

Whitelist in CISCO Secure Email Gateway

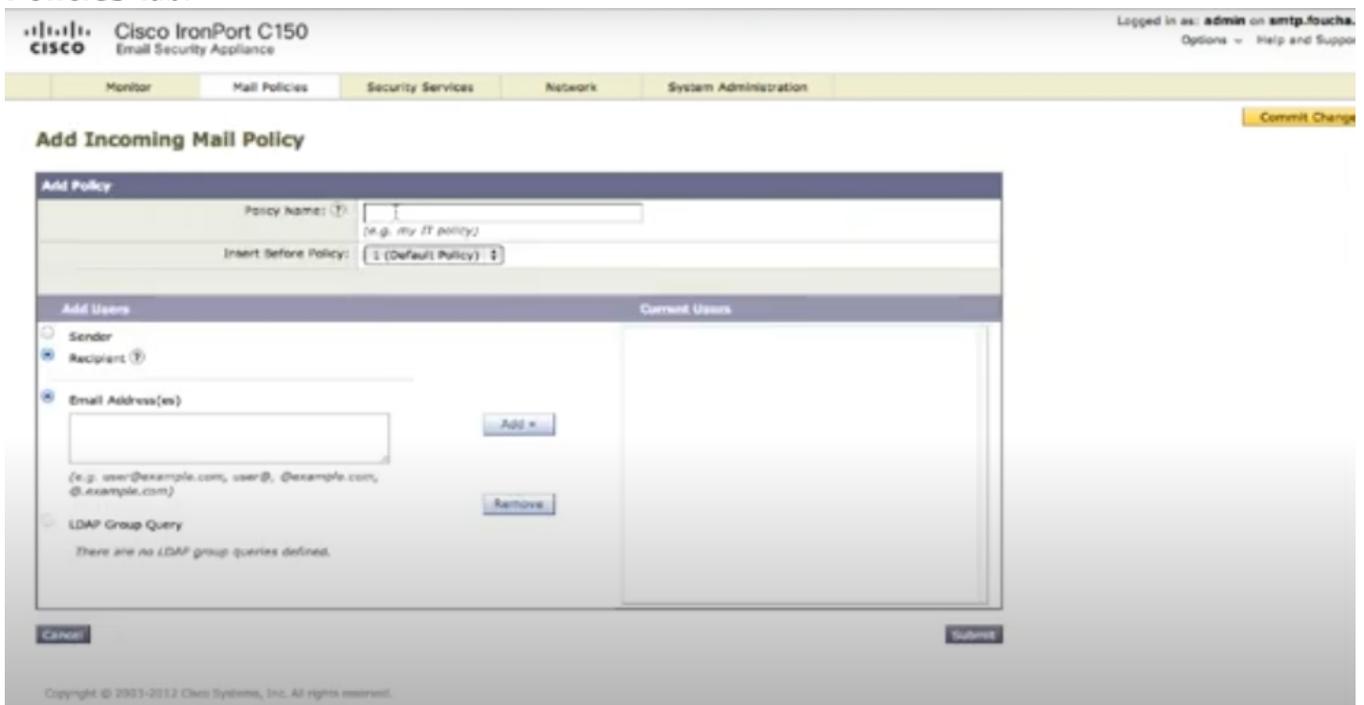
If you're using Cisco Secure Email Gateway spam filtering, you can whitelist CyTech to allow our simulated phishing test emails and training notifications through to your end users.

The instructions below include information from the Cisco whitelisting article. If you run into issues whitelisting CyTech in Cisco Secure Email Gateway, we recommend reaching out to Cisco for specific instructions. You can also contact our support team whenever you need assistance.

Whitelisting Cisco Secure Email Gateway

To whitelist CyTech in Cisco Secure Email Gateway, do the following:

1. From the Cisco Secure Email Gateway admin console, navigate to the **Incoming Mail Policies** tab.



The screenshot displays the Cisco IronPort C150 Email Security Appliance admin console. The top navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System Administration'. The 'Mail Policies' tab is selected. The main content area is titled 'Add Incoming Mail Policy' and contains a form for creating a new policy. The form includes a 'Policy name' field with a placeholder '(e.g. my IT policy)', an 'Insert Before Policy' dropdown menu set to '(Default Policy)', and a section for 'Add Users'. Under 'Add Users', there are radio buttons for 'Sender', 'Recipient', and 'Email Address(es)'. The 'Email Address(es)' option is selected, and there is a text input field for email addresses, an 'Add +' button, and a 'Remove' button. Below the input field, there is a note: '(e.g. user@example.com, user@.example.com, @example.com)'. There is also an 'LDAP Group Query' section with a note: 'There are no LDAP group queries defined.' At the bottom of the form, there are 'Cancel' and 'Submit' buttons. The top right corner of the console shows 'Logged in as: admin on smtp.fouca.' and 'Options - Help and Support'. A 'Commit Change' button is visible in the top right corner of the page.

2. Select **HAT Overview**. Please ensure that **InboundMail lister** is selected.
3. Click **WHITELIST**. If you do not see **WHITELIST**, you can create your own group named "WHITELIST".
4. Click **Add Sender** and add our domains. **Note:** Contact CyTech for the list of domain names.
5. Click **Submit** and then **Commit Changes**.

Note: After following this article, we recommend setting up a test phishing campaign to 1-2 users to ensure your whitelisting was successful. As a last resort, we suggest reaching out to your service provider for assistance.

Disable Spam Scanning

To disable spam scanning in Cisco Secure Email Gateway, do the following:

1. From the Cisco Secure Email Gateway admin console, navigate to the **Incoming Mail Policies** tab.
2. Click **WHITELIST**. If you do not see **WHITELIST**, you can create your own group named "WHITELIST".
3. Disable Spam Scanning for the whitelisted

The screenshot shows the Cisco IronPort C150 admin console interface. The top navigation bar includes 'Monitor', 'Mail Policies', 'Security Services', 'Network', and 'System Administration'. The 'Mail Policies' tab is active. The page title is 'Incoming Mail Policies'. A success message states: 'Success — The policy "Blocklist" was added.' Below this is a search bar for 'Find Policies' with an 'Email Address' field and radio buttons for 'Recipient' and 'Sender'. A table lists the policies:

Order	Policy Name	Anti-Spam	Anti-Virus	Content Filters	Outbreak Filters	Delete
1	Whitelist	Use (default)	[use default]	[use default]	[use default]	[Delete]
2	Blocklist	[use default]	[use default]	[use default]	[use default]	[Delete]
Default Policy		IronPort Anti-Spam Positive: Quarantine Suspected: Quarantine Marketing Messages: Disabled	Sophos Encrypted: Deliver Uncannable: Deliver Virus Positive: Drop	Disabled	Retention Time: Virus: 1 day	

At the bottom right of the table, there is a 'Key' section with 'Default', 'Custom', and 'Disabled' options. The 'Whitelist' policy name and its 'Anti-Spam' setting are highlighted with a red box.

The screenshot shows the 'Mail Policies: Anti-Spam' configuration page. The 'Policy' dropdown is set to 'Whitelist'. Under the 'Enable Anti-Spam Scanning for This Policy' section, the 'Disabled' radio button is selected and highlighted with a red box. The page is divided into several sections:

- Anti-Spam Settings:** Policy: Whitelist. Radio buttons for 'Use Settings from Default Policy (IronPort Anti-Spam)' and 'Use IronPort Anti-Spam service' are unselected. The 'Disabled' radio button is selected.
- Positively-Identified Spam Settings:** 'Apply This Action to Message:' is set to 'Deliver'. 'Send to Alternate Host (optional):' is empty. 'Add Text to Subject:' is set to 'Prepend' and 'SPAM'.
- Suspected Spam Settings:** 'Enable Suspected Spam Scanning:' is set to 'No'. 'Apply This Action to Message:' is set to 'Deliver'. 'Send to Alternate Host (optional):' is empty. 'Add Text to Subject:' is set to 'Prepend' and 'SUSPECTED SPAM'.
- Marketing Email Settings:** 'Enable Marketing Email Scanning:' is set to 'No'. 'Apply This Action to Message:' is set to 'Deliver'. 'Send to Alternate Host (optional):' is empty.

Skipping Outbreak Filter Scanning

The instructions above for whitelisting Cisco Secure Email Gateway do not prevent Secure Email Gateway's Outbreak Filter from scanning emails from our IPs or domain names. If you are experiencing issues with our emails being quarantined, you may also need to set our IPs or hostnames to bypass this filter.

To skip Outbreak Filter Scanning, do the following:

1. From your Cisco Secure Email Gateway admin console, navigate to the **Incoming Mail Policies** tab.
 2. Under the **Message Modification** section, enter our IP addresses or domain names in the **Bypass Domain Scanning** table. **Note:** Contact CyTech for the list of IPs or domain names.
 3. Click **Submit** and then **Commit Changes**.
-

Troubleshooting

If Cisco Secure Email Gateway is flagging CyTech's simulating phishing emails as spam or removing attachments from these emails, you may need to troubleshoot further in Cisco Secure Email Gateway.

For a potential troubleshooting method, see the steps below. If you don't see the solution you're looking for, we recommend reaching out to Cisco Ironport for assistance.

1. Create an individual **HAT Mail Flow Policy** specifically for CyTech.
2. In this policy, disable **Spam Detection** and **Virus Protection**. For more information, see Cisco Ironport's [Mail Flow Policy documentation](#).
3. Add a sender group for our IP addresses or hostnames. **Note:** Contact CyTech for the list of IPs or hostnames.
4. Apply the policy to the sender group. For more information, see Cisco Ironport's [Message Handing documentation](#).

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #6

Created 5 December 2024 07:17:11 by David Napoleon Romanillos

Updated 11 December 2024 13:06:16 by Aldion Pueblos