Configuring User Management

https://campus.barracuda.com/doc/84967463/

Overview of the User Management Page

User Management in the Hosted Console website involves the creation of user accounts, and the configuration of Account Policies that define the password rules and login behavior for the accounts. The User Management page contains links to the Users page and the Policies page.

The Users page contains controls to add new users, edit existing user records, and disable or lockout user accounts.

For more information, see the following topics:

Creating User Accounts

Modifying User Accounts

Deleting User Accounts

The Policies page contains controls to manage the access rules and password policy for the Hosted Console website. For more information, see Account Policies.

Creating User Accounts

1. In the Hosted Console website, click **Configuration** > **User Management**.
2. In the **Blueprints** list, click the blueprint that you want to work with.
3. Click the **Users** tab.
4. Click **Create User Account**.
5. Type the logon name to be used in the **User Name** box.
6. In the **First Name** box, type the first name of the user.
7. In the **Last Name** box, type the last name of the user.
8. If desired, in the **Password** box, type the account password.
9. If desired, in the **Confirm Password** box, type the account password again.
10. In the **Email** box, type the email address for the user.
    This is the email address where email alerts will be sent, if applicable.
    Note: Two user accounts cannot have the same email address.
11. Ensure the **Account is Disabled** check box is cleared.
12. Click **Save**.

13. Click the **Roles** tab and see User Configuration Window Roles Tab for instructions about adding roles to the user.
14. Click the **Object Access** tab and see User Configuration Window Object Access Tab for instructions about configuring Object Access for the user.
15. Click **Save**.

Modifying User Accounts

The User Configuration dialog box displays the details of users in the VAR Admin website, which may be updated from this location.

Also, User Accounts may be locked out or unlocked by accessing the User Configuration page for a user. An account that has been locked out may not be used to login to the Hosted Console web console until it has been unlocked. Accounts may be locked out manually or automatically in response to a violation of the Account Policies.

The User list can be used to choose which user is currently displayed.

To edit the details of a Hosted Console User

1. In the Hosted Console website, click **Configuration** > **User Management**.
2. Click the **Users** hyperlink.
3. Click the user from the Users listing.
4. Make any required changes to the **First Name**, **Last Name**, and **Email** boxes.
5. To change the **User Account** password, click the Reset Password hyperlink.
6. Enter the new password for the User Account in the **New Password** and **Confirm New Password** boxes.
   The password must conform to the defined Account Policies.
7. Click the **Save** button to finalize the change or the **Cancel** button to abort the operation.
8. To disable the user account, select the **Account is Disabled** check box.
9. To prevent the user from being able to log into the Hosted Console website, select the **Account is Locked Out** check box.
10. Click the **Save** button to proceed or the **Cancel** button to abort the operation.

Deleting User Accounts

1. In the Hosted Console website, click **Configuration** > **User Management**.
2. Click the **Users** hyperlink to open the users page.
3. Click the **Delete** link that corresponds with the user you want to delete.

Account Policies

Barracuda Managed Workplace Account Policies add additional security to the Hosted Console website, defining how users can access it and protecting it against brute force attacks.

To enable an Account Policy

1. In the Hosted Console website, click **Configuration** > **User Management**.
2. Click **Account Policies**.
3. Select the corresponding check box and configure any values required.

User Settings

Item	Description
User session expires after X minutes	Causes the user to be logged out of the Hosted Console website after a defined period of inactivity. **Default**: 90 minutes
Lock account after X failed login attempts within a X period	Causes a user account to be locked out after a configurable amount of failed login attempts during a defined period of time. **Default**: 5 failed login attempts in 3 minutes

Accounts that are locked out are unable to access the Hosted Console website until another user unlocks the account.

Password Settings

Item	Description
Force user to change password after administrative reset	Causes users to change their password upon the first login if their password has been reset to active by an Administrator.
Keep a history of X passwords	Causes users to create new passwords and not reuse previous passwords. **Default**: 5 days
Enforce alphanumeric passwords	Enforces the use of letters and numbers in passwords.
Enforce special characters in passwords	Enforces that at least one special character must be used in passwords.
Password minimum length is x characters	Enforces a minimum length for the password.
Password expires after x days: Send notification x days before password expires	Sets a password expiration time.

© 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.