How to Configure Authentication

https://campus.barracuda.com/doc/6553647/

This article explains how to configure the the Barracuda Web Security Service Manager with users and groups which can be matched to tagged incoming traffic so user-specific policies can be enforced, and reports for specific users and groups can be generated. For authentication options with the Barracuda Web Security Service Connector, refer to Authentication with the Barracuda Web Security Service Connector.

Configuring Barracuda Web Security Service with User/Group Identities

To configure Barracuda Web Security Service users and groups, you can upload an LDIF file (a snapshot of authentication information output from your authentication system); alternatively, you can use the Barracuda Networks Directory Sync tool to synchronize user/group information on the Barracuda Web Security Manager to your authentication system.

You can also enter user and group information manually through the Barracuda Web Security Service Manager. Manually entered user and group identifications must correspond exactly to those tagged in traffic, or they will never be applied.

Configuring your System so Traffic can be Tagged with User/Group Identities

Using a pure SAAS configuration of the Barracuda Web Security Service, the traffic arriving at the service is not tagged with any user identification, so only global policy enforcement or reporting is possible.

The Barracuda Web Security Agent tags user information on all traffic it proxies to the cloud. These identifications allow the Barracuda Web Security Service to distinguish between traffic sent from different users, and if configured to do so, policies and reports can be applied for matching users or groups configured on the Barracuda Web Security Service Manager. See Overview.

The Barracuda Web Security Service Connector can also tag traffic with user and group information. If you are deploying a Barracuda Web Security Service Connector and proxy traffic to the Barracuda Web Security Service for enforcement, you need to configure the Barracuda Web Security Service Manager with user/group information. See Using the Barracuda Web Security Service Connector.

Group Management

You can specify groups in one of two ways:

- In directory services (such as Active Directory or LDAP) on your network. You can define and maintain groups in one place for both networking and for the web security service.
- In the Barracuda Web Security Service Manager interface. You can create or edit group information manually.

Obtaining User and Group Information

There are three ways to add user and group information to the Barracuda Web Security Service:

- Upload an LDIF file, exported from your LDAP, into the service.
- Push LDAP data from your network up to the service using the Barracuda Networks Directory Sync Utility.
- Manually create groups (or edit information already imported).

How Methods Interact

You can use the three methods above to manage user and group information. Be aware of the following interactions:

- Edit imported user or group information manually, but manual edits or additions may be overwritten when they intersect with incoming imported data.
- The Barracuda Networks Directory Sync tool simply overwrites existing data when executed.
- Directory Upload allows you to choose between an overwrite option and a merge option. The overwrite option simply overwrites existing data.

Directory Upload options do not consider the domain; all usernames and groups are treated as a single domain. Usernames and groups should be unique across all domains being uploaded. Duplicates will be overwritten.

Directory Upload

Barracuda Networks Directory Sync

Group Information and GPO Proxying

Manually Creating and Managing Groups

Creating a Group

You can create groups while you are creating a rule, or you can set them up on the **CONFIGURATION** tab. For more information about creating groups when you create a rule, see Creating Rules for the Barracuda Web Security Service.

1. In the Barracuda Web Security Service Manager, select the **CONFIGURATION** tab.
2. Select **Group Management**.
3. Select **Manual Group Management**.
4. Select **Add New Group**.
5. Type the **Name** for this group, and then **Save Changes**.
6. Now you can add members to the group by selecting **Add New Member**.
7. Enter the **Name**, and then click **Add**.
   The names of group members must be identical to the names used for networking.
8. Click **OK** if prompted to acknowledge the saved changes.
9. Repeat steps 6 through 8 until you have added all group members.

Editing a Group

Any manual edits you make will be overwritten if you subsequently upload or synchronize data from your LDAP server. If you plan to use Barracuda Networks Directory Sync or Directory Upload , it is best to edit the data on your LDAP server, rather than manually editing the Barracuda Web Security Service database.

1. In the Barracuda Web Security Service Manager, select the CONFIGURATION tab.
2. Select **Group Management**.
3. Select the name of the group you want to edit to do any of the following:

- Change the group name by editing the Name field, and then Save Changes.
- Add new group members by selecting Add NewMember, enter the user name, and **Save Changes**.
- Delete users selecting the X icon under Delete and then Save Changes.

Deleting a Group

You cannot delete a group used by a rule, a scheduled report, or by a **Configuration Profile** on the **Web Security Agent** tab. For more information about centrally managing Barracuda Web Security Agents v. 3.3 or later, see Using the Barracuda WSA with the Barracuda Web Security Service.

To delete a group:

1. In the Barracuda Web Security Service Manager, select the **CONFIGURATION** tab.
2. Select **Group Management**.
3. Select the X icon under **Delete** for the group you want to delete.
4. Confirm you want to delete the selected group.