Tuning and Monitoring the Default Spam and Virus Settings

https://campus.barracuda.com/doc/3211284/

If you make setting changes, allow a few minutes for the changes to take effect.

Once email is flowing through the Barracuda Email Security Service, use the **Message Log** page to see which messages are being blocked or quarantined and for what reasons based on the current Barracuda Email Security Service settings. Click on a message in the **Message Log** to view message details including the action and reason the message was blocked or quarantined. See Understanding the Message Log for more information.

Per-Domain Management

Configure specific settings, including spam and virus settings, policies for inbound and outbound mail, and quarantine settings for each domain you add to the service by drilling down via the **Domains > Domain Manager** page. Click the **Manage** link for the domain you want to configure using the same feature configuration pages available at the global level for the domain. For example, you can turn off virus scanning for a domain that is internal and already protected by an anti-virus solution or customize content and attachment filtering policies for each domain based on the type of email you expect to be flowing to and from the domains.

Important

When you click the **Manage** link on the **Domains > Domain Manager** page, the settings you change apply to that domain specifically and override global settings for that domain.

To reset the domain from domain-specific policies to the global domain management, click the flag icon, and click **Reset to account policies**.

Basic Spam and Virus Checking

By default, virus scanning is enabled in the Barracuda Email Security Service and the system checks for definition updates on a regular basis (hourly by default). Virus scanning takes precedence over all other mail scanning techniques; email coming from exempt IP addresses, sender domains, sender email addresses, or recipients is scanned for viruses and blocked if a virus is detected.

Advanced Threat Protection

In addition to basic virus scanning, you can select to subscribe to the Barracuda Advanced Threat Protection (ATP) service. ATP is a cloud-based virus scanning service that applies to inbound messages, analyzing email attachments in a separate, secured cloud environment to detect new threats and determine whether to block such messages.

Use the **Inbound Settings > Anti-Spam/Antivirus** page to enable or disable virus checking. If you enable **Use Barracuda Real-Time System** on the **Inbound Settings > Anti-Spam/Antivirus** page, the Barracuda Email Security Service checks unrecognized spam and virus fingerprints against the latest virus threats logged at Barracuda Central.

Use the **Inbound Settings > Anti-Spam/Antivirus** page to enable or disable spam filtering mechanisms and set scoring for spam categories. Once you change the settings, use the **Dashboard** and **Message Log** pages to monitor and tune your configuration.

View Email Statistics

The **Dashboard** page provides an email statistics overview for inbound and outbound mail traffic protected by the Barracuda Email Security Service including:

- A graph of the geographic origins of threats detected by the Barracuda Email Security Service
- Email statistics of the number of inbound and outbound messages blocked, allowed, and quarantined for the selected time period, either the **Last 24 Hours** or **Last 30 Days**
- Top domains for which mail has been processed by the system
- Top blocked domains, recipients, and senders for the selected time period

Click the **Help** (?) icon on the **Dashboard** page for more information.

Each time you log into the Barracuda Email Security Service, the **Dashboard** page displays. If you have added domains which are not yet verified by the service, a warning message displays at the top of the page. Click on the link to complete the verification process for the domain.

Figures