

Create API Logins

Manage API Access

This document explains how to create API logins (`apiuser` and `apiauth`) from the WAP portal. You may login to the WAP portal with your root logins on port 5555.

Create API User and Password

Go to **Preferences >> API Manager**

Go to **Create API Account**

Now enter the API User Name and password, Re-enter Password, and Select the Remote Access Options.

API User Name - A user name for the API which we will use with the `apiuser`

Password - A password for the API user, which we will use with the `apiauth`

Remote Access Options - If you like to allow the api user to connect from any IP, you can choose to **Allow any IP**. If you like to restrict access from certain IPs, you can enter the restricted IPs by selecting Allow the following IPs Only.

Allowing Any IP is called Open Access.

Restricting the access by IP is called Restricted Remote Access. It is recommended to connect via secured IPs.

After creating the API user account, you may need to store the api password to a secured location. You can't retrieve the API password once created. You can only reset the password.

The API passwords are stored in the UNIX password hash format.

Revision #4

Created 12 December 2022 12:20:28 by Eenos Official Editor

Updated 11 December 2023 06:50:58 by Jessi