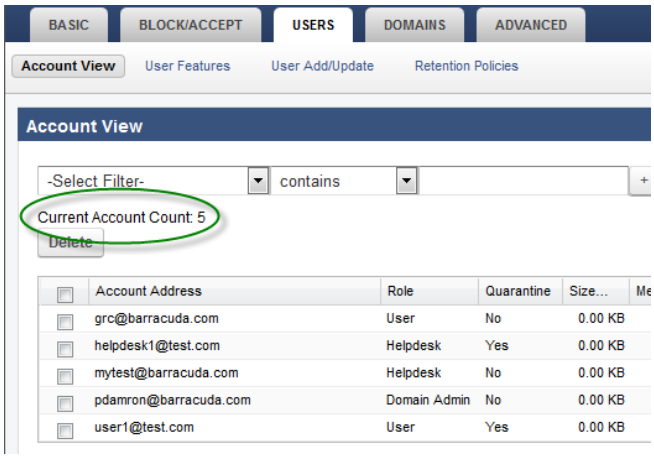
Creating and Managing Accounts

https://campus.barracuda.com/doc/3866683/

With the Barracuda Email Security Gateway 300 and higher, you can enable per-user quarantine and the system will create user accounts to enable access to quarantine settings and messages. The Barracuda Email Security Gateway 600 and higher supports per-user account spam score settings. There are two ways of creating user accounts on the Barracuda Email Security Gateway - automatically and manually. Depending on how the administrator configures the Barracuda Email Security Gateway, user accounts may be configured to display a quarantine inbox for individual use, or accounts may only provide users with the ability to manage their own whitelist and blocklist of email addresses and domains or spam scoring levels.

To find the number of user accounts created on the Barracuda Email Security Gateway, go to the **USERS > Account View** page. See **Current Account Count** above the table.



Account Roles

In addition to the administrator account role, which includes permissions to configure all settings on the Barracuda Email Security Gateway, four other account roles with associated levels of permissions are available:

- *User*, the default account role whose permissions are limited to managing their own quarantine account to the degree enabled by the administrator.
- *Auditor*, a unique account (you can only create one instance) whose role it is to monitor the **Outbound Quarantine** - deleting, rejecting or allowing delivery of messages based on policy. This account already exists on the Barracuda Email Security Gateway and must be enabled on the **BASIC > Administration** page. Note that email privacy can be protected by limiting the Auditor account to only viewing message entries, not actual message contents. Use the **Secondary Authorization** feature, configurable on the **BASIC > Administration** page.

- *Helpdesk* (available on the Barracuda Email Security Gateway 300 and higher), with increased permissions.
- *Domain Admin* (available on the Barracuda Email Security Gateway 600 and higher), the role with the most permissions other than the administrator. This role can configure certain types of policy for the domains assigned to their account.

Thus you can delegate various levels of authority to members of your organization for administering quarantine accounts, monitoring outbound quarantined mail and managing per-domain level settings on the Barracuda Email Security Gateway.

Once accounts are created, each account (with the exception of *Auditor*) can be assigned a role other than the default *User* role from the **USERS > Account View** page at the global level or at the per-domain level. This feature is especially useful for ISPs/web hosting providers to give helpdesk and more sophisticated technical support personnel access to domain and per-user account configuration for groups of users. See Role-based Administration for details on role-based permissions and web interface navigation.

Automatic Account Creation

The Barracuda Email Security Gateway automatically creates accounts when all of the following conditions are met:

- The **New User Quarantine State** feature is set to *On* on the **BASIC > Quarantine** page:
- The administrator enables quarantine and sets quarantine type to *Per-User* on the **BASIC > Quarantine** page. For more information on enabling quarantine, refer to Managing Inbound Quarantine.
- The Barracuda Email Security Gateway receives an email that needs to be quarantined, which triggers creation of the account.

The Barracuda Email Security Gateway automatic account creation process is as follows:

1. Checks the recipient email address against the Local database or the LDAP server as specified at the per-domain level on the **USERS > Single Sign-On** page (Barracuda Email Security Gateway 400 and higher), as well as the **Explicit Users to Accept For** text box on the **USERS > Valid Recipients** page. To increase security, you can configure the Barracuda Email Security Gateway to validate the receiving email address (using LDAP or the SMTP command RCPT TO) before it creates an account. This helps prevent the Barracuda Email Security Gateway from creating accounts for invalid users.
2. Creates a new account with *User* level permissions (See Roles and Navigating the Web Interface for more information about account roles and permissions) for the recipient if the address does not exist. The Barracuda Email Security Gateway uses the email address of the recipient as the username of the account and auto-generates a password.
3. If **Single Sign-On** is not enabled, the Barracuda Email Security Gateway sends the account

holder an email with the login information so they can access their quarantine inbox. With **Single Sign-On** enabled:
    - The account holder will be able to log into the Barracuda Email Security Gateway with their regular network credentials.
    - The account holder can alternatively log in with an *alias* as well. If the per-domain **Unify Email Aliases** option is set to *Yes*, then when a user logs in with an alias, that user will be directed to the primary account. Please see the **USERS > LDAP Configuration** page at the per-domain level for details on this option.
4. Places the quarantined message in the account holder's quarantine inbox.
5. Sends a quarantine summary report to the account holder.

The settings chosen in the Default User Features section of the **USERS > User Features** page are applied to all new accounts that are created.

When to Disable Automatic Creation of Accounts

If your LDAP server is running slowly, email will still be processed by the Barracuda Email Security Gateway but unavailability of your LDAP server could result in creation of invalid quarantine accounts for unverified users on the Barracuda Email Security Gateway. In this case it may be preferable to disable automatic account creation by setting the **New User Quarantine State** to *Off* from the **BASIC > Quarantine** page. User accounts can be manually created in bulk as described below.

Another reason to disable automatic creation of accounts is that you may not want all of your users to have quarantine inboxes to manage, access to whitelist/blocklist capabilities, etc. In that case, you can manually create user accounts for those individuals for whom it is appropriate, as described in the next section.

Manually Creating User Accounts

In addition to the two cases mentioned above, you will want to manually create user accounts with the **USERS > User Add/Update** page when you want to override the default quarantine, virus and spam checking settings for specific account holders. Creating the account before the Barracuda Email Security Gateway automatically creates it enables you to initially configure the account settings if they are different from the default settings for other users.

The Barracuda Email Security Gateway allows for account holders to manage various aspects of spam and virus checking and whitelist/blocklist behavior for their email without having to manage a quarantine inbox on the system. By doing this you can enable global quarantine, but create per-user settings for user control of spam and virus checking features.

For example, if you want your users to be able to maintain their own whitelists and blocklists of email

addresses and domains, but you don't want to use resources on the Barracuda Email Security Gateway to store quarantine messages, or you don't want to have to train or depend on users to manage their quarantine inboxes, you can easily create accounts from the **USERS > User Add/Update** page for one or more users and disable their quarantine inbox(es). Then, on the **USERS > User Features** page, enable the features over which you want those users to have control by entering the same list of new account names (email addresses) in the **User Account(s)**: text box in the **User Features Override** section of the page.

Account Creation by Users

Another way to manually create accounts on the Barracuda Email Security Gateway is to use the **Create New Password** button on the login page which new users can click to create an account with their email address as their username. Their password will be emailed to the email address they enter in the username field.

Single Sign-On and User Authentication

> Single Sign-On is a per-domain setting available on the Barracuda Email Security Gateway 400 and higher.

If Single Sign-On is enabled for a particular domain, account holders associated with that domain can log into the Web interface of the Barracuda Email Security Gateway with their regular network credentials to manage their accounts.

When enabling Single Sign-On for a domain, you should also configure **HTTPS/SSL Access Only** at the global level on the **ADVANCED > Secure Administration** page to protect the transmission of network passwords. See How to Enable SSL for Administrators and Users to configure SSL on the Barracuda Email Security Gateway 400 and higher.

Assigning Features to User Accounts

The **USERS > User Features** page enables the administrator to enable or disable user control over their account settings:

- For newly created accounts, in the **Default User Features** section of the page
- For existing accounts, in the **User Features Override** and the **Default User Features** sections of the page

These features provide the user's ability to enable or disable the following:

- Whitelist/blocklist of email addresses and domains
- Quarantine inbox
- Notification settings - email address for receiving a quarantine summary report, and notification intervals
- Use of a personal Bayesian database
- Spam scanning (on/off)
- Setting spam tag, quarantine and block score levels (Barracuda Email Security Gateway 600 and higher)

For all of the user features enabled by the administrator, the *Domain Admin* account role can override the global setting and disable any **Default User Features** for newly created accounts. BOTH the *Domain Admin* and *Helpdesk* account roles can override the global settings for existing accounts in the **User Features Override** section of the **USERS > User Features** page on a per-domain basis.

To enable account holders (including *Domain Admin, Helpdesk* and *User* roles) to edit preferences/user features for their accounts, make sure that the **Enable User Features** setting on the per-domain **BASIC > Quarantine** page is turned *On*.

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, with the rest of your users receiving quarantined messages in their standard email inbox. Those quarantined messages will have a tag prepended to the subject line indicating that the Barracuda Email Security Gateway suspects the message to be spam. See How Quarantine of Inbound Mail Works for more information.

Figures

1. NumActiveUsers.png