

This Quick Start Guide will help get Sendio up and running quickly. It assumes you have experience configuring email servers and networking equipment. Read this entire guide to understand this process. Detailed Installation Guide, Administration Manual, User Guide, Backup & Restore Guide, and LDAP Configuration Guide can be downloaded from <https://sendio.com/support/documentation-and-support-tools/>

Overview

This Quick Start Guide covers the following steps. If you are using the Sendio virtual appliance, skip steps 1 and 3.

1. Gathering all the required hardware (skip if using the Sendio virtual appliance)
2. Determining the IP addresses, usernames and passwords of various systems and accounts
3. Physically installing the appliance in a rack (skip if using the Sendio virtual appliance)
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
- Ethernet cable
- AC power cord (included with appliance)
- VGA monitor
- Rack-mounting kit (included with the ESP500 only)
- Keyboard



STEP 2: ADDRESSES AND ACCOUNTS

Gather the following network information:

- IP address of your internal email server
- IP address of your directory server
- Username and password for accessing your directory server for Sendio LDAP synchronization (a user account with read-only access to all users and groups, and a password that does not expire are required)

STEP3: PHYSICAL INSTALLATION

1. Install Sendio in an equipment rack. Refer to the Installation Guide or the Rack Installation Guide 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 powers on, as it is designed to restart automatically in the event of a power failure. If the system does not power on automatically, press the power button on the front panel of the appliance.

STEP 4: FIREWALL MODIFICATIONS

Deploy Sendio 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 headquarters	ESP appliance	Remote access by Sendio Support
TCP 25	Out	ESP appliance	All Public IPs	SAV Requests and Bounces, outbound email
TCP 25 (NOTE 1)	In	All Public IPs	ESP appliance	Sending domains - outbound mail servers
TCP/UDP 53 (NOTE 2)	Out	ESP appliance	All Public IPs	Domain Name Service (DNS)
TCP 80	In (NOTE 3)	All Public IPs (optional)	ESP appliance	External access to ESP appliance web interface
TCP 80	Out	ESP appliance	All Public IPs	IP Reputation, anti-virus, anti-spam, software updates
TCP 443 (NOTE 3)	In	All Public IPs (optional)	ESP Appliance	Secure HTTPs External access to ESP Appliance web interface
TCP 443	Out	ESP appliance	All Public IPs	Software updates
UDP 123	Out	ESP appliance	All Public IPs	Network Time Protocol (NTP)

NOTE (1): Complete all configuration steps in this guide before routing live inbound TCP port 25 traffic to the ESP appliance.

NOTE (2): If you use an internal DNS server, we recommend you allow outbound DNS access as well. That way, if your local DNS server fails, Sendio's access to public DNS servers ensures uninterrupted email flow.

NOTE (3): 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.

Sendio Headquarters IP Addresses

IP address: 206.82.219.132

The following information will help customers who require more detail about Sendio’s outbound packet flows on TCP ports 80 and 443. We recommend opening these TCP ports to all public IP addresses because the IP addresses listed below can change. By allowing completely open access, you will not need to update your firewall rules in the future.

Sophos anti-spam, AntiVirus, Zero Hour Anti-Virus, and IP Reputation Services (Host Name and IP Address)TCP Port 80 outbound from Sendio to these hosts:

sendio.com sendio.net sophos.com sophosxl.net ntp.org

Sendio Software Updates

TCP port 80 and TCP port 443 outbound from Sendio to these IP addresses:

TCP ports 80 and 443 outbound access to 66.240.197.232. TCP ports 80 and 443 outbound access to 66.240.197.224.

File Types

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 Ips & DNS

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

Login: sysconfig

Password: admin

You will change this default password in STEP 8.

```
Sendio I.C.E. Box (2.6.17-1.2142_FC4smp)
>> public: 64.58.146.34
>> eth0: 192.168.3.204
>> eth1: 172.16.38.1
node1 login: _
```

2. Navigate to the **Network Configuration** section.

3. If you will be using Sendio to process outbound email (highly recommended for maximum effectiveness), enter the IP address(es) of the internal email server(s) that will send outbound email through Sendio in the Sender Host Addresses field.

```
System Control
System Configuration
Network Configuration
Network Diagnostics
Directory Management

Network Configuration Settings
Sender Host Addresses: 192.168.3.30, 192.168.3.99,
192.168.3.18
DNS Address List: 68.4.16.30, 68.4.16.30,
68.6.16.30, 127.0.0.1
eth0 IP Address: 192.168.3.55
eth0 Netmask: 255.255.255.0
eth0 Gateway: 192.168.3.1
```

4. Configure the IP Address, subnet mask, and Gateway settings of your network port.

```
eth0 IP Address: 216.23.184.4
eth0 Netmask: 255.255.255.192
eth0 Gateway: 216.23.184.1

[ ] Use Custom DNS Servers?
```

5. You have a Use Custom DNS Servers option. If you uncheck this radio button, Sendio uses the internet root DNS servers automatically. If using your internal DNS servers, check Use Custom DNS Servers and enter your server IP addresses as a comma-separated list into DNS Server IP Addresses. By default, if Sendio cannot reach your internal servers, alternative DNS servers on the Internet will be used.



6. Save your settings.

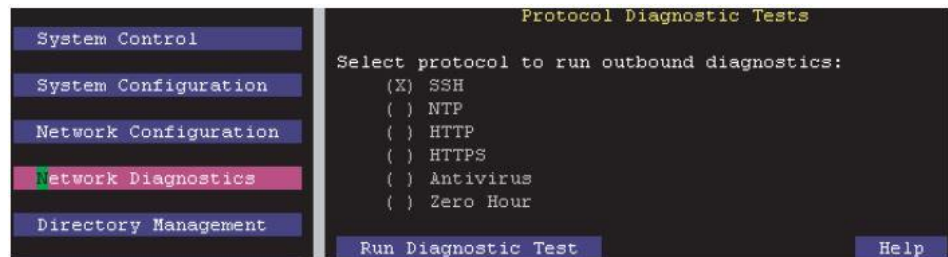
Note: Create an internal DNS entry for access to the Sendio web UI (eg., nospam.yourdomain.com).

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 the eth0 IP Address set in STEP 5 on page 3 is assigned properly.

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

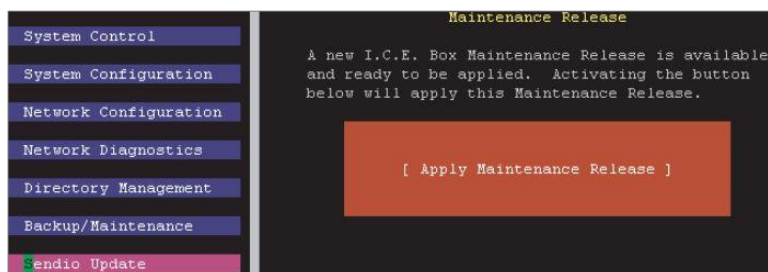
b. Use the SMTP Diagnostic Tests to verify outbound SMTP connectivity to mx1.hotmail.com. (Verify that a definition for reverse DNS (rDNS) is in place for the appliance's public IP address. The output shows what rDNS is currently in place. Ask your ISP to configure the rDNS entry for you.)

c. Use the DNS Lookup section to verify successful DNS lookup of example.com

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.



STEP 8: SYSTEM CONFIGURATION

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

2. Confirm services are configured to reflect those shown to the right.

3. Navigate to the System Configuration menu option.

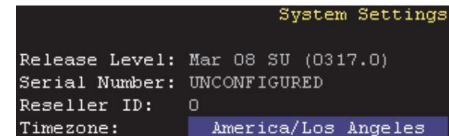
4. Set the correct time zone for Sendio.

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).



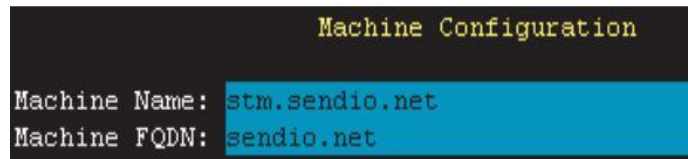
Machine Name should match the DNS hostname associated with your Sendio appliance's public IP address used for its outbound emails. That is, the reverse DNS of the public IP should be the same as your machine name. The Machine name should also have a public DNS A-record that matches the appliance public IP.



Note: Be sure a reverse DNS lookup (rDNS) on the appliance's public IP address results in the hostname you set in STEP 6. To verify the rDNS setup, use an online tool such as <http://www.mxtoolbox.com>. The formal name for rDNS is a PTR record.

7. **Save your settings.**

8. Set the sysconfig password. The password must be between 5 and 8 characters and use both letters and numbers.

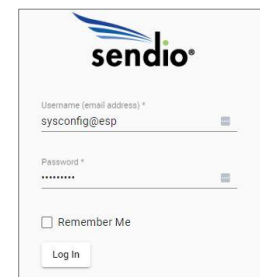


Note: The sysconfig password must be changed. Failure to do so will prohibit access to the Sendio appliance web interface.

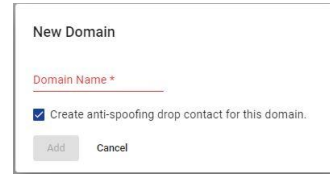
STEP 9: DIRECTORY SERVICES

1. Open a web browser and navigate to the Sendio web UI using the Sendio IP address or machine name.

2. At the dialog box, type sysconfig@esp and the password entered in STEP 8 on page 5.



3. In the Sendio web interface, click the Domains menu. At the Domains page, click “+” to open a pop-up window, enter a domain that will be protected by the Sendio appliance (domain.com), and click the Create button.



A small form titled "New Domain" with a "Domain Name" input field, a checked checkbox for "Create anti-spoofing drop contact for this domain.", and "Add" and "Cancel" buttons.

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 “+” to open the pop-up window.

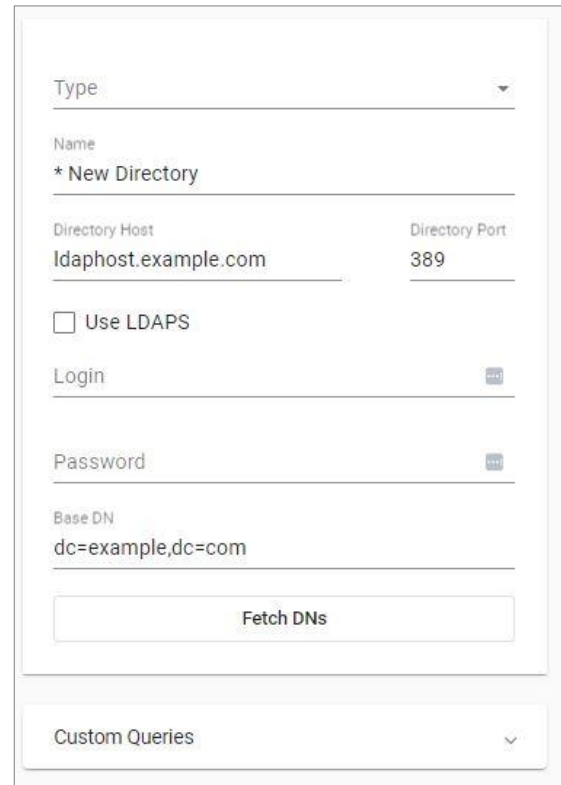
7. Select the Directory Type.

8. Give the Directory a name

9. Configure the Directory Host, either in IP address or hostname. Verify the Port number. Microsoft Active Directory defaults to port 3268, while other LDAP servers default to port 389.

10. Enter the Login user and Password created earlier.

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.



A larger form for configuring a directory. It includes fields for "Type", "Name" (with a dropdown showing "* New Directory"), "Directory Host" (with "ldaphost.example.com"), "Directory Port" (with "389"), a checkbox for "Use LDAPS", "Login" and "Password" fields with eye icons, and a "Base DN" field with "dc=example,dc=com". A "Fetch DNs" button is at the bottom. Below the form is a "Custom Queries" dropdown.

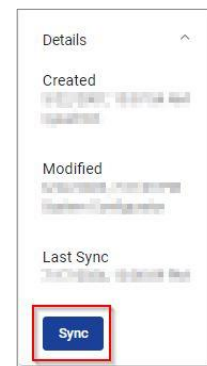
EXAMPLE: cn=users, dc=example, dc=com

12. Click the Fetch DNs button and select the appropriate Base DN if needed. You can use Custom Queries also.

13. **Save your changes.**

14. Synchronize the directory.

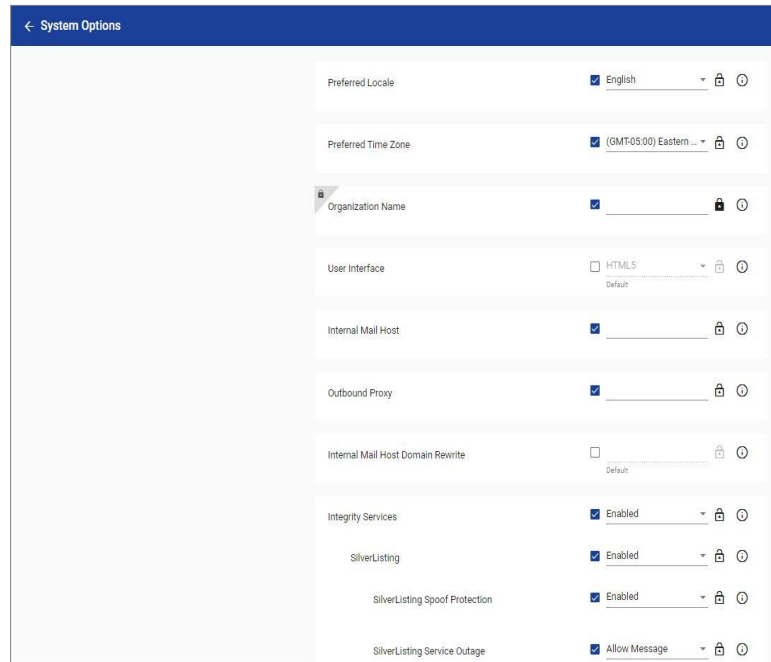
Note: After your directory is synced, user single sign-on to Sendio will be functional. Any user can then log in to Sendio using the same credentials the user uses to log in to his computer and email account (e.g., email address and network password).



A details panel for a directory. It shows "Created" and "Modified" timestamps, and "Last Sync" information. A blue "Sync" button is highlighted with a red box at the bottom.

STEP 10: SYSTEM OPTIONS

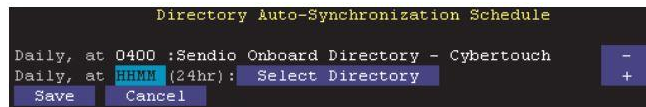
1. Using the Sendio web interface, click the System > Options tab.
2. Set the Internal Mail Host to the IP address of the internal email server.
3. Set the Organization Name to the company name that will be used in SAV messages.
4. Set the Preferred Time Zone.
5. Set Integrity Services to Enabled .
6.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



STEP 11: SET AUTOMATIC DIRECTORY SYNCHRONIZATION SCHEDULE

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.

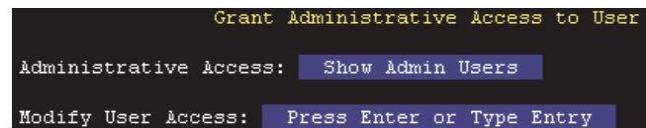


3. Arrow over to HHMM and remove all letters. Enter time for synchronization in military time format (i.e. 2200).
4. Arrow over the + sign and press Enter to add new synchronization schedule.
5. **Save your settings.**

STEP 12: SET ADMIN USER

1. Using the console interface, navigate to the Directory Management section.

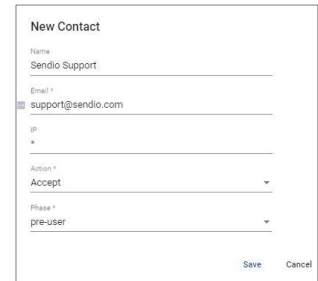
2. Arrow over to Press enter or Type Entry. Enter users last name and press Enter.



3. Select the appropriate user with the space bar. Tab to highlight Select and press Enter.
4. Move to Grant Full Admin Access, and then press Enter.
5. **Save your settings.**
6. Repeat for additional Admins.

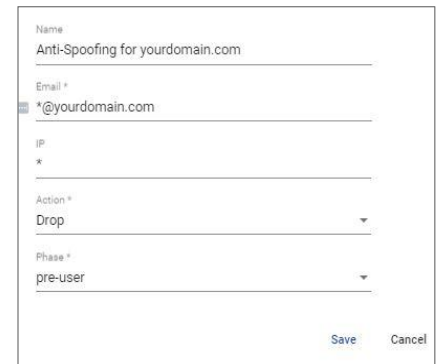
STEP 13: SET CONTACTS

1. In the Sendio web interface, click System > Contacts > three dots in the upper right-hand corner to create a System contact entry to accept all email from Sendio Support. Use email support@sendio.com.



2. In the Sendio web UI, review the System > Contacts page and confirm there is a System drop contact to counter spoofing (incoming email with sender addresses belonging to your own domain). This was created when you entered the domain name in the Domains section.

- If you use Cloud-based services such as NETSUITE®, Constant Contact®, Salesforce® to send email that appears as being internal to your organization, create a corresponding System Accept contact (Pre-User). In some cases, you may choose to remove the anti-spoofing contact.



- If desired, you can build the initial list of company contacts. In most organizations, an existing list of email contacts can be imported into Sendio. From accounting applications to CRM to an Exchange Public Folder, the email addresses can be exported to a CSV file that can then be exported into Sendio from Sendio web UI > System > Contacts > Actions > Import Contacts. After creating the CSV of existing email contacts, import the CSV into System Contacts.

STEP 14: CONFIGURE SENDIO BACKUPS

Refer to the Backup & Restore Guide – Sendio Appliances (<https://sendio.com/support/documentation-and-support-tools/>) for instructions on configuring the daily Sendio backup. It is critical to have backups configured and scheduled before you proceed to STEP 15.

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 UI 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 or Office 365 to route outbound email through Sendio. Refer to the instructions from your internal email server manufacturer for details on how to smart host your email server. For Microsoft Exchange, refer to the Exchange Smart Hosting Guide or the Sendio and Office 365 Integration document for MS Office 365 (<https://sendio.com/support/documentation-and-support-tools/>).

Congratulations! Your Sendio appliance is now configured successfully. For additional information, visit the Documentation Support page (<https://sendio.com/support/documentation-and-support-tools/>) or submit a support ticket.

The process for support tickets is located here: <https://sendio.com/support/submit-support-ticket/>