Creating and Managing Domains
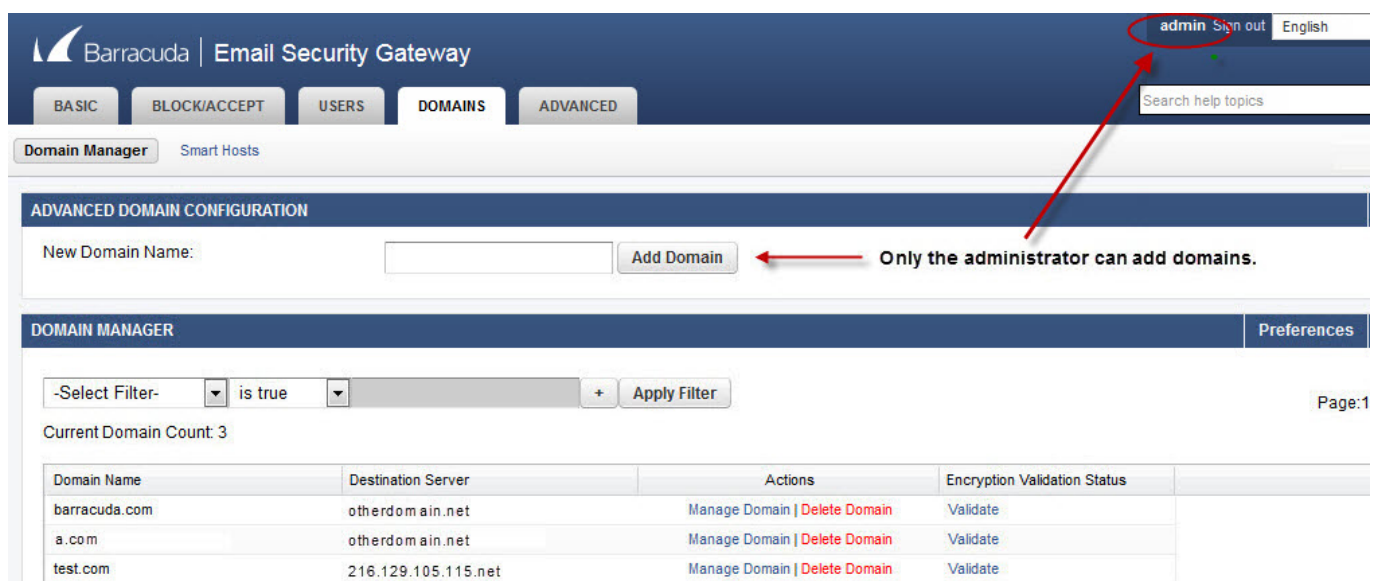
https://campus.barracuda.com/doc/3866635/

Your Barracuda Email Security Gateway only accepts emails addressed to domains that it has been configured to recognize. Settings for individual domains can be configured by the administrator and, with some restrictions, by the **Domain Admin** and **Helpdesk** account roles as described in Roles and Navigating the Web Interface. All three roles will see a **DOMAINS** tab from which they can click **Manage Domain** next to the domain for which to edit the domain-level settings.

Only an administrator can add or delete domains using the controls available in the **DOMAINS** page. The administrator can also add domains from the **BASIC > IP Configuration** page. Domains added from either page are initially configured with whatever you have specified your default global settings to be.

If the administrator deletes a domain, all user accounts associated with that domain will also be deleted from the Barracuda Email Security Gateway. A confirmation dialog box will prompt you to confirm whether or not you want to delete a domain.

Clicking the **Manage Domain** link for a particular domain will show some or all of the **BASIC, USERS, BLOCK/ACCEPT, OUTBOUND QUARANTINE** and **ADVANCED** tabs, depending on the permissions level of the logged in account role.

Figure 1: The administrator can add domains on which to filter email.

Domain Level Settings

Some settings are only configurable at the domain level, while others are configurable at both the global and domain levels, with the domain level setting taking precedence.The **Domain Admin** role or the **Admin** role can override some global settings for spam and virus checking and quarantine at the domain level.

Setting values on a per-domain basis overrides the values configured at the global in the web interface. However, if you have never changed a particular setting for a domain, any global level changes to that feature will be applied for that domain. This also means that any changes you make to the global values of the Barracuda Email Security Gateway will NOT be inherited by the domains that you edit and for which you have changed configuration values.

Basic configuration of a domain consists of identifying the name of the domain (and/or a specific sub-domain) and specifying a destination mail server. Additional settings available for a domain are dependent on the model of your Barracuda Email Security Gateway, and can include any or all of the following:

- Destination Mail Server
- Enabling of spam scanning and setting spam score limits for the domain
- Enabling or disabling virus scanning
- Per-user quarantine enable/disable
- Control over which features users can see and configure for their accounts (see Controlling Access to Account Features).
- A defined global quarantine email address (for the domain only)
- Option to reject messages from same domain name. If set to **Yes**, the Barracuda Email Security Gateway will reject email where the FROM envelope or header address domain matches the domain (in the TO address). This feature provides protection from 'spoofing' of the domain.
- Option to require an encrypted TLS connection when receiving email *from* either ALL or specified domains. See the **ADVANCED > Email Protocol** page at the domain level for details.
- Option to require an encrypted TLS connection when relaying email *to* specified destination domains. See the **ADVANCED > Email Protocol** page at the domain level for details.
- IP address/range, Sender domain, Sender email and Recipient filtering. Note: BLOCK/ACCEPT policies created at the per-domain level do NOT apply to outbound messages - they only apply to inbound messages for that domain.
- LDAP configuration
- Option to specify local database of valid recipients (if not using LDAP) and alias linking
- Single Sign-On with various authentication mechanisms
- Emailreg.org: option to require header, body or subject content filtering on mail from registered email addresses
- Ability to validate the domain and specify an image for branding encrypted email messages and notifications sent to the recipient. Note that encryption policy can only be set at the global level by the administrator.

The Barracuda Email Security Gateway 400 and higher contains support for APIs that can be used to automate the steps for creating and configuring multiple domains on the Barracuda Email Security Gateway.

Figures

1. adminAddsDomains.jpg