

Managing Users (J-Web Procedure)

You can use the Users Configuration page for user information to add new users to a switching platform. For each account, you define a login name and password for the user and specify a login class for access privileges.

To configure users:

1. In the J-Web interface, select **Configure > System Properties > User Management**.

The User Management page displays details of users, the authentication order, the RADIUS servers and TACACS servers present.

2. Click **Edit**.
3. Click any of the following options on the **Users** tab:
 - **Add**—Select this option to add a user. Enter details as described in Table 1.
 - **Edit**—Select this option to edit an existing user's details. Enter details as described in Table 1.
 - **Delete**—Select this option to delete a user.
4. Click any desired option on the **Authentication Methods and Order** tab:
 - **Authentication Order**—Drag and drop the authentication type from the Available Methods section to the Selected Methods. Click the up or down buttons to modify the authentication order.
 - **RADIUS server**—Click one:
 - **Add**—Select this option to add an authentication server. Enter details as described in Table 2.
 - **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 2.
 - **Delete**—Select this option to delete an authentication server from the list.
 - **TACACS server**—Click one:
 - **Add**—Select this option to add an authentication server. Enter details as described in Table 2.
 - **Edit**—Select this option to modify the authentication server details. Enter details as described in Table 2.
 - **Delete**—Select this option to delete an authentication server from the list.

Table 1: User Management > Add a User Configuration Page Summary

Field	Function	Your Action
User Information		
Username (required)	Specifies the name that identifies the user.	Type the username. It must be unique within the switching platform. Do not include spaces, colons, or commas in the username.
Full Name	Specifies the user's full name.	Type the user's full name. If the full name contains spaces, enclose it in quotation marks. Do not include colons or commas.
Login Class (required)	Defines the user's access privilege.	Select the user's login class from the list: <ul style="list-style-type: none"> ■ operator ■ read-only ■ super-user/superuser ■ unauthorized <p>This list also includes any user-defined login classes.</p>
Login Password (required)	Specifies the login password for this user.	Type the login password for this user. The login password must meet these criteria: <ul style="list-style-type: none"> ■ The password must be at least 6 characters long. ■ It can include alphabetic, numeric, and special characters, but not control characters. ■ It must contain at least one change of case or character class.
Confirm Password (required)	Verifies the login password for this user.	Retype the login password for this user.

Table 2: Add an Authentication Server

Field	Function	Your Action
IP Address	Specifies the IP address of the server.	Type the server's 32-bit IP address, in dotted decimal notation.
Password	Specifies the password of the server.	Type the password of the server.
Confirm Password	Verifies that the password of the server is entered correctly.	Retype the password of the server.
Server Port Number	Specifies the port with which the server is associated.	Type the port number.
Source Address	Specifies the source address of the server.	Type the server's 32-bit IP address, in dotted decimal notation.
Retry Attempts	Specifies the number of login retries allowed after a login failure.	Type the number. NOTE: Only 1 retry is permitted for a TACACS server.

Table 2: Add an Authentication Server *(continued)*

Field	Function	Your Action
Timeout	Specifies the time interval to wait before the connection to the server is closed.	Type the interval in seconds.

Related Topics ■ [Configuring Management Access for the EX-series Switch \(J-Web Procedure\)](#)

