



Sendio® Email System Protection Appliance

Quick Start Guide – Sendio Hosted

Sendio 6.x and 7.x

This Quick Start Guide will help get your new Sendio Hosted Service instance up and running quickly. It assumes you have experience configuring email servers and firewalls. Read this entire guide to understand this process. In addition to this Quick Start Guide, the Administration Manual, Email Continuity Administration Manual, and User Guide are helpful for learning to use the product. All documentation is available at www.sendio.com/support/documentation.

NOTE: If you are using Microsoft Office 365™ for your email hosting, see [“APPENDIX A: SENDIO AND MICROSOFT OFFICE 365™” on page 9](#) for additional details.

OVERVIEW

With the Sendio Hosted Service, you can manage your entire email protection solution from a web-based interface, with no on-site hardware to manage. Your solution is served via a Tier 3 data center, with highly redundant hardware, power, and Internet bandwidth. Inbound emails route through your Sendio-hosted instance automatically via an MX record entry in public DNS. Outbound emails route through Sendio (if desired) via a Smarthost or relay setting in your mail server. All Sendio-hosted customers are provided a dedicated public IP address for email flows for maximum control.

This Quick Start Guide covers the following steps.

1. Determining the IP addresses, user names and passwords of various systems and accounts
2. Modifying your firewall settings
3. Verifying SMTP communications
4. Using the web interface to configure directory services
5. Entering your mail server public IP address into the *System/Internal Mail Host* field
6. Set “Sender Host Addresses” for outbound email
7. Setting the directory auto-synchronization schedule
8. Granting Administrator access to one or more users
9. Change the sysconfig password
10. Setting Contacts
11. Routing email traffic through Sendio
12. Enable the Queue Summary Email (Optional)

NOTE: Some steps in this guide require you to use PuTTY for SSH connections to Sendio. Before proceeding, download the free PuTTY software client from www.putty.org to your computer, and then use it for SSH connections to Sendio as directed in this guide.

STEP 1: IP ADDRESSES AND ACCOUNTS AND LOGIN INFORMATION

Gather the following information:

- Public IP address of your internal email server
- Public IP address of your directory server (Note: Your directory server may not be currently accessible on a public IP address and this will need to be changed in your firewall. For more information, see “Modifying Your Firewall Settings”)
- User name 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)
- Login URL, Administrator Login ID, and password for your Sendio Hosted instance (provided after your purchase)
- Public IP address for your Sendio Hosted Instance (provided after your purchase)
- Host name of your Sendio-hosted instance, which is used for the MX record and Smarthost (provided after your purchase)

STEP 2: FIREWALL MODIFICATIONS

Certain ports must be open to ensure proper operation, as shown below.

Port	Direction	Origin	Destination	Usage
TCP 25	In	Public IP of your Sendio Hosted Instance	Mail server Public IP	Incoming email from Sendio data center
TCP 3268 (see Notes 1 and 2)	In	Public IP of your Sendio Hosted Instance	Directory server Public IP	User import to Sendio, user single sign-on support
TCP 389 (see Notes 1 and 2)	In	Public IP of your Sendio Hosted Instance	Directory server Public IP	User import to Sendio, user single sign-on support
TCP 636 (see Notes 1 and 2)	In	Public IP of your Sendio Hosted Instance	Directory server Public IP	LDAP over SSL; automatic user import to Sendio, user single sign-on support

NOTE 1: Only one of the three TCP ports specified (3268, 389, or 636) is required for access to your directory server. TCP port 3268 is the most common for Microsoft Exchange. TCP port 636 will likely involve extra provisioning steps coordinated with Sendio Tech Support.

NOTE 2: If you use a cloud email hosting service, such as 1&1, Hostgator™, Hosted Exchange, Microsoft Office 365™, or Google Apps™, you may not have an onsite directory server. If you do not have an on-site directory server, contact Sendio Tech Support for assistance with manual user import steps.

STEP 3: VERIFYING SMTP COMMUNICATIONS

- Launch the Sendio SSH (PuTTY) interface and log in to your hosted instance.
 - Login ID** = sysconfig (Note: for this interface, login is not `sysconfig@esp`)
 - Password** = same password as the web interface.
- Navigate to **Network Diagnostics**.
- Scroll down to the **Email Test** section.
- In **SMTP Server**, enter your mail server public IP address.
- In **To**, enter a valid email address for your domain.
- Click **Run Diagnostic Test**, and confirm that email is received by the person whose email address you entered in **To** in the previous step.



Email Test

STEP 4: DIRECTORY SERVICES

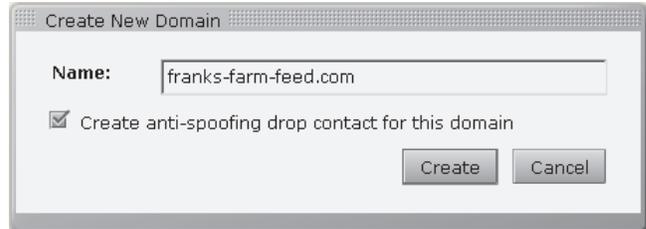
1. Open a web browser and navigate to the Sendio web interface (for example, `http://hostname.sendio.com`).
2. When the dialog box opens, type `sysconfig@esp` and the password provided by Sendio.
3. In the Sendio web interface, click the **Domains** menu option to show the **Domains** page, click the **New** button to open a pop-up window, enter the domain to 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. For most installations, the Base DN will suffice and no OU is required. This ensures that all email addresses and distribution groups are added properly to Sendio. If desired, select the specific OU that will be synchronized to the Sendio appliance.

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

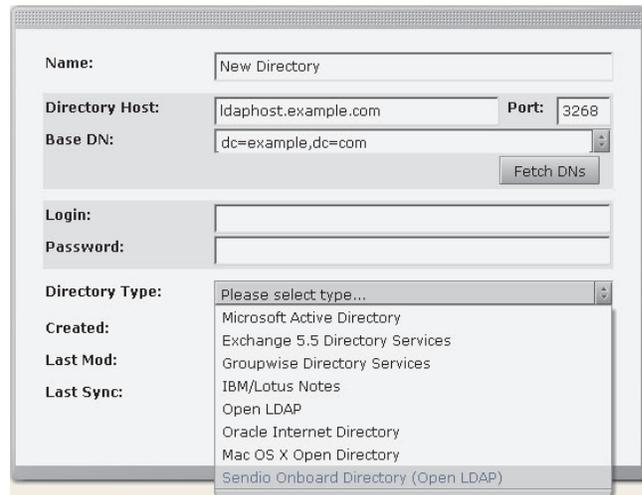
12. Enter the Synchronization User *Login* and *Password* that you gathered in STEP 1. This may require a domain prefix such as `mydomain\username`.
13. **Save your changes.**
14. Click the **Actions** button and select the *Synchronize Selected Directories* option.
15. After you select **Synchronize Selected Directories**, a pop-up similar to the one to the right appears. If the pop-up never displays the status **Directory Service Available**, your firewall may not be configured correctly to allow access from your Sendio hosted instance. If you receive an **Authentication Failed** error, the Login syntax or password is incorrect.
16. If synchronization succeeds, click **Accounts**. Within this **Accounts** section, all users and distribution groups in your company should be displayed.



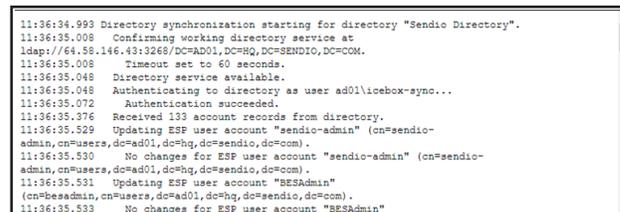
Web Interface Login



Create New Domain



Create New Directory



Pop-up After Selecting Synchronize Selected Directories

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).

STEP 5: SYSTEM OPTIONS (MAIL SERVER PUBLIC IP)

Enter your mail server public IP address, organization name, and preferred time zone.

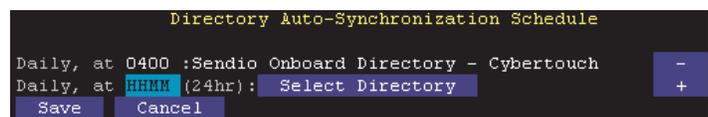
1. Using the Sendio web interface, click the **System > Options** tab.
2. Set the *Internal Mail Host* to the public IP address of your mail server.
3. Set the *Organization Name* to the company name that will be used in SAV messages.
4. Set the *Preferred Time Zone*.
5. **Save your settings.**

STEP 6: SENDER HOST ADDRESS FOR OUTBOUND EMAIL

1. Log in to the Sendio SSH (PuTTY) interface of your hosted instance.
 - **Login ID** = sysconfig (Note: for this interface, login is not `sysconfig@esp`)
 - **Password** = same password as the web interface.
2. After logging in, navigate to **Network Configuration**.
3. In the **Sender Host Addresses** field, enter the outbound public IP address for your organization's outbound emails.

STEP 7: SET AUTOMATIC DIRECTORY SYNCHRONIZATION

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



Directory Synchronization

STEP 8: SET ADMIN USER

1. Using the Sendio SSH (PuTTY) 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.



Admin Users

STEP 9: CHANGE YOUR sysconfig PASSWORD

1. If desired, change the sysconfig password by navigating to the **System Configuration** section of the Sendio SSH (PuTTY) interface.
2. Enter the new password.



sysconfig Console Password

NOTE: The password must be between 5 and 8 characters, and contain both letters and numbers. We recommend your password contain 8 characters or more.

STEP 10: SET CONTACTS

1. In the Sendio web interface, click **System > Contacts > New** to create a **System** contact entry to accept all email from Sendio Support. Use the email *support@sendio.com*.
2. In the Sendio web interface, 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®, or Blackberry® to send email that appears as being internal to your organization, create a corresponding System *Accept* contact (*Pre-User*). Common System *Accepts* for Blackberry, for example, are **@*.blackberry.net* and **@srs.bis.na.blackberry.com*. 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 interface > System > Contacts > Actions > Import Contacts**. After creating the CSV of existing email contacts, import the CSV into System Contacts.

New System Contact

Anti-Spoofing Contact

STEP 11: ROUTE EMAIL TRAFFIC THROUGH SENDIO

1. For Inbound traffic routing log into the control panel of your authoritative DNS server and change your MX record to the host name that was provided to you by Sendio (for example, *hostname.sendio.com*).
2. Confirm that your MX record has been changed and is visible in public DNS by using www.mxtoolbox.com. Enter your domain name and click the **MX Lookup** icon.
3. Use the Global Views/Inbound Messages of the Sendio web interface to verify that traffic is flowing. It may take 1 hour or more until you see email flowing.
4. Send a final test email from an external account. When you receive a sender address verification (SAV) email, reply to it, and then verify the test message is released from Sendio to your inbox.

5. Configure your internal email server to route outbound email through Sendio. You will tell your mail server to relay email to your Sendio host name (for example: `hostname.sendio.com`).

NOTE: If desired, you can route outbound email through Sendio several days prior to routing inbound email. Outbound email sent by any user results in the email recipient becoming a Contact for that user automatically, without requiring the Contact to be pre-imported.

NOTE: If your email domain currently has an SPF record in public DNS, we highly recommend explicitly adding your Sendio IP address to the SPF record at least 24 hours prior to routing outbound email through Sendio. For example, if your current SPF record is “v=spf1 mx -all” and your Sendio IP address is hypothetically 216.23.184.4, change it to “v=spf1 mx ip4:216.23.184.4 -all”. www.mxtoolbox.com is a helpful resource for checking your current SPF record in public DNS, and www.openspf.org a resource for helping define or edit an SPF record. Contact Sendio Tech Support with questions.

*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* on the Sendio web site (<http://www.sendio.com/support/documentation>).*

STEP 12: ENABLE THE DAILY OR TWICE-PER-DAY QUEUE SUMMARY EMAIL (OPTIONAL)

If desired, you can enable the Sendio Queue Summary email for all users or individual users. This email is sent directly to a user’s Inbox and summarizes the held email messages for the past 28 hours. Users can easily Accept and Drop messages via https links within the email. See the “Administration Manual” (Section 5) in the Documentation section of our web site (<http://www.sendio.com/support/documentation>) for details.

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

APPENDIX A: SENDIO AND MICROSOFT OFFICE 365™

If you moved your Microsoft Exchange environment to the Microsoft Office 365 cloud solution, refer to this Appendix for additional guidance on the required setup steps for Sendio.

User Import and Single Sign-On

Hybrid Office 365

If you use a hybrid (or “Federated”) setup with Office 365, have Sendio synchronize to the public IP address of your onsite Active Directory Server over TCP port 3268. See step 4 of this guide for information about setting up the directory sync and see step 7 for information about automating the directory sync (i.e., to run automatically once per day or more frequently).

The directory sync allows for easy and automated import of new users into Sendio. It also allows for single sign-on to Sendio, which allows any user to log in to Sendio using the same credentials that user uses to log in to his computer and email account (e.g., email address and network password).

Non-Hybrid Office 365

If you do not use a hybrid setup with Office 365, manually import users to Sendio by setting up an onboard LDAP directory within your Sendio hosted instance, with users added via a free LDAP software client that you download to your PC or Mac from the following Sendio web site (see the section “Open Source LDAP Downloads”):

<http://www.sendio.com/support/documentation-and-support-tools/>

To save time, Sendio can also import your users for you. Send an email to support@sendio.com with an attachment containing a list of users in a comma-separated value (*.csv) file that has two columns:

- One column for the person’s first name and last name.
- One column for the email address.

Example:

```
Joe Smith, jsmith@domain.com
```

Be sure the *.csv file includes all distribution groups that receive email from the Internet.

Example:

```
Sales, sales@domain.com
```

If a person has multiple email addresses, add extra columns to the *.csv file as needed.

Example:

```
Joe Smith, jsmith@domain.com, joesmith@domain.com
```

For non-hybrid setups, create user passwords manually as needed:

1. Import your users, and then click **Accounts**.
2. Find the Account and go to its **Details** tab. You will see a **Create** button for a local password. Provide this password to the user, so the user can log in and change the password if desired.



Details		Addresses	SilverList
Directory:	Sendio Directory		
Directory DN:	cn=John.Randall,ou=operations,ou=public,dc=ad01,dc=hq,dc=sendio,dc=com		
Directory GUID:	11242b71-3f42-4cb7-be1f-499e6df97190		
Account Type:	User		
First Name:	John	Local Password	
Last Name:	Randal	<input type="button" value="Create"/>	
Created:	5/20/08 10:36 AM		
Created By:	sysadmin		
Last Mod:	5/20/08 10:36 AM		
Last Mod By:	sysadmin		
		Directory Password	
		<input type="button" value="Verify"/>	

Details Tab

Routing Outbound Email from Office 365 to Sendio

When routing outbound email from Office 365 through Sendio, all Microsoft IP addresses (based on their SPF record) must be entered into the **Sender Host Addresses** field of the Sendio Putty (SSH) interface.

See Step # 6 of this guide for information about "Sender Host Addresses." Based on the SPF record for "spf.protection.outlook.com," you need to enter all of the Microsoft IP address ranges into **Sender Host Addresses**.

23.103.128.0/19,23.103.191.0/24,23.103.198.0/23,23.103.200.0/21,23.103.208.0/21,40.92.0.0/14,40.107.0.0/17,40.107.128.0/17,64.4.22.64/26,65.55.88.0/24,65.55.169.0/24,94.245.120.64/26,104.47.0.0/17,134.170.140.0/24,157.55.158.0/23,157.55.234.0/24,157.56.110.0/23,157.56.112.0/24,207.46.51.64/26,207.46.100.0/24,207.46.101.128/26,207.46.163.0/24,213.199.154.0/24,213.199.180.0/24,216.32.180.0/23

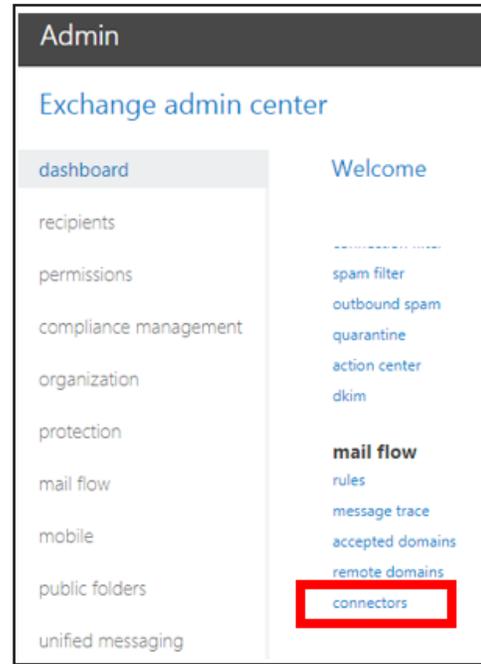
The following additional step must be performed in the Sendio web interface to ensure that other domains using Microsoft Office 365 can get email through Sendio to your domain without issues.

1. Navigate to System/Outbound Control.
2. Change the **Unknown Sender Address** setting to **Allow Message**.

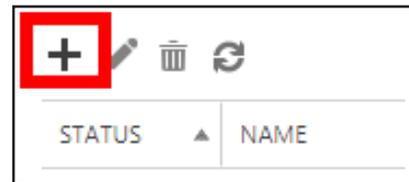
Routing Outbound Email from Office 365 to Sendio from the Microsoft Office 365 Portal

To get the Smarthost to Sendio enabled, follow this path of mouse clicks in the Office365 Portal:

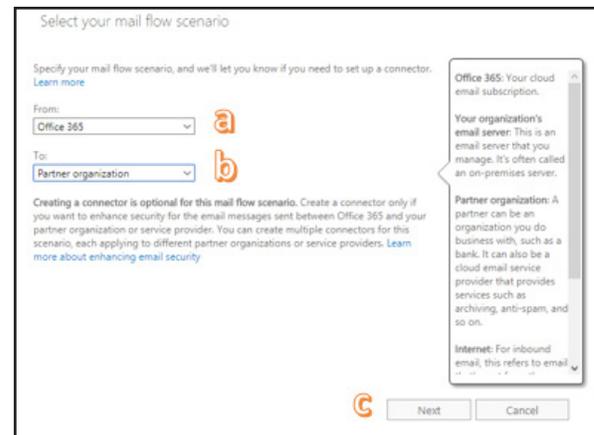
1. Open the Exchange Online Admin Portal (typically the following URL: <https://outlook.office365.com/ecp/>).
2. Under “Mail Flow, click on **Connectors**.
3. Click the New connector button.
4. Select the From server and the To server:
 - a. Select **Office 365** as the “From:” server.
 - b. Select **Partner organization** as the “To:” server.
 - c. Click the **Next** button.



Connectors Link



New Connector Button



Selecting From and To Servers

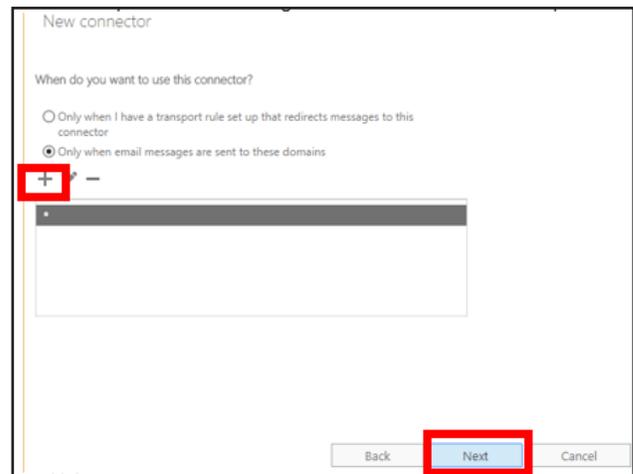
5. Provide a name and description for the connector.
6. Turn on the connector by checking **Turn it on**, and then click the **Next** button.
7. Select the **Only when email messages are sent to these domains** option.
8. Click the **Add** button, enter * as the value of the domain, click **OK**, and click **Next**.



Providing a Connector Name and Description



Turning on the Connector

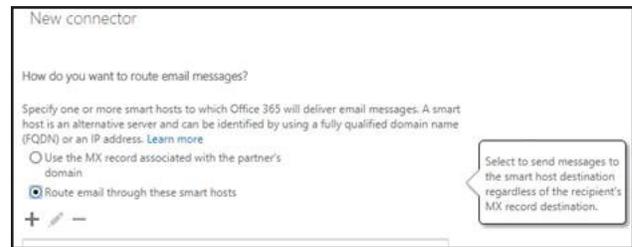


Selecting New Connector Options (1 of 2)



Selecting New Connector Options (2 of 2)

9. Select the **Route email through these smart hosts** option, and then click the **Add** button.
10. Enter your company's Sendio Host name (*xxxx.sendio.com*), and then click **Save**.
11. Click **Next**.



New connector

How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

Use the MX record associated with the partner's domain

Route email through these smart hosts

+ -

Select to send messages to the smart host destination regardless of the recipient's MX record destination.

Selecting Route email through these smart hosts



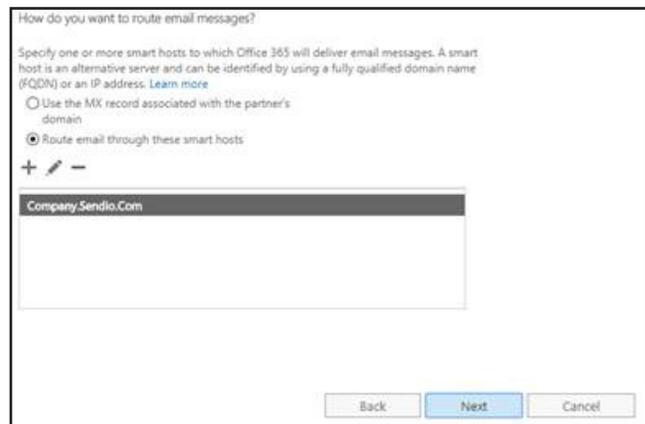
add smart host

Specify the smart host's fully qualified domain name (FQDN) or IPv4 address.
or 192.168.3.2

Company.Sendio.Com

Save Cancel

Entering Your Company's Sendio Host Name



How do you want to route email messages?

Specify one or more smart hosts to which Office 365 will deliver email messages. A smart host is an alternative server and can be identified by using a fully qualified domain name (FQDN) or an IP address. [Learn more](#)

Use the MX record associated with the partner's domain

Route email through these smart hosts

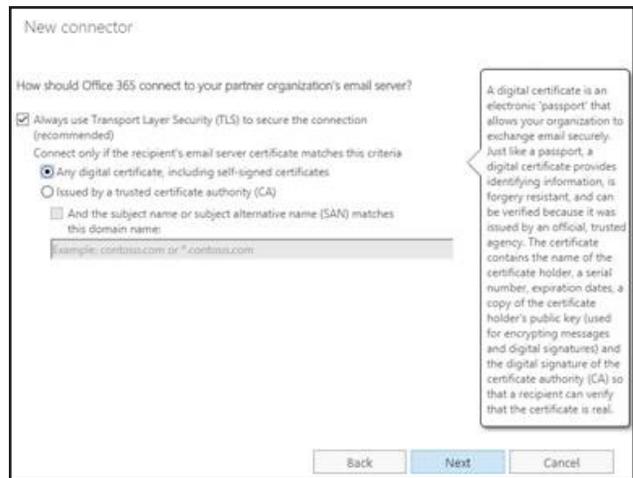
+ -

Company.Sendio.Com

Back Next Cancel

Clicking Next

12. Select **Always use Transport Layer Security (TLS)** and **Any Digital Certificate**, and then click **Next**.
13. Confirm the connection settings, and then click **Next**.

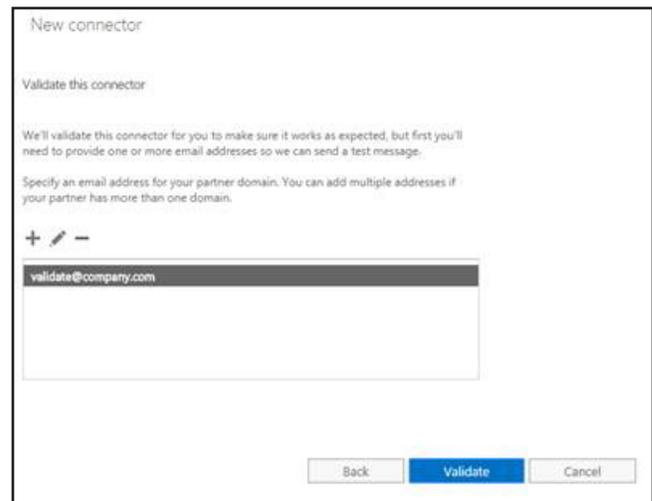


Selecting Always use Transport Layer Security (TLS) and Any Digital Certificate



Confirming Connection Settings

14. Enter an external validation email address (such as **@gmail.com** or **@yahoo.com**), and then click **Validate**.
15. Confirm that you received the test email from the previous step.
16. Send a standard test message from one of your Office365 email accounts to the same external email address (**@gmail.com** or **@yahoo.com**). Confirm that the email is received and that it was routed through Sendio. To check the latter information, go to **Global Views/Outbound Messages** in the Sendio Admin UI.



The screenshot shows a web interface titled "New connector". Below the title is a section "Validate this connector" with the following text: "We'll validate this connector for you to make sure it works as expected, but first you'll need to provide one or more email addresses so we can send a test message." Below this is a sub-section: "Specify an email address for your partner domain. You can add multiple addresses if your partner has more than one domain." There is a list of email addresses with a "+" icon to add, a pencil icon to edit, and a "-" icon to remove. One address, "validate@company.com", is visible in a dark grey bar. At the bottom right, there are three buttons: "Back", "Validate" (highlighted in blue), and "Cancel".

Entering an External Validation Email Address

