sendio®

Sendio® Email System Protection Appliance

# Quick Start Guide

Sendio 5.0

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

This *Quick Start Guide* will help get Sendio up and running quickly. It assumes that you have experience configuring email servers and networking equipment. Please read the entire *Quick Start Guide* first to make sure you understand the scope of the process. A detailed *Installation Guide*, as well as the *Administration Manual, User Guide, Backup & Restore Guide* and *LDAP Configuration Guide*, can be downloaded from **www.sendio.com/support/documentation**.

## OVERVIEW

This *Quick Start Guide* covers the following steps:

1. Gathering all of the required hardware
2. Determining the IP addresses, user names and passwords of various systems and accounts
3. Physically installing the appliance in a rack
4. Modifying your firewall settings
5. Configuring system IP addresses and network settings
6. Verifying communications
7. Checking for software updates
8. Using the console interface to set system configuration parameters
9. Using the web interface to configure directory services
10. Setting the IP address of the system internal mail host
11. Setting the directory auto-synchronization schedule
12. Granting Administrator access to one or more users
13. Setting Contacts
14. Configuring Sendio Backups
15. Routing email traffic through Sendio

## STEP 1: HARDWARE

Verify that you have the following items:

- Sendio appliance (e.g. ESP166, ESP360, ESP430)
- AC power cord (included with the appliance)
- Rack mounting kit (included with the ESP360 and ESP430 only)
- Ethernet cable
- VGA monitor
- Keyboard

## STEP 2: ADDRESSES AND ACCOUNTS

Gather the following network information:

- IP address of your internal email server
- IP address of your directory server
- User name and password for accessing your directory server for Sendio LDAP synchronization (a user account with standard user privileges and a ***password that does not expire*** is required)

## STEP 3: PHYSICAL INSTALLATION

1. Install Sendio in an equipment rack. Detailed instructions are in *Appendix B* of the *Installation Guide* or the *Rack Installation Guide* that was shipped with your unit.
2. Connect an Ethernet cable from your network switch to the port labeled NETWORK at the back of the appliance.
3. Connect a VGA monitor, keyboard, and AC power cord to the appliance.
4. The system should power on as it is designed to restart automatically in the event of a power failure. If the system does not automatically power on press the power button on the front panel of the appliance.

## STEP 4: FIREWALL MODIFICATIONS

Sendio should be deployed behind your corporate firewall. Certain ports must be open to ensure proper operation, as shown below.

| PORT | DIRECTION | ORIGIN | DESTINATION | USAGE |
|---|---|---|---|---|
| TCP 22 | In | Sendio Trusted Subnet (listed below) | ESP appliance | Remote access by Sendio Support |
| TCP 25 | ***Out*** | ESP appliance | * | SAV Requests & Bounces, outbound e-mail |
| TCP/UDP 53 | ***Out*** | ESP appliance | * | Domain Name Service (DNS) |
| TCP 80 | In [(1)] | * (optional) | ESP appliance | External access to ESP appliance web interface |
| TCP 80 | ***Out*** | ESP appliance | Sendio Trusted Subnet (listed below) | Sendio Updates |
| TCP 443 | In [(1)] | * (optional) | ESP appliance | Secure HTTPS External access to ESP appliance web interface |
| TCP 443 | ***Out*** | ESP appliance | Sendio Trusted Subnet (listed below) | Sendio Updates |
| UDP 123 | ***Out*** | ESP appliance | * | Network Time Protocol (NTP) |
| TCP/UDP 6277 | ***Out*** | ESP appliance | * | DCC Bulk Tagging Service |

*Table of Firewall Port Configurations*

NOTE [(1)]: Inbound TCP 80 and/or TCP 443 is required only if access to the Sendio web interface is to be available from an external connection.

The following is Sendio's trusted subnet:

Starting IP address: 64.58.146.32
Subnet Mask: 255.255.255.224 [27 bits]
Range Notation: 64.58.146.32/27 (255.255.255.224)
Address range: 64.58.146.32 - 64.58.146.63

The following addresses are Commtouch services that require TCP 80 **Outbound** access:

1. 65.74.168.210
2. 216.163.188.45
3. 208.50.223.240
4. 116.92.1.80

OR

1. resolver1.t.ctmail.com
2. resolver2.t.ctmail.com
3. resolver3.t.ctmail.com
4. resolver4.t.ctmail.com
5. resolver5.t.ctmail.com

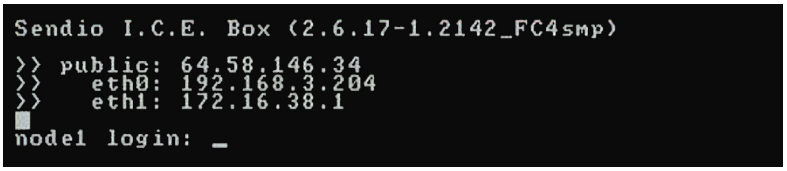
The firewall and any other security devices must permit the following file types over port 80/443 for update purposes: .rpm, .xml, .xml.gz, .xml.md5, .tar.gz, .avc, .ini, .dt, .cfg, .mhk, .lst, .set, .vnd, .klb, and .ver.

## STEP 5: CONFIGURING ADDRESSES

1. Using the VGA monitor and keyboard, login to the console interface with the default admin login:

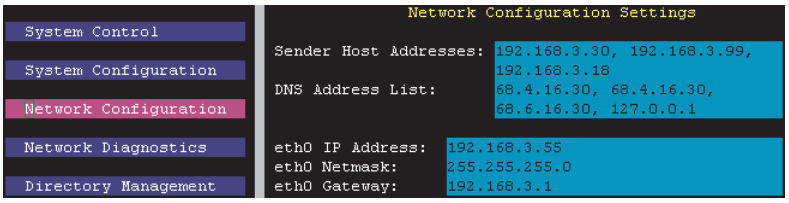
   **Login:** `sysconfig`
   **Password:** `admin`

   (this default password will be changed in STEP 8).




*sysconfig Console Login*

2. Navigate to the **Network Configuration** section.
3. If you will be using Sendio for processing outbound email (***highly recommended*** for maximum effectiveness), enter the IP address(es) of the internal email server(s) that will be sending outbound email through Sendio in the *Sender Host Addresses* field.




*Network Configuration*

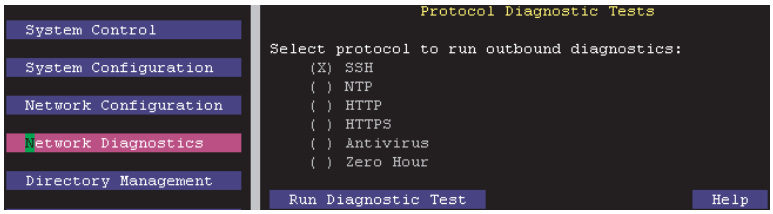
4. Configure the *IP Address*, subnet mask, *Gateway*, and DNS settings (in a comma separated list). Using 127.0.0.1 in the DNS Address list will instruct Sendio to use the internet root DNS servers.
5. **Save your settings.**

> NOTE: Create an internal DNS entry for access to the Sendio web interface (e.g., nospam.yourdomain.com).

> NOTE: Once Network Settings are configured and Sendio is accessible over the network, the console interface can be accessed from another computer via a secure shell (SSH) connection using a telnet/ssh client such as PuTTY (a freeware download).

## STEP 6: VERIFYING COMMUNICATIONS

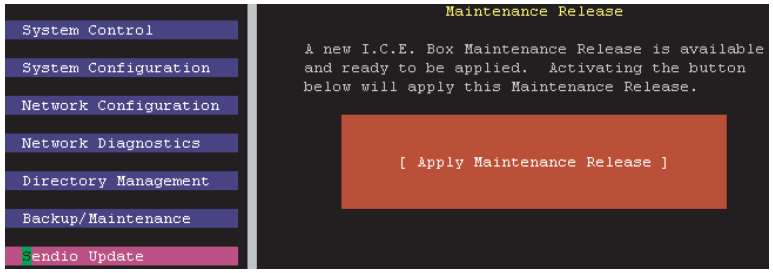
1. Using another computer on your network, **`ping`** the Sendio IP address to ensure that the *eth0 IP Address* set in STEP 5 above has been properly assigned.
2. Using the SSH (PuTTY) interface, navigate to the **Network Diagnostics** section:
   a. Use the *Protocol Diagnostic Tests* to verify outbound connectivity on all listed protocols
   b. Use the *SMTP Diagnostic Tests* to verify outbound SMTP connectivity to *mx1.hotmail.com*. *(Verify that a definition for reverse DNS (rDNS) is in place for the appliance's public IP address. The output shows what rDNS is currently in place. Ask your ISP to configure the rDNS entry for you.)*
   c. Use the DNS Lookup section to verify successful DNS lookup of *example.com*




*Network Diagnostics*

## STEP 7: SENDIO UPDATE

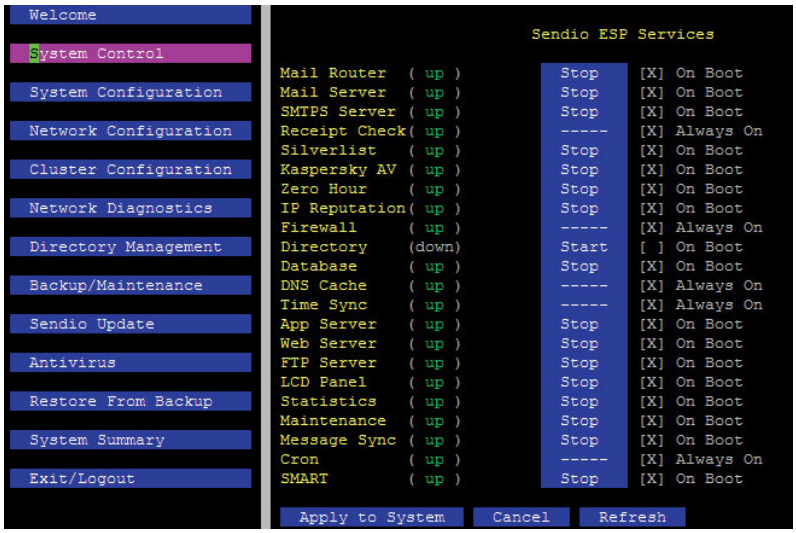
1. Using the Sendio SSH (PuTTY) interface, navigate to the **Sendio Update** section
2. Install any available *Maintenance Release* software updates.



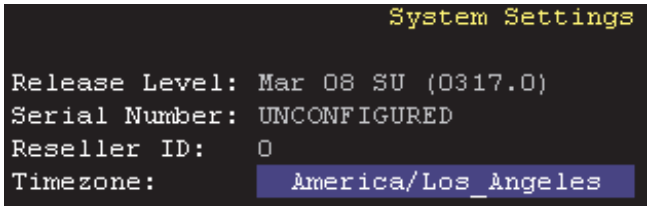

*Sendio Update*

## STEP 8: SYSTEM CONFIGURATION

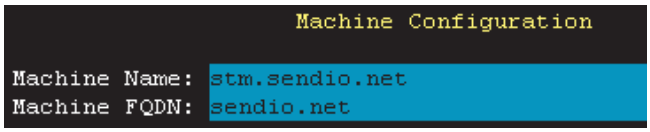
1. Using the Sendio SSH (PuTTY) interface, navigate to the **System Control** section.



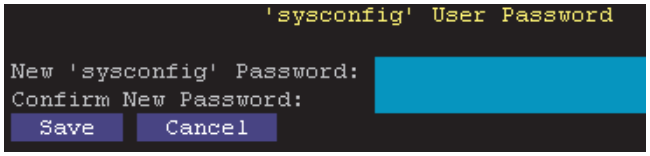

*System Control*



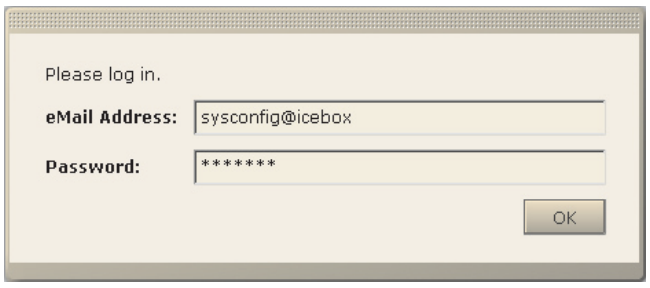

*Time Zone*




*Machine Configuration*




*sysconfig Console Password*




*[10] Web Interface Login*

2. Confirm services are configured to reflect those shown to the left.
3. Navigate to the **System Configuration** menu option.
4. Set the correct time zone for Sendio.
5. **Save your settings.**
6. Set the *Machine Name* (e.g. **mail.mydomain.com**) and *Fully Qualified Domain Name* (domain name only, such as **mydomain.com**).

   *Machine Name* should match the DNS hostname associated with your firewall's public IP address (i.e. the result of a reverse DNS lookup on the public IP address).

NOTE: Make sure that a reverse DNS lookup (rDNS) on the appliance's public IP address results in the hostname you set in step 5 above. To verify the rDNS setup, we recommend using an online tool such as http://www.mxtoolbox.com.

7. **Save your settings**
8. Set the *sysconfig* password. The password must be between 5 and 8 characters in length and use both letters and numbers.

**NOTE:** The *sysconfig* password must be changed. Failure to do so will prohibit access to the Sendio appliance web interface.

## STEP 9: DIRECTORY SERVICES

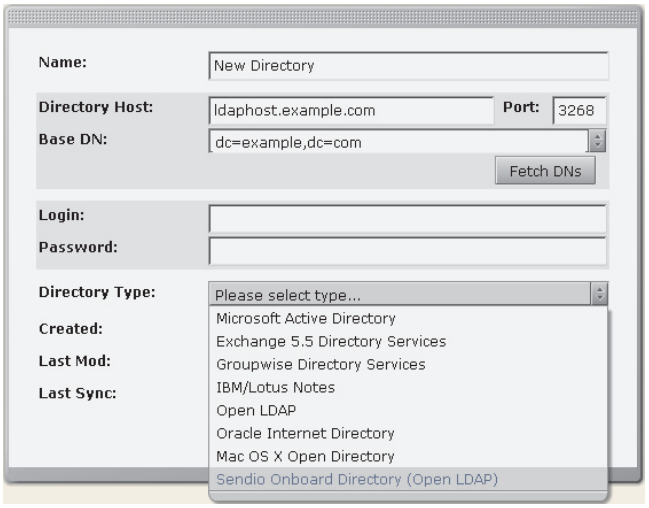
1. Open a web browser and navigate to the Sendio web interface using the Sendio IP address.
2. When the dialog box opens, enter **`sysconfig@icebox`**, and the password that you established in STEP 8 above.

3. Using the Sendio web interface, click the **Domains** menu option to show the **Domains** page, click the **New** button to open the pop-up window, enter the domain that will be protected by the Sendio appliance (*@domain.com), and click the **Create** button.
4. Repeat for multiple domains
5. Create a Synchronization User on your directory server.
6. Using the Sendio web interface, click the **Directories** menu option to show the **Directories** page, and click the **New** button to open the pop-up window.
7. Enter the IP address of the directory server.
8. Select the *Directory Type.*
9. Verify the *Port* number.
    - Microsoft Active Directory defaults to port 3268, while other LDAP servers default to port 389.
10. Click the **Fetch DNs** button and select the appropriate Base DN.
11. Select the OU that will be synchronized to the Sendio appliance. Optionally, manually enter a prefix to the Base DN setting (i.e. “ou=users” or “cn=Departments”) to specify or narrow the scope of synchronization.

**EXAMPLE:** `cn=users, dc=example, dc=com`

12. Enter the Synchronization User *Login* and *Password* that you gathered in STEP 2. This may require a domain prefix such as “mydomain\username”.
13. **Save your changes.**
14. Click the **Actions** button and select the *Synchronize Selected Directories* option.


*Create New Domain*

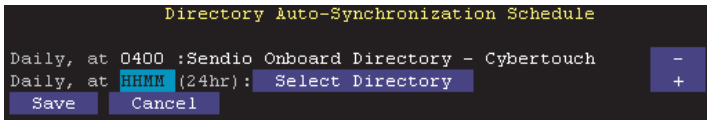



*Create New Directory*

## STEP 10: SYSTEM OPTIONS

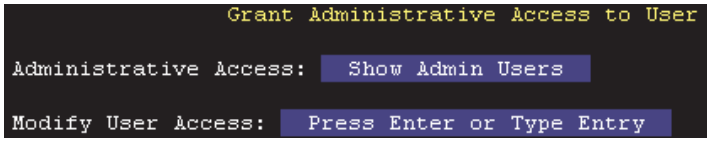
1. Using the Sendio web interface, click the **System > Options** tab.
2. Set the *Internal Mail Host* to the IP address of the internal email server.
3. Set the *Organization Name* to the company name that will be used in SAV messages.
4. Set the *Preferred Time Zone*.
5. Set *Integrity Services* to *Enabled* .
6. Set *SilverListing* to *Enabled*.
7. **Save your settings.**
8. **Restart the Sendio appliance from the SSH (PuTTY) interface > System Control > Reboot Sendio ESP.**

## STEP 11: SET DIRECTORY SYNCHRONIZATION




*Directory Synchronization*

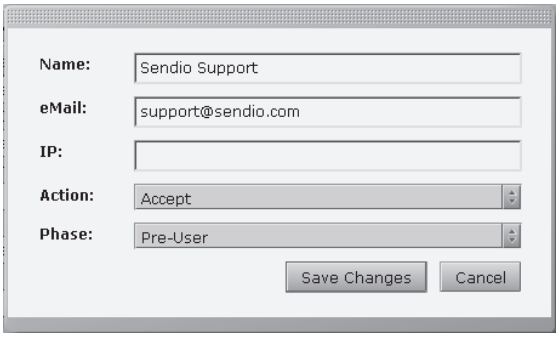
1. Using the Sendio SSH (PuTTY)interface, navigate to the **Directory Management** section.
2. Arrow over to **Select Directory** and press *Enter.* Press *Enter* again to accept default selection.
3. Arrow over to **HHMM** and remove all letters. Enter time for synchronization in military time format (i.e. 2200).
4. Arrow over the the **+** sign and press *Enter* to add new synchronization schedule.
5. **Save your settings.**



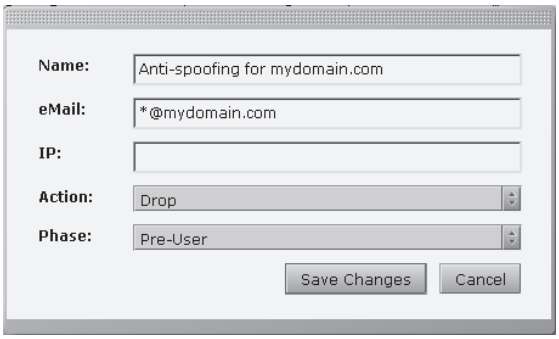

*Admin Users*

## STEP 12: SET ADMIN USER

1. Using the console interface, navigate to the **Directory Management** section.
2. Arrow over to **Press enter or Type Entry**. Enter users last name and press *Enter*.
3. Select the appropriate user with the space bar. Tab to highlight **Select** and press *Enter*.
4. Arrow to **Grant Full Admin Access**. Press *Enter*.
5. **Save your settings.**
6. Repeat for additional Admins.




*New* **System** *Contact*

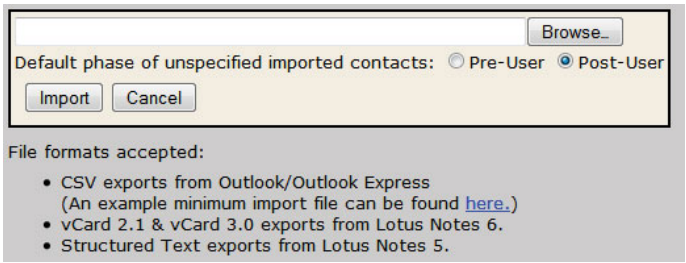



*Anti-Spoofing Contact*

## STEP 13: SET CONTACTS

1. Using the Sendio web interface, create a **System** contact entry to accept all email from Sendio Support by clicking **System > Contacts > New.** Use the email *support@sendio.com*.
2. Using the Sendio web interface, verify that a **System** drop contact exists to counter spoofing (incoming email with sender addresses belonging to your own domain) by reviewing the **System > Contacts** page. This was created when you entered the domain name in the Domains section.

- If external **Blackberry users** exist, and you don't use a Blackberry Enterprise Server, create a System *Accept* contact (*Pre-User*) for *@*.blackberry.net and one for *@srs.bis.na.blackberry.com.
- It is very important to build the initial list of company contacts. In most organizations there is an existing list of email contacts that can be imported into Sendio. From accounting applications to CRM to an Exchange Public Folder, this existing list of email addresses can very likely be exported to a CSV which can then be exported in to Sendio from **Sendio web interface > System > Contacts > Actions > Import Contacts**. Once the CSV of existing email contacts is created, import the CSV in to System Contacts.



## STEP 14: CONFIGURE SENDIO BACKUPS

Please refer to the *Sendio Backup & Restore Guide* for instructions on configuring the daily Sendio backup. It is very important to have backups configured and scheduled before you proceed to Step 14. The *Sendio Backup & Restore Guide* can be found on the Sendio web site at **http://www.sendio.com/support/documentation**.

## STEP 15: ROUTE EMAIL TRAFFIC

1. On your firewall, direct inbound SMTP traffic (TCP port 25) to the IP address of your ESP appliance.
2. View the LOGS section of the web interface to verify that traffic is flowing.
3. Send a final test email from an external account, reply to the *SAV Request,* and verify the test message is released from the *Pending Queue*.
4. Configure your internal email server to route outbound email through Sendio. *Please refer to the instructions from your internal email server's manufacturer for details on how to smart host your email server*. For Microsoft Exchange please refer to the *Exchange Smart Hosting Guide* on the Sendio web site at **http://www.sendio.com/support/documentation**.

Congratulations! Your Sendio appliance has been successfully configured. For additional support please visit the Sendio FAQ at **http://www.sendio.com/faq**.