

Controlling Access to Account Features

<https://campus.barracuda.com/doc/3866630/>

When accounts are created by the Barracuda Email Security Gateway, permissions are automatically assigned for users to manage their account features based on what is configured on the **USERS > User Features** page in the **Default User Features** section. *Domain Admin* roles can further limit user access to these features based on what the administrator has enabled at the global level.

For example, if the **Whitelist/Blocklist** feature is set to *No* (disabled) at the global level in the **Default User Features** section of the **USERS > User Features** page, the *Domain Admin* role will not see or be able to control that setting for accounts in domains that they manage.

Configurable user account features include:

- Quarantine Inbox - allow the account holder to enable their quarantine inbox on the Barracuda Email Security Gateway, or disable it such that quarantined messages go to their regular email inbox.
- Spam scanning - allow the account holder to enable or disable
- Edit frequency at which quarantine notifications are sent to the account holder
- Add addresses and domains to a whitelist or blocklist
- Use Bayesian filtering
- Allow account holder to set their own tag, quarantine and block levels according to spam scoring

If allowed permissions by the administrator, the *Domain Admin* can edit the **Default User Features** settings (i.e. disabling certain features that were enabled at the global level by the administrator) at the domain level for account holders in the domain. The *Helpdesk* role does not have this permission.

Overriding Default Account Features Settings

The **User Features Override** section of the **USERS > User Features** page allows you to make exceptions to the rules specified above for particular account holders. *Domain Admin* and *Helpdesk* roles can view and set override of user feature defaults ONLY for features that are enabled in the **Default User Features** section by the administrator. Consequently, nothing will appear on the **USERS > User Features** page for *Domain Admin* and *Helpdesk* roles if all **Default User Features** options have been set to *No* by the administrator.

User overrides only apply when the domain level setting in **Default User Features** matches the global setting.

Assigning Quarantine Inbox Permissions to Selected Users

One of the most common scenarios for overriding quarantine settings is when you want to provide a few "power users" with a quarantine inbox on the Barracuda Email Security Gateway and have the rest of your users receive quarantine messages in their standard email inbox. Providing a user with a quarantine inbox gives them greater control over how their messages are quarantined, but also requires them to manage their quarantine queue. For this reason, you may only want to provide a quarantine inbox to a subset of sophisticated users. In this example, you would do the following:

- Set the quarantine type to **Per-user** on the **BASIC > Quarantine** page.
- Set the **New User Quarantine State** to *Off* so that accounts are not automatically created by the Barracuda Email Security Gateway when needed (for conditions under which new accounts can be automatically created, see [Automatic Account Creation](#)).
- Enable the features you want those account holders to be able to manage for their accounts on the **USERS > User Features** page.
- In the **User Account** text box in the **User Account Create/Update** section of the **USERS > User Add/Update** page, enter the email addresses of the users you for whom you want to create a quarantine inbox and set **Enable User(s) Quarantine** to *Yes* in the same section.
- Set the **Email New User(s)** option to *Yes* to email login information to the new users.

If you enable user quarantine, you should remove any mailing lists you may have added on the **ADVANCED > Explicit Users** page and public folders so no per-user accounts are created based on those email addresses.

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.