Deploying Layered Email Security

This paper is intended for users of Websense Email Security who want to add Websense Hosted Email Security to deploy a layered email security solution.

In this paper:

- Review the goals of the layered email security solution.
- Become familiar with the recommended layered configuration.
- Follow step-by-step instructions for adding Hosted Email Security.
- Follow step-by-step instructions for adjusting Websense Email Security.
- Access related resources.

What is Layered Email Security?

Websense layered email security combines Hosted Email Security with your on-site Websense Email Security server to deliver comprehensive, high-capacity email security.

Hosted Email Security provides:

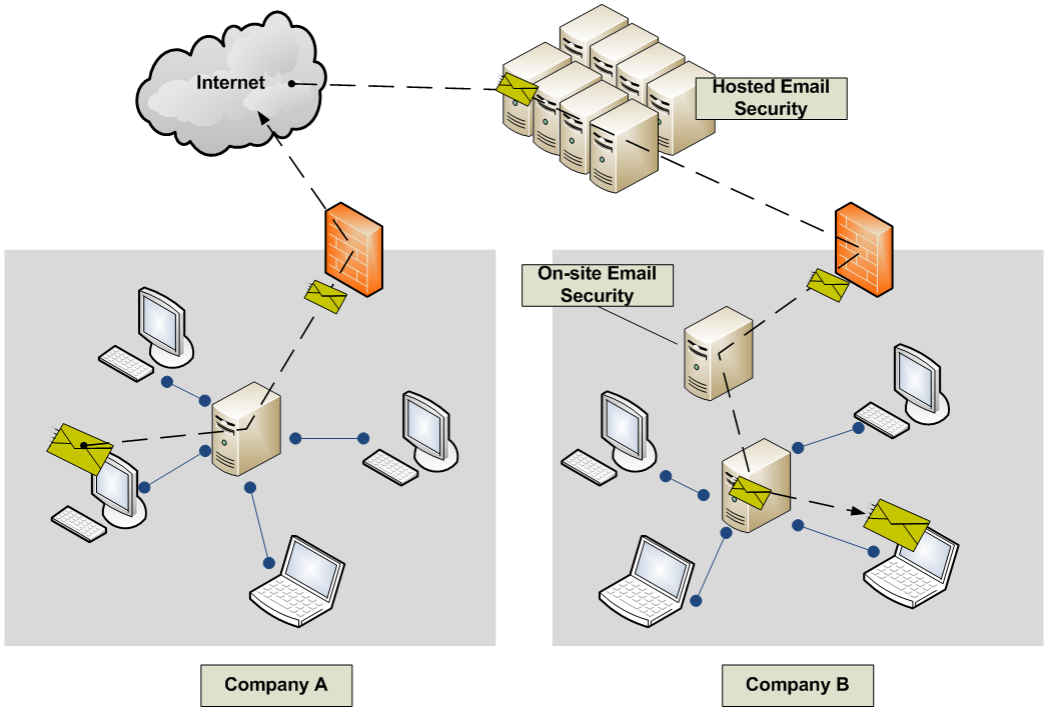
- a layer of Internet-based messaging security that is outside your network and away from your premises
- strong, Internet-based email connectivity protection: senders with bad reputations, including spammers, never connect to your network
- immediate expanded capacity because:
  - hosted filtering instantly adjusts to meet current demand
  - hosted filtering eliminates most spam, reducing the email stream to Websense Email Security by as much as 90%
- a service-level agreement (SLA) for service uptime

Websense Email Security provides:

- expanded on-site capacity, because most spam is removed by hosted filtering, significantly reducing the volume of your inbound email stream
- multiple antivirus technologies that provide extensive, integrated protection
- a second layer of antispam filtering
- additional, customizable content filtering, including dictionary analysis and URL categorization
- configurable, granular outbound email filtering

In the following diagram, Company A is sending a message to Company B. Company B has deployed a layered solution

- Hosted Email Security performs connection management and filters out spam before it reaches the gateway.
- Websense Email Security performs antivirus filtering, a second layer of spam filtering and content filtering. It also checks outbound email for sensitive content.



Recommended Configuration for Layered Email Security

Websense recommends the following configuration to achieve an efficient, high-value, layered email security solution:

Hosted Email Security:

- Receives all inbound messages for your domains
- Is the sole sender of email to on-site Websense Email Security
- Filters for spam only; spam filtering settings minimize false-positives (on-site filtering performs a second screening)
- Receives outbound email from Websense Email Security
- Does *not* use the end-user quarantined message notification facility (End-User Message Report), in favor of the on-site facility: Personal Email Manager

Websense Email Security:

- Receives inbound email from Hosted Email Security *only*
- Optionally uses only secure communication (TLS) with Hosted Email Security
- Performs antivirus filtering
- Performs a second layer of spam filtering
- Performs content filtering, including dictionary analysis and URL categorization, as required
- Filters outbound messages for sensitive and confidential content
- Routes outbound messages to Hosted Email Security
- Optionally uses Personal Email Manager to provide end-user notification and management of messages quarantined by Websense Email Security
- Uses Report Central for Websense Email Security reporting

Although this is the recommended configuration, Hosted Email Security and Websense Email Security are highly configurable and can be tailored to satisfy diverse needs.

Adding Hosted Email Security

This section explains how to set up Hosted Email Security for the first time. See *Reconfiguring Websense Email Security* for instructions on reconfiguring Websense Email Security.

There are 3 steps to setting up Hosted Email Security:

1. Register for the Hosted Email Security Antispam service.
2. Activate the service and set up email routing.
3. Configure email policies for spam detection.

Register for the Hosted Email Security service

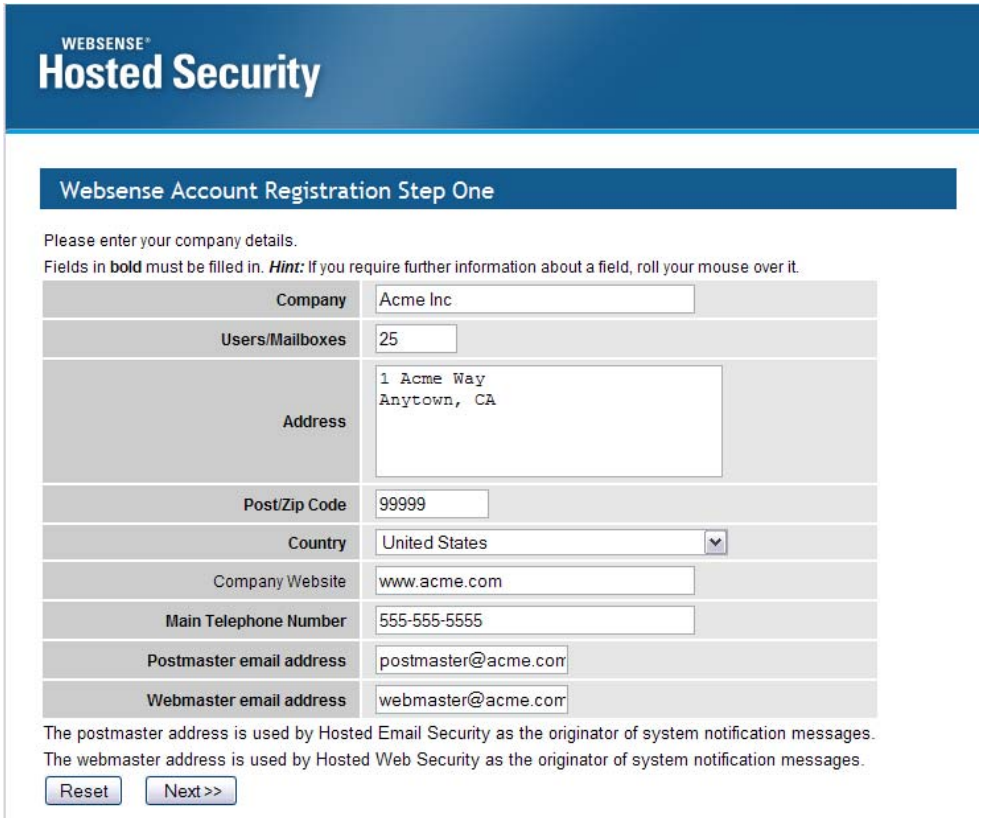
Contact your Websense reseller or your Websense Sales Representative to request access to the following Hosted Email Security service:

- Hosted Antispam

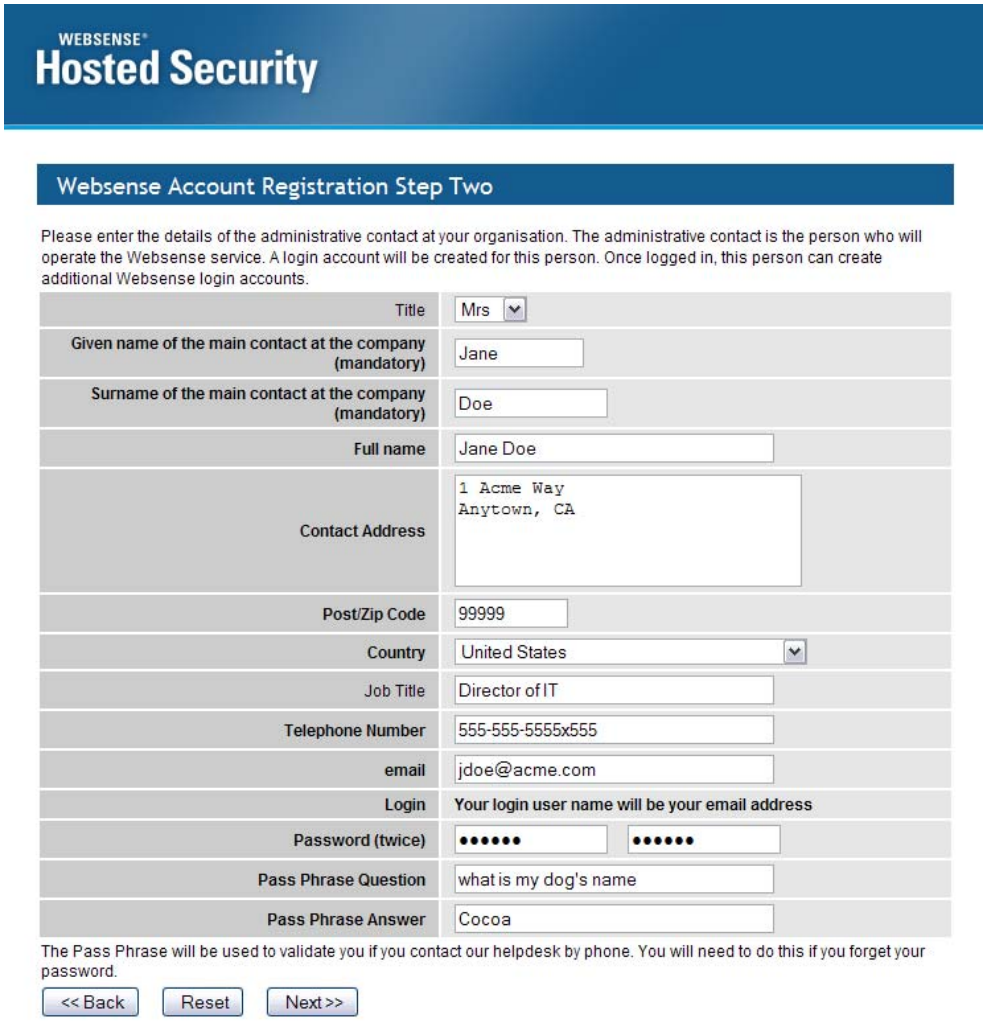
Enterprise customers may be asked to complete a technical environment survey so that we can help you prepare for the service.

A confirmation email is sent to you.

1. Click the link in your email that says “Click here to begin the registration wizard”.
2. Verify or reset your account information as needed. Click **Next**.



3. Verify or reset your email administrator's details as needed (name, address, telephone number, email address, and password for the administrator account). Click **Next**.



4. Enter the domain(s) for which the account is to process email, for example “acme.com”. Enter the primary domain in the field provided. Click **Add Another** to add another domain. Domains that are not listed are denied by the service. Click **Next** when done.

5. Enter the IP address and name of your inbound, receiving mail server (the mail gateway server or servers to which Hosted Email Security will send mail when it is received from the Internet). This should be the server that is running Websense Email Security. If Websense Email Security is running on more than one server, click **Add Another** and choose an order of preference for each from the drop-down list. Click **Next** when done.

Note

If you have an upstream SMTP gateway between the Websense Email Security server and the firewall, enter the IP address and name of this server.

6. Enter the IP address of your outbound, sending mail server (the mail server or servers from which Hosted Email Security will receive mail sent to the Internet). This should be the server that is running Websense Email Security. You must set up at least one outbound route for the hosted service to be active. Click Next when done.

7. A Registration Complete screen is displayed.

   A security check is then carried out by our engineers. Once complete, your account is activated and you receive a confirmation email advising you of the next steps. This normally takes less than 24 hours.

Activate and set up the Hosted service

When you receive login information in your confirmation email, log into the Hosted Security portal by clicking the link that is provided or visiting www.mailcontrol.com/ login/login_form.mhtml. Enter your username and password into the fields provided.

Accept the license terms and conditions

The first screen that appears lists all the licenses that you have pending for your account. To activate a license, you must accept the terms of your license contract. Click the contract name to view the contract and review its terms. If they are acceptable, close the contract, check the **Accept license** box, and click **Accept**. This enables your account.

Set up inbound email routing

When you ran the registration wizard, you entered the IP address and name of your Websense Email Security server (the mail server or servers to which Hosted Email Security will send mail when it is received from the Internet). Before we sent you your login and confirmation, we verified connectivity with your inbound server.

The only thing you need to do for inbound mail is modify the Mail eXchange (MX) records in your organizations' Domain Name System (DNS).

An MX record is an entry in a DNS database that defines the host willing to accept mail for a given machine. Your MX records must route email through Hosted Email Security to your Internet mail gateway.

Contact your DNS manager (usually your Internet service provider (ISP)) and ask them to change the MX record with the smallest preference value to the customer-specific DNS record listed in your confirmation email (the one that ends in **in.mailcontrol.com**). For example, they might change MX Preference 1 from:

```
acme.com. IN MX 50 wes.acme.com.
```

to

```
acme.com. IN MX 5 cust0000-1.in.mailcontrol.com.
```

Make sure they include the trailing period.

Because Hosted Email Security has a guaranteed 99.999 percent uptime with a geographically distributed network and multiple layers of resilience, you do not need any fallback MX records in addition to the customer-specific DNS records we have provided you.

It normally takes about 24 hours to propagate changes to your MX records across the Internet.

To view your MX records, you can use the tool on our Web site:

www.websense.com/SupportPortal/SurfMxRecordChecker.aspx

Enter your domain name, for example acme.com, and click **Check MX record**.

Set up outbound email routing

In order for Hosted Email Security to scan your outbound email, it must be routed through the Hosted Email Security service using the customer-specific DNS records we provided you. The way you configure your email system depends on how the email servers are set up in your organization.

Determine the route that email currently takes when intended for an Internet recipient and identify the last server in your organization. We call this your Internet mail gateway, and in this case it is the server running Websense Email Security. This either routes mail directly to the recipient mail system by looking up the destination mail server address using DNS MX records, or it routes mail to a Simple Mail Transfer Protocol (SMTP) relay at your ISP.

The Hosted Email Security service accepts mail from the IP address you specified as your outbound route when you completed the registration process.

You are required to use the customer-specific DNS records provided to you in your confirmation email to route outbound email to the Hosted Email Security service. Do not use the specific IP addresses to which these records resolve, because these could change. Should this happen and you have not used the customer-specific DNS records, you will be unable to send outbound email to the service until you make configuration changes.

Before you change the configuration of your Internet mail gateway, check that you have connectivity through any intervening firewalls to the Hosted Email Security service.

On your Internet mail gateway, enter the following command, replacing *cust0000-s.out.mailcontrol.com* with the customer-specific DNS records from your confirmation email:

```
telnet cust0000-s.out.mailcontrol.com 25
```

The following message results:

```
220 cluster-[x].mailcontrol.com ESMTP MailControl
```

Enter **quit** and press return to close the connection.

You are now ready to change the configuration of your Internet mail gateway. See *Set up outbound email routing*.

Once you have changed your Internet mail gateway configuration, you can test the delivery of outbound email via Hosted Email Security by sending to an echo address. For example:

```
echo@uk.psi.net
```

If your email does not get through, check its progress using Message Center in the Hosted Email Security customer portal or contact the Websense Hosted Security support helpdesk.

Restrict connections to your mail servers

We strongly recommend that you prevent servers on the Internet from sending email directly to your mail servers, ignoring your MX records. If this is not prevented then email can be maliciously routed directly to your mail servers, bypassing Hosted Email Security. You may be able to do this at your corporate firewall or on your Internet mail gateway by restricting incoming SMTP traffic from any source other than Hosted Email Security. We recommend that you block all SMTP traffic except that from all IP address ranges that Hosted Email Security uses. These can be found in the support section of the Hosted Email Security portal in an FAQ titled “Service IP addresses.”

Configure Hosted Email Security policies for the Layered Solution

To configure a policy in Hosted Email Security, select **Setup > Hosted Email Security Settings**, and then click the name of the policy to configure. If you have not previously configured a policy, click the policy named **DEFAULT**. You can rename the default policy to something more meaningful to your organization, especially if you plan to create multiple policies.

Notice that each policy has multiple tabs to configure. For layered email security, you need only configure the following:

- General tab. For more information, see *Disable annotations and notifications*.
- Antispam tab. For more information, see *Set up antispam options*.

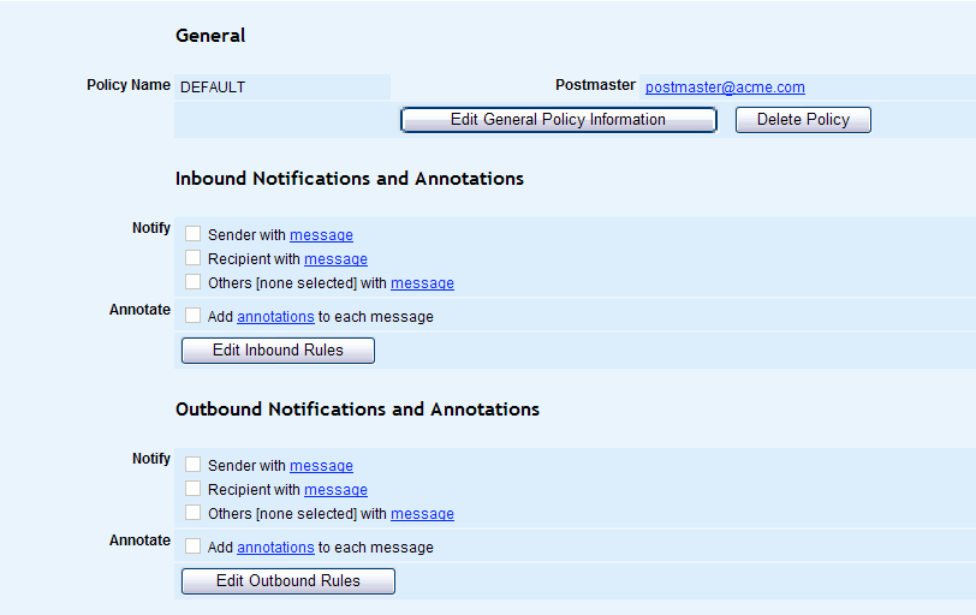
> **NOTE**
> Although the Antivirus, Content Filter and Encryption tabs are visible in the portal, these are not required for layered email security.

Disable annotations and notifications

On the **General** tab, we recommend that you switch off all annotations and notifications in Hosted Email Security, and use Websense Email Security’s Personal Email Manager for all notifications. This prevents multiple notifications from being sent to end users from different products.

1. Click **Edit Inbound Rules**.
2. In the **Notify** area, clear all 3 check boxes.
3. In the **Annotate** area, clear the check box.
4. Click **Submit**.

5. Click **Edit Outbound Rules**, then repeat steps 2-4.



Domains tab

The settings on the **Domains** tab are taken from the information provided in the Registration Wizard. If you want to use additional domains, see Chapter 5 of the *Hosted Security Administrator's Guide* for further instructions.

Connections tab

The inbound and outbound connection settings on the **Connections** tab are taken from the information provided in the Registration Wizard. You do not need to change anything on this tab.

Set up antispam options

Click the **Antispam** tab on the policy to view or modify rules for spam protection.

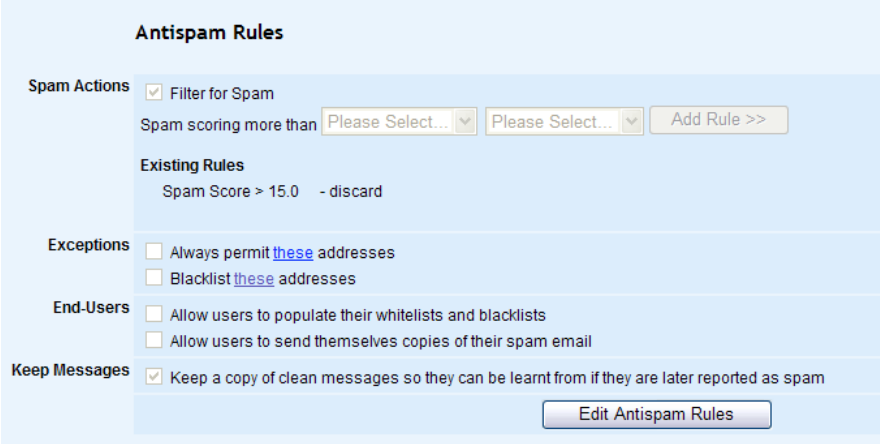
All email is assigned a spam score. The score is visible in the message header and message tracking results. The higher the score, the more likely it is to be spam. Many rules are used to generate the spam score, including analysis of the words within the message, where it came from, its headers, and comparisons with other spam and non-spam email.

The recommended antispam deployment in Hosted Email Security for the layered solution ensures that the bulk of spam is discarded while minimizing the chance of false positives.

To set up the recommended antispam rules:

1. Click **Edit Antispam Rules**.
2. Ensure **Filter for Spam** is selected.
3. Delete all existing rules *except* **Spam Score > 15.0 - discard**. This discards any email with a spam score greater than 15.
4. In the **Exceptions** area, clear all check boxes.

5. In the **End Users** area, clear all check boxes.
6. Ensure **Keep Messages** is selected.
7. Click **Submit**.



Using secure communication

Hosted Email Security always attempts to use secure TLS communication. If you want to use secure communication from Hosted Email Security to Websense Email Security, ensure it is configured in Websense Email Security. For more information, see *Enable secure communication*.

Reconfiguring Websense Email Security

To achieve a layered solution with Hosted Email Security, several adjustments must be made to Websense Email Security. There are 7 primary activities and 3 optional activities:

1. Back up the current configuration.
2. Enable TLS if you want to use secure communication with Hosted Email Security.
3. Adjust the connection settings.
4. Review and adjust the Websense Email Security Anti-spam and Anti-virus rules.
5. If enabled, disable Directory Harvest Detection.
6. Restart and monitor the system.
7. When the email stream is verified to be coming from Hosted Email Security, delete all other relays from the server configuration.

Optionally:

1. Review the content analysis rules.
2. Review the outbound email filtering rules.
3. Review the scheduled tasks.

Back up the configuration

It is prudent to back up the configuration database before making changes.

1. Open Database Tools. Select **Start > All Programs > Websense Email Security > Database Tools**.
2. Select **Configuration Database Management**. The Configuration Database wizard opens.
3. Select **Backup database to a file**. The **SQL/MSDE Server details** screen displays.
4. Specify the location of the server that contains the database to be backed up.
   - To connect to the server through a trusted connection, select the **Use trusted connection** check box.
   - To connect to the server using the username and password you specify, clear the **Use trusted connection** check box and enter the username and password.
5. Click **Next**. The **Configuration Database Backup Details** dialog box displays.
6. Select the database from the drop-down list. The default is “STEMConfig”.
7. Enter or browse to the location where the database is to be saved. The default location and filename is: Program files\Websense Email Security\Database\STEMConfig_<date>.bak
8. Click **Next**. A summary of your options displays.
9. If you need to change any details, click **Back**. If the options are correct, click **Next**.
10. A progress bar displays. A confirmation screen displays when the backup is complete. Click **Finish**.

Enable secure communication

If you intend to use secure communication (TLS) with Hosted Email Security, TLS must be enabled in Websense Email Security. No special configuration is required on Hosted Email Security.

1. Set up a self-signed or CA signed certificate for SSL communication. Open **Server Configuration** > **Administration** > **Certificate Management** and click **Certification Manager**. Follow the instructions in the wizard to create and install a certificate.
2. Enable TLS in the Server Configuration. Open **Server Configuration** > **Receive Service** > **ESMTP Commands**, check **Enable STARTTLS,** and click **OK**.
3. When each Hosted Email Security mail relay is added, enable the option that enforces encryption on that relay. (This is step 8 in the procedure for adding relays. See *Add Hosted Email Security as a mail relay*.)

For more information, see “Certificate Manager” and “ESMTP commands” in Chapter 3 of the Websense Email Security Administrator’s Guide.

Add Hosted Email Security as a mail relay

In the layered solution, all inbound email is received *only* from Hosted Email Security.

In this step, you should document the existing mail relays and add the Hosted Email Security IP addresses. When the cut over is complete, you can delete the non-Hosted Email Security relays.

Because Hosted Email Security is a managed service, the service may occasionally alter the route of email *within the service*. To do this invisibly, without requiring changes, you must specify all the IP ranges listed below as direct mail relays. These addresses are in Classless Inter-Domain Routing (CIDR) format, as required by Websense Email Security.

- 80.69.8.176/28
- 85.115.32.0/19
- 85.119.2.128/26
- 86.111.216.0/21
- 116.50.56.0/21
- 208.87.232.0/21
- 217.68.146.128/26
- 217.69.20.128/26
- 217.79.216.128/26

To set up a direct mail relay:

1. Open the **Monitor** and select **File** > **Server Configuration**.
2. In the **Server Configuration** console, select **Email Connection Management** > **Mail Relays** > **Direct** tab.
3. Click **Add**. The **Connected Mail Relay Properties** dialog box displays.
4. Enter the range of server IP addresses.
5. Enter a description for the mail relay, for example “Hosted Email Security Relay 1”.
6. Check the **Trusted mail relay** box.
7. Select the **Outbound and Inbound** relay type.

8. If you are using secure communication with Hosted Email Security, check the **Email received from this IP address must be via an encrypted connection** box. Be sure to complete the TLS configuration described in *Enable secure communication*.
9. Click **OK**.
10. Repeat steps 3 to 8 for all of the IP ranges listed above.

For more information about mail relays, see Chapter 3 of the Websense Email Security Administrator's Guide.

Set up outbound email routing

It is recommended that you route outbound email through Websense Email Security and then through Hosted Email Security. This improves spoofed NDR filtering and provides visibility of onward delivery of outbound email.

The Hosted Email Security service accepts mail from the IP address you specified as your outbound route when you completed the registration process. You must use the customer-specific DNS records provided in your confirmation email to route outbound email to Hosted Email Security. *Do not use* the specific IP addresses to which these records resolve because they could change.

1. In the **Server Configuration** console, select **Send Service > Routing**.
2. In the **Undefined route** area, select **Use default route**.
3. Click **Configure**. The **Default Routes Configuration** dialog box displays.
4. Click **Add** and enter the DNS records provided by the Hosted Email Security service in the confirmation email you received after you completed the registration process.
5. Click **OK** to accept the new routes, and click **OK** again to accept the changes to the routing configuration.

See also *Set up outbound email routing* in the Hosted Email Security section of this paper.

For more information on configuring the Send Service, see Chapter 3 of the Websense Email Security Administrator's Guide.

Verify and adjust the Anti-virus and Anti-spam rules

If the Anti-spam and Anti-virus rules are enabled, no changes are necessary. However, the recommended settings do not require any subscription services, therefore if you are using subscription services, you may want to discontinue them to save money.

Anti-virus settings:

1. Open the **Rules Administrator** and select **Virus Protection Rules - (Policy Type: Virus)**.
2. If **Anti-Virus Malware Scanning - Isolate message that contain a Virus or Malware** is not enabled, enable it.
3. In the right bottom pane, double click **if Anti-Virus Engines detects a Virus/Malware**. The **Properties for Anti-Virus Malware Scanning** dialog displays.
4. Uncheck **Anti-Virus Agent (McAfee)**.
5. Check **Authentium (Command Antivirus)**.
6. In the **Action** field, select an action.
7. Click **OK** to save the changes.

8. If **Zero-Hour Virus Protection - Isolate Virus threats found by Zero-Hour virus scanning engine** is not enabled, enable it.
9. Click **Save** in the **Rules Administrator** to save the changes.

Anti-spam settings:

1. Open the Rules Administrator and select **Spam Rules - (Policy Type: Spam)**.
2. If **Anti-Spam Agent -DFP - Isolate spam triggered by Anti-Spam Agent Digital Fingerprint Component** is not enabled, enable it. The **Rules Import Wizard** opens.
3. Click **Next** and select the isolate queue **Anti-Spam Agent -DFP**. Click **Next** and then **Finish** to exit.
4. If **Anti-Spam Agent Isolate messages triggered by Anti-Spam Agent Heuristics or LexiRule Components** is not enabled, enable it. The **Rules Import Wizard** opens.
5. Click **Next** and select the isolate queue **Anti-Spam Agent**. Click **Next** and then **Finish** to exit.
6. If **Anti-Spam Agent Internet Threat Database - Spam - Isolate message containing Spam, Phishing, Fraud and Spyware related URLS** is not enabled, enable it. The **Rules Import Wizard** opens.
7. Click **Next** and select the isolate queue **Internet Threat DB -Spam**. Click **Next** and then **Finish** to exit.
8. Click **Save** in the **Rules Administrator** to save the changes.

Disable Directory Harvest Detection

At this time, Directory Harvest Detection (DHD) cannot be used with Hosted Email Security. If DHD is enabled in your configuration, it should be disabled now.

1. In the Server Configuration console, select **Email Connection Management > Directory Harvest Detection**.
2. De-select **Enable Directory Harvest Detection**.
3. Click **OK**.

For more information, see “Directory Harvest Detection” in Chapter 3 of the Websense Email Security Administrator’s Guide.

Restart and monitor

You have completed the required reconfiguration activities. You can now restart the Websense Email Security services and monitor receipt of inbound messages.

When the MX record change has fully propagated (see *Activate and set up the Hosted service*), all of your inbound email should come exclusively from Hosted Email Security. When this is true, go back to the Server Configuration console, remove all non-Hosted IP addresses (follow the directions below) and restart the Receive Service. Be sure to enable **Deny connections from all direct relays NOT listed** (step 4 below).

To remove non-Hosted mail relays:

1. Open the **Monitor** and select **File > Server Configuration**.
2. In the **Server Configuration** console, select **Email Connection Management > Mail Relays > Direct** tab.
3. For each non-Hosted **Relay Source** listed, select the entry and click **Delete**.
4. Check the **Deny connections from all direct relays NOT listed** box.
5. Click **OK**.

Additional review and configuration

In addition to the required changes described above, Websense recommends that you review your:

- Inbound content filtering rules
- Outbound content filtering rules
- Scheduled tasks

Personal Email Manager

Websense recommends that you use Personal Email Manager for end-user notification and management of messages isolated by Websense Email Security. This allows end-users to manage their isolated messages from a single source.

If you have not already installed Personal Email Manager, follow the instructions in the *Personal Email Manager Installation Guide*. For information on the configuration and use of Personal Email Manager, see *Personal Email Manager Configuration Tool Guide* and *Personal Email Manager Administrator's Guide*.

Resources

The following additional resources are available to help you tailor your layered email security solution and to answer questions that may arise as you work with Websense software.

Datasheets and white papers:

Websense Hybrid Messaging Security Web page

Websense Hybrid Messaging Security Datasheet

Websense Hybrid Messaging Security White Paper

Websense Hosted Email Security Datasheet

Websense Email Security Datasheet

Documentation:

Hosted Email Security

The following is available from the **Support** area of the Hosted Security portal:

Hosted Security Administrator's Guide

Websense Email Security

Websense Email Security Installation Guide

Websense Email Security Administrator's Guide

Personal Email Manager Installation Guide

Personal Email Manager Configuration Tool Guide

Personal Email Manager Administrator's Guide

Knowledge Base:

For Websense Email Security knowledge base articles and FAQs, go to http://kb.websense.com

For Hosted Email Security knowledge base articles and FAQs, go to the **Support** area of the Hosted Security portal, and click **FAQs**.