

# Web and MAC Authentication

---

## Contents

Overview .....	4-2
Client Options .....	4-3
General Features .....	4-4
How Web and MAC Authentication Operate .....	4-5
Authenticator Operation .....	4-5
Web-based Authentication .....	4-5
MAC-based Authentication .....	4-7
Terminology .....	4-9
Operating Rules and Notes .....	4-10
General Setup Procedure for Web/MAC Authentication .....	4-12
Do These Steps Before You Configure Web/MAC Authentication ..	4-12
Additional Information for Configuring the RADIUS Server To Support MAC Authentication .....	4-14
Configuring the Switch To Access a RADIUS Server .....	4-15
Configuring Web Authentication on the Switch .....	4-17
Overview .....	4-17
Configure the Switch for Web-Based Authentication .....	4-18
Configuring MAC Authentication on the Switch .....	4-22
Overview .....	4-22
Configure the Switch for MAC-Based Authentication .....	4-23
Show Status and Configuration of Web-Based Authentication .....	4-26
Show Status and Configuration of MAC-Based Authentication .....	4-28
Client Status .....	4-30

## Overview

Feature	Default	Menu	CLI	Web
Configure Web Authentication	n/a	—	4-17	—
Configure MAC Authentication	n/a	—	4-22	—
Display Web Authentication Status and Configuration	n/a	—	4-26	—
Display MAC Authentication Status and Configuration	n/a	—	4-28	—

---

Web and MAC Authentication are designed for employment on the “edge” of a network to provide port-based security measures for protecting private networks and the switch itself from unauthorized access. Because neither method requires clients to run any special supplicant software, both are suitable for legacy systems and temporary access situations where introducing supplicant software is not an attractive option. Both methods rely on using a RADIUS server for authentication. This simplifies access security management by allowing you to control access from a master database in a single server. (You can use up to three RADIUS servers to provide backups in case access to the primary server fails.) It also means the same credentials can be used for authentication, regardless of which switch or switch port is the current access point into the LAN.

**Web Authentication (Web-Auth).** This method uses a web page login to authenticate users for access to the network. When a user connects to the switch and opens a web browser the switch automatically presents a login page. The user then enters a username and password, which the switch forwards to a RADIUS server for authentication. After authentication, the switch grants access to the secured network. Other than a web browser, the client needs no special supplicant software.

---

### Note

---

Client web browsers may not use a proxy server to access the network.

**MAC Authentication (MAC-Auth).** This method grants access to a secure network by authenticating devices for access to the network. When a device connects to the switch, either by direct link or through the network, the switch forwards the device’s MAC address to the RADIUS server for authentication. The RADIUS server uses the device MAC address as the username and

password, and grants or denies network access in the same way that it does for clients capable of interactive logons. (The process does not use either a client device configuration or a logon session.) MAC authentication is well-suited for clients that are not capable of providing interactive logons, such as telephones, printers, and wireless access points. Also, because most RADIUS servers allow for authentication to depend on the source switch and port through which the client connects to the network, you can use MAC-Auth to “lock” a particular device to a specific switch and port.

---

**Note**

On 5300xl switches running software release E.09.xx, 802.1X port-access and either Web authentication or MAC authentication can be concurrently configured on the same port, with a maximum of 32 clients allowed on the port. (The default is one client.)

On all switches covered by this guide, Web authentication, MAC authentication, MAC lockdown, MAC lockout, and port-security are mutually exclusive on a given port. Also, LACP must be disabled on ports configured for any of these authentication methods.

---

## Client Options

Web-Auth and MAC-Auth provide a port-based solution in which a port can belong to one, untagged VLAN at a time. However, where all clients can operate in the same VLAN, the switch allows up to 32 simultaneous clients per port. (In applications where you want the switch to simultaneously support multiple client sessions in different VLANs, design your system so that such clients will use different switch ports.)

In the default configuration, the switch blocks access to clients that the RADIUS server does not authenticate. However, you can configure an individual port to provide limited services to unauthorized clients by joining a specified “unauthorized” VLAN during sessions with such clients. The unauthorized VLAN assignment can be the same for all ports, or different, depending on the services and access you plan to allow for unauthenticated clients.

Access to an optional, unauthorized VID is configured in the switch when Web and MAC Authentication are configured on a port.

## General Features

Web and MAC Authentication on the Series 5300XL switches include the following:

- On a port configured for Web or MAC Authentication, the switch operates as a port-access authenticator using a RADIUS server and the CHAP protocol. Inbound traffic is processed by the switch alone, until authentication occurs. Some traffic from the switch is available to an unauthorized client (for example, broadcast or unknown destination packets) before authentication occurs.
- Proxy servers may not be used by browsers accessing the switch through ports using Web Authentication.
- You can optionally configure the switch to temporarily assign “authorized” and “unauthorized” VLAN memberships on a per-port basis to provide different services and access to authenticated and unauthenticated clients.
- Web pages for username and password entry and the display of authorization status are provided when using Web Authentication.
- You can use the RADIUS server to temporarily assign a port to a static VLAN to support an authenticated client. When a RADIUS server authenticates a client, the switch-port membership during the client’s connection is determined according to the following hierarchy:
  1. A RADIUS-assigned VLAN
  2. An authorized VLAN specified in the Web- or MAC-Auth configuration for the subject port.
  3. A static, port-based, untagged VLAN to which the port is configured. A RADIUS-assigned VLAN has priority over switch-port membership in any VLAN.
- You can allow wireless clients to move between switch ports under Web/MAC Authentication control. Clients may move from one Web authorized port to another or from one MAC authorized port to another. This capability allows wireless clients to move from one access point to another without having to reauthenticate.
- Unlike 802.1x operation, clients do not need supplicant software for Web or MAC Authentication; only a web browser (for Web Authentication) or a MAC address (for MAC Authentication).
- You can use “Show” commands to display session status and port-access configuration settings.

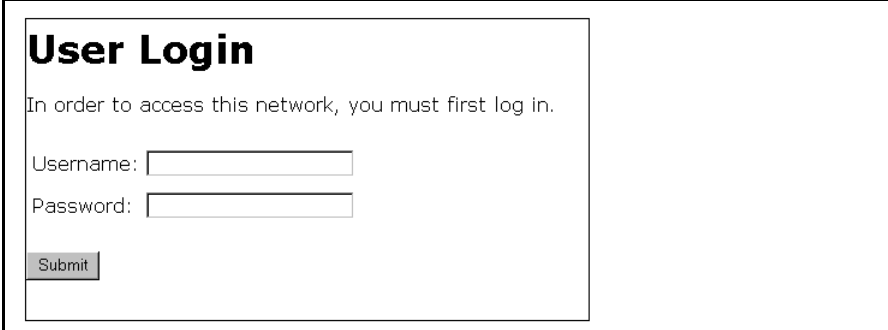
# How Web and MAC Authentication Operate

## Authenticator Operation

Before gaining access to the network clients first present their authentication credentials to the switch. The switch then verifies the supplied credentials with a RADIUS authentication server. Successfully authenticated clients receive access to the network, as defined by the System Administrator. Clients who fail to authenticate successfully receive no network access or limited network access as defined by the System Administrator.

## Web-based Authentication

When a client connects to a Web-Auth enabled port communication is redirected to the switch. A temporary IP address is assigned by the switch and a login screen is presented for the client to enter their credentials.



The image shows a web-based user login screen. It features a title "User Login" in bold black text. Below the title is a message: "In order to access this network, you must first log in." There are two input fields: "Username:" followed by a text box, and "Password:" followed by a text box. Below these fields is a "Submit" button. The entire form is enclosed in a black border.

**Figure 4-1. Example of User Login Screen**

The temporary IP address pool can be specified using the **dhcp-addr** and **dhcp-lease** options of the **aaa port-access web-based** command. If SSL is enabled on the switch and **ssl-login** is enabled on the port the client is redirected to a secure login page (<https://...>).

The switch passes the supplied username and password to the RADIUS server for authentication.

## Authenticating...

Please wait while your credentials are verified.

**Figure 4-2. Progress Message During Authentication**

If the client is authenticated and the maximum number of clients allowed on the port (**client-limit**) has not been reached, the port is assigned to a static, untagged VLAN for network access. If specified, the client is redirected to a specific URL (**redirect-url**).

## Access Granted

You have been authenticated. Please wait while network connection refreshes itself.

Time (sec) Remaining:

**Figure 4-3. Authentication Completed**

The assigned VLAN is determined, in order of priority, as follows:

1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the authorized VLAN (**auth-vid** if configured) and temporarily drops all other VLAN memberships.
3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.
4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.

The assigned port VLAN remains in place until the session ends. Clients may be forced to reauthenticate after a fixed period of time (**reauth-period**) or at any time during a session (**reauthenticate**). An implicit logoff period can be set if there is no activity from the client after a given amount of time (**logoff-period**). In addition, a session ends if the link on the port is lost, requiring reauthentication of all clients. Also, if a client moves from one port to another and client

moves have not been enabled (**client-moves**) on the ports, the session ends and the client must reauthenticate for network access. At the end of the session the port returns to its pre-authentication state. Any changes to the port's VLAN memberships made while it is an authorized port take affect at the end of the session.

A client may not be authenticated due to invalid credentials or a RADIUS server timeout. The **max-retries** parameter specifies how many times a client may enter their credentials before authentication fails. The **server-timeout** parameter sets how long the switch waits to receive a response from the RADIUS server before timing out. The **max-requests** parameter specifies how many authentication attempts may result in a RADIUS server timeout before authentication fails. The switch waits a specified amount of time (**quiet-period**) before processing any new authentication requests from the client.

Network administrators may assign unauthenticated clients to a specific static, untagged VLAN (**unauth-vid**), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients the port is blocked and no network access is available. Should another client successfully authenticate through that port any unauthenticated clients on the **unauth-vid** are dropped from the port.

## MAC-based Authentication

When a client connects to a MAC-Auth enabled port traffic is blocked. The switch immediately submits the client's MAC address (in the format specified by the **addr-format**) as its certification credentials to the RADIUS server for authentication.

If the client is authenticated and the maximum number of MAC addresses allowed on the port (**addr-limit**) has not been reached, the port is assigned to a static, untagged VLAN for network access.

The assigned VLAN is determined, in order of priority, as follows:

1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the Authorized VLAN (**auth-vid** if configured) and temporarily drops all other VLAN memberships.
3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.

## Web and MAC Authentication

### How Web and MAC Authentication Operate

- 
- 
- 
4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.

The assigned port VLAN remains in place until the session ends. Clients may be forced to reauthenticate after a fixed period of time (**reauth-period**) or at any time during a session (**reauthenticate**). An implicit logoff period can be set if there is no activity from the client after a given amount of time (**logoff-period**). In addition, a session ends if the link on the port is lost, requiring reauthentication of all clients. Also, if a client moves from one port to another and client moves have not been enabled (**addr-moves**) on the ports, the session ends and the client must reauthenticate for network access. At the end of the session the port returns to its pre-authentication state. Any changes to the port's VLAN memberships made while it is an authenticated port take affect at the end of the session.

A client may not be authenticated due to invalid credentials or a RADIUS server timeout. The **server-timeout** parameter sets how long the switch waits to receive a response from the RADIUS server before timing out. The **max-requests** parameter specifies how many authentication attempts may result in a RADIUS server timeout before authentication fails. The switch waits a specified amount of time (**quiet-period**) before processing any new authentication requests from the client.

Network administrators may assign unauthenticated clients to a specific static, untagged VLAN (**unauth-vid**), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients the port remains in its original VLAN configuration. Should another client successfully authenticate through that port any unauthenticated clients are dropped from the port.



## Terminology

**Authorized-Client VLAN:** Like the Unauthorized-Client VLAN, this is a conventional, static, untagged, port-based VLAN previously configured on the switch by the System Administrator. The intent in using this VLAN is to provide authenticated clients with network access and services. When the client connection terminates, the port drops its membership in this VLAN.

**Authentication Server:** The entity providing an authentication service to the switch. In the case of a Series 5300XL switch running Web/MAC-Authentication, this is a RADIUS server.

**Authenticator:** In ProCurve switch applications, a device such as a Series 5300XL switch that requires a client or device to provide the proper credentials (MAC address, or username and password) before being allowed access to the network.

**CHAP:** Challenge Handshake Authentication Protocol. Also known as “CHAP-RADIUS”.

**Client:** In this application, an end-node device such as a management station, workstation, or mobile PC linked to the switch through a point-to-point LAN link.

**Redirect URL:** A System Administrator-specified web page presented to an authorized client following Web Authentication. ProCurve recommends specifying this URL when configuring Web Authentication on a switch. Refer to **aaa port-access web-based [e] < port-list > [redirect-url < url >]** on page 4-21.

**Static VLAN:** A VLAN that has been configured as “permanent” on the switch by using the CLI **vlan < vid >** command or the Menu interface.

**Unauthorized-Client VLAN:** A conventional, static, untagged, port-based VLAN previously configured on the switch by the System Administrator. It is used to provide limited network access and services to clients who are not authenticated.

## Operating Rules and Notes

- The switch supports concurrent 802.1X and either Web- or MAC-authentication operation on a port (with up to 32 clients allowed). However, concurrent operation of Web- or MAC-authentication with other types of authentication on the same port is not supported. That is, the following authentication types are *mutually exclusive* on a given port:
  - Web Authentication (with or without 802.1X)
  - MAC Authentication (with or without 802.1X)
  - MAC lockdown
  - MAC lockout
  - Port-Security
- Order of Precedence for Port Access Management (highest to lowest):
  - a. MAC lockout
  - b. MAC lockdown or Port Security
  - c. Port-based Access Control (802.1x) or Web Authentication or MAC Authentication

---

### Note on Port Access Management

---

When configuring a port for Web or MAC Authentication, be sure that a higher precedent port access management feature is not enabled on the port. For example, be sure that Port Security is disabled on a port before configuring the port for Web or MAC Authentication. If Port Security is enabled on the port this misconfiguration does not allow Web or MAC Authentication to occur.

- VLANs: If your LAN does not use multiple VLANs, then you do not need to configure VLAN assignments in your RADIUS server or consider using either Authorized or Unauthorized VLANs. If your LAN does use multiple VLANs, then some of the following factors may apply to your use of Web-Auth and MAC-Auth.
  - Web-Auth and MAC-Auth operate only with port-based VLANs. Operation with protocol VLANs is not supported, and clients do not have access to protocol VLANs during Web-Auth and MAC-Auth sessions.
  - A port can belong to one, untagged VLAN during any client session. Where multiple authenticated clients may simultaneously use the same port, they must all be capable of operating on the same VLAN.

- During an authenticated client session, the following hierarchy determines a port's VLAN membership:
    1. If there is a RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to this VLAN and temporarily drops all other VLAN memberships.
    2. If there is no RADIUS-assigned VLAN, then, for the duration of the client session, the port belongs to the Authorized VLAN (if configured) and temporarily drops all other VLAN memberships.
    3. If neither 1 or 2, above, apply, but the port is an untagged member of a statically configured, port-based VLAN, then the port remains in this VLAN.
    4. If neither 1, 2, or 3, above, apply, then the client session does not have access to any statically configured, untagged VLANs and client access is blocked.
  - After an authorized client session begins on a given port, the port's VLAN membership does not change. If other clients on the same port become authenticated with a different VLAN assignment than the first client, the port blocks access to these other clients until the first client session ends.
  - The optional "authorized" VLAN (**auth-vid**) and "unauthorized" VLAN (**unauth-vid**) you can configure for Web- or MAC-based authentication must be statically configured VLANs on the switch. Also, if you configure one or both of these options, any services you want clients in either category to access must be available on those VLANs.
- Where a given port's configuration includes an unauthorized client VLAN assignment, the port will allow an unauthenticated client session only while there are no requests for an authenticated client session on that port. In this case, if there is a successful request for authentication from an authorized client, the switch terminates the unauthorized-client session and begins the authorized-client session.
  - When a port on the switch is configured for Web or MAC Authentication and is supporting a current session with another device, rebooting the switch invokes a re-authentication of the connection.
  - When a port on the switch is configured as a Web- or MAC-based authenticator, it blocks access to a client that does not provide the proper authentication credentials. If the port configuration includes an optional, unauthorized VLAN (**unauth-vid**), the port is temporarily placed in the unauthorized VLAN if there are no other authorized clients currently using the port with a different VLAN assignment. If an authorized client is using the port with a different VLAN or if there is no unauthorized VLAN configured, the unauthorized client does not receive access to the network.

- Web- or MAC-based authentication and LACP cannot both be enabled on the same port.

---

#### **Note on Web/ MAC Authentication and LACP**

---

The switch does not allow Web or MAC Authentication and LACP to both be enabled at the same time on the same port. The switch automatically disables LACP on ports configured for Web or MAC Authentication.

---

## General Setup Procedure for Web/MAC Authentication

### Do These Steps Before You Configure Web/MAC Authentication

1. Configure a local username and password on the switch for both the Operator (login) and Manager (enable) access levels. (While this is not required for a Web- or MAC-based configuration, ProCurve recommends that you use a local user name and password pair, at least until your other security measures are in place, to protect the switch configuration from unauthorized access.)
2. Determine which ports on the switch you want to operate as authenticators. Note that before you configure Web- or MAC-based authentication on a port operating in an LACP trunk, you must remove the port from the trunk. (refer to the “Note on Web/MAC Authentication and LACP” on page 4-12.)
3. Determine whether any VLAN assignments are needed for authenticated clients.
  - a. If you configure the RADIUS server to assign a VLAN for an authenticated client, this assignment overrides any VLAN assignments configured on the switch while the authenticated client session remains active. Note that the VLAN must be statically configured on the switch.
  - b. If there is no RADIUS-assigned VLAN, the port can join an “Authorized VLAN” for the duration of the client session, if you choose to configure one. This must be a port-based, statically configured VLAN on the switch.

- c. If there is neither a RADIUS-assigned VLAN or an “Authorized VLAN” for an authenticated client session on a port, then the port’s VLAN membership remains unchanged during authenticated client sessions. In this case, configure the port for the VLAN in which you want it to operate during client sessions.

Note that when configuring a RADIUS server to assign a VLAN, you can use either the VLAN’s name or VID. For example, if a VLAN configured in the switch has a VID of 100 and is named **vlan100**, you could configure the RADIUS server to use either “100” or “vlan100” to specify the VLAN.

4. Determine whether to use the optional “Unauthorized VLAN” mode for clients that the RADIUS server does not authenticate. This VLAN must be statically configured on the switch. If you do not configure an “Unauthorized VLAN”, the switch simply blocks access to unauthenticated clients trying to use the port.
5. Determine the authentication policy you want on the RADIUS server and configure the server. Refer to the documentation provided with your RADIUS application and include the following in the policy for each client or client device:
  - The CHAP-RADIUS authentication method.
  - An encryption key
  - One of the following:
    - If you are configuring Web-based authentication, include the user name and password for each authorized client.
    - If you are configuring MAC-based authentication, enter the device MAC address in both the username and password fields of the RADIUS policy configuration for that device. Also, if you want to allow a particular device to receive authentication only through a designated port and switch, include this in your policy.
6. Determine the IP address of the RADIUS server(s) you will use to support Web- or MAC-based authentication. (For information on configuring the switch to access RADIUS servers, refer to “Configuring the Switch To Access a RADIUS Server” on page 4-15.)

## Additional Information for Configuring the RADIUS Server To Support MAC Authentication

On the RADIUS server, configure the client device authentication in the same way that you would any other client, except:

- Configure the client device's (hexadecimal) MAC address as both username and password. Be careful to configure the switch to use the same format that the RADIUS server uses. Otherwise, the server will deny access. The switch provides four format options:

**aabbccddeeff** (the default format)

**aabbcc-ddeeff**

**aa-bb-cc-dd-ee-ff**

**aa:bb:cc:dd:ee:ff**

---

### **Note on MAC Addresses**

---

Letters in MAC addresses must be in lowercase.

- If the device is a switch or other VLAN-capable device, use the base MAC address assigned to the device, and not the MAC address assigned to the VLAN through which the device communicates with the authenticator switch. Note that each switch covered by this guide applies a single MAC address to all VLANs configured in the switch. Thus, for a given switch, the MAC address is the same for all VLANs configured on the switch. (Refer to the chapter titled "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.)

## Configuring the Switch To Access a RADIUS Server

---

### RADIUS Server Configuration Commands

radius-server	
[host <ip-address>]	below
[key < global-key-string >]	below
radius-server host <ip-address> key <server-specific key-string>	4-16

---

This section describes the minimal commands for configuring a RADIUS server to support Web-Auth and MAC Auth. For information on other RADIUS command options, refer to chapter 6, “RADIUS Authentication and Accounting” .

**Syntax:** [no] radius-server

[host < ip-address >]

*Adds a server to the RADIUS configuration or (with **no**) deletes a server from the configuration. You can configure up to three RADIUS server addresses. The switch uses the first server it successfully accesses. (Refer to “RADIUS Authentication and Accounting” on page 6-1.)*

[key < global-key-string >]

*Specifies the global encryption key the switch uses with servers for which the switch does not have a server-specific key assignment (below). This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key. (Default: Null.)*

**Syntax:** radius-server host < ip-address > key <server-specific key-string>  
[no] radius-server host < ip-address > key

*Optional. Specifies an encryption key for use during authentication (or accounting) sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key, above.*

*The **no** form of the command removes the key configured for a specific server.*

For example, to configure the switch to access a RADIUS server at IP address 192.168.32.11 using a server specific shared secret key of '1A7rd':

```
ProCurve Switch 5308xl(config)# radius-server host 192.168.32.11
ProCurve Switch 5308xl(config)# radius-server host 192.168.32.11 key 1A7rd

ProCurve Switch 5308xl(config)# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 3
Global Encryption Key :

Server IP Addr   Auth Port   Acct Port   Encryption Key
-----
192.168.32.11   1812     1813     1A7rd

ProCurve Switch 5308xl(config)# █
```

**Figure 4-4. Example of Configuring a Switch To Access a RADIUS Server**



# Configuring Web Authentication on the Switch

## Overview

1. If you have not already done so, configure a local username and password pair on the switch.
2. Identify or create a redirect URL for use by authenticated clients. ProCurve recommends that you provide a redirect URL when using Web Authentication. If a redirect URL is not specified, web browser behavior following authentication may not be acceptable.
3. If you plan to use multiple VLANs with Web Authentication, ensure that these VLANs are configured on the switch and that the appropriate port assignments have been made. Also, confirm that the VLAN used by authorized clients can access the redirect URL.
4. Use the **ping** command in the switch console interface to ensure that the switch can communicate with the RADIUS server you have configured to support Web-Auth on the switch.
5. Configure the switch with the correct IP address and encryption key to access the RADIUS server.
6. Configure the switch for Web-Auth:
  - a. Configure Web Authentication on the switch ports you want to use.
  - b. If the necessary to avoid address conflicts with the secure network, specify the base IP address and mask to be used by the switch for temporary DHCP addresses. The lease length for these temporary IP addresses may also be set.
  - c. If you plan to use SSL for logins configure and enable SSL on the switch before you specify it for use with Web-Auth.
  - d. Configure the switch to use the redirect URL for authorized clients.
7. Test both authorized and unauthorized access to your system to ensure that Web Authentication works properly on the ports you have configured for port-access using Web Authentication.

---

### Note

Client web browsers may not use a proxy server to access the network.

## Configure the Switch for Web-Based Authentication

Command	Page
<b>Configuration Level</b>	
aaa port-access web-based dhcp-addr	4-18
aaa port-access web-based dhcp-lease	4-18
[no] aaa port-access web-based [e] <port-list>	4-19
[auth-vid]	4-19
[client-limit]	4-19
[client-moves]	4-19
[logoff-period]	4-20
[max-requests]	4-20
[max-retries]	4-20
[quiet-period]	4-20
[reauth-period]	4-20
[reauthenticate]	4-20
[redirect-url]	4-21
[server-timeout]	4-21
[ssl-login]	4-21
[unauth-vid]	4-22

---

**Syntax:** aaa port-access web-based dhcp-addr <ip-address/mask>

*Specifies the base address/mask for the temporary IP pool used by DHCP. The base address can be any valid ip address (not a multicast address). Valid mask range value is <255.255.240.0 - 255.255.255.0>. (Default: 192.168.0.0/255.255.255.0)*

**Syntax:** aaa port-access web-based dhcp-lease <5 - 25>

*Specifies the lease length, in seconds, of the temporary IP address issued for Web Auth login purposes. (Default: 10 seconds)*

**Syntax:** [no] aaa port-access web-based [e] < port-list>

*Enables web-based authentication on the specified ports. Use the **no** form of the command to disable web-based authentication on the specified ports.*

**Syntax:** aaa port-access web-based [e] < port-list> [auth-vid <vid>]]

no aaa port-access web-based [e] < port-list> [auth-vid]

*Specifies the VLAN to use for an authorized client. The Radius server can override the value (accept-response includes a vid). If **auth-vid** is 0, no VLAN changes occur unless the RADIUS server supplies one.*

*Use the **no** form of the command to set the **auth-vid** to 0. (Default: 0).*

**Syntax:** aaa port-access web-based [e] < port-list> [client-limit <1-32>]

*Specifies the maximum number of authenticated clients to allow on the port. (Default: 1)*

**Note:** *On 5300xl switches running software release E.09.xx or greater, where Web Auth and 802.1X can operate concurrently, this limit includes the total number of clients authenticated through both methods.*

**Syntax:** [no] aaa port-access web-based [e] < port-list> [client-moves]

*Allows client moves between the specified ports under Web Auth control. When enabled, the switch allows clients to move without requiring a re-authentication. When disabled, the switch does not allow moves and when one does occur, the user will be forced to re-authenticate. At least two ports (from port(s) and to port(s)) must be specified.*

*Use the **no** form of the command to disable client moves between ports under Web Auth control. (Default: disabled – no moves allowed)*

**Syntax:** aaa port-access web-based [e] < port-list> [logoff-period <60-9999999>]

*Specifies the period, in seconds, that the switch enforces for an implicit logoff. This parameter is equivalent to the MAC age interval in a traditional switch sense. If the switch does not see activity after a logoff-period interval, the client is returned to its pre-authentication state. (Default: 300 seconds)*

**Syntax:** aaa port-access web-based [e] < port-list> [max-requests <1-10>]

*Specifies the number of authentication attempts that must time-out before authentication fails. (Default: 2)*

**Syntax:** aaa port-access web-based [e] < port-list> [max-retries <1-10>]

*Specifies the number of the number of times a client can enter their user name and password before authentication fails. This allows the reentry of the user name and password if necessary. (Default: 3)*

**Syntax:** aaa port-access web-based [e] < port-list> [quiet-period <1 - 65535>]

*Specifies the time period, in seconds, the switch should wait before attempting an authentication request for a client that failed authentication. (Default: 60 seconds)*

**Syntax:** aaa port-access web-based [e] < port-list> [reauth-period <0 - 9999999>]

*Specifies the time period, in seconds, the switch enforces on a client to re-authenticate. When set to 0, reauthentication is disabled. (Default: 300 seconds)*

**Syntax:** aaa port-access web-based [e] < port-list> [reauthenticate]

*Forces a reauthentication of all attached clients on the port.*

**Syntax:**   aaa port-access web-based [e] < port-list > [redirect-url <url>]  
no aaa port-access web-based [e] < port-list > [redirect-url]

*Specifies the URL that a user is redirected to after a successful login. Any valid, fully-formed URL may be used, for example, `http://welcome-server/welcome.htm` or `http://192.22.17.5`. ProCurve recommends that you provide a redirect URL when using Web Authentication.*

**Note:** *The `redirect-url` command accepts only the first 103 characters of the allowed 127 characters.*

*Use the **no** form of the command to remove a specified redirect URL.*

*(Default: There is no default URL. Browser behavior for authenticated clients may not be acceptable.)*

**Syntax:**   aaa port-access web-based [e] < port-list > [server-timeout <1 - 300>]

*Specifies the period, in seconds, the switch waits for a server response to an authentication request. Depending on the current **max-requests** value, the switch sends a new attempt or ends the authentication session.  
(Default: 30 seconds)*

**Syntax:**   [no] aaa port-access web-based [e] < port-list > [ssl-login]

*Enables or disables SSL login (`https` on port 443). SSL must be enabled on the switch.*

*If SSL login is enabled, a user is redirected to a secure page, where they enter their username and password. If SSL login is disabled, a user is not redirected to a secure page to enter their credentials.*

*Use the **no** form of the command to disable SSL login.  
(Default: disabled)*

---

**Syntax:**   aaa port-access web-based [e] <port-list> [unauth-vid <vid>]  
              no aaa port-access web-based [e] <port-list> [unauth-vid]

*Specifies the VLAN to use for a client that fails authentication. If **unauth-vid** is **0**, no VLAN changes occur.*

*Use the **no** form of the command to set the **unauth-vid** to **0**.  
(Default: 0)*

---

## Configuring MAC Authentication on the Switch

### Overview

1. If you have not already done so, configure a local username and password pair on the switch.
2. If you plan to use multiple VLANs with MAC Authentication, ensure that these VLANs are configured on the switch and that the appropriate port assignments have been made.
3. Use the **ping** command in the switch console interface to ensure that the switch can communicate with the RADIUS server you have configured to support MAC-Auth on the switch.
4. Configure the switch with the correct IP address and encryption key to access the RADIUS server.
5. Configure the switch for MAC-Auth:
  - a. Configure MAC Authentication on the switch ports you want to use.
6. Test both the authorized and unauthorized access to your system to ensure that MAC Authentication works properly on the ports you have configured for port-access.

## Configure the Switch for MAC-Based Authentication

Command	Page
<b>Configuration Level</b>	
aaa port-access mac-based addr-format	4-23
[no] aaa port-access mac-based [e] < port-list >	4-23
[addr-limit]	4-24
[addr-moves]	4-24
[auth-vid]	4-24
[logoff-period]	4-24
[max-requests]	4-24
[quiet-period]	4-25
[reauth-period]	4-25
[reauthenticate]	4-25
[server-timeout]	4-25
[unauth-vid]	4-25

**Syntax:** aaa port-access mac-based addr-format  
<no-delimiter|single-dash|multi-dash|multi-colon>

*Specifies the MAC address format to be used in the RADIUS request message. This format must match the format used to store the MAC addresses in the RADIUS server. (Default: no-delimiter)*

**no-delimiter** — specifies an aabbccddeeff format.

**single-dash** — specifies an aabbcc-ddeeff format.

**multi-dash** — specifies an aa-bb-cc-dd-ee-ff format.

**multi-colon** — specifies an aa:bb:cc:dd:ee:ff format.

**Syntax:** [no] aaa port-access mac-based [e] < port-list >

*Enables MAC-based authentication on the specified ports. Use the **no** form of the command to disable MAC-based authentication on the specified ports.*

**Syntax:** aaa port-access mac-based [e] < port-list > [addr-limit <1-32>]

*Specifies the maximum number of authenticated MACs to allow on the port. (Default: 1)*

***Note:** On 5300xl switches running software release E.09.xx or greater, where MAC Auth and 802.1X can operate concurrently, this limit includes the total number of clients authenticated through both methods.*

**Syntax:** [no] aaa port-access mac-based [e] < port-list > [addr-moves]

*Allows client moves between the specified ports under MAC Auth control. When enabled, the switch allows addresses to move without requiring a re-authentication. When disabled, the switch does not allow moves and when one does occur, the user will be forced to re-authenticate. At least two ports (from port(s) and to port(s)) must be specified. Use the **no** form of the command to disable MAC address moves between ports under MAC Auth control.*

*(Default: disabled – no moves allowed)*

**Syntax:** aaa port-access mac-based [e] < port-list > [auth-vid <vid>]

no aaa port-access mac-based [e] < port-list > [auth-vid]

*Specifies the VLAN to use for an authorized client. The RADIUS server can override the value (accept-response includes a vid). If **auth-vid** is 0, no VLAN changes occur unless the RADIUS server supplies one. Use the **no** form of the command to set the **auth-vid** to 0. (Default: 0).*

**Syntax:** aaa port-access mac-based [e] < port-list >  
[logoff-period] <60-999999>

*Specifies the period, in seconds, that the switch enforces for an implicit logoff. This parameter is equivalent to the MAC age interval in a traditional switch sense. If the switch does not see activity after a logoff-period interval, the client is returned to its pre-authentication state. (Default: 300 seconds)*

**Syntax:** aaa port-access mac-based [e] < port-list > [max-requests <1-10>]

*Specifies the number of authentication attempts that must time-out before authentication fails. (Default: 2)*



**Syntax:** aaa port-access mac-based [e] < port-list > [quiet-period <1 - 65535>]

*Specifies the time period, in seconds, the switch should wait before attempting an authentication request for a MAC address that failed authentication.  
(Default: 60 seconds)*

**Syntax:** aaa port-access mac-based [e] < port-list > [reauth-period <0 - 9999999>]

*Specifies the time period, in seconds, the switch enforces on a client to re-authenticate. When set to 0, reauthentication is disabled. (Default: 300 seconds)*

**Syntax:** aaa port-access mac-based [e] < port-list > [reauthenticate]

*Forces a reauthentication of all attached clients on the port.*

**Syntax:** aaa port-access mac-based [e] < port-list > [server-timeout <1 - 300>]

*Specifies the period, in seconds, the switch waits for a server response to an authentication request. Depending on the current **max-requests** value, the switch sends a new attempt or ends the authentication session.  
(Default: 30seconds)*

**Syntax:** aaa port-access mac-based [e] < port-list > [unauth-vid <vid>]

no aaa port-access mac-based [e] < port-list > [unauth-vid]

*Specifies the VLAN to use for a client that fails authentication. If **unauth-vid** is 0, no VLAN changes occur.*

*Use the **no** form of the command to set the **unauth-vid** to 0.  
(Default: 0)*

## Show Status and Configuration of Web-Based Authentication

Command	Page
show port-access [ <i>port-list</i> ] web-based	4-26
[clients]	4-26
[config]	4-26
[config [auth-server]]	4-27
[config [web-server]]	4-27
show port-access <i>port-list</i> web-based config detail	4-27

**Syntax:** show port-access [*port-list*] web-based

*Shows the status of all Web-Authentication enabled ports or the specified ports. The number of authorized and unauthorized clients is listed for each port, as well as its current VLAN ID. Ports without Web Authentication enabled are not listed.*

**Syntax:** show port-access [*port-list*] web-based [clients]

*Shows the port address, Web address, session status, and elapsed session time for attached clients on all ports or the specified ports. Ports with multiple clients have an entry for each attached client. Ports without any attached clients are not listed.*

**Syntax:** show port-access [*port-list*] web-based [config]

*Shows Web Authentication settings for all ports or the specified ports, including the temporary DHCP base address and mask. The authorized and unauthorized VLAN IDs are shown. If the authorized or unauthorized VLAN ID is 0 then no VLAN change is made, unless the RADIUS server supplies one.*

**Syntax:** show port-access [*port-list*] web-based [config [auth-server]]

*Shows Web Authentication settings for all ports or the specified ports, along with the RADIUS server specific settings for the timeout wait, the number of timeout failures before authentication fails, and the length of time between authentication requests.*

**Syntax:** show port-access [*port-list*] web-based [config [web-server]]

*Shows Web Authentication settings for all ports or the specified ports, along with the web specific settings for password retries, SSL login status, and a redirect URL, if specified.*

**Syntax:** show port-access *port-list* web-based config detail

*Shows all Web Authentication settings, including the Radius server specific settings for the specified ports.*

## Show Status and Configuration of MAC-Based Authentication

Command	Page
show port-access [ <i>port-list</i> ] mac-based	4-28
[clients]	4-28
[config]	4-28
[config [auth-server]]	4-29
show port-access <i>port-list</i> mac-based config detail	4-29

**Syntax:** show port-access [*port-list*] mac-based

*Shows the status of all MAC-Authentication enabled ports or the specified ports. The number of authorized and unauthorized clients is listed for each port, as well as its current VLAN ID. Ports without MAC Authentication enabled are not listed.*

**Syntax:** show port-access [*port-list*] mac-based [clients]

*Shows the port address, MAC address, session status, and elapsed session time for attached clients on all ports or the specified ports. Ports with multiple clients have an entry for each attached client. Ports without any attached clients are not listed.*

**Syntax:** show port-access [*port-list*] mac-based [config]

*Shows MAC Authentication settings for all ports or the specified ports, including the MAC address format being used. The authorized and unauthorized VLAN IDs are shown. If the authorized or unauthorized VLAN ID is 0 then no VLAN change is made, unless the RADIUS server supplies one.*

**Syntax:** show port-access [*port-list*] mac-based [config [auth-server]]

*Shows MAC Authentication settings for all ports or the specified ports, along with the Radius server specific settings for the timeout wait, the number of timeout failures before authentication fails, and the length of time between authentication requests.*

**Syntax:** show port-access *port-list* mac-based config detail

*Shows all MAC Authentication settings, including the Radius server specific settings for the specified ports.*

## Client Status

The table below shows the possible client status information that may be reported by a Web-based or MAC-based **'show... clients'** command.

Reported Status	Available Network Connection	Possible Explanations
authenticated	Authorized VLAN	Client authenticated. Remains connected until logoff-period or reauth-period expires.
authenticating	Switch only	Pending RADIUS request.
rejected-no vlan	No network access	<ol style="list-style-type: none"><li>1. Invalid credentials supplied.</li><li>2. RADIUS Server difficulties. See log file.</li><li>3. If unauth-vid is specified it cannot be successfully applied to the port. An authorized client on the port has precedence.</li></ol>
rejected-unauth vlan	Unauthorized VLAN only	<ol style="list-style-type: none"><li>1. Invalid credentials supplied.</li><li>2. RADIUS Server difficulties. See log file.</li></ol>
timed out-no vlan	No network access	RADIUS request timed out. If unauth-vid is specified it cannot be successfully applied to the port. An authorized client on the port has precedence. Credentials resubmitted after quiet-period expires.
timed out-unauth vlan	Unauthorized VLAN only	RADIUS request timed out. After the quiet-period expires credentials are resubmitted when client generates traffic.
unauthenticated	Switch only	Waiting for user credentials.