Creating Users and Groups

https://campus.barracuda.com/doc/6160396/

The Barracuda Web Security Gateway distinguishes between two basic classes of the users who access websites and web applications from client machines that it has been configured to protect: *local users* and *domain users.*

You can apply filtering and blocking policies as well as exception rules to both classes of users, and, with several user authentication methods to chose from in the Barracuda Web Security Gateway, you can apply such rules and policies to specific users, groups, LDAP organizational units (OUs) or machines. Authentication options are addressed below.

You can also view the following information about both local users and domain users:

- Account details
- Traffic Log
- Applications Log
- Warned Activity
- Reports output

Local users are shown as anonymous until they authenticate in the Barracuda Web Security Gateway system by providing login information in order to proceed to a blocked or warned web page or application.

Domain users are shown as anonymous until they become authenticated in the Barracuda Web Security Gateway system by providing credentials to their respective authentication service that has been integrated with the Barracuda Web Security Gateway. Authenticated domain users are shown by username, client IP address, and group membership.

In some cases, you may need to create local accounts as well as enable your Barracuda Web Security Gateway to look up domain accounts. For example, if your regular employees have LDAP accounts but contract employees do not, then you might need to create local accounts for the contractor employees.

Local Users

You can define Local users by listing their existing usernames in the **USERS/GROUPS > New Users** page. The Barracuda Web Security Gateway authenticates these users from its local database. To apply Web Security Gatewaying policies (and exception rules to your filtering policies) to multiple local users, you can assign local users to local groups that you define in the **USERS/GROUPS > Local Groups** page.

You can also create IP subnet-based groups - i.e. groups of users who access websites and web applications from client machines within specific ranges of IP addresses. Define IP subnet-based groups of local users in the **USERS/GROUPS > IP Groups** page. Note that MAC addresses are not supported.

Domain Users

The Barracuda Web Security Gateway can authenticate domain users using your existing authentication service. You can integrate the Barracuda Web Security Gateway with any of the following types of authentication servers:

- LDAP
- NTLM
- Kerberos

Doing so enables you to apply Web Security Gatewaying policies and policy exceptions to your domain users without having to re-create local accounts for these users.

Creating Local User Accounts

Use the **USERS/GROUPS > New Users** page to create a local database of users that the Barracuda Web Security Gateway will authenticate. If you want users to be authenticated using your existing user authentication service instead, go to the **USERS/GROUPS > Authentication** page and enter the information for your authentication server.

Local user accounts cannot be used to log into the web interface. You can only use the default admin account to log into the web interface.

If you want a new user account to be a member of a group, be sure the group already exists on the **USERS/GROUPS > Local Groups** page.

Viewing and Managing Accounts

The **USERS/GROUPS > Account View** page displays all the user accounts that have either been created locally on your Barracuda Web Security Gateway or which reside in your LDAP database. This page lets you view details about each account and make the following changes to any locally created accounts:

- Edit a local account by assigning it to a group or enabling/disabling the account
- Change the password of a local account
- Delete a local account

To quickly locate a specific account, use the filter feature at the top of the page to search for specific patterns in the account details.

Creating Local Groups

Use the **USERS/GROUPS > Local Groups** page to create groups for your local users. The most common reason to create a group is so you can apply an exception policy to multiple users at the same time instead of to individual users. For example, you can create a Finance group and create a policy that allows members of that group to browse financial sites, while blocking those sites from other users on the network.

To create a group, enter the group name in the provided field and click **Add**. To assign an existing user to this group, go to the **USERS/GROUPS > Accounts View** page and click **Edit** next to the account that you want to join the group. A user can belong to multiple groups.

> When you navigate to the **USERS/GROUPS > Local Groups** page, the Barracuda Web Security Gateway will only display groups for which you have created an exception. For this reason, it is possible that you won't always see all groups associated with users. To refresh the Groups list, click the **Sync Now** button in the **Group Membership Synchronization** section of the **USERS/GROUPS > Authentication** page.
>
> Note that the **Sync Now** button will only be displayed on that page if you have configured an LDAP, NTLM or Kerberos server..

Creating IP Address Groups

The **USERS/GROUPS > IP Subnets/Groups** page lets you create a group for a single or range of IP addresses. The most common reasons to create an IP group is to apply an exception policy to:

- Multiple users on the same subnet. In this case, enter the subnet mask for the subnet in the provided field.
- A static IP address. In this case, enter the static IP address in the provided field.

After you enter the IP address or subnet mask and click Add, you can assign an exception policy to

the IP group on the **BLOCK/ACCEPT > Exceptions** page.

Assigning Policy to LDAP Organizational Units

If you are using an Active Directory or other LDAP server, you can create policy exceptions for individual members of an organizational unit or for the entire unit. The Barracuda Web Security Gateway can lookup the organizational units defined on your server after you have configured the server(s) on the **USERS/GROUPS > Authentication** page. See the **Applies To** field on that page in the **Add Exception** section. You can select the server, then click the **Lookup** button to view OUs in your server.