INTEGRATION GUIDE

FOR

sendio® & Office 365 Exchange

Safeguarding your Data

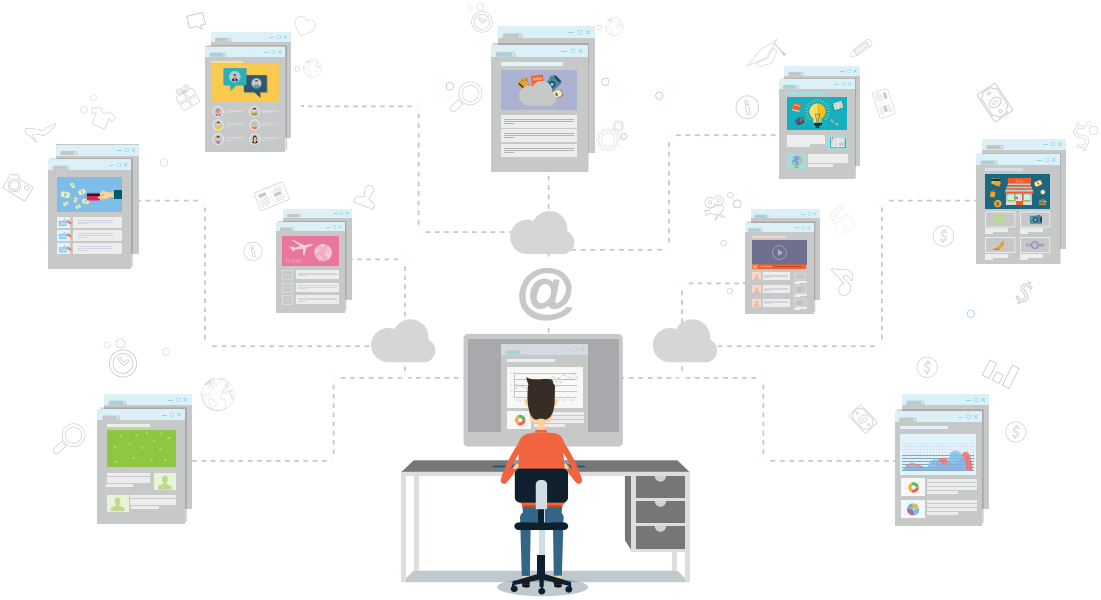
Considering you've made it to this point, you likely understand the importance of safeguarding your company's data and network with another line of defense outside of the built-in Office 365 Exchange spam and security methods. Whether it was an undesirable amount of spam leaking into an employee's inbox or a serious compromise that motivated a plan of action for your company, you've already taken the first steps to a better email management and security system. Before diving deeper into the integration process, we'll review some reasons why Sendio is a good choice for added protection to Exchange.

Why Sendio?

There are email security functions that Office 365 handles well, but others that Sendio handles more efficiently. In short, Office 365 offers extensive filtering features to prevent traditional spam and malware in the email traffic from reaching the user. Sendio stops traditional spam and malware with the same effectiveness as Office 365 but with less reliance on content filtering and therefore much fewer false positives. In addition, Sendio stops all forms of unwanted email (newsletters, marketing offers, etc.) from reaching a user's inbox, which maximizes day-to-day productivity. Sendio also combats one of the most common flaws of most email spam and security systems: social engineering. Because many threats and spam emails are introduced through the vulnerability of the recipient, Sendio works by ensuring the sender is legitimate by requiring the sender to take an action that only real, human senders can take. This method, in addition to other modern detection methods, allows Sendio to be a trusted security and spam solution add-on for any business utilizing Office 365 Exchange.

"Sendio stops both traditional spam and malware with the same effectiveness as Office 365 but with less reliance on content filtering and therefore much fewer false positives."

The Integration Process



Both Office 365 and Sendio are hosted services, operating from the cloud. Consequently, combining them does not involve any hardware modifications, merely some reconfiguring for both services. An experienced administrator can expect to complete the task in two hours, although the administrator will need to plan time to gather requirements prior to integration.

Integration of

sendio® & Office 365 Exchange

can be completed in the following

12 STEPS

STEP 1

Gather Information

The administrator will need to gather the IP address, log-in information, and other account information about the systems involved in the integration.

This includes:

- The IP address of any internal email server.
- The public IP address of any directory server. It will have to be made accessible through a public IP address if it is not already.
- The user name and password for accessing any directory server, with read-only access to all users and groups. The password must not expire.
- The log-in URL, administrator log-in ID, and password for the Sendio-hosted instance.
- The public IP address for the Sendio-hosted instance.
- Host name for the Sendio-hosted instance.

STEP 2

Modify the Firewall Settings

Three ports in the firewall must be open in the inbound direction for successful integration:

- TCP 3268, from the public IP of the Sendio-hosted instance to the public IP of the directory server, for importing user data to Sendio and for single-sign-on support.
- TCP 389, same as TCP 3268
- TCP 636, from the public IP of the Sendio-hosted instance destination to the public UP of the directory server, for LDAP over SSL, to automatically import user data to Sendio, and for user single-sign-on support

Only one of the above TCP ports is required for access to a directory server. If there is no on-site directory server (i.e. a non-hybrid setup on Office 365), Sendio tech support will supply manual user import steps, and no customer firewall changes are required.

STEP 3

Verify SMTP Communications

The Simple Mail Transfer Protocol (SMTP) is typically used for outbound mail, so its functioning must be verified in the course of integration. This is done through the Sendio cloud interface, using the following steps:

1. Launch the Sendio SSH (PuTTY) interface and log in to the hosted instance.
2. Navigate to "Network Diagnostics."
3. Scroll down to the "Email Test" section.
4. In "SMTP Server," enter your mail server public IP address.
5. In "To," enter a valid email address for your domain.
6. Click "Run Diagnostic Test" and confirm that the test email was received by the email address entered in the preceding step.

STEP 4

Sync the Office 365 and Sendio Directory Services

After the directory is synched, user single-sign-on to Sendio will be functional, and any user can log into Sendio using the same credentials as for that user's computer and email account. How it is done depends on whether Office 365 is purely hosted or a hybrid hosted/local server setup.

Hosted Setup:

With a purely hosted implementation of Office 365, manually import users to Sendio by setting up an onboard LDAP directory within the Sendio-hosted instance, with users added via a free LDAP software client. This client can be downloaded to a desktop from the Open Source LDAP Downloads in Sendio's support and documentation. They can also be found below:

- Open LDAP Browser Software
- Open LDAP Tutorial

Sendio can also complete the implementation of importing. A request for assistance in the importing can be sent to support@sendio.com with an attachment containing a list of users in a comma-separated value (CSV) file with two columns:

- One for the person's first name and last name
- One for the email address

Example: Joe Smith, jsmith@domain.com

Be sure that 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 file as needed.

Example: Joe Smith, jsmith@domain.com, joesmith@domain.com

Hybrid Setup:

For a hybrid setup, Sendio can synchronize to the public IP address of your on-site Active Directory Server over TCP port 3268, or 389, or 636. To do that, open a Web browser and navigate to the Sendio Web interface (e.g. http://hostname.sendio.com). ***Then do the following:***

1 When the dialog box opens, type sysconfig@esp and the password provided by Sendio.

2 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.

3 Repeat for multiple domains.

4 Create a Synchronization User on your directory server.

5 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.

6 Enter the IP address of the directory server.

7 Select the Directory Type.

8 Verify the port number. Microsoft Active Directory defaults to port 3268, while other LDAP servers default to port 389.

9 Click the "Fetch DNs" button and select the appropriate Base DN. (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.)

10 Enter the Synchronization User Login and Password that you gathered in Step 1. This may require a domain prefix such as mydomain\username.

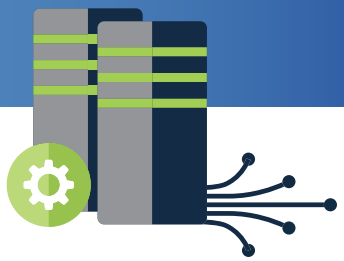
11 Save your changes.

12 Click the "Actions" button and select the "Synchronize Selected Directories" option.

13 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 log-in syntax or password is incorrect.

14 If synchronization succeeds, click "Accounts." This section should display all your users and distribution groups.

STEP 5



Set Mail Server Options

1. Remaining in the Sendio Web interface, click the **"System > Options"** tab.
2. Input the Office 365 primary host name into the Sendio "Internal Mail Host" field. The format of the host name will be domain-com.mail.protection.outlook.com. For example, if your domain was foo.com, then the host name will be foo-com.mail.protection.outlook.com.
3. Input the company name that will be used in the sender address verification (SAV) messages in the "Organization Name" field.
4. Adjust the "Preferred Time Zone" setting.
5. Save your settings.

STEP 6

Outbound Email Settings

To set the outbound email address, log into the Sendio SSH (PuTTY) interface of your hosted instance using sysconfig as the log-in ID and the same password as the Web interface. Then navigate to "Network Configuration." In the "Sender Host Addresses" field, enter the outbound public IP address for your organization's outbound emails.

You must also enter all Microsoft IP addresses into the "Sender Host Addresses" field:

65.55.113.64/26, 65.55.126.0/25, 65.55.169.0/24, 65.55.174.0/25,65.55.78.128/25, 65.55.83.128/27,65.55.88.0/24, 65.55.94.0/25,70.37.151.128/25, 111.221.23.128/25, 111.221.66.0/25, 111.221.69.128/25,111.221.112.0/21, 131.107.0.0/16,132.245.0.0/16, 134.170.132.0/24,134.170.140.0/24, 157.55.9.128/25,157.55.11.0/25, 157.55.40.32/27, 157.55.47.0/24, 157.55.49.0/25,157.55.61.0/24, 157.55.116.128/26,157.55.133.0/24, 157.55.157.128/25,157.55.206.0/23, 157.55.224.128/25, 157.55.225.0/25, 157.55.234.0/24, 157.56.24.0/25, 157.56.73.0/24,157.56.91.0/27, 157.56.96.0/19,157.56.192.0/19, 157.56.232.0/21, 157.56.240.0/20, 207.46.4.128/25,207.46.51.64/26, 207.46.58.128/25, 207.46.100.0/24, 207.46.108.0/25, 207.46.163.0/24, 207.46.198.0/25, 213.199.154.0/24, 213.199.177.0/26, 213.199.180.128/26, 216.32.180.0/23

To ensure that other domains using Office 365 can get email through Sendio to your domain without issues, navigate to ***"System < Outbound Control"*** and change the "Unknown Sender Address" setting to "Allow Message."

STEP 7

Set Automatic Directory Synchronization

Log in to the Sendio SSH (PuTTY) interface of your hosted instance and do the following:

1. Navigate to “Directory Management.”
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 the time for synchronization in military time format (e.g. 2200).
4. Arrow over the + sign and press “Enter” to add the new synchronization schedule.
5. Save your settings.

STEP 8

Grant Administrator Access to One or More Users

Using the Sendio SSH (PuTTY) interface, navigate to the “Directory Management” section and then do the following:

1) Arrow over to “Press Eenter or Type Entry.” Enter the user’s last name and press “Enter.”
2) Select the appropriate user with the space bar. Tab to highlight “Select” and then press “Enter.”
3) Move to “Grant Full Admin Access” and then press “Enter.”
4) Save your settings.
5) Repeat to designate additional administrators.

STEP 9

Change the Sysconfig Password

If changing the Sysconfig password is desired, navigate to the Systems Configuration of the Sendio SSH (PuTTY) interface. There, enter the new password. It should be at least eight characters long and should contain both letters and numbers.

STEP 10

Set Contacts

In the Sendio Web interface, click ***"System > Contacts > New"*** to create a contact entry to accept all email from Sendio Support, at support@sendio.com.

Then, in the Sendio Web interface, review the ***"System > Contacts"*** page to confirm that there is a System drop contact to counter spoofing (i.e. incoming email with sender addresses belonging to your own domain).

When using a cloud-based service to send email that appears as though it is internal to your organization, create a corresponding "System Accept" contact. Select "Pre-User" for the "Phase" entry. In some cases, you may choose to remove the anti-spoofing contact.

STEP 11

Route Outbound Email Traffic through Sendio

To route outbound email from the Office 365–hosted service to Sendio, do the following in the Office 365 Portal:

1. Navigate to "Service Settings/Mail Flow/Outbound Connector."
2. Create or edit outbound connector to "route through SmartHosts" (instead of "use MX") and enter your Sendio host name (e.g. hostname.sendio.com).
3. For connector type, select "Partner Connector."
4. For the "Scope/Sender Domains" field in the "Outbound Connector," type an asterisk (*) only.

STEP 12

Route Inbound 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 (e.g. 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 one 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.

You're Done!

At this point, you have integrated Office 365 with Sendio email security services and can enjoy the best of both worlds—a hosted office environment with centralized software management, with email security that turns the trouble posed by spam, phishing, and malware into fading memories.

If you're ready to enhance Office 365 with the latest in email security, in a way that requires no hardware investment, and can be accomplished during a long lunch break, request a demo to see Sendio in action today if you haven't already.

REQUEST A DEMO

Connect and share!

Resources

- Sendio FAQ
- Quick Start Guide–Sendio hosted

sendio®

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