Welcome to Cisco ScanSafe Email Control

Thank you for choosing the Cisco ScanSafe Email Control service. This guide focuses on how to configure your Email Control service and the best practices that should be followed.

When your ISP has updated your MX records and you have notified customer support that the changes have been made, you will receive a final provisioning emai.

This provisioning mail indicates that your service is ready to be tailored to your chosen security policies, to protect your users and infrastructure from malware and unwanted or inappropriate content.

All system configurations are administered using the ScanCenter Web interface as explained in the provisioning email. The provisioning email includes the login credentials for ScanCenter. If for any reason this email has not been received, contact customer support.

To successfully use the service, the following tasks need to be completed:

Step 1 Change DNS MX records to point to Cisco ScanSafe’s servers.

Step 2 Test mail flow from Cisco ScanSafe’s serversto your servers

Step 3 Configure your inbound email servers

Step 4 Configure global inbound account settings

Step 5 Configure global inbound user account settings

Step 6 Finally, add your users to the system to enable the Email Control service.

MX Record Changes

To begin filtering email for users in your domain, you must first change the domain's DNS MX RECORDS to point to Cisco ScanSafe's servers.

Caution Change DNS records only AFTER you have confirmed that the data

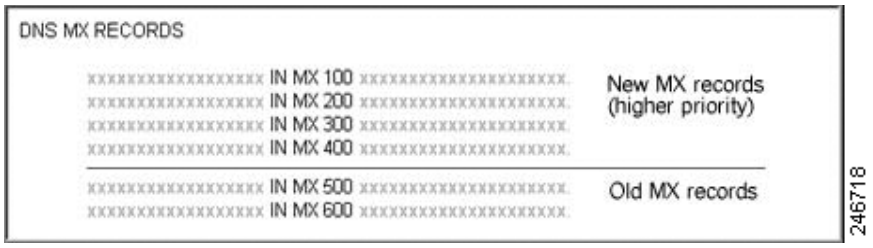
Step 1 Verify the domain listed in your provisioning email, and locate the DNS MX records in this email. If you canot find this email, contact customer support. These are the DNS records that must be inserted for the domain.

Step 2 Go to your DNS service to access the DNS records for the domain listed in the email.

Caution Do not change MX records for any domain other than the one listed in your email. You can add other domains to the service and change their records, later.

Step 3 At your DNS service, change the TTL (Time to Live) setting for your DNS records to 600 seconds (10 minutes), or as close to that as possible. The TTL setting (typically measured in seconds) determines how long it can take for the DNS change to go into effect. The TTL is often set by default to a high number, so lowering it ensures that your change takes effect promptly.

Step 4 Insert the new DNS MX records listed in your email, at a *higher than* your domain's existing records. In the example below, priority is shown using the numbers 100-600, where 100 has a highest priority.



For example, an original MX record might look like this:

- example.com. IN MX 100 mailhost1.example.com
- example.com. IN MX 200 mailhost2.example.com

The activation email lists the new MX records:

The DNS MX RECORDS you will need to set for your company:

- example.com. IN MX 100 example.com.s81a.psmtp.com
- example.com. IN MX 200 example.com.s82a.psmtp.com
- example.com. IN MX 300 example.com.s81b.psmtp.com
- example.com. IN MX 400 example.com.s82b.psmtp.com

The company inserts the new records above their old MX records, and change their priority to be lower than the new records.

- example.com. IN MX 100 example.com.s81a.psmtp.com
- example.com. IN MX 200 example.com.s82a.psmtp.com
- example.com. IN MX 300 example.com.s81b.psmtp.com
- example.com. IN MX 400 example.com.s82b.psmtp.com
- example.com. IN MX 500 mailhost1.example.com
- example.com. IN MX 600 mailhost2.example.com

Caution Be careful not to insert the word "domain" instead of your actual domain name. An example of incorrect records:

- example.com. IN MX 100 domain.com.s81a.psmtp.com
- example.com. IN MX 200 domain.com.s82a.psmtp.com
- example.com. IN MX 300 DOMAIN.COM.s81b.psmtp.com

Frequently Asked Questions

What are DNS MX records?

When your domain is registered, it is assigned several DNS records, which enable it to be located on the Internet. These include MX records, which direct the domain's mailflow. Each MX record points to an email server that's configured to process mail for that domain. There is typically one record that points to a primary server, then additional records that point to one or more backup servers. For users to send and receive email, their domain's MX records must point to a server that can process their mail.

Currently, your domain's records are probably pointing to servers at your company, or to an ISP's servers if your domain is hosted by an ISP. To filter email through the Email Control service, you must insert new records that instead point to ScanSafe's data center's servers.

I'm not sure how to change my domain's MX Records

If your company manages its own email servers (that is, if you don't have an ISP), then your network administrator should be able to insert the new records for you. Contact this person, refer them to the instructions above, and provide the provisioning email you received, which lists the exact records that need to be inserted.

If your domain is hosted by an external ISP, contact your ISP, request that they change your domain's MX records, and provide them with this same information.

My domain is hosted by an ISP. Is that OK?

In most cases, yes. However, before having your ISP change the DNS records for your domain, make sure that they will allow your domain to route email traffic to an external server, such as the ScanSafe data center server. Some ISPs and some hosting companies might not allow this. If this is the case, talk with them about a workaround before making any DNS changes, or mail flow to users in your domain might fail. You can also contact your ISP's technical support for more information.

What if my domain's MX records aren't prioritized using a 100-600 numbering scheme?

Priority is usually indicated using the numbers 100-600, where 100 has the highest priority. But if your DNS service prioritizes them differently, for example, using a 1-6 numbering scheme, that's OK, too. You can use any scheme, as long as the new entries are inserted at a higher priority than any existing entries.

Why is the priority of MX records important?

Inserting the new MX records at a higher priority than your existing records directs mail flow to ScanSafe data center servers where it can get filtered, instead of sending it directly to your server where no filtering occurs.

An MX record consists of three parts: the domain name, a priority, and an email host. The priority indicates which record gets looked at first when determining where to route a message sent to the domain. Normally, the primary server named in the record with the highest priority is used. But if that server isn't available, the next highest priority's record is evaluated, which is typically a backup server.

What is a TTL setting?

When you change a domain's MX records to point at a different server, the change doesn't take effect immediately. Instead, it has to propagate throughout the Internet. How long this takes can depend on the current TTL, or Time to Live setting. This is typically measured in seconds, so a TTL of 3,600, for example, means it might take up to an hour for the changed to propagate. Shortening the TTL can make the change propagate more quickly.

While you're waiting for this to happen, the domain continues to point to its current server, and users' mail flow continues as usual.

What if my domain has IP blocking enabled?

If your domain is set up to block mail from specific IP addresses, you'll have to reestablish this blocking after changing the domain's MX records. After the new DNS records propagate, go to Connection Manager in the Administration Console. Click the Help link at the top of any screen, and navigate to the Connection Manager topic for instructions.

When should I delete my old MX records?

When you have completed the activation process, and users in your domain are successfully sending and receiving filtered email, you can delete your old MX records. Until then, however, it's a good idea to retain these records.

For example, if you accidentally enter the new records incorrectly, the DNS service won't be able to find a data center server to direct mail to. If your old records are still available, it will use them to deliver mail directly to your server, just as before. If instead you have deleted your old records, the DNS service would not have anywhere to direct traffic, so all mail to your domain would bounce, never reaching users.

Test Mail Flow

The first step is to confirm mail flow through the ScanSafe infrastructure. The Web interface can be seen below where the mail flow tests are highlighted.

MX Records Tests

Step 1 In ScanCenter, click the **Email** tab to display the **Email** menus.

Step 2 Click **MX Record Test**.

Step 3 Click the required **Domain** in the list.

Step 4 Click **Test**.

If the test was unsuccessful this means that the MX record changes have not yet been completed by your ISP. You should arrange for the MX records to be changed as soon as possible. Contact customer support if you require assistance.

Frequently Asked Questions

Why did this test fail?

If this test fails, the most likely reason is that your new MX records have not yet propagated. If you have not waited the duration of the TTL, do so, and then try the test again.

If you have waited the full duration of the TTL and the test fails, troubleshoot as follows:

- Verify that all records were entered correctly. For example, if the error message reports that a particular record couldn't be found, that record might have been mistyped. If so, enter it again, wait for the TTL to expire, and try the test again.
- Verify that your primary and secondary name servers are properly synchronized with the new DNS records. Typically, entering records for the primary name server updates the secondary name server, as well, but with some DNS services, you may have to update the secondary nameserver manually.
- Verify that your ISP is compatible with the email protection service, in particular, that it will allow your domain to route email traffic to an external server. Some ISPs and hosting companies may not allow this. If this is the case, talk with them about a workaround. You can also contact your ISP's technical support for more information.

Caution Do not delay in fixing this problem, as email to your domain might be bouncing back to senders, without reaching users.

SMTP Message Test

The next step after you have checked that the MX records have been updated successfully is to test email flow to your email users.

Step 1 In ScanCenter, click the **Email** tab to display the **Email** menus.

Step 2 Click **SMTP Message Test**.

Step 3 Enter a valid email address within the domain that has been configured and tested in the previous test.

Step 4 Click **Test Mail Flow to your Server**.

Step 5 Click **Test**.

The Output if successful is shown below:

```
Establish connection...
Sending HELO
Sending MAIL FROM
Sending RCPT TO
Sending data
End of data dot
Success
The email data center can deliver email to this email server from an external email
server.
```

The output if unsuccessful is shown below:

```
The email server is not available. Check your filrewall or email server for settings
that might prevent delivery.
```

Repeat the same steps for the remaining radio buttons. The test descriptions are self explanatory.

Frequently Asked Questions

What if the SMTP test fails?

This test fails if for some reason your server cannot be reached at the test address you entered. To troubleshoot the problem:

- Check your provisioning email and verify that you entered the correct email server host name and domain name when you signed up for service. If you did not, see below.
- Verify that the test email address you entered has a working email account on the server. The address must exist on your server for this test to succeed.
- Verify that your server is indeed available, for example, that it can send and
- receive email properly for other users.

Before continuing with activation, you need to determine the cause of the failure and fix it. Look at the message itself for an indication of what failed, and look in your mail server logs for the exact SMTP error returned. Both of these pieces of information can help you resolve the issue.

What if I don't receive the test message?

If your test succeeds but you don't receive the test message, your firewall or mail server might have an anti-spoofing feature turned on. To proceed, turn off any email filtering which prevented spoofing and run the test again. For information on configuring spoofing, consult the product documentation or support resources for your firewall or mail server. The Email Control service will provide comprehensive filtering against spam, so spoofing protection at your mail server is not needed.

What if I signed up with the wrong email server host name?

If the email server host name in your provisioning email isn't correct, do the following:

- On the Delivery Manager page, click the Edit link, and verify that your email server's host name is properly entered under Email Servers. If it isn't, enter it correctly and click Save.

What if I signed up with the wrong domain name?

If the domain name in your "MX Record" email isn't correct, do the following:

- On the Domains page, verify that your domain name is listed correctly. If it isn't, click the Add Domain button at the top right of the page.
- On the Add Domain page, enter the correct domain name and click Save.

Where can I find additional documentation about the service?

Additional information is available here:

http://www.google.com/support/appsecurity/bin/answer.py?hl=en&answer=87514