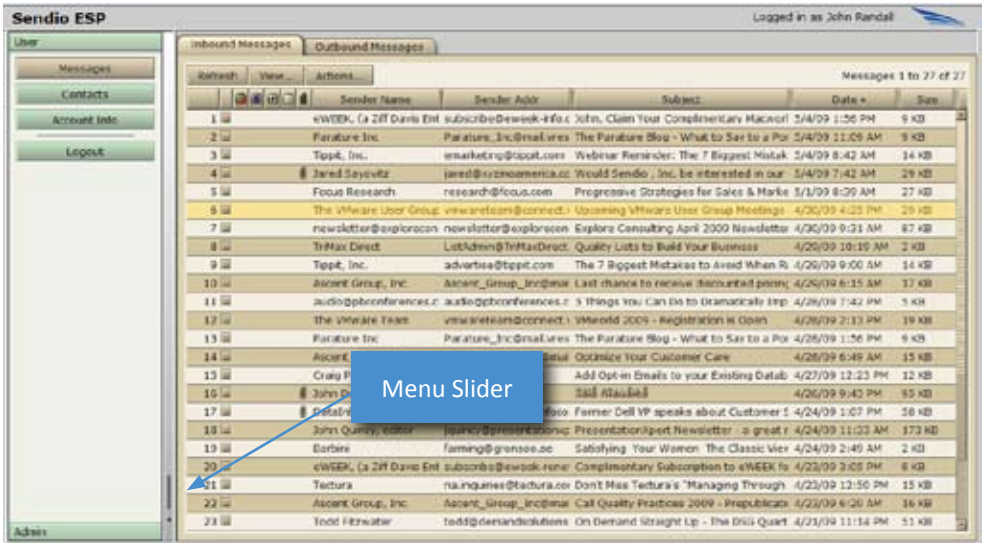
If an *unlocked* option is set at a lower level, and then the option is *locked* at a higher level, the lower level settings are ignored.

Some configuration options have only a pre-defined set of choices available, while others are set by typing in values. Those with pre-defined values use a drop-down list to present the choices that can be selected.

Some configuration options take numerical input that is set by controlling a "slider bar" with your mouse. Moving a slider bar all the way to the right causes the value to be set to *Unlimited* if appropriate. Slider bar controls do not permit precision value setting.

HIDING THE NAVIGATION MENU

Sometimes it is desirable to hide the **User** or **Admin** navigation menu so that there is more room to see the page display. Clicking on the *Menu Slider* causes the navigation menu to close or reopen. [17] [18]

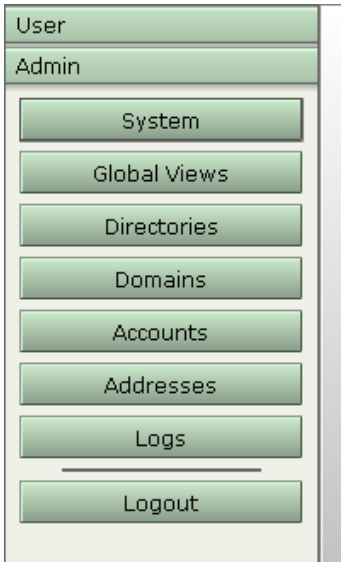


[17] Navigation Menu Open

[18] Navigation Menu Closed

This page intentionally left blank

SECTION 4: ADMIN MENU OVERVIEW



[19] Admin Navigation Menu

The **Admin** menu has seven navigation buttons that allow the **Administrator** to access distinct parts of the Sendio system.

The System menu button opens a group of tabbed pages that allow the **Administrator** to configure system-wide options for Sendio. Functions such as the Internal Mail host settings, anti-virus actions and corporate policy settings are configured here.

The Global Views menu option gives the **Administrator** views across both *Inbound* and *Outbound Message Queues* of all the user accounts on Sendio.

The Directories menu option is where the directory services connection (such as LDAP or Active Directory) is specified.

All the email domains that will receive traffic through Sendio are defined from the Domains menu option. This essentially defines the address spaces that are handled by Sendio.

From the Accounts menu option, an **Administrator** can access information about any user account. User options, addresses, contacts and message queues can be managed.

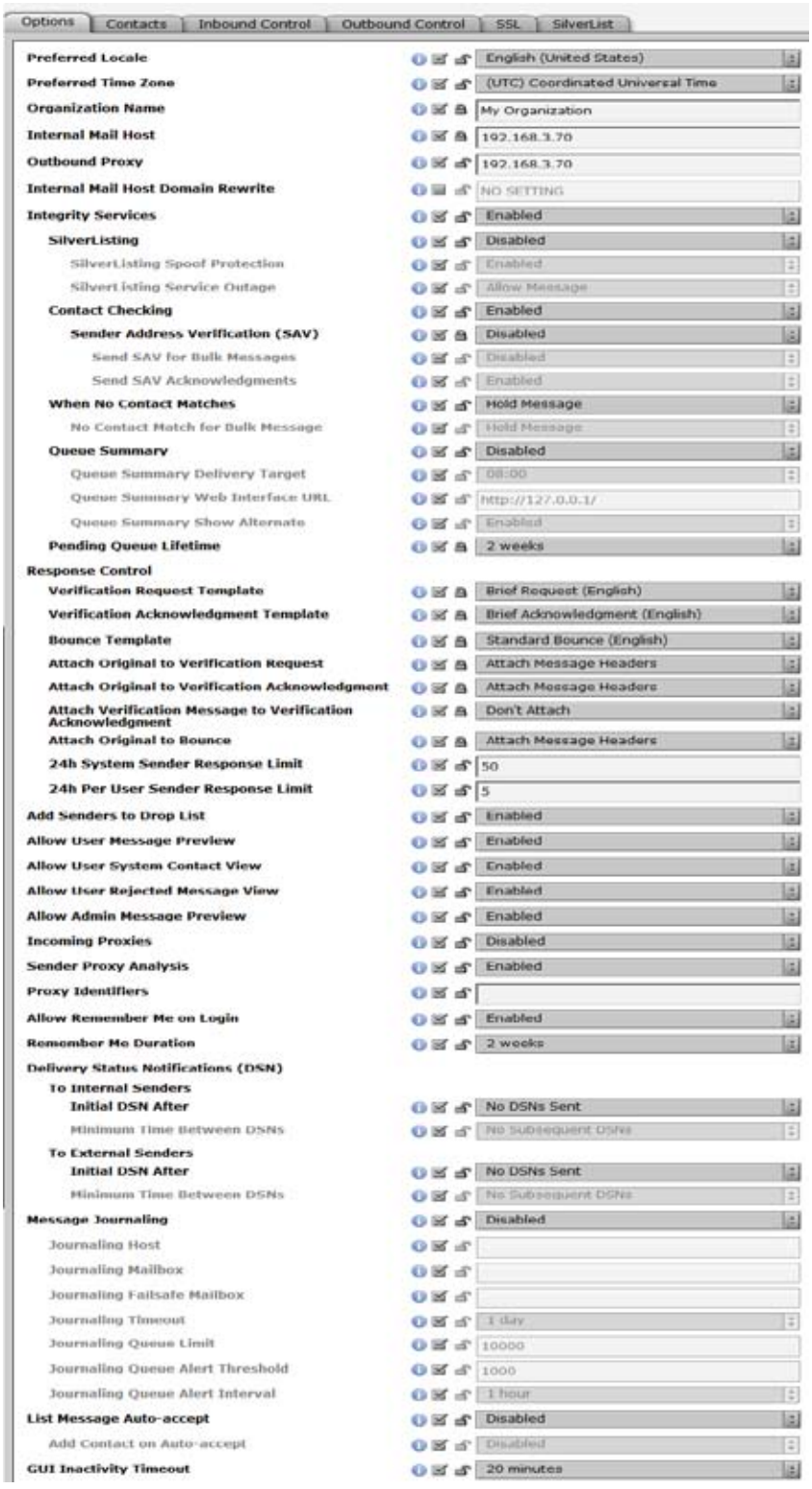
The Addresses menu option displays a cross reference of email addresses to their associated accounts. **Address** options can be managed

The Logs menu option provides a real-time interface to the SMTP, SMTPS, HTTP(s), SAV, MTA. FTP, Pass-Through and Auto-Accept logs on Sendio. There is an export function from any of these logs.

The following sections will describe the system functions and display pages available through each of the **Admin** menu buttons.

This page intentionally left blank

SECTION 5: SYSTEM PAGES



[20] The **Admin > System > Options** *Page*

The System button on the **Admin** menu provides access to the majority of Sendio configuration functions. These functions are divided into six areas identified on the six page tabs: **Options**, **Contacts**, **Inbound Control**, **Outbound Control**, **SSL**, and **SilverList**.

The default view of the **Admin > System** pages is the **Contacts** page. It is not possible to change the default view of the **Admin > System** pages.

THE SYSTEM > OPTIONS PAGES

The **Admin > System > Options** pages [20] display a list of options for Sendio that can be set at the **System** level. Many of the 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: (Default: *English (United States)*) The preferred locale for choosing display language and formats. Currently, only *English (United States)* is available.

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

Organization Name: (Default: *"My Organization"*) The name of the organization Sendio is serving. The value is 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. This option can be set at the **Domains** level allowing different organizational units to be served separately with distinct organization names in the SAV messages, and at the **Accounts** and **Addresses** level if desired.

Internal Mail Host: (Default: *No Setting*) The machine name or IP address 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 by 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 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 email through that proxy by entering the IP address or hostname into this field.

Internal Mail Host Domain Rewrite: (Default: *No Setting*) If set, this value rewrites the domain 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 SilverListing, Sender Address Verification 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 GUI. 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 which bypass Integrity Services are displayed in a different log than normal messages. This log can be viewed by clicking the "Passthrough Log" button in the Logs tab of the web GUI.

> **NOTE:** Accounts/Users with Integrity Services disabled are unable to receive 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 process is enabled. Please see the SilverListing section later in this document for more information.

Sendio 6 only

SilverListing Spoof Protection: (Default: *Enabled*) Indicates whether or not the SilverListing process is applied to messages which are received from email addresses in a Contact list but from a IP which has not previously passed the SilverList test. Please see the SilverListing 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 Sender Address Verification 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*.

Sendio 6 only

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

Sendio 6 only

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

Sendio 6 only

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

Sendio 6 only

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**. See *Section 12: Queue Summary* for more details.

Queue Summary Delivery 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 12: Queue Summary* for more details.

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. See *Section 12: Queue Summary* for more details.

Queue Summary Show Alternate: (Default: *Enabled*) Enables the display of bulk messages in the email notification below the standard *Pending Queue* summary.

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. This 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.

Verification Request Template: (Default: *Standard Request (English)*) This option can be modified to change between English, Spanish and combination templates. See *Section 16: SAV Messages* for more details.

Verification Acknowledgement Template: (Default: *Standard Request (English)*) This option can be modified to choose 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 this may cause other servers to mistake an SAV Request for a 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. Attaching the entire message is discouraged.

Attach Verification Message to Verification Acknowledgement: (Default: *Don't Attach*) Indicates whether or not to attach a copy of the RETURNED VERIFICATION MESSAGE to the verification acknowledgement message. Can be set to attach the entire verification 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 this may cause other servers to mistake the bounce message for a spam messages.

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 this may cause other servers to mistake the bounce message for a 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.

Sendio 6 only

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

Sendio 6 only

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

Allow User System Contact View: (Default: *Enabled*) Allows the **System** level contacts to be visible by **Users**. **Users** will be able to click on **User > Contacts > System Contacts** and view a table of the **System** contacts.

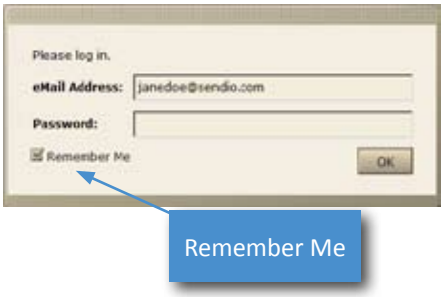
Allow User Rejected Message View: (Default: *Enabled*) Allows the **Rejected Messages** view to be visible by **Users**. **Users** will be able to click on **Inbound Messages > Views > Rejected Messages** and view a table of the **Rejected** messages.

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

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, this value should be set to *Enabled*.

> **NOTE:** In some cases, firewalls can be configured to be mail proxies. The test is whether the firewall makes store-and-forward decisions regarding accepting email.

Sender Proxy Analysis: (Default: *Enabled*) Sendio is capable of determining 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, this value should be set to *Enabled*.



[21] Remember Me login check box

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 interface login screen [21]. Selecting *Remember Me* instructs the web interface 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 for how long the system should wait before requiring re-authentication of login credentials if a user checks the *Remember Me* box on the login screen. Options are 1, 2, 3, 4, 5, 6 days, or 1, 2, 3, 4 weeks.

Delivery Status Notifications: Controls the generation of Delivery Status Notifications to internal and external recipients. Delivery Status Notifications are generated when Sendio is not able to immediately deliver a message.

To Internal Senders > Initial DSN After: (Default: *No DSNs Sent*) Specifies when the initial Delivery Status Notification is generated for *Outbound* messages and delivered to internal senders. Options are No DSNs Sent, 5 minutes, 20 minutes, 1 hour, 4 hours, 8 hours or 1 day.

To Internal Senders > Minimum Time Between DSNs: (Default: *No Subsequent DSNs*) Specifies when additional Delivery Status Notification are generated for *Outbound* messages and delivered to internal senders. Options are No Subsequent DSNs, 1 hour, 4 hours, 8 hours, 1 or 2 days.

To External Senders > Initial DSN After: (Default: *No DSNs Sent*) Specifies when the initial Delivery Status Notification is generated for *Inbound* messages and delivered to external senders. Options are No DSNs Sent, 5 minutes, 20 minutes, 1 hour, 4 hours, 8 hours or 1 day.

To External Senders > Minimum Time Between DSNs: (Default: *No Subsequent DSNs*) Specifies when additional Delivery Status Notification are generated for *Inbound* messages and delivered to external senders. Options are No Subsequent DSNs, 1 hour, 4 hours, 8 hours, 1 or 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*) Turns the Message Journaling feature On or Off.

Journaling Host: (Default: *No setting*) Hostname or IP address of journaling/ archiving host to which a copy of all messages will be sent.

Journaling Mailbox: (Default: *No setting*) Email address of mailbox on the internal email server to which a copy of all messages will be sent. If *Journaling Host* is configured with an IP address or Host Name messages will be delivered to the mailbox on the *Journaling Host*.

Journaling Failsafe Mailbox: (Default: *No setting*) Email address of mailbox on a separate email server to which a copy of all messages will be sent in the event the *Journaling Host* or *Journaling Mailbox* are unreachable. If a permanent failure is returned by the *Journaling Host* the *Journaling Failsafe Mailbox* will be tried immediately. If Sendio is unable to contact the *Journaling Host* the *Journaling Failsafe Mailbox* will be used once the *Journaling Timeout* (below) has been exceeded.

Journaling Timeout: (Default: *1 day*) The amount of time Sendio will continue to attempt sending of messages to the *Journaling Host* before sending to the *Journaling Failsafe Mailbox*. Options are 1, 2, 4 or 12 hours, 1, 2, 3, 4, 5 or 6 days or 1 or 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* messages are sent to administrators. Options are every 10, 20 or 30 minutes or 1, 2, 3 or 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.

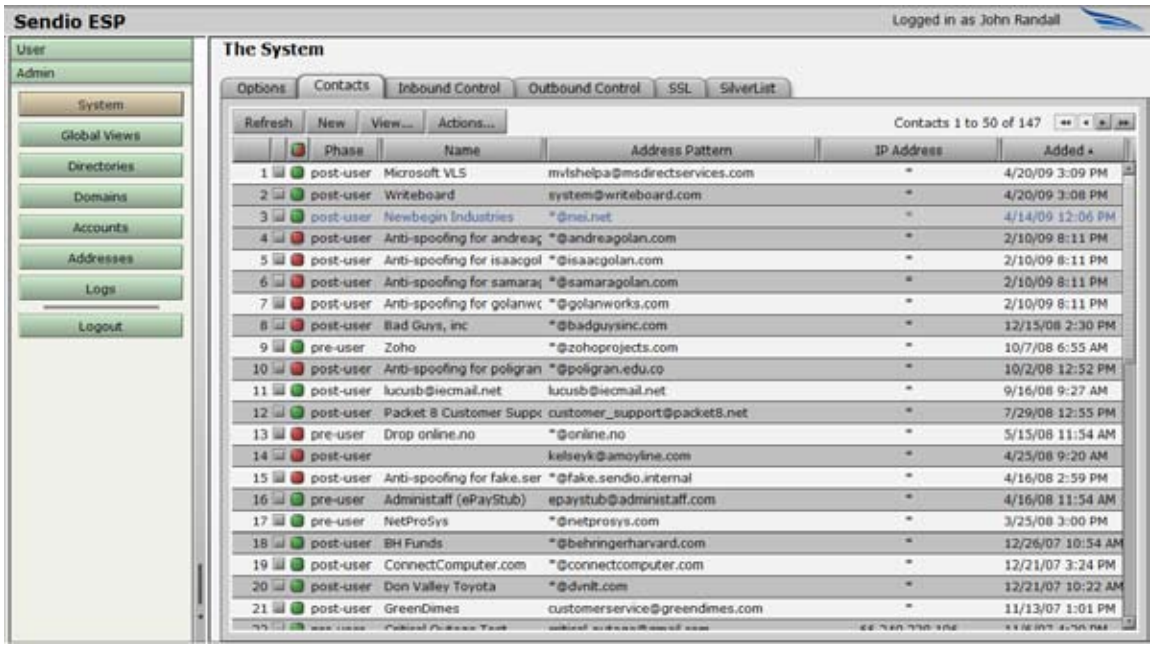
Add Contact on Auto-Accept: (Default: *Disabled*) If a list message is accepted via the *List Message Auto Accept* option, should an *Account Contact* be automatically created for the sending email address.

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 are every 10, 20 or 30 minutes or 1, 2, 3 or 4 hours.

NOTE: Remember to click the Save Options button if any changes are made to any options or else the changes will be lost when you exit.

THE SYSTEM > CONTACTS PAGE

The **Admin > System > Contacts** page displays a table of system-wide contacts. [22] These addresses represent individuals or organizations whose emails are to be either "accepted", "held" or "dropped" on a system-wide basis if they are received by Sendio.



[22] The **Admin > System > Contacts** *Page*

NOTE: It is suggested that **System** contacts be compiled and imported into Sendio prior to full deployment to reduce the initial number of SAV messages to known contacts, if desired. See **Admin > System > Contacts > Actions** below.

On the left side of the page is a column with a square two-color icon in the header:  . Each record in the table has either a green, a red or a white/gray icon in this column.

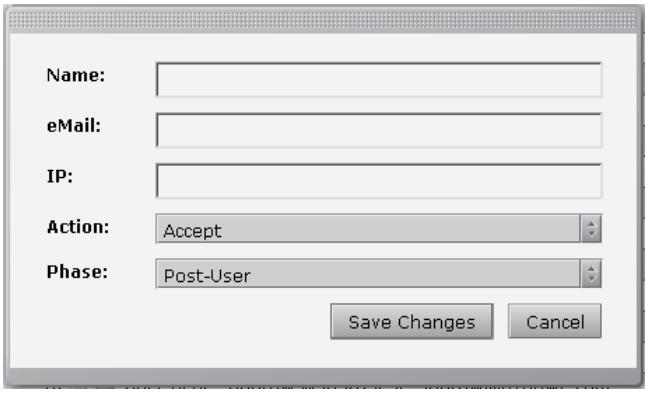
- A green icon indicates that the address of this "sender" is on the system *Accept-List* and that messages from this sender are to be immediately delivered to the destination inbox.
- A red icon indicates that the address of this "sender" is on the system *Drop-List* and that messages from this sender are to be immediately discarded and not delivered to the destination inbox.
- A white/gray icon indicates that the address of this "sender" is on the system *Hold-List* and that messages from this sender are to be held in a user's *Pending Queue*, and either manually released to the inbox or simply allowed to "age out" of the queue.

Creating a New Contact

To enter a new contact, click the New button. The pop-up window shown in Figure [23] appears. Enter the name and email address of the contact in the appropriate fields. One or more wildcards (*) may be used at any point in the email address.

NOTE: The *Name* field is for display purposes only.

To add an entire domain to the *Accept-List*, the email format is **`*@domainname.com`**.



[23] Create a New Contact

IP Field

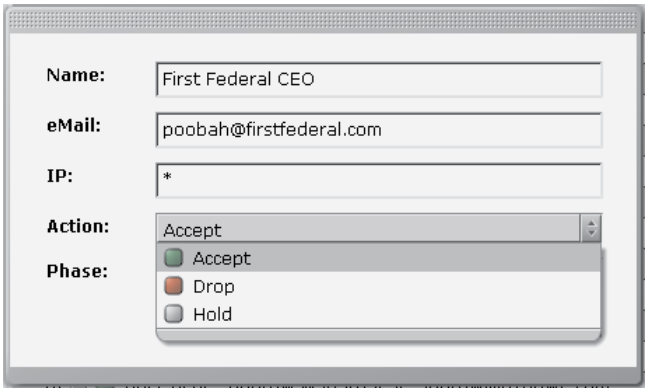
The *IP* field allows you to input a specific IP address from which the corresponding email address must originate. Mail from this email address with a different IP address will not match the *Contact*. If left blank, the *IP* field will be filled with a "*" indicating that this particular contact's email can come from any IP address.

NOTE: At this time it is not possible to list IP addresss by range. Each IP address will require a separate *Contact* entry.

Action Field

The *Action* field has three options on a drop-down menu [24].

- *Accept* adds the contact to the system *Accept-List*
- *Drop* adds the contact to the system *Drop-List*
- *Hold* adds the contact to the system *Hold-List*

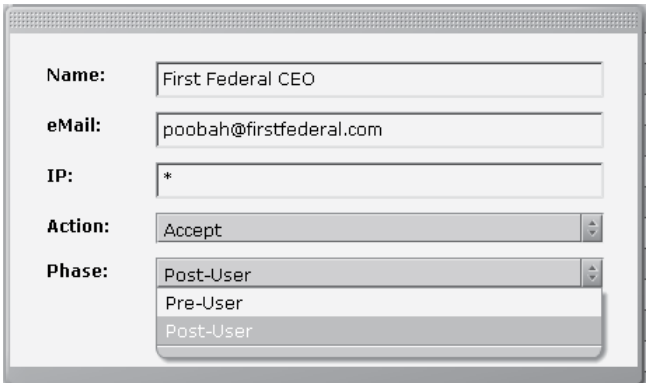


[24] Action Options

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

The *Hold* action leaves a message visible in the *Message Queue* for manual handling. Having a *Hold* contact is also like having no contact at all, but prevents Sendio from sending an SAV message out. It can be useful for dealing with domains that use auto-responders when there is a desire for Sendio to avoid sending SAV messages to these auto-responders.

Phase Field



[25] Phase Options

A System Contact also has a *Phase* indication. [25] The phase of a contact indicates the order in which the contact is checked against the **System**-, **Domain**- and **User**-based *Contact Lists*.

The order of checking contacts is:

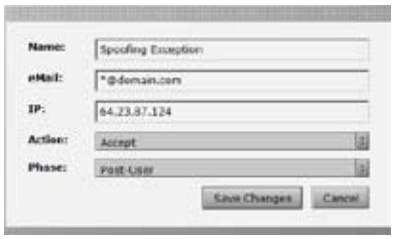
1. System Pre-User
2. Domain Pre-User
3. User
4. Domain Post-User
5. System Post-User

A *Phase* of *Pre-User* will prevent **Users** from overriding a **System** *Contact*, while *Post-User* allows them to customize their *Contact* lists.

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** List.

If a contact is on multiple *Contact Lists* with conflicting workflow definitions (eg 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*.



[26] Anti-Spoofing Contact Exception

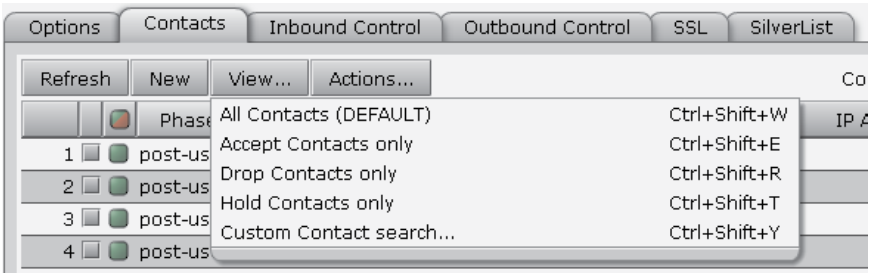
> **NOTE:** By default, when a new *Domain* is added a *Drop Contact* entry for your organization domain(s) is added, with a *Post-User* phase [26]. The format would be `*@yourdomain.com`. The reason for this is that only your email server should generate messages from your domain. If a message from the internet is coming into your organization ***from*** your domain, then some type of "spoofing" is probably occurring and the message will be rejected.

Changing Contact Information

To change any of the information in an existing contact, select the record and click **Actions... >** *Edit Selected Contact*, or double-click the contact entry in the *Contact List*. The pop-up window will be displayed. Modify the contact information and save the changes.

Changing the View of the Contacts Page

The default view of the **Admin > System > Contact** page shows all contacts. Clicking on the View... button opens a drop-down menu with other view options. There are also shortcut keys that can be used to initiate these views. [27]

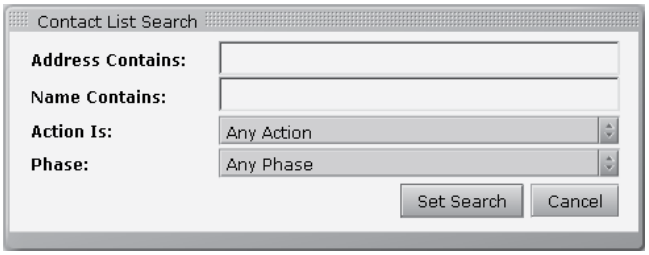


[27] **Admin > System > Contacts > View** *Menu*

Custom Contact search...

If a specific contact needs to be located, the *Custom Contact search...* option can be used.

In the *Contact List Search* pop-up window [28], a portion of the address or name, the *Action* to *Accept*, *Drop* or *Hold*, and the *Phase* of the contact can be entered; it is not necessary to enter all three. Once the information has been entered, click the *Set Search* button, and the screen will display the results of the custom filter request. If an expected contact does not display, reduce the requirements in the custom filter.

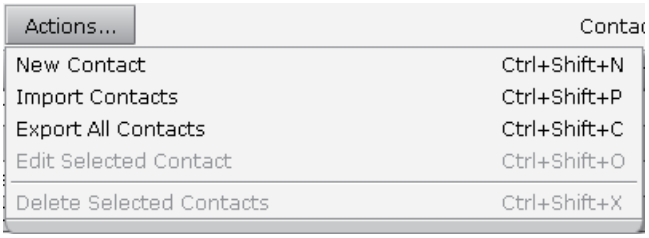


[28] Contact List Search Window

System > Contacts > Actions Options

The Actions... button opens a drop-down menu as shown in Figure [29].

The *New Contact* action provides the same function as the New button described above.



[29] **Admin > System > Contacts > Actions...** *Menu*

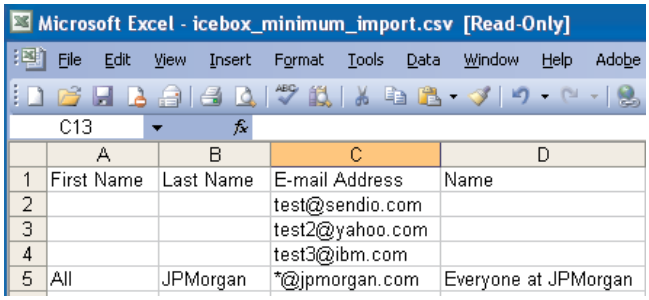
Import Contacts

The *Import Contacts* action opens a window, shown in Figure [30], which guides you through the process of importing a set of contacts from an external source. Three formats are supported:

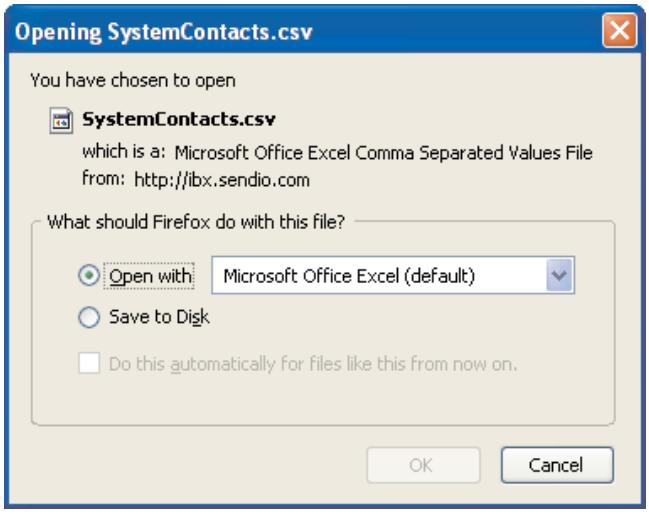
- Comma Separated Value (CSV)
- vCard 2.1 and vCard 3.0 from Lotus Notes 6
- Structured Text exports from Lotus Notes 5

These contacts can be from an MS Exchange database or other email system, an enterprise CRM system such as Oracle or SAP, or from any other contact database.

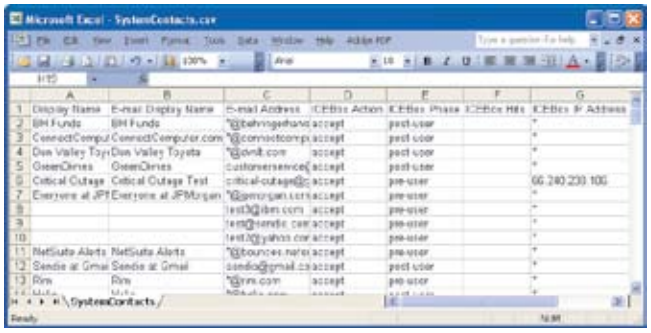
[30] Import System Contacts Window



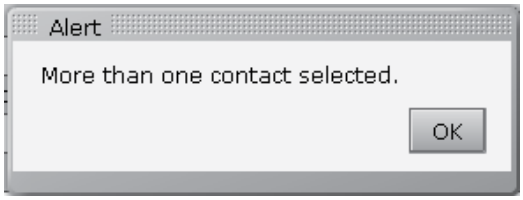
[31] System Contact Import CSV File Structure



[32] Export System Contacts Dialog



[33] Exported System Contacts



[34] Alert Dialog

The CSV file must be structured in a specific format, shown in Figure [31]. An example is viewable by clicking on the word "here" in the pop-up window instructions.

In the import window, click the *Browse…* button to specify the CSV file to import. Select whether the imported contacts are to be configured as *Pre-User* or *Post-User*, and then click the *Import* button. All imported contacts will be added to the **System** *Accept-List*.

NOTE: When exporting a contact list from MS Outlook, accept all the defaults in the export action. The resulting file will be in the correct format for import into the Sendio system.

TROUBLESHOOTING TIP: An import will be unsuccessful if there is no header row as indicated in the example file. The columns can be in any order.

Export All Contacts

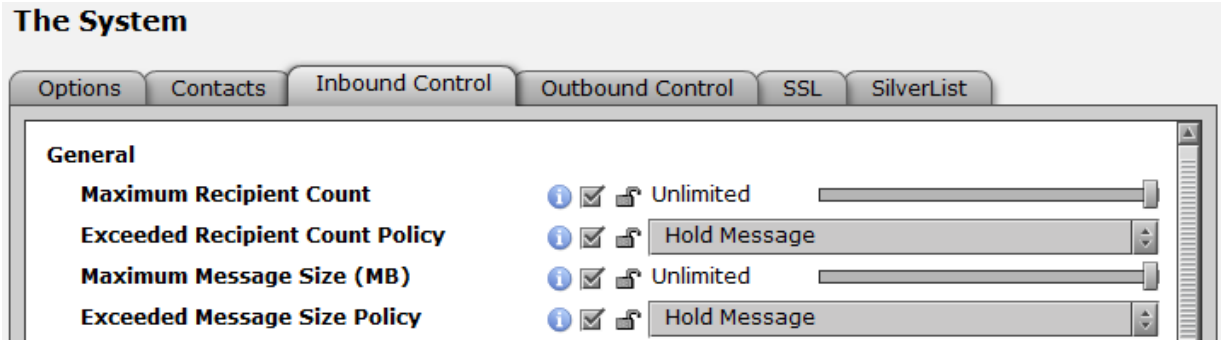
The *Export All Contacts* action executes a process to write all of the contacts to a CSV file, readable by MS Excel and other applications. A dialog box shown in Figure [32] opens, where you specify what to do with the exported file. A portion of an exported file is also shown in Figure [33].

Edit Selected Contact

Select a record to edit by clicking the record or the check box next to the record number. Then click **Actions...** *Edit Selected Contact.* Only one contact can be edited at a time. If more than one record is selected, an *Alert* dialog box will be displayed as shown in Figure [34].

Delete Selected Contacts

The *Delete Selected Contacts* action causes all of the records that have been selected (by clicking their check box) to be removed. If a contact is removed, and a message is subsequently received from that address, the sender will receive an SAV message.



[35] **System > Inbound Control** *General Group*

THE SYSTEM > INBOUND CONTROL PAGE

The **Admin > System > Inbound Control** page displays a list of options that specify how Sendio should process inbound messages. These options are grouped by related functions. Figure [35] shows the *General* group.

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.

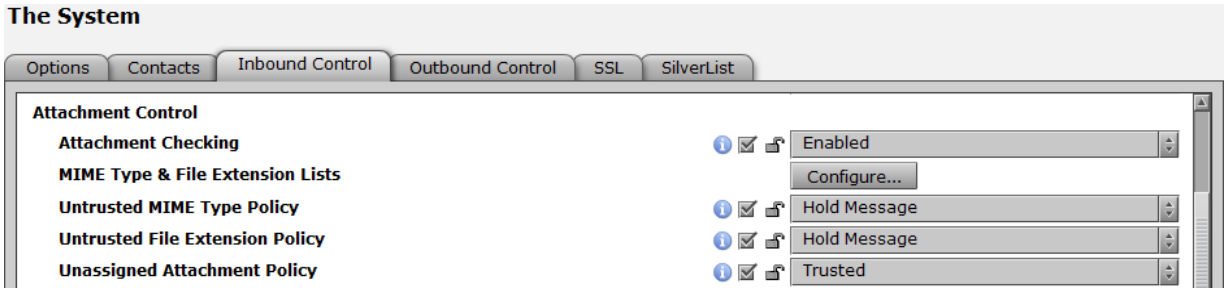
Exceeded Recipient Count Policy: (Default: *Hold*) Allows the **Administrator** to determine the disposition of a message that violates the maximum value set in the option above. Choices for this value are *Hold* and *Reject*.

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.

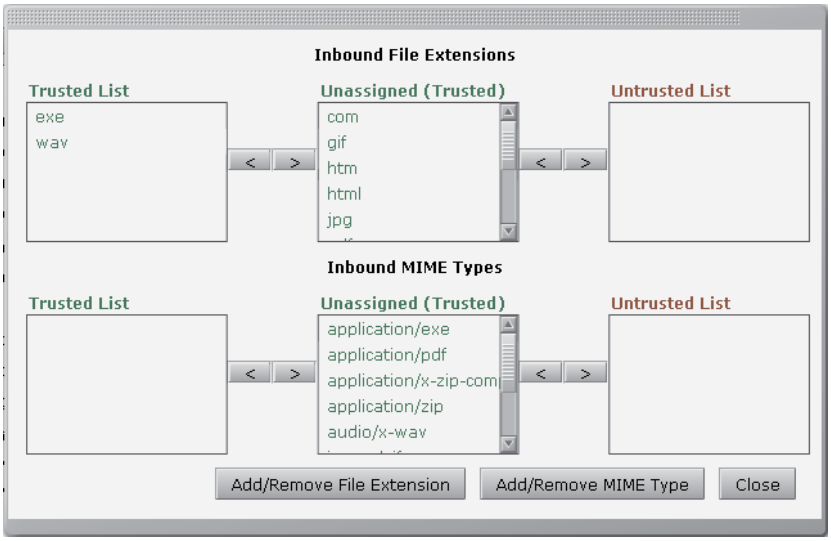
Exceeded Message Size Policy: (Default: *Hold*) Allows the **Administrator** to determine the disposition of a message that violates the maximum value set in the option above. Choices for this value are *Hold* and *Reject*.

Attachment Control

Figure [36] shows the *Attachment Control* options group.



[36] **System > Inbound Control** *Attachment Control Group*



[37] Attachment Configuration Pop-up Window

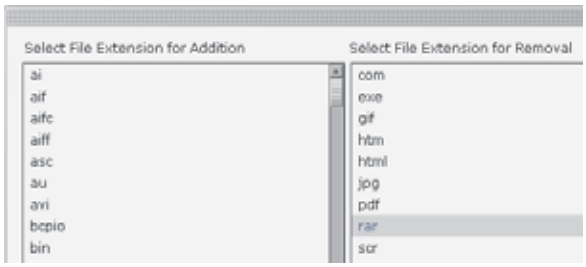
Attachment Control specifies how attachments to messages are to be handled by Sendio. By default, *Attachment Control* is *Disabled*, meaning all attachments from valid/verified senders to known recipients are passed through the system. The **Administrator** must specify which attachment types to process, and whether to *Hold* or *Reject* an *Untrusted* attachment.

Clicking on the Configure... button opens the *Attachment Configuration* window, shown in Figure [37].

Attachments are classified into two groups: File Extensions and MIME Types. In each group, specific attachment types can be assigned to the *Trusted* List, the *Unassigned List*, or the *Untrusted* List. Different processing actions can be specified for each List. By default, all types start as *Unassigned*.

Attachment types are moved between lists by clicking on the name to highlight it, and then clicking one of the arrows to move it to a different list.

Modifications in the *Attachment Configuration* window are effective as soon as they are made.



[38] Additional File Extension and MIME Types

NOTE: To move an Extension or Type from the *Trusted* List to the *Untrusted* List directly, click the farthest right hand arrow.

Once the attachments are classified, the handling policies are then set. The defaults are *Hold* for types on the *Untrusted* Lists and *Allow* for the rest of the attachment types.

WARNING: Making these modifications during peak business hours may impact system performance for a brief period.

Sendio recognizes hundreds of file extensions and MIME types. [38] A set of commonly used extensions and MIME Types is pre-populated into the *Unassigned* Lists. Clicking on the Add/Remove buttons allows other extensions and MIME types to be added for policy management purposes.

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 a number of services, including SPF checking and **Contact** checking.

[39] **Admin > System > Inbound Control** *Sender IP Address Groups*

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.

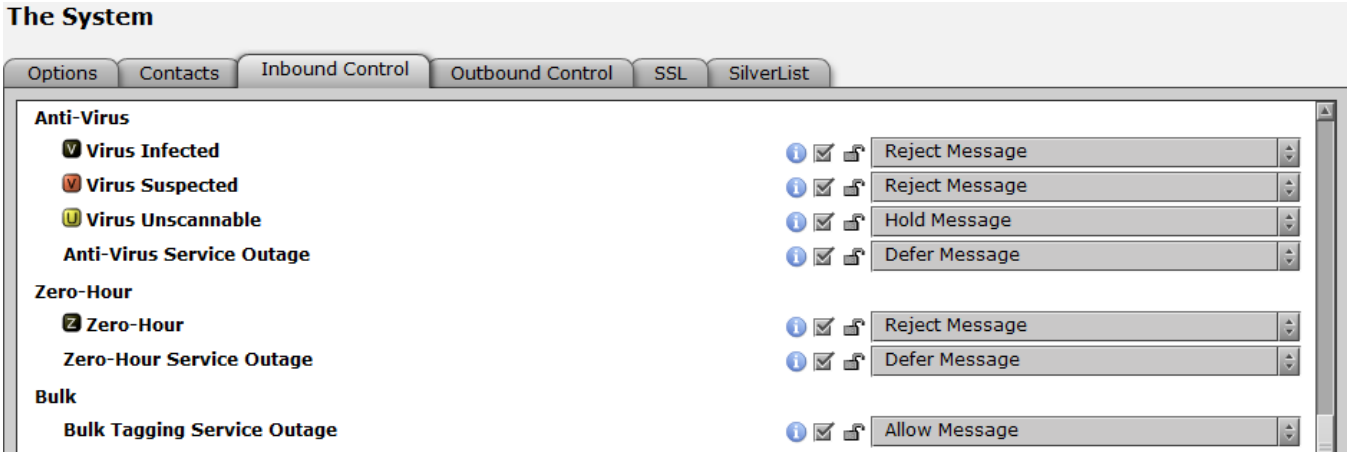
Sendio 6 only

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 service is only availalbe when using the Commtouch Zero Hour package.

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 a number of 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).

NOTE: If a proxy is specified, but some email is received by Sendio without passing through the proxy, this is a network mis-configuration and will confuse Sendio message processing.



[40] **System > Inbound Control** *Anti-Virus, Zero-Hour and Bulk Groups*

Anti-Virus

Sendio includes two distinct services for providing anti-virus protection: traditional signature-based scanning for "known" viruses and a "zero-hour" "recurrent pattern detection" (RPD) technology (licensed from Commtouch) that helps identify outbreaks of previously unknown viruses.

The next two groups on the **Admin > System > Inbound Control** page, shown in Figure [40], configure policies for the anti-virus services. The policy choices are *Reject*, *Hold* and *Allow*. The icons on the left of these options are used within the *Inbound* and *Outbound* message queue displays to signify the disposition of the message.

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. The corresponding icon is a black square with a white "V"  .

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. The corresponding icon is a red square with a black "V"  .

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. The corresponding icon is a yellow square with a black "U"  .

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

WARNING: If there are no other means of checking for virus infections downstream of Sendio in the messaging path (such as email server-based or desktop client-based), then it is strongly recommended that message delivery be *Deferred* until the anti-virus service is restored.

Zero-Hour

When a new virus is released, one characteristic is typically to try to multiply and spread as quickly as possible before the anti-virus vendors identify the "signature" of the new virus and update their databases. Using Recurrent Pattern Detection (RPD), this rapid propagation can frequently be identified and measures can then be taken. This concept is known as "zero-hour" or "zero-day" protection, since it attempts to provide protection from "time zero" (when a new virus is released) until the virus is identified and blocked with signature scanning.

Zero-Hour technology has been proven effective at limiting the scope of new virus outbreaks.

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 of time, messages can either be deferred until the protection resumes or can be forwarded on without scanning.

Bulk

Recurrent Pattern Detection (RPD) used in the Zero-Hour anti-virus service also provides a facility to "tag" certain messages that, while not malicious as in a true virus, are being sent in large volumes across the Internet. These messages are sometimes referred to as "bulk" mailings. Examples are email newsletters to large distribution lists or press releases to many recipients.

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 of time. The default is *Allow*.

ANTI-SPOOFING STANDARDS

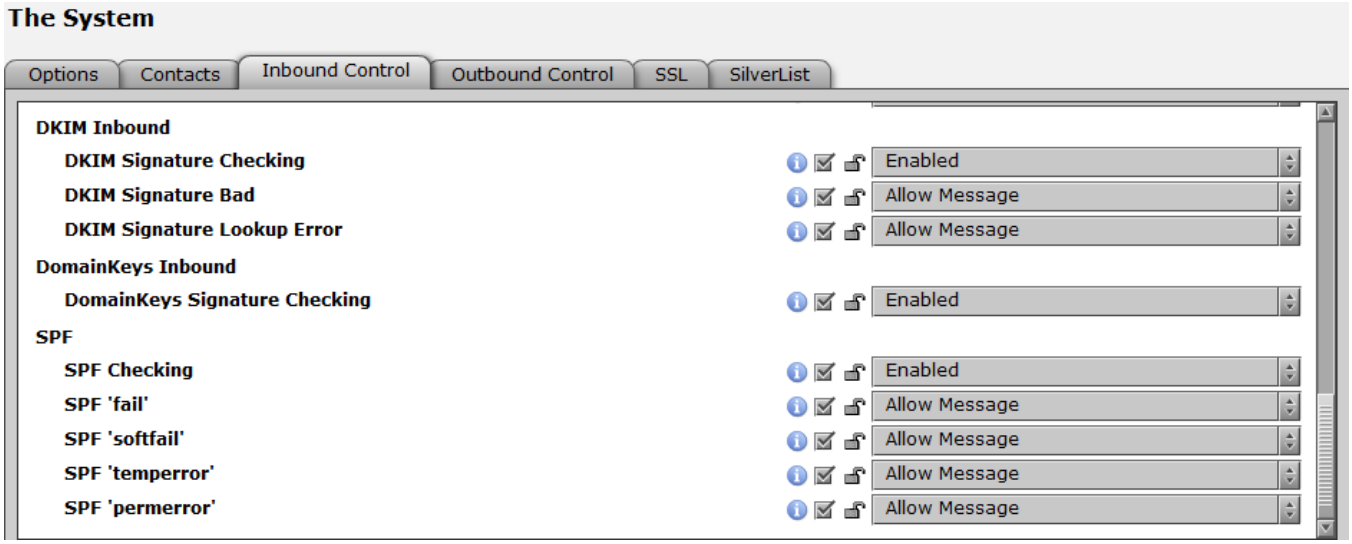
The final three groups on the **Admin > System > Inbound Control** page [41] provide controls for configuring two international standards for defeating attempts by criminals to send unwanted email messages that pretend to be from a legitimate source. This type of email attack is known as "spoofing".

Sendio supports both the "DomainKeys Identified Mail" (DKIM) and "Sender Policy Framework" (SPF) techniques for identifying "spoofed" messages.

These settings define how Sendio handles incoming messages that incorporate either SPF or DKIM certification. (Configuring Sendio to certify outbound messages is described in the **Admin > System > Outbound Control** section.)

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 concepts are described in more detail in *Section 8: Domains Pages* and *Section 12: DKIM Primer*.



[41] **Admin > System > Inbound Control** *DKIM Inbound and SPF Groups*

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 sub-domain 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 as a result 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. In the event that 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 in the event that the DKIM process cannot be performed.

DomainKeys Inbound

DomainKeys is a proprietary technology that preceded DKIM. It is used by a small number of companies, but has legacy value to certain organizations. All current installations of DomainKeys are being replaced by DKIM.

DomainKeys Signature Checking: (Default: *Enabled*) Sendio can be configured to check for DomainKeys and verify the validity of the key. The results of the check are in the delivery headers, but the Administrator cannot enact any policy against the result.

SPF

Sender Policy Framework is a Microsoft-led standard for email anti-spoofing. For further information on SPF, please consult **`www.openspf.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 occured 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 permament error occured during the SPF check. This is very likely due to an incorrect SPF record for the sending domain. Available 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.

THE SYSTEM > OUTBOUND CONTROL PAGE

The configuration options on the **Admin > System > Outbound Control** page in Figure [42] 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 the **Inbound Controls**, options are organized into groups.

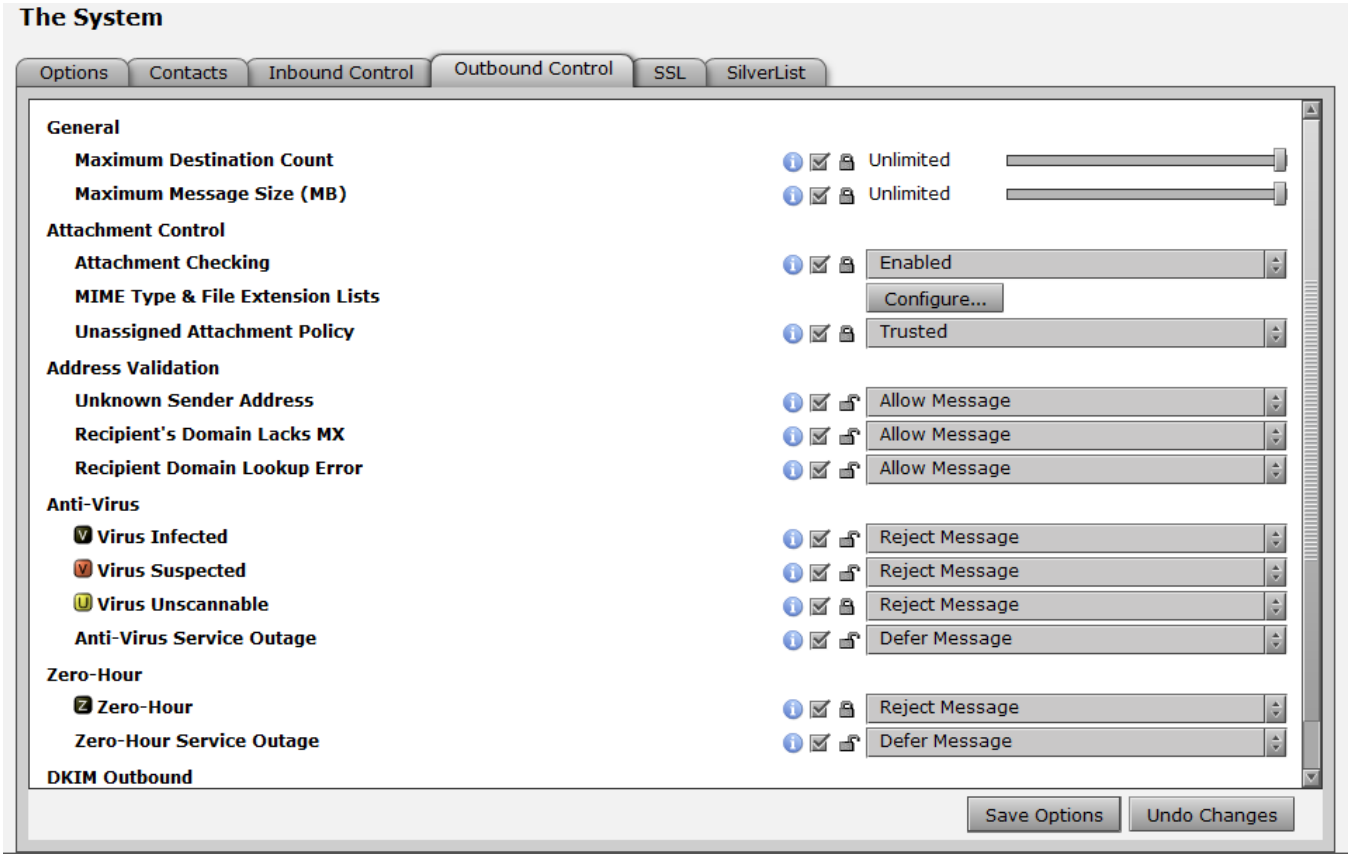
General

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 Configure... button to open the definition page and specify which attachment types are allowed to go out and which are



[42] **System > Outbound Control** *Page*

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 & Zero-Hour

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 unavailable. Refer to the Anti-Virus and Zero-Hour discussions in the **Admin > System > Inbound Control** section for details.

DKIM Outbound

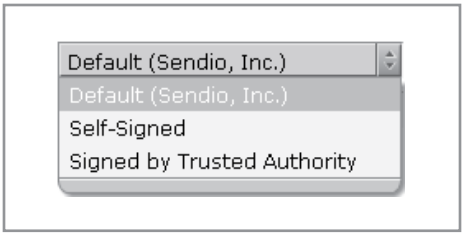
DKIM Signing: (Default: *Disabled*) Specifies whether Sendio is to sign out-going messages with DKIM certificates. The specific configuration of DKIM options is done at the **Domain** level, accessed via the 

button on the **Admin** navigation menu.

THE SYSTEM > SSL PAGE

It is recommended that **User** access to the Sendio web interface be made over an SSL connection. The SSL certificate can be a Sendio default, or can be specified via the options on the **Admin > System > SSL** page [44].

Certificate Name: (Default: *Sendio, Inc.*) Specifies the name of the SSL certificate to use for secure access to the Sendio web interface. The three options are shown in the drop-down list, in Figure [43].

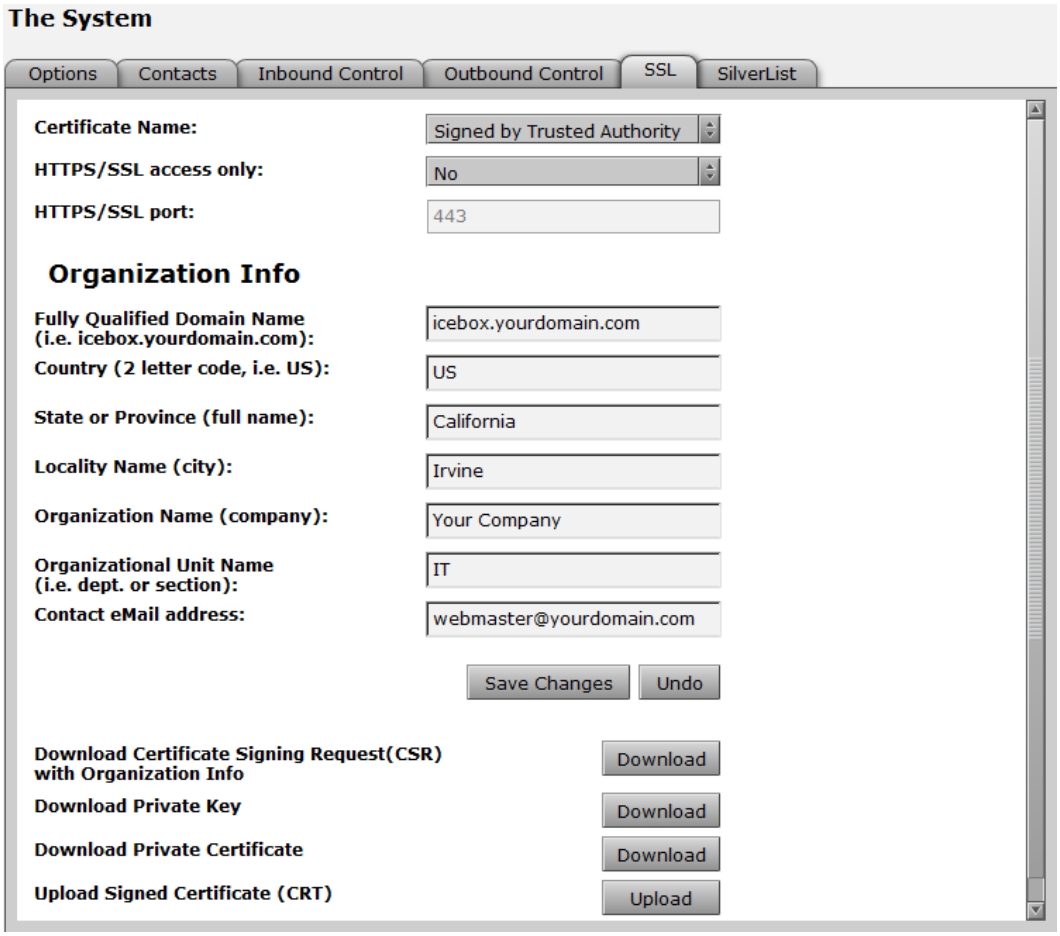


[43] **Admin > System > SSL** *Certificate Name Drop-Down Menu*

> **NOTE:** *Self-Signed* and *Signed by Trusted Authority* certificate names should not be selected unless 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://.

HTTPS/SSL port: This option is fixed to port 443.



[44] **System > SSL** *Page*

The certificate request process requires that you provide the Certificate Authority (CA) with a Certificate Signing Request (CSR). The process is as follows:

- A CSR is generated within 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
- Select *Signed by Trusted Authority* from the Certificate Name drop-down menu [44]

NOTE: The certificate must be in base64 format for Sendio to accept and recognize it.

In order to convert a binary certificate to base 64 in Windows, do the following:

- Open the certificate in Windows Explorer
- Select the "Details" tab
- Click the "Copy to File..." button
- Select "Base-53 encoded X.509 (.CER)" as the file format

The resulting file may then be uploaded to Sendio.

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.

THE SYSTEM > SILVERLIST PAGE

Sendio *SilverListing* service is an enhanced implementation of an anti-spam technique commonly known as "greylisting." The basic concept is that most spam-sending systems are optimized for maximum output only. In contrast, all commercial email servers, such as MS Exchange, Lotus Notes or Novell GroupWise, support all SMTP components for both inbound and outbound message flow.

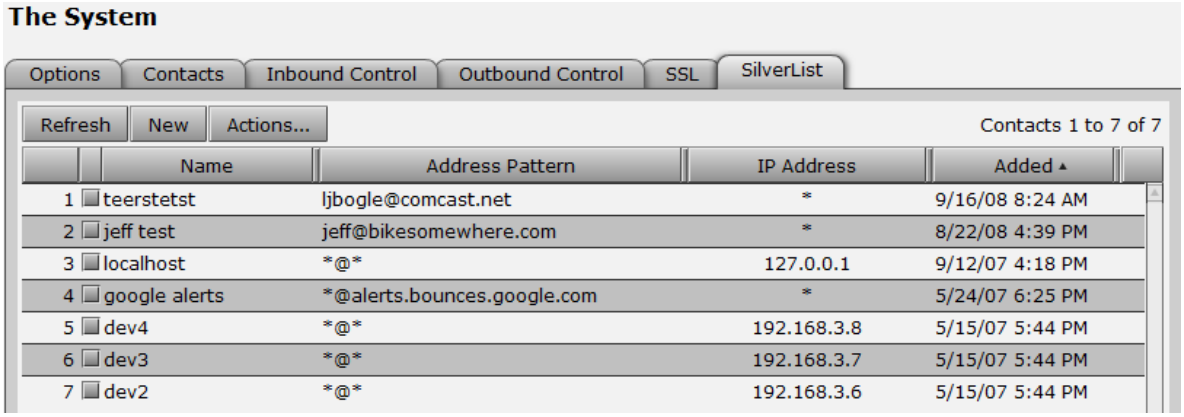
The *SilverListing* process is combined with the Contact Checking process to provide a highly effective spam management mechanism. SAV messages will be sent to only those sending systems that are *Established* as identified by the *SilverList* process. The *SilverList* function will not be performed for those contacts and IP addresses that are already on an *Accept-List*.

With the *SilverList* service of Sendio enabled, when a request-to-send email initiation message is received from an email server with a previously unknown IP address, Sendio writes the IP address to a *SilverList* with a status of *Waiting* and then does not acknowledge the sending servers request. Per the SMTP protocol, after a short period of time a legitimate email server would decide that the initial request had been lost somewhere in transit across the Internet, and would resend the request-to-send message. In contrast, spam-sending systems will not resend the request and will simply move on to send the next spam message somewhere else.

If Sendio never receives a second request-to-send from the *Waiting* IP address, then it is presumed that the sender is a spammer and the IP address is ultimately dropped from the *SilverList.* No actual email content is ever received by Sendio. In contrast, if a second request-to-send message is received, then the IP address on the *SilverList* is updated to a status of *Established* and the standard SMTP transaction proceeds. This process has the effect of blocking a very large percentage of the spam that attempts to get through Sendio.

In addition, Sendio checks whether a subsequent sender's IP address is already on the *SilverList* with an *Established* status and, if it is, the system skips the *Waiting* process and simply proceeds with the SMTP transaction.

The **Admin > System > SilverList** page, shown in Figure [45], displays a table of addresses that have been manually entered by an **Administrator** as permanent entries on the *SilverList.* Any messages from these addresses skip the *SilverListing* process. Addresses that are "learned" by becoming *Established* dynamically are listed on *SilverList* tables at the individual **User Accounts** level.

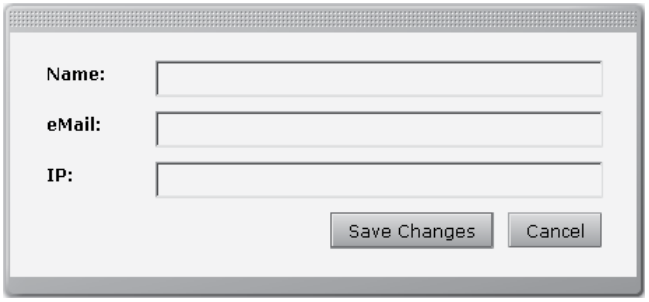


[45] **System > SilverList** *Page*

To add a *SilverList* table entry, click the New button to open the pop-up window shown in Figure [46].

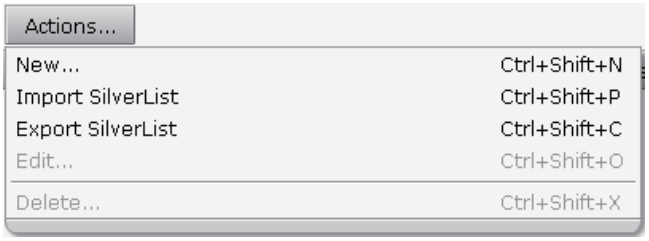
Enter the Name and email information. The Name is used for display purposes only.

While an IP address entry is not required, it is strongly advised that one is specified to provide further assurance that the sending domain is coming from the appropriate IP address. Note, however, that if the IP address of the domain changes, then this entry will need to be modified to reflect the change

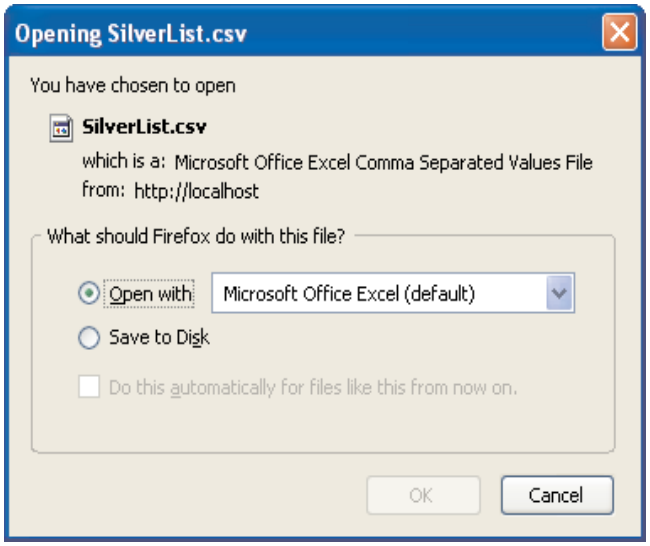


[46] **Admin > System > SilverList > New**
Create Entry Pop-up Window

SilverList entries may also be exported and imported in much the same fashion as contacts by clicking on the Actions... button [47]. *Export SilverList...* opens a widow as shown in Figure [48].



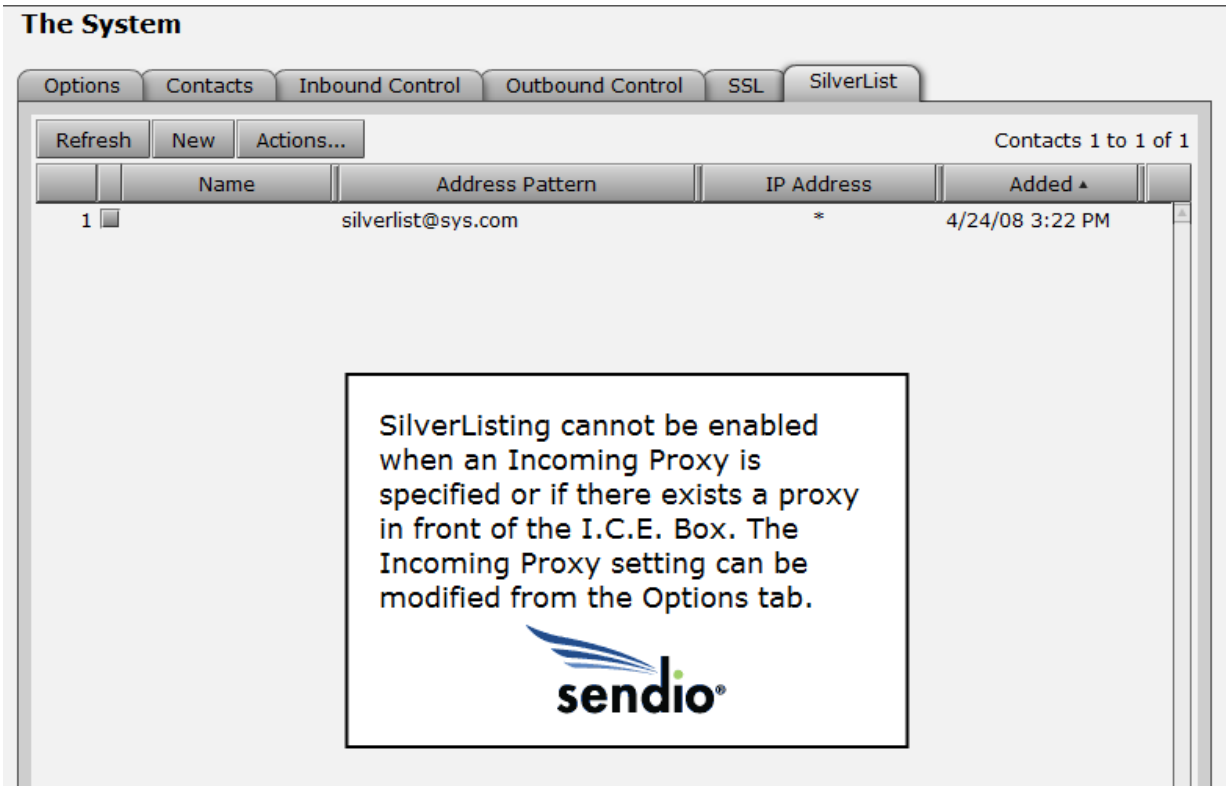
[47] **Admin > System > SilverList > Actions**
Drop-Down Menu



[48] **Admin > System > SilverList > Actions**
Export Pop-up Window

NOTE: SilverListing does not function behind a proxy. Consequently, the contents of the SilverList tab will be unavailable when the proxy function is enabled, as shown in Figure [49].

NOTE: **Administrators** will see a *SilverList* tab on their **User > Account Info** page. **Users** without administrative rights will not see this tab.



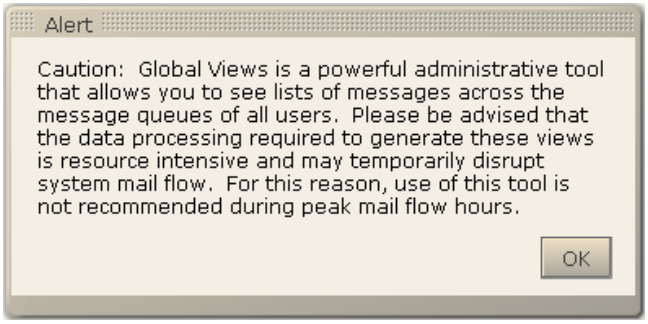
[49] SilverList and Incoming Proxy Message

This page intentionally left blank

SECTION 6: GLOBAL VIEWS PAGES

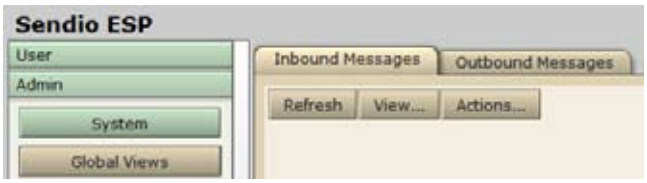
The Global Views pages on the **Admin** Menu gives **Administrators** a facility to see an aggregate view of the various message queues for all users. Many **Administrators** find a **Global View** of all *Held* messages to be particularly useful. Most held messages will be a result of specific policy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

A **Global View** displays a table 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 requirement of an additional policy.



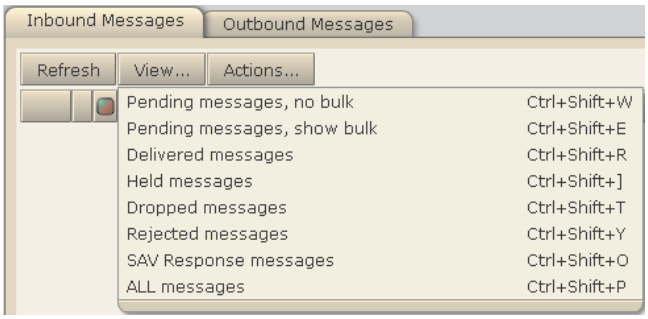
[50] **Admin > System > Global Views** *Warning Message*

Because the **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 GUI first displays an *Alert* to remind the **Administrator** about this potential impact [50].



[51] **Admin > System > Global Views** *Tabs*

After closing the *Alert* window, the **Administrator** then selects either the **Admin > Global Views > Inbound Messages** or the **Outbound Messages** tab, shown in Figure [51].



[52] **Global Views > Inbound Messages** *View Options*

Clicking the View... button opens a drop-down menu for each tab that lists the various view options, as shown in Figures [52] and [53].

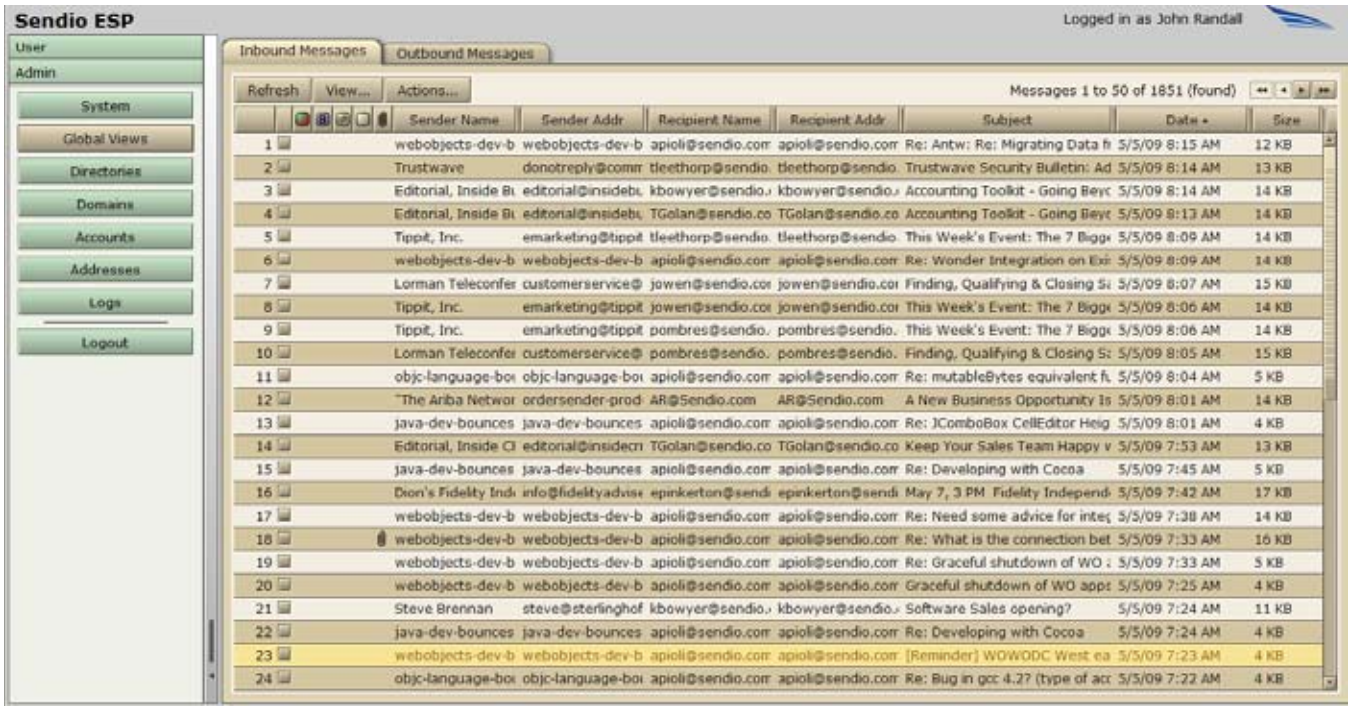
When a particular *View* is selected, the corresponding table is displayed. An example is shown in Figure [56].

[53] **Global Views > Outbound Messages** *View Options*

If one or more messages in a **Global Views** table are selected (by clicking the check boxes), a number of *Actions* can be taken by selecting from the Actions... button drop-down lists, as shown in Figures [54] and [55].

[54] **Global Views > Inbound Messages > Actions** *Drop-Down Menu*

[55] **Global Views > Outbound Messages > Actions** *Drop-Down Menu*



[56] Global View of Pending Messages, No Bulk

SECTION 7: DIRECTORIES PAGES

The Directories page on the **Admin** menu displays a table of all the directories and / or Organizational Units ("OUs") that contain the mail recipient information. An example is shown in Figure [58]. Sendio is capable of synchronizing with multiple directories.

In order to synchronize with a directory, a username must be created on the directory. This username requires only basic (or "read-only") rights with a password that is set to "never expire".

Sendio can be set to synchronize with a Directory Service automatically. This is configured through the *sysconfig* interface, described in the *Installation Guide*.

CREATING A NEW DIRECTORY

To add a directory, click the New button on the **Directories** page. A pop-up window will be displayed [57].

[57] **Admin > Directories > New** *Pop-up Window*

Name: The name Sendio will be used to reference this directory configuration.

Directory Host: Either the IP address (*preferred*) or URL to the Organizational directory. It is recommended that the primary directory be used in the case of a primary and backup architecture.

> **NOTE:** A Directory Host URL will work only if Sendio is set to use the organization's internal DNS.

Port: This typically points to the Global Catalog which exists on port 3268. The alternate common setting is port 389 which indicates an LDAP environment.

If the information and connection is successful, clicking on the Fetch DNs button will retrieve the "Domain Names" (DNs) present on the LDAP Directory. If no DNs are fetched, then the host name / port combination should be verified as well as the connectivity between Sendio and the Directory server.

Some directories do not provide DNs, so the **Administrator** must type them in manually.

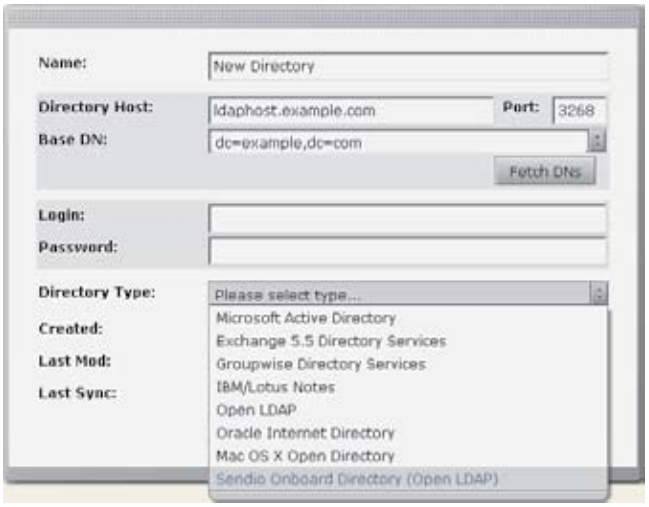
The specific OU (Organizational Unit) should be pre-pended to the Base DN to specify the location of the **Users** with mail attributes.

[58] **Admin > Directories** *Page*

EXAMPLE	ou=users, dc=example, dc=com

Once the connectivity has been established, enter the *Login* and *Password* and select the *Directory Type* from the drop-down menu as shown in Figure [59].

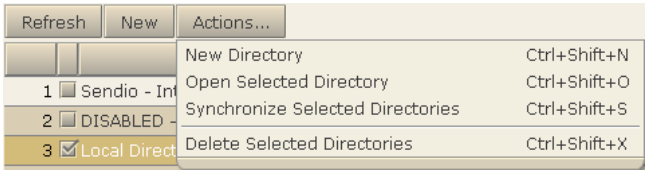
Click the Save Changes button to save the new *Directory* definition.



[59] **Admin > Directories > New** *Directory Type Drop-Down Menu*

MODIFYING AN EXISTING DIRECTORY DEFINITION

Double-click on a **Directories** table row, or click the record check box, press Actions... and choose **Open Selected Directory** [60]. Modify the record as appropriate and save the changes.



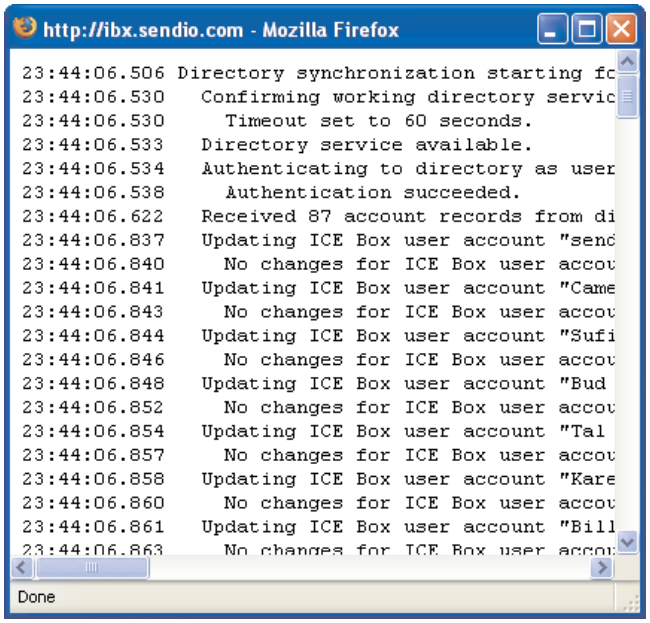
[60] **Admin > Directories > Actions** *Drop-Down Menu*

MANUALLY SYNCHRONIZING DIRECTORIES

Select one or more **Directories** by clicking on the respective check boxes.

Select **Synchronize Selected Directories** from the Actions... menu. The synchronization screen in Figure [61] will be displayed, indicating new addresses and accounts that have been added to Sendio.

WARNING: Email for recipient addresses that are not synchronized will get bounced back to the sender. Please ensure that the necessary mail recipients are within the directory that you have just synchronized, and the domain to which the addresses belong is in the list of **Domains** (See *Section 8: Domains Pages*).



[61] Directory Synchronization

ACTIVE DIRECTORY OBJECTS

The users that are imported are those with a mail attribute within Active Directory. Inactive accounts that have not been deleted from Active Directory will also be imported.

Groups, mail enabled folders, and distribution lists are treated in the same fashion as any other account from an Sendio perspective.

If a group or distribution list is mail enabled all messages that are delivered to this account will be distributed to all members of the Distribution List by the internal Exchange server.

Sendio is perfectly capable of recognizing and processing messages for mail enabled Public Folders.

When accounts are deleted from Active Directory they are **NOT** deleted from Sendio. Active Directory accounts which have been deleted will be noted by a red X on the Accounts page. If the Active DIrectory account is truly no longer in use you will need to manually purge the account from Sendio.

This page intentionally left blank

SECTION 8: DOMAINS PAGES

Sendio can provide email integrity services to multiple email domains simultaneously.

EXAMPLE

Frank owns 4 companies, each with their own IT infrastructure and email system.

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

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

Domains are managed by selecting the Domains button on the **Admin** navigation menu. When the **Domains** pages open, the display shows all of the currently configured domains in a table, as shown in Figure [63].

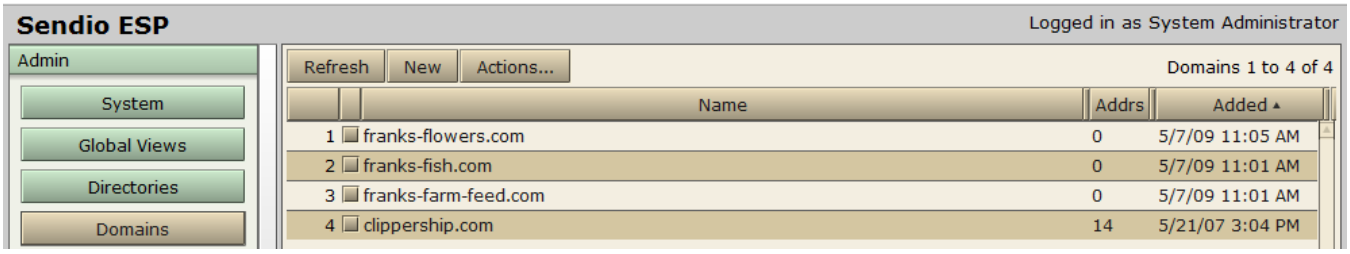
CREATING A NEW DOMAIN

[62] **Admin > Domains > New** *Pop-up Window*

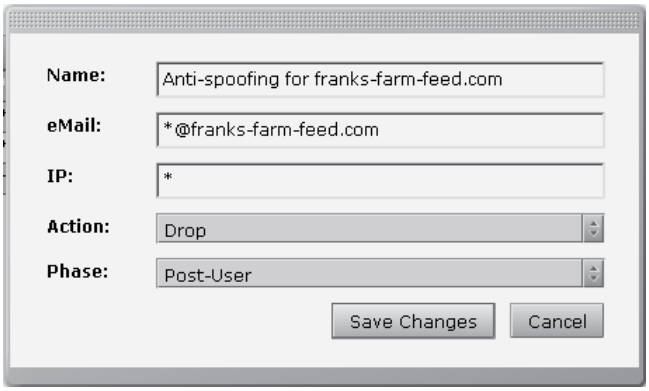
Clicking the New button displays the *Create New Domain* pop-up window. [62]

Name: The fully qualified domain name (e.g. sendio.com or sendio.net)

Clicking the *Create anti-spoofing drop contact for this domain* check box causes the system to automatically add a contact to the **System** *Drop-List*, as described in *Section 5: System Pages, System Contacts Tab, Creating a New Contact.* An example is shown in Figure [64]. This *System Drop Contact* prevents Sendio from accepting spoofed messages from the internal email domain.



[63] **Admin > Domains** *Page*



[64] Anti-Spoofing Drop Contact Auto-Created in System Drop-List

[65] **Admin > Domains** *Configuration Pages*

[66] **Admin > Domains** *Configuration Options Page*

DOMAIN-LEVEL CONFIGURATION

Many of the options described in **Admin > System > Options** Pages in *Section 5* can be modified at the **Domain** level.

To access the configuration pages for a specific **Domain**, double-click on the record in the **Domains** table display [63].

Domain configuration pages are a set of tabbed pages. The default view is of the **Details** page, which provides some timestamp information. [65]

Clicking the **Options** tab displays the **Admin > Domains > Options** page list of options. [66]

With two exceptions, the options on the **Admin > Domains > Options** list are equivalent to the options on the **Admin > System > Options** page. The exceptions, for DKIM, are described later in this section.

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. If the **System** level option is *unlocked*, then it can be changed at the **Domain** level if desired.

Clicking the check box for an option that is not "grayed-out" allows the **Administrator** to change the setting for that option. It can then be *locked* if it should not be overridden at the **Account (User)** level.

DKIM Signing

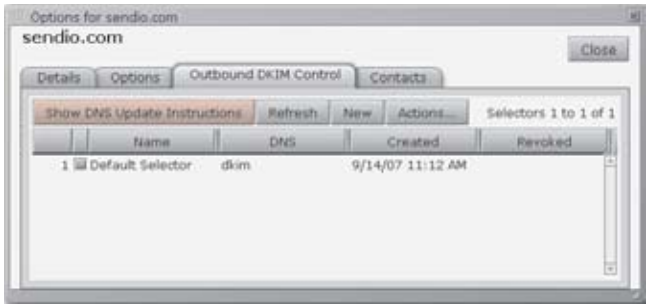
NOTE: DomainKeys Identified Mail (DKIM) support is enabled at the **System** level for Sendio overall, but is configured on a per-**Domain** basis.

Sendio has the capability to "sign" outbound mail. This functionality provides the potential of significantly reducing the processing load to the email server.

Sendio can be configured to use DKIM to sign all outgoing mail, or DKIM signing can be restricted to a domain or an organization. The third tab on a **Domain** configuration page shows the configuration tab for **Outbound DKIM Control**, shown in Figure [67].

DKIM signs body and selected parts of header. This feature will add entries to the envelope header of each email. Signature is transmitted in this DKIM-Signature header. There is a Public key stored in DNS or in _domainkey subdomain as specified in the system options tab. The namespace can be divided using selectors and it allows multiple keys for aging and delegation.

A selector is added to the domain name, used to find DKIM public key information. It is specified as an attribute for a



[67] **Admin > Domains** *Configuration Outbound DKIM Control Page*

DKIM signature, and is recorded in the DKIM-Signature header field.

Validation uses the selector as an additional name component, to give differential DNS query names. There are different DKIM DNS records associated with different selectors, under the same domain name.

EXAMPLE
Jun2009.eng._domainkey.example.com

Hence, selectors are used to permit multiple keys under the same organization's domain name. This can be used to give separate signatory controls among departments, date ranges, or third parties acting on behalf of the domain name owner.

The DKIM tab above is the primary location for configuring DKIM signing. There are five basic steps to the process:

1. On the Domain Options page, set the DKIM Prefix, if necessary. This is not a required entry.
2. On the Domain Options page, choose the selector as shown below. There is a default selector that is normally chosen.
3. Create a DKIM signature for the selector.
4. Create DNS Entry by first choosing the Selector that will be used. Click on the pink button to Execute Reset DKIM DNS Script. With the Selector still chosen, click on the Actions button and select Show DNS Update Instructions. This will generate a pop-up screen with the DNS Entry that will be required. In the DNS entry shown below, the public side of the DKIM key will be displayed and this will be used to match the private key that Sendio is signing. Note the bolded entry on the third line below matches the DNS name that is given when the Selector is created.

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

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

5. Enable DKIM signing from the Outbound Control tab from the System menu option.

After the above 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 zone file.

This page intentionally left blank

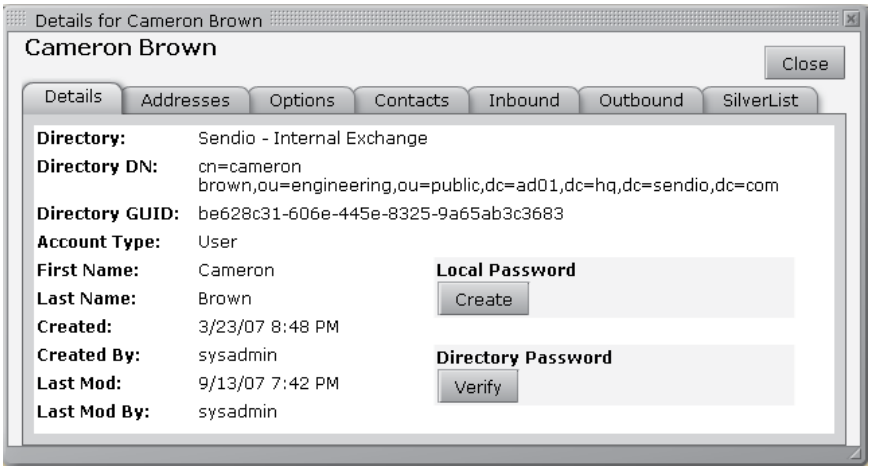
SECTION 9: ACCOUNTS PAGES

The Accounts button on the **Admin** menu displays a table of the accounts that are being managed by Sendio. An example of the **Accounts** page is shown in Figure [69]. Prior to deployment, the Administrator should review the list that has been imported.

There are two icon columns in the **Accounts** table.

The red X icon indicates users that have been deleted or moved from the external LDAP directory (i.e. Active Directory, GroupWise, Lotus Notes, etc.), or removed from the scope of synchronization. These users can be safely deleted once verified that they were not removed from the directory in error. While Sendio maintains synchronization with the external LDAP directory, deletions on Sendio are not reflected in the external LDAP directory. In other words, the synchronization is in reality a one-way import and provides a backup in the event that an account is erroneously removed from the external LDAP directory.

The gold key icon identifies users that have local passwords to Sendio. This password is set on either the **Admin > Accounts ... Details** tab as described below or on the **User > Account Info > Details** page.

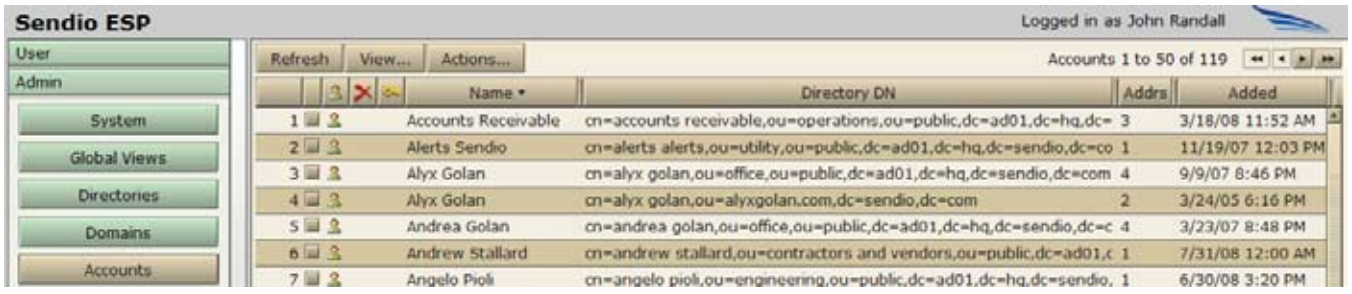


[68] **Admin > Accounts** *Individual Record Tabbed View*

Double-clicking on an **Accounts** record opens a view of that account, as shown in Figure [68]. The default page shows the **Details** of the user. The **Details** and **Addresses** tabbed pages contain the same information as shown in the **User > Account Info** pages.

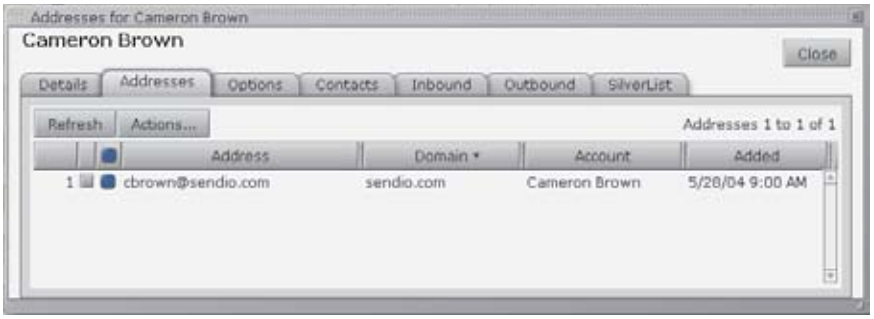
Local Password

The **Accounts ... Detail** screen allows the Administrator to set a local Sendio password on behalf of the user. In other words, instead of utilizing a network password, the user can use the local password to log in to Sendio. This is very useful in the case of a user with an executive assistant. The assistant can



[69] **Admin > Accounts** *Page*

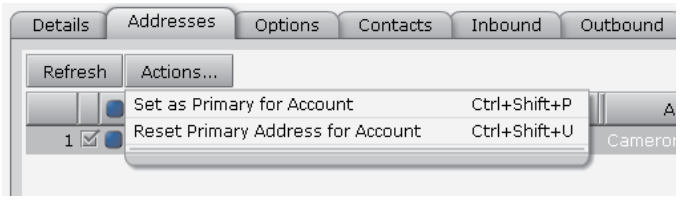
be granted a local password to view the message queue and contacts of the user without compromising the network password of the user.



[70] **Admin > Accounts ... Addresses** *Page*

Addresses

The **Addresses** page shows all of the addresses associated with the particular account. [70] If there are multiple addresses listed, the one with the blue square icon identifies the *Primary* addresses for the account. This designation may come from an external directory setting, or can be manually set from the Actions... menu, shown in Figure [71].



[71] **Admin > Accounts ... Addresses > Actions** *Drop-Down Menu*

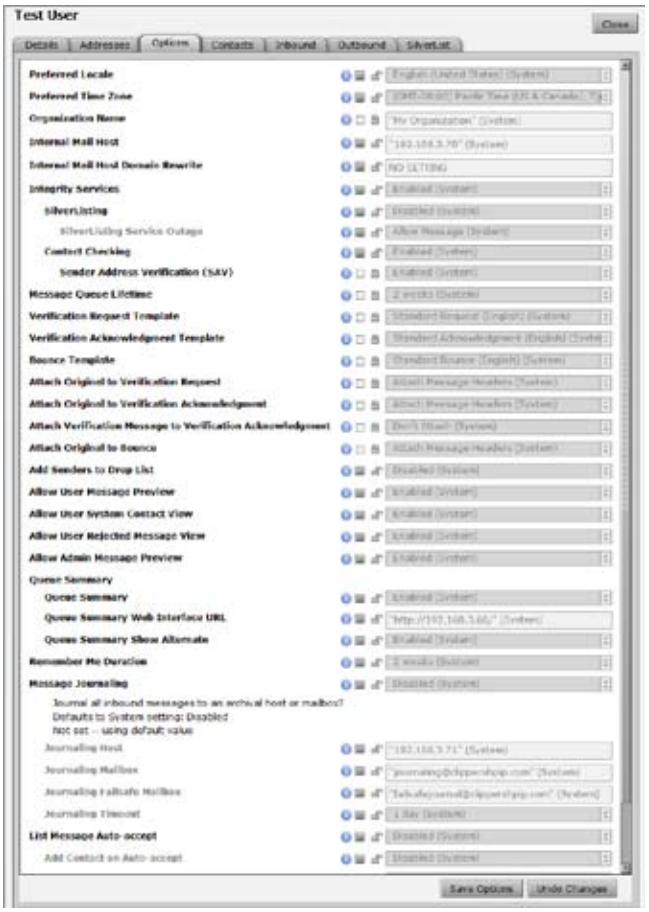
Primary Address for Account

This is the address where system messages and the Queue Summary (if enabled) will be sent. This *Primary* designation can be overridden by clicking on the **Reset...** menu option.

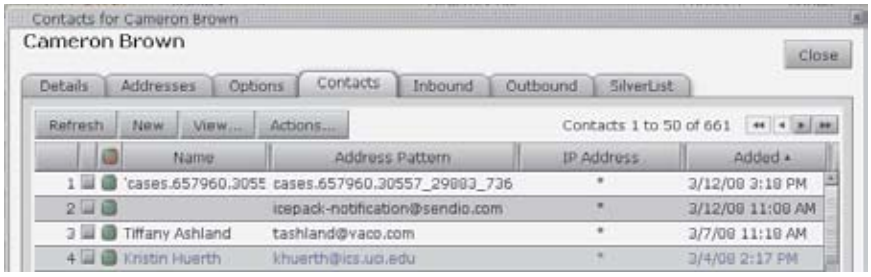
NOTE: If the address that is designated as the primary address is removed from the Active Directory, then the next synchronization will remove the primary designation and the system will promote the first address in the list as primary.

Options

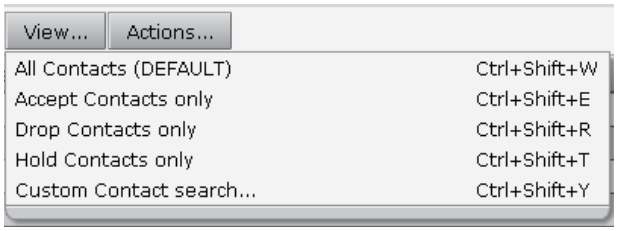
The **Admin > Accounts ... Options** page allows an Administrator to configure, for an individual account, the options previously described for the **Admin > System > Options** page and the **Admin > Domains ... Options** page. [72]



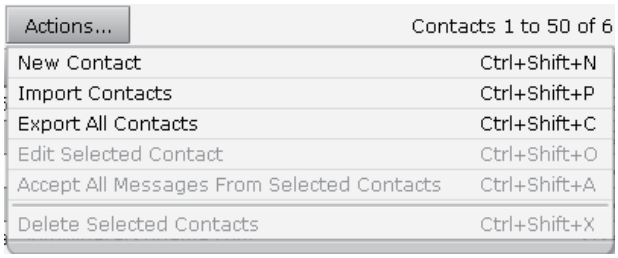
[72] **Admin > Accounts ... Options** *Page*



[73] **Admin > Accounts ... Contacts** *Page*



[74] **Admin > Accounts ... Contacts View...** *Drop-Down Menu*



[75] **Admin > Accounts ... Contacts Actions...** *Drop-Down Menu*

[76] **Admin > Accounts ... View**

Contacts

The **Admin > Accounts ... Contacts** page [73] allows an Administrator to see all of the contacts for a particular account. This view is equivalent to what a User will see on the **User > Contacts** page.

The View... and Actions... buttons open drop-down menus as shown in Figures [74] and [75]. The **Actions...** drop-down menu has a unique option *Accept All Messages From Selected Contacts*.

Inbound and Outbound

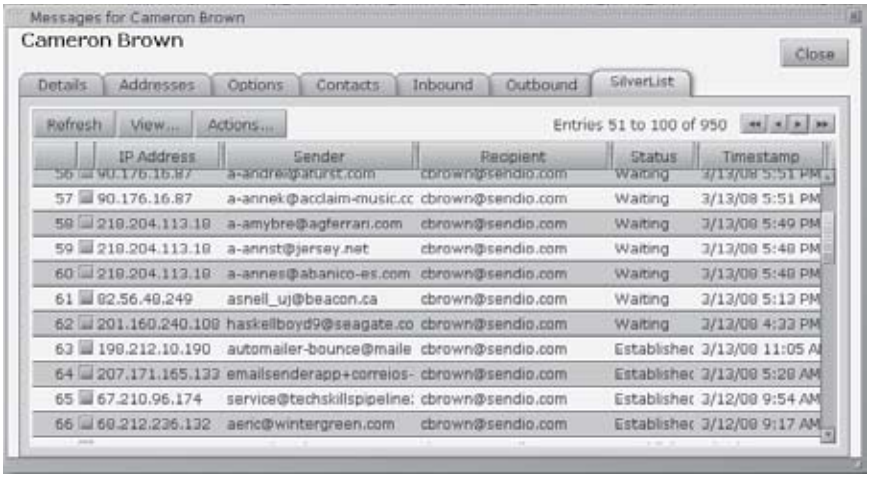
The **Admin > Accounts ... Inbound** and **Outbound** pages allow an **Administrator** to see all of the message queues for the account, and perform all of the **Actions** that a **User** can do. For both pages the view can be changed as shown in figure [76].

SilverList

The **Admin > Accounts ... SilverList** page allows an Administrator to see the status of all IP addresses that are being processed, or have been processed and *Established*, by the *SilverList* service for a particular account. [77]

The **Status** column shows the disposition of the SMTP connection that has come in to the system. The values in this column are *Established* and *Waiting*.

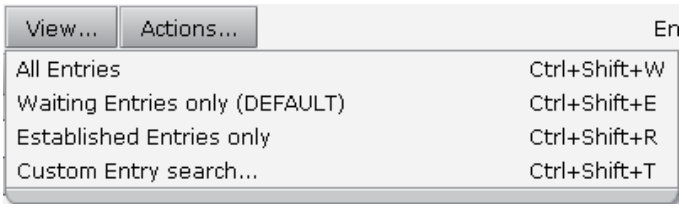
IP addresses that are *Waiting* are still being processed by the *SilverList* service. Those that *Established* have been verified and passed by the service.



[77] **Admin > Accounts ... SilverList** *Page*

The Sendio *SilverList* database will keep the record for 30 days from the most recent successful connection.

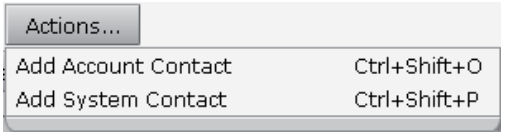
The **SilverList** table is searchable on the **Status** entry or by creating a custom search from the **View...** menu. [78]



[78] **Admin > Accounts ... SilverList View...** *Drop-Down Menu*

Add Contact

An **Account** or **System** contact can be added directly from the **SilverList** table. Select the entry with the address that is targeted to be added, click on the Actions... button and select one of the two choices, as shown in Figure [79].



[79] **Admin > Accounts ... SilverList Actions...** *Drop-Down Menu*

NOTE: Adding the address as a contact in the **System** does NOT deliver the message as in the *Pending Queue* display.

SECTION 10: ADDRESSES PAGES

The **Admin > Addresses** pages list the addresses that are recognized by Sendio as valid recipient addresses. Every **User**, or **Account**, has at least one **Address** associated with it and some have many **Addresses**.

EXAMPLE

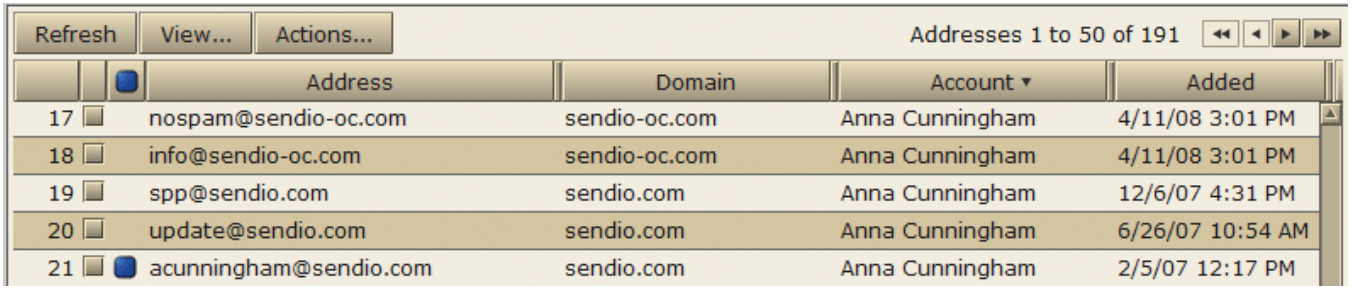
At Frank's Farm Feed, Frank has his personal address, and is also in charge of sales and customer service. He has three addresses that Sendio covers:

- frank@franks-farm-feed.com
- sales@franks-farm-feed.com
- service@franks-farm-feed.com

Frank also has two addresses at Frank's Furniture:

- frank@franks-furniture.com
- sales@franks-furniture.com

In Figure [80], user Anna Cunningham has five addresses associated with her account. The *acunningham@sendio.com* record has a blue square icon that signifies that this address is the *Primary* address for the account.

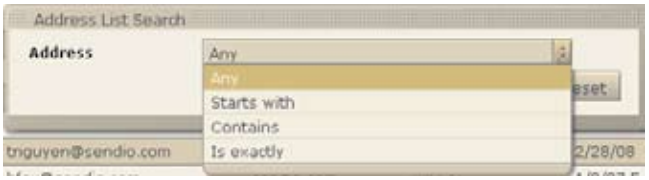


	Address	Domain	Account	Added
17	nospam@sendio-oc.com	sendio-oc.com	Anna Cunningham	4/11/08 3:01 PM
18	info@sendio-oc.com	sendio-oc.com	Anna Cunningham	4/11/08 3:01 PM
19	spp@sendio.com	sendio.com	Anna Cunningham	12/6/07 4:31 PM
20	update@sendio.com	sendio.com	Anna Cunningham	6/26/07 10:54 AM
21	acunningham@sendio.com	sendio.com	Anna Cunningham	2/5/07 12:17 PM

[80] **Admin > Addresses** *Page*

Clicking the View... button opens the *Address List Search* window, shown in Figure [81]. There are several options for searching for an address, selectable from a drop-down menu, shown in Figure [82].

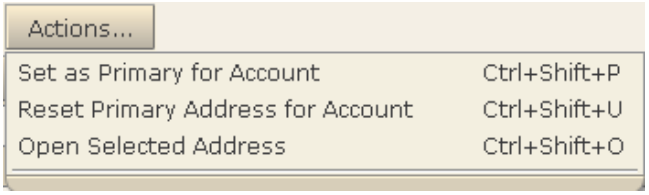
[81] **Admin > Addresses** *Address Search Window*



[82] Address Search Window Search Options

[83] Use Regular Expression Syntax Check Box

Clicking the Actions... button opens a drop-down menu shown in Figure [84].



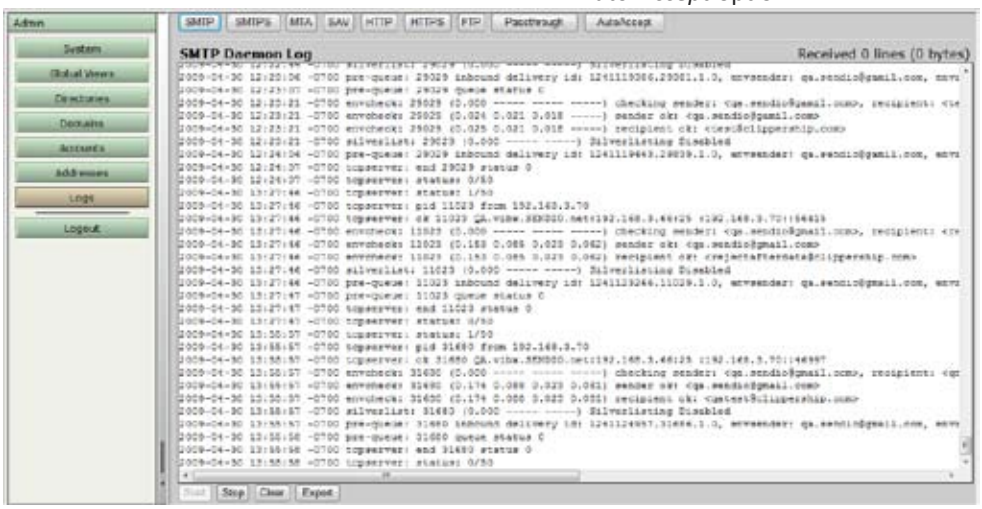
[84] **Admin > Addresses** > **Actions...** *Drop-Down Menu*

SECTION 11: LOGS

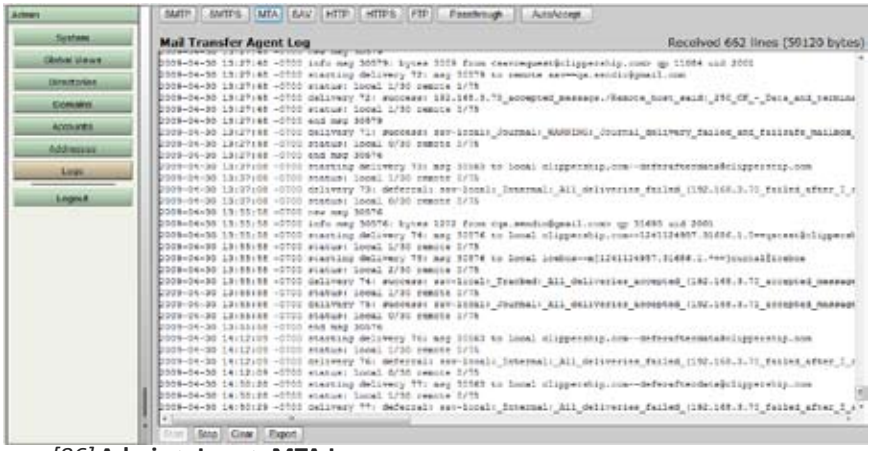
Sendio maintains a set of log files that track all of the message transactions and workflow processes. The logs can be viewed on the **Admin > Logs** pages.

There are nine logs available:

- 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
- SAV: the Sender Address Verification requests on the system
- 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
- Pass-Through: the messages that are not processed using *Integrity Services*
- Auto-Accept: the messages that are processed using the *List-Message Auto-Accept* option



[85] **Admin > Logs > SMTP Log**



[86] **Admin > Logs > MTA Log**

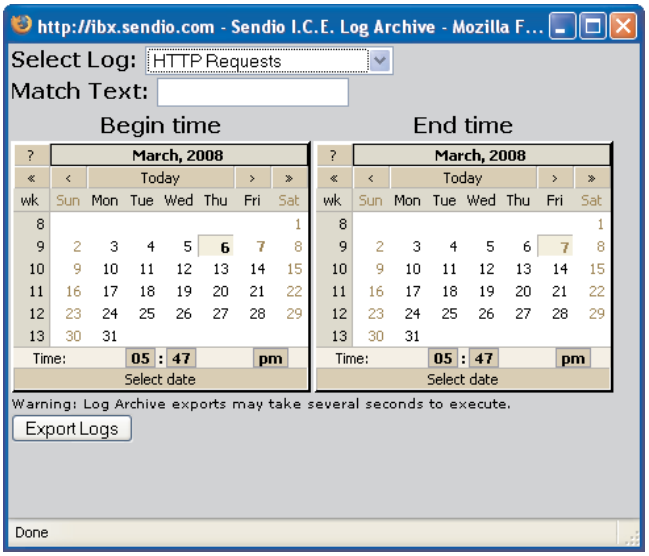
These logs are not yet available through an API.

Figures [82] and [84] show examples of the SMTP and MTA logs.

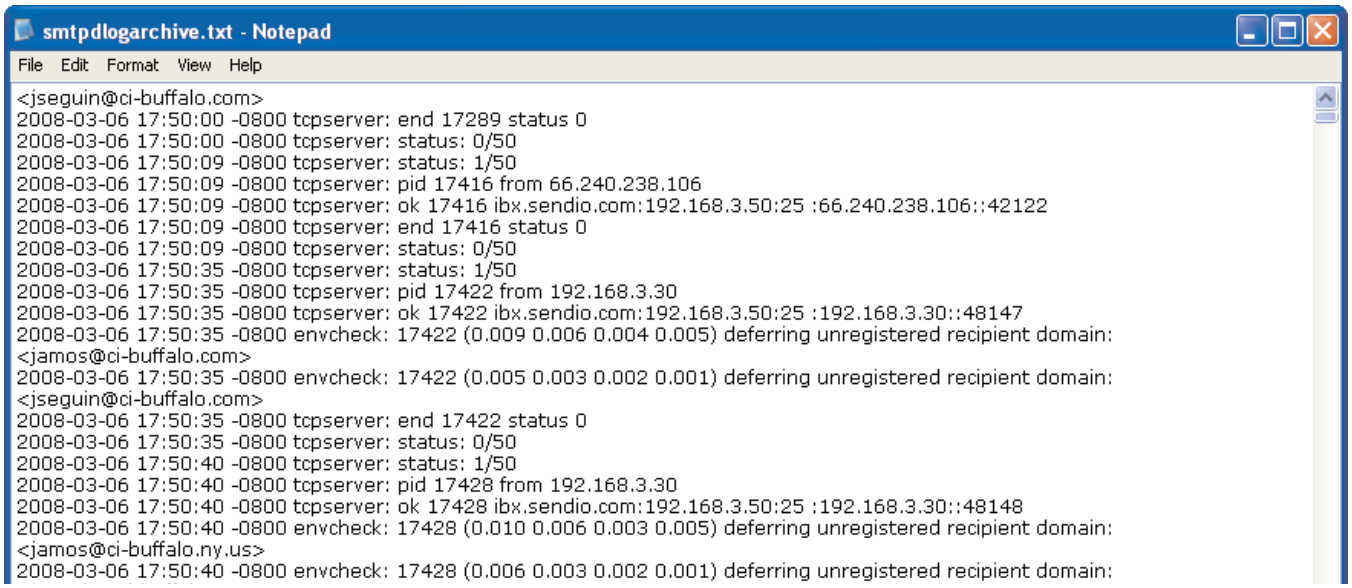
Exporting

The logs can also be exported to a text (.TXT) file, shown in Figure [89]. The dialog box in Figure [88] allows the **Administrator** to enter date boundaries and a useful "matching criteria" for the export.

Exporting defaults the the previous 24 hours. Click on different dates to change the start/stop days of the log information. To change the hour or minute of the log data click the value to increase or shift-click to descrease.



[88] Log Export Criteria



[89] **Admin > Logs** *Export Example*

SECTION 12: QUEUE SUMMARY

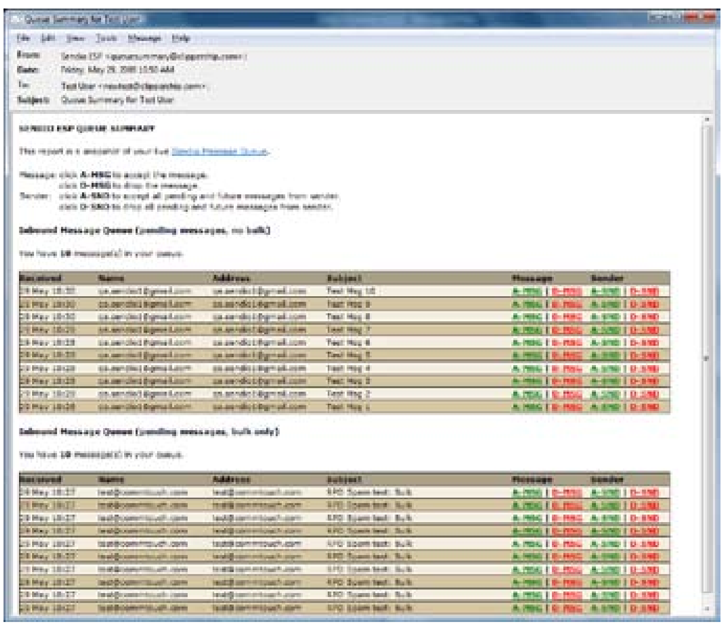
If enabled, a *Queue Summary* email that shows the most recent 50 records in a user's *Pending Queue* will be sent to that user's inbox. This email is a brief and concise means of communicating the recent additions to a user's *Pending Queue*.

If the *Remember Me* option in the **Admin > System > Options** page is Enabled, four "actions" available from this email, by clicking on a link:

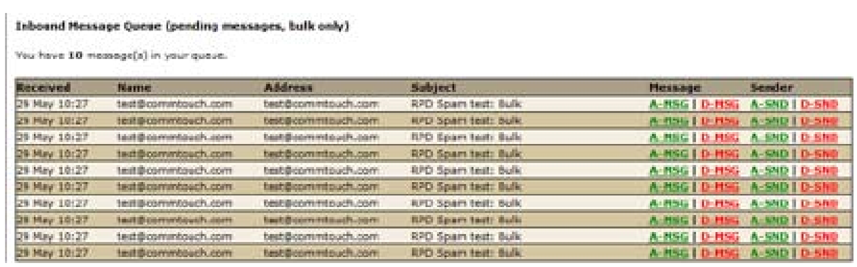
- a message can be released [**A-MSG**]
- a message can be dropped [**D-MSG**]
- a message can be released and the sender address can be added to the user's *Accept-List* [**A-SND**]
- a message can be dropped and the sender address can be added to the user's *Drop-List* [**D-SND**]

These functions are completely analogous to the functions on Sendio web interface.

> **NOTE:** It is a good practice to deploy both an internal and external DNS name that is identical for use in the configuration of access to the Queue Summary. In this way, both internal and external users can take advantage of this feature.



[90] Typical Queue Summary Message



Inbound Message Queue (pending messages, bulk only)

You have **10** message(s) in your queue.

Received	Name	Address	Subject	Message	Sender
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND
29 May 10:27	test@commtouch.com	test@commtouch.com	RPD Spam test: Bulk	A-MSG | D-MSG	A-SND | D-SND

[91] Queue Summary Message Addition When "Show Alternate" Option is Enabled

This page intentionally left blank

SECTION 13: DKIM PRIMER

Per the DKIM.org Web site:

> *DomainKeys Identified Mail (DKIM) lets an organization take rSendioonsibility for a message while it 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 delivery. Technically, DKIM provides a method for validating a domain name identity that is associated with a message through cryptographic authentication.*
>
> *The first version of DKIM synthesized and enhanced Yahoo!'s DomainKeys and Cisco's Identified Internet Mail specifications. The IETF has now approved the revised specification as a Proposed Standard and published it as RFC 4871.*

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 email senders' MTAs or edge devices to generate "public/private key pairs" and then publish the public keys into their Domain Name System (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 into 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 content were not altered in any way during their trip 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 for use with 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 was written on.

DKIM History

Yahoo has been working on a solution to the spam and phishing problem since at least 2003, when it introduced the core DomainKeys technology. By 2004, the company was signing all of its outgoing mail with DomainKeys as well as verifying all incoming mail. By 2005, over 300 million email messages a day were going through this verification at Yahoo alone. The U.S. patent, number 6,986,049, was assigned to Yahoo. In late May of 2007, the Internet

Engineering Task Force (IETF) approved DomainKeys Identified Mail as a proposed standard, RFC 4871. This move lends an extra layer of legitimacy to the email authentication framework, and will help give the system an edge over Microsoft's proposed Sender ID system.

With this nod from the IETF, Yahoo and the other companies involved in DKIM's creation plan to work with ISPs, enterprises, e-commerce organizations, financial institutions and (yes) the open source community to ensure that the specification is quickly adopted and incorporated into many future products. Other supporters of the DKIM standard include AOL, EarthLink, IBM, VeriSign, IronPort Systems, Cox Communications and Trend Micro.

Scenario

Suppose that eBay wants to send an email to some of their users about their accounts. And suppose that it uses DKIM. That means eBay's outgoing mail server will add a digital signature to the message – usually embedded in the message headers, where human eyes do not see it. The digital signature serves the same purpose as a human one; it's proof that the mail came from the source it says it came from.

The system needs to be used by both the sender's and recipient's mail servers to be truly effective. **It is also worth noting that this system will not flag spam sent by a legitimate company.**

What DKIM will do is make it easier to track abusive domain owners. That alone can be a huge help in the battle against spam.

As use of DKIM becomes more widespread, spammers will be forced to use fewer and fewer domains. As mentioned before, domains with legitimate DomainKeys will be easier to trace; therefore if they start abusing the system and permitting spam to go through, it will be much easier to see where such email is coming from. Also, once DKIM is more widely used, it should stop phishing attacks so long as the DomainKeys can't be forged.

INTERESTING MARKET NOTE

So far, DKIM has been adopted by 48 percent of large online retailers. Unfortunately, a number of very large retailers have not yet adopted DKIM; these include Dell, Wal-Mart, Target, Gap and Macy's. It is understandable why they have been slow to adopt the technology since there is a considerable effort required to deploy it. Recipients only need to have email accounts with email providers that support DKIM, such as Yahoo! Mail and Google's Gmail. But senders must generate a public/private key pair, add the public key to their DNS entry as a TXT record, and make the private key available to the MTA software.

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 fairly 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.

SECTION 14: 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 as a result 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 rSendioonding 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 15: 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 [92]
- Notification that a *Maintenance Release* is scheduled for Automatic Installation when no *Alert Addresses* have been specified in *sysconfig* shell [93]
- Notification that a *Maintenance Release* has been downloaded to Sendio and is available for manual installation [94]
- Notification that a *Maintenance Release* has been successfully automatically installed [95]

Notice Date: 2008-02-29 23:54,

This automated notification is to inform you that Sendio has finished downloading a new Maintenance Release that is ready to be installed.

Current Sendio Version: Mar 08 SU (0227.0)
Maintenance Release Version: Mar 08 SU (0229.8)
Automatic Update Scheduled: Sun Mar 02, 12:00 AM PST

You have Automatic Updates enabled (recommended). If you take no further action, Mar 08 SU (0229.8) will be installed at your next scheduled update time on Sun Mar 02 at 12:00 AM PST. 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. Log into the sysconfig console.
2. Navigate to “Sendio Update” on the left side of sysconfig interface and press Enter.
3. Navigate to the “Apply Maintenance Release” button and press Enter.

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

1. Log into the sysconfig console.
2. Navigate to “Backup/Maintenance” on the left side of sysconfig interface and press Enter.
3. Navigate to the “System Automatic Update” section and use the “Add” and “Delete” buttons to change the schedule.
4. Navigate to the “Save” button at the bottom of the “System Automatic Update” section after making changes and press Enter.

[92] Maintenance Release Scheduled for Automatic Installation

==========
NOTICE
==========
You received this message because no 'Alert Addresses' have been specified via the Sysconfig shell.

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

Notice Date: 2008-03-03 18:40,

This automated notification is to inform you that Sendio has finished downloading a new Maintenance Release that is ready to be installed.

Current Sendio Version: Mar 08 SU (0227.0)
Maintenance Release Version: Mar 08 SU (0303.0)
Automatic Update Scheduled: Tue Mar 04, 12:00 AM PST

You have Automatic Updates enabled (recommended). If you take no further action, Mar 08 SU (0303.0) will be installed at your next scheduled update time on Tue Mar 04 at 12:00 AM PST. 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. Log into the sysconfig console.
2. Navigate to "Sendio Update" on the left side of sysconfig interface and press Enter.
3. Navigate to the "Apply Maintenance Release" button and press Enter.

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

1. Log into the sysconfig console.
2. Navigate to "Backup/Maintenance" on the left side of sysconfig interface and press Enter.
3. Navigate to the "System Automatic Update" section and use the "Add" and "Delete" buttons to change the schedule.
4. Navigate to the "Save" button at the bottom of the "System Automatic Update" section after making changes and press Enter.

[93] Maintenance Release Scheduled for Automatic Installation; No Alert Addresses Specified

Notice Date: 2008-03-01 10:38,

This automated notification is to inform you that Sendio has finished downloading a new Maintenance Release that is ready to be installed.

Current Sendio Version: Mar 08 SU (0229.6)
Maintenance Release Version: Mar 08 SU (0229.9)
Automatic Update Scheduled: N/A. Automatic Updates disabled

You do not currently have Automatic Updates enabled. To get the benefits of the new release, you will need to do one of the following:

o Enable Automatic Updates
o Install this Maintenance Release manually.

To enable Automatic Updates:

1. Log into the sysconfig console.
2. Navigate to “Backup/Maintenance” on the left side of sysconfig interface and press Enter.
3. Navigate to the “System Automatic Update” section and check the “Automatic Updates Enabled?” checkbox.
4. Review and change the schedule if required.
5. Navigate to the “Save” button at the bottom of the “System Automatic Update” section after making changes and press Enter.

To manually install this Maintenance Release:

1. Log into the sysconfig console.
2. Navigate to “Sendio Update” on the left side of sysconfig interface and press Enter.
3. Navigate to the “Apply Maintenance Release” button and press Enter.

[94] Maintenance Release Available for Manual Installation

At 2008-03-01 00:04:25,
Sendio successfully updated to software version Mar 08 SU (0229.8).

[95] 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

[96] 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 threshhold 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

[97] Journaling Queue Alert Notification

SECTION 16: SAV MESSAGES

Part of Sendio email integrity workflow is 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 three messages 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 not a spam-bot
- **SAV Acknowledgement**: the message that thanks a now "known" email sender for "rSendioonding" to the challenge message
- **SAV Bounce**: the message that is sent if an SAV response is received for a message that is no longer in an Sendio message queue (timed-out or deleted), or if there are multiple recipients for a message with different policies that makes an SMTP reject inappropriate

Examples of these three templates are shown in Figures [98], [99] and [100].

Each of these SAV message templates are available in four language versions:

From: "[username]" <[useraddr]>
To: "[origfromname]" <[origsenderaddr]>
Subject: [orgname] requests that you verify your email address: please REPLY to this email. -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]
X-Priority: 1
Priority: Urgent
Importance: high

Message from "[username]"

I recognize from your email address that this is the first message I have received from you since [orgname] 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:

[origconfirmaddr]

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

Thank you!

[username]

100% spam-free email provided by Sendio (http://[sendiourl])

[98] SAV Request Template

- English
- English / Spanish
- Spanish / English
- Spanish

From: "[username]" <[useraddr]>
To: "[vfyfromname]" <[vfysenderaddr]>
Subject: Accepted: Sender Address Authentication -- [timestamp]
References: [origmsgid], [vfymsgid]
In-Reply-To: [vfymsgid]

That was easy! Thanks for your help.

Your address verification has been completed and your original message has been delivered. In the future you may enjoy the confidence of knowing that all your messages will be promptly delivered to my Inbox.

[responsereason]

_____
Sender Address Verification (SAV) provided by Sendio.

To find out how you can have 100% spam-free email, please visit Sendio at
http://[sendiourl]/how-sender-authentication-works.html

[99] SAV Acknowledgement Template

From: "[username]" <[useraddr]>
To: "[origfromname]" <[origsenderaddr]>
Subject: Problem with your message -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]

'The Sender Address Verification (SAV) system at [orgname] has encountered a problem with the message you sent:

[responsereason]

_____
100% spam-free email provided by Sendio (http://[sendiourl])

[100] SAV Bounce Template

From: “[username]” <[useraddr]>
To: “[origfromname]” <[origsenderaddr]>
Subject: [orgname] requests that you verify your email address: please REPLY to this email. -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]
X-Priority: 1
Priority: Urgent
Importance: high

Message from “[username]”

I recognize from your email address that this is the first message I have received from you since [orgname] 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:

[origconfirmaddr]

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

Thank you!

[username]

100% spam-free email provided by Sendio (http://[sendiourl])

Un mensaje de “[username]”

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 rSendioonda a este mensaje al presionar la opción RSendioonder 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 rSendioonda a este mensaje, asegúrese de que la dirección a la cual esta contestando sea:

[origconfirmaddr]

Si usted no rSendioonde a este pedido de verificación de dirección durante [pending_lifetime], o si su rSendiouesta no es enviada a la dirección indicada arriba, su mensaje original nunca será dSendioachado.

Muchas Gracias!

[username]

Correo electrónico 100% libre de spam proveído por Sendio, Inc. (http://[sendiourl])

[101] SAV Request Template - English/Spanish

From: “[username]” <[useraddr]>
To: “[vfyfromname]” <[vfysenderaddr]>
Subject: Accepted: Sender Address Authentication -- [timestamp]
References: [origmsgid], [vfymsgid]
In-Reply-To: [vfymsgid]

That was easy! Thanks for your help.

Your address verification has been completed and your original message has been delivered. In the future you may enjoy the confidence of knowing that all your messages will be promptly delivered to my Inbox.

[responsereason]

_____
Sender Address Verification (SAV) provided by Sendio.

To find out how you can have 100% spam-free email, please visit Sendio at
http://[sendiourl]/how-sender-authentication-works.html

Así de Fácil! Gracias por su colaboración.

Su Verificación de Dirección ha sido realizada y su mensaje original dSendioachado a la casilla de correos. En el futuro usted podrá estar asegurado que sus mensajes pasaran directo a mi casilla de correo.

[responsereason]

_____
Verificación de Dirección del Remitente (SAV) realizado por SENDIO.

Si usted también desea parar el Spam en forma definitiva, por favor visíte a Sendio al
http://[sendiourl]/how-sender-authentication-works.html

[102] SAV Acknowledgement Template - English/Spanish

From: “[username]” <[useraddr]>
To: “[origfromname]” <[origsenderaddr]>
Subject: Problem with your message -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]

The Sender Address Verification (SAV) system at [orgname] has encountered a problem with the message you sent:

[responsereason]

_____
100% spam-free email provided by Sendio (http://[sendiourl])

Este mensaje fue generado por el Sendio I.C.E. appliance.

Su correo electrónico fue aceptado por el Sendio, pero no pudo ser dSendioachado a su destino final. Si usted cree que el recibir este mensaje es un error, por favor comuníquese con su administrador de sistema.

Los detalles le siguen:

[responsereason]

_____
Correo electrónico 100% libre de spam proveído por Sendio, Inc. (http://[sendiourl])

[103] SAV Bounce Template - English/Spanish

From: “[username]” <[useraddr]>
To: “[origfromname]” <[origsenderaddr]>
Subject: [orgname] le pide que usted verifique su dirección de correo electrónico: por favor RSendioONDA a este mensaje. -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]
X-Priority: 1
Priority: Urgent
Importance: high

_____

Un mensaje de “[username]”
_____

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 rSendioonda a este mensaje al presionar la opción RSendioonder 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 rSendioonda a este mensaje, asegúrese de que la dirección a la cual esta contestando sea:

[origconfirmaddr]

Si usted no rSendioonde a este pedido de verificación de dirección durante [pending_lifetime], o si su rSendiouesta no es enviada a la dirección indicada arriba, su mensaje original nunca será dSendioachado.

Muchas Gracias!

[username]

_____
Correo electrónico 100% libre de spam proveído por Sendio, Inc. (http://[sendiourl])

_____

Message from “[username]”
_____

I recognize from your email address that this is the first message I have received from you since [orgname] 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:

[origconfirmaddr]

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

Thank you!

[username]

_____
100% spam-free email provided by Sendio (http://[sendiourl])

[104] SAV Request Template - Spanish/ English

From: “[username]” <[useraddr]>
To: “[vfyfromname]” <[vfysenderaddr]>
Subject: Aceptado: Autenticación de Dirección del Remitente -- [timestamp]
References: [origmsgid], [vfymsgid]
In-Reply-To: [vfymsgid]

Así de Fácil! Gracias por su colaboración.

Su Verificación de Dirección ha sido realizada y su mensaje original dSendioachado a la casilla de correos. En el futuro usted podrá estar asegurado que sus mensajes pasaran directo a mi casilla de correo.

[responsereason]

_____
Verificación de Dirección del Remitente (SAV) realizado por SENDIO.

Si usted también desea parar el Spam en forma definitiva, por favor visíte a Sendio al
http://[sendiourl]/how-sender-authentication-works.html

That was easy! Thanks for your help.

Your address verification has been completed and your original message has been delivered. In the future you may enjoy the confidence of knowing that all your messages will be promptly delivered to my Inbox.

[responsereason]

_____
Sender Address Verification (SAV) provided by Sendio.

To find out how you can have 100% spam-free email, please visit Sendio at
http://[sendiourl]/how-sender-authentication-works.html

[105] SAV Acknowledgement Template - Spanish/ English

From: “[username]” <[useraddr]>
To: “[origfromname]” <[origsenderaddr]>
Subject: Su mensaje no pudo ser dSendioachado -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]

Este mensaje fue generado por el Sendio I.C.E. appliance.

Su correo electrónico fue aceptado por el Sendio, pero no pudo ser dSendioachado a su destino final. Si usted cree que el recibir este mensaje es un error, por favor comuníquese con su administrador de sistema.

Los detalles le siguen:

[responsereason]

_____
Correo electrónico 100% libre de spam proveído por Sendio, Inc. (http://[sendiourl])

The Sender Address Verification (SAV) system at [orgname] has encountered a problem with the message you sent:

[responsereason]

_____
100% spam-free email provided by Sendio (http://[sendiourl])

[106] SAV Bounce Template - Spanish/ English

From: “[username]” <[useraddr]>
To: “[origfromname]” <[origsenderaddr]>
Subject: [orgname] le pide que usted verifique su dirección de correo electrónico: por favor RSendioONDA a este mensaje. -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]
X-Priority: 1
Priority: Urgent
Importance: high

_____

Un mensaje de “[username]”
_____

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 rSendioonda a este mensaje al presionar la opción RSendioonder 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 rSendioonda a este mensaje, asegúrese de que la dirección a la cual esta contestando sea:

[origconfirmaddr]

Si usted no rSendioonde a este pedido de verificación de dirección durante las próximas 2 semana, o si su rSendiouesta no es enviada a la dirección indicada arriba, su mensaje original nunca será dSendioachado.

Muchas Gracias!

[username]

_____
Correo electrónico 100% libre de spam proveído por Sendio, Inc. (http://[sendiourl])

[107] SAV Request Template - Spanish

From: “[username]” <[useraddr]>
To: “[vfyfromname]” <[vfysenderaddr]>
Subject: Aceptado: Autenticación de Dirección del Remitente -- [timestamp]
References: [origmsgid], [vfymsgid]
In-Reply-To: [vfymsgid]

Así de Fácil! Gracias por su colaboración.

Su Verificación de Dirección ha sido realizada y su mensaje original dSendioachado a la casilla de correos. En el futuro usted podrá estar asegurado que sus mensajes pasaran directo a mi casilla de correo.

Su mensaje original se encuentra adjunto.

_____
Verificación de Dirección del Remitente (SAV) realizado por SENDIO.

Si usted también desea parar el Spam en forma definitiva, por favor visíte a Sendio al
http://[sendiourl]/how-sender-authentication-works.html

[108] SAV Acknowledgement Template - Spanish

From: “[username]” <[useraddr]>
From: “[username]” <[useraddr]>
To: “[origfromname]” <[origsenderaddr]>
Subject: Su mensaje no pudo ser dSendioachado -- [timestamp]
References: [origmsgid]
In-Reply-To: [origmsgid]

Este mensaje fue generado por el Sendio I.C.E. appliance.

Su correo electrónico fue aceptado por el Sendio, pero no pudo ser dSendioachado a su destino final. Si usted cree que el recibir este mensaje es un error, por favor comuníquese con su administrador de sistema.

Los detalles le siguen:

[responsereason]

_____
Correo electrónico 100% libre de spam proveído por Sendio, Inc. (http://[sendiourl])

[109] SAV Bounce Template - Spanish

GLOSSARY

Applications Programming Interface (API)

This is an interface that can be used by a third party to programmatically access data in a secure fashion on Sendio.

DNS (port 53) Access

This port provides the Distributed Naming Service (DNS) access to Sendio. DNS is a service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet, however, is really based on IP addresses. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

External Address (Primary)

If you do not have a Sendio cluster, this is the only external address you must provide. This is the public address that will be NAT'ed to the server so that it may be configured. The accuracy of this address is very important.

External Cluster Address

If you have a Sendio cluster, then you may provide a secondary address that is movable within the firewall. This address cannot be bound to a MAC address, or Sendio will not failover properly as intended.

External Network Gateway

Strictly speaking, a gateway is a means by which users of one computer system can gain access to another without making a separate connection. The external gateway is the address that is essentially provided by the ISP that allows other network components to access the firewall and external network.

Firewall Address

This is the public IP address of your firewall. This may or may not be the public-facing IP for your mail traffic, i.e., the MX record for your mail.

Graphical User Interface (GUI)

This is a user interface for interacting with a computer which employs graphical images and text to represent the information and actions available to the user.

HTTP (port 80) Access

This port provides Sendio with a method to automatically update its internal software and provides web interface access to Sendio for end users and for administrative purposes.

HTTPS (port 443) Access

This port provides Sendio with a method to update its internal software automatically and provide web interface access to Sendio for end users and for administrative purposes.

Internal Cluster Address (Primary)

If you do not have a Sendio cluster, then this is the only internal cluster address you must provide. This address is the internal address of Sendio that allows the secure connection from the internet. In many cases, this address begins with a 10.xxx.xxx.xxx or 192.168.xxx.xxx.

Internal Cluster Address (Secondary)

If you have a Sendio cluster, then you may provide a secondary address that is movable within the firewall. This address cannot be bound to a MAC address, or Sendio will not failover properly as intended.

Internal Mail Gateway

This is the address of the email server where Sendio should deliver mail after processing. It should be an internal address. If Sendio and the mail server are on different LAN segments or cross a DMZ, it is imperative that the firewall is configured in such a way as to allow access from Sendio to the mail server.

Internal Network Gateway

This is the internal network address that Sendio and other network components will use to access the outside world.

LDAP Communication URL

The LDAP Communication URL is sometimes called the Active Directory URL. Sendio communicates with your Connection Directory Server through this URL for address and account synchronization. For proper functionality, Sendio must have a valid connection to an LDAP compliant domain controller. The common ports for this communication are 389 for LDAP users or 3268 for Microsoft's Global Catalog.

LDAP Username/Password

Sendio requires a user name and password for proper connectivity to the Domain Controller on your network. This user does not need a mail box, requires only basic permissions, and the password must be set to never expire.

MTA

Mail Transfer Authority. This abbreviation is the generic term that references the server that processes the messaging within an organization. Typical examples are Exchange and Lotus Notes.

NTP (port 123) Access

The Network Time Protocol (NTP) port allows time synchronization between devices. Bidirectional access is required. If you do not want to provide this access to Sendio, you will need to provide the name and address of an internal time server.

SMTP (port 25) Access

The Simple Mail Transport Protocol (SMTP) port provides basic communication between Sendio and other mail servers on your network and on the Internet. Port 25 is required for sending SAV requests, and as such requires the ability to originate and complete connections on port 25. Note that this is NOT an open relay. Make sure that Sendio is permitted to make unrestricted connections to your Exchange server for SMTP. Disable any rate limiting, as Sendio will become the sole source of traffic to your mail server.

SSH (port 22) Access

Secure shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. This port provides Sendio with a method to automatically update its internal software and to provide Sendio access to the server for maintenance, troubleshooting or updates.

sendio®
The eMail Integrity Company

Sendio, Inc.

4911 Birch, Suite 150

Newport Beach, CA 92660 USA

+1.949.274.4375

www.sendio.com