



CHAPTER 42

Configuring Web-Based Proxy Authentication

This chapter describes how to configure web-based proxy authentication on the Catalyst 6500 series switches.

**Note**

For complete syntax and usage information for the commands that are used in this chapter, refer to the *Catalyst 6500 Series Switch Command Reference* publication.

**Note**

For information on configuring IEEE 802.1X authentication, see [Chapter 40, “Configuring 802.1X Authentication.”](#)

**Note**

For information on configuring MAC address authentication bypass, see [Chapter 41, “Configuring MAC Authentication Bypass.”](#)

**Note**

For information on using port security to block input to an Ethernet, Fast Ethernet, or Gigabit Ethernet port when the MAC address of the station attempting to access the port is different from any of the MAC addresses that are specified for that port, see [Chapter 38, “Configuring Port Security.”](#) That chapter also provides information on using port security to filter the traffic that is destined to or received from a specific host that is based on the host MAC address.

**Note**

For information on configuring authentication, authorization, and accounting (AAA) to monitor and control access to the command-line interface (CLI) on the Catalyst 6500 series switches, see [Chapter 39, “Configuring the Switch Access Using AAA.”](#)

**Note**

For information on configuring network admission control, see [Chapter 44, “Configuring Network Admission Control.”](#)

This chapter consists of these sections:

- [Understanding How Web-Based Proxy Authentication Works, page 42-2](#)
- [Interaction with Other Features, page 42-7](#)
- [Default Web-Based Proxy Authentication Configuration, page 42-8](#)
- [Web-Based Authentication Guidelines and Restrictions, page 42-8](#)
- [Configuring Web-Based Proxy Authentication, page 42-9](#)

Understanding How Web-Based Proxy Authentication Works

The Catalyst 6500 series switch provides web-based proxy authentication in cases where the network client does not have IEEE 802.1X host support. Web-based proxy authentication is authentication through a standard web-based interface (HTTP/HTTPS) of the front-end systems for client identity and credential input.

With 802.1X port-based authentication, a *supplicant* is required to provide access to the LAN and switch services and respond to requests from the switch.



Note

802.1X uses the term *supplicant* for *client* or *host*. In this publication, we use *host* instead of *supplicant* because *host* is used in the Catalyst 6500 series CLI syntax.

Web-based proxy authentication supports full 802.1X authentication and provides support for nonhost-capable clients.

See the “Configuring 802.1X Authentication” chapter for 802.1X authentication information.

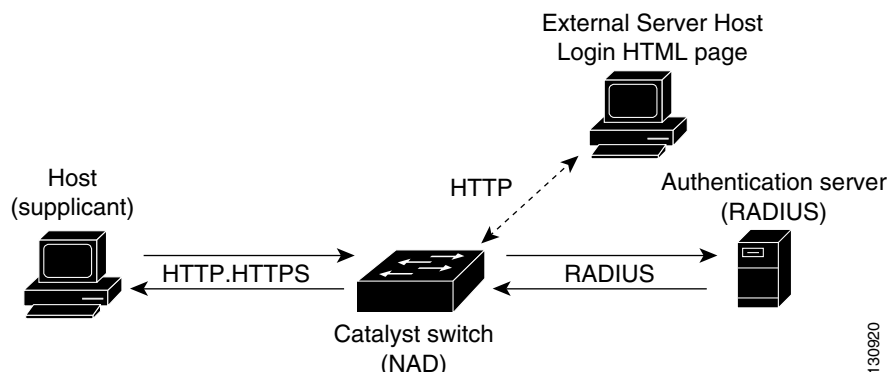
These sections describe how web-based proxy authentication works:

- [Device Roles, page 42-2](#)
- [Authentication Initiation and Message Exchange, page 42-3](#)

Device Roles

Web-based proxy authentication provides authentication through a standard web-based interface as shown in [Figure 42-1](#).

Figure 42-1 Device-integrated Web-Based Proxy Authentication



Host (Supplicant)—Once you enable web-based proxy authentication, the host can request access to the LAN and switch services and respond to requests from the switch.

Switch—The network access device (NAD), or the Catalyst 6500 series switch, hosts all the HTML pages when the host is connected to the switch port that is enabled for web-based authentication. The login web page is hosted on an external web server. When the host receives an IP address, the web browser is opened. When an HTTP packet is intercepted, the URL redirects the client to the location of the external login web page URL. You can directly download the login page from the external web server. If an external login page is not configured, a default login page is sent.

The credentials, which include the username, password, and any other options, are input at the host. The host then submits the page. The Catalyst 6500 series switch intercepts this HTTP POST request, establishes the connection, and retrieves the POST request. Once the POST request is retrieved, the Catalyst 6500 series switch processes the web page and extracts the credentials.

Authentication server—The server validates the identity of the host and notifies the switch if the host is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the host. The Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server; it is available in Cisco Secure Access Control Server version 3.0. RADIUS operates in a client/server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients.

Authentication Initiation and Message Exchange

The host is connected to the switch port that needs to perform web authentication. When the host receives an IP address, a web browser is opened. When an HTTP packet is intercepted, the network access device (NAD) establishes the TCP connection with the host and sends the login page if it is stored locally on the switch, or the URL redirects the client to the location of the external login page URL so that the client directly downloads the login page from the external web server.

You can enter the credentials including the username, the password, and any other options and submit the page from the host. The NAD intercepts this information, establishes a connection, and retrieves the request. The NAD then processes the web page information and extracts the credentials, which are authenticated using an external AAA server (RADIUS). Based on the results of the authentication, the NAD sends an authentication success or an authentication failure page to the client as follows:

- If the authentication succeeds, NAD updates the policy-based ACLs (PBACLs) with the new policy groups that are received from RADIUS for this host. The URL redirects the client to the URL that the client initially tried to access.
- If the authentication fails, the NAD sends a Login-fail web page to the host, that lists the login-fail and input fields. If an external login-fail page is specified, the NAD URL redirects the client to the location of the login-fail page.

If the login or login-fail page points to an external web server, then the default policy allows HTTP access to this web server even before the host is authenticated.



Note

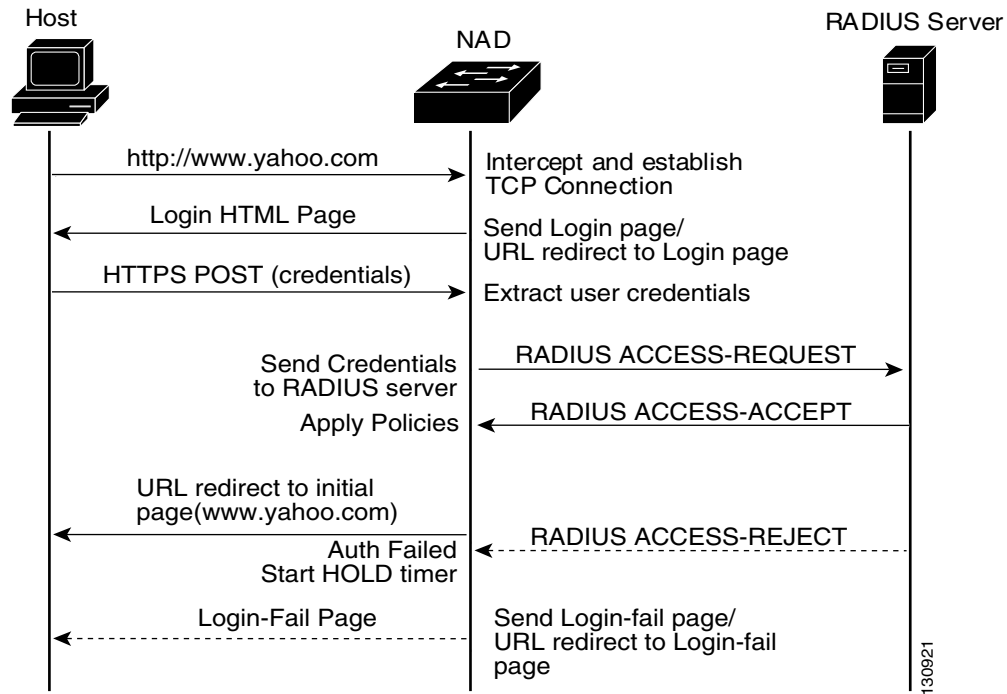
If the default policy does not allow HTTP access and external pages, the client cannot download these web pages and web-based proxy authentication does not work.

The login/login-fail page contains the same variable names and types for the username, passwords, and any other fields that the NAD is programmed to process. A default page is used in the absence of a configured login file on the NAD.

The initial login page is sent using HTTP and HTTPS and is used for submitting user credentials to the Catalyst 6500 series switch. Until HTTPS functionality is fully operational, HTTP is used for credential transfer.

The authentication initiation and message exchange sequence of events is shown in [Figure 42-2](#).

Figure 42-2 Authentication Initiation and Message Exchange



Host Detection and HTTP Traffic Interception

Address Resolution Protocol (ARP) inspection is used to address hosts with static IP addresses assigned. When ARP inspection receives any ARP request on a web-authenticated port, web-based proxy authentication is triggered for a host IP address. If web-based proxy authentication is enabled on a port that is operational, the web-based proxy authentication is initiated on all IP addresses in the Dynamic Host Configuration Protocol (DHCP) snooping table. If a DHCP snooping entry does not exist, web-based proxy authentication is not triggered until a DHCP snooping entry is created or an ARP request is received.

Once the host is detected, the HTTP traffic from the host is intercepted and redirected to the supervisor engine. This process is called URL redirection. To configure URL redirection, you must configure an ACL to redirect all TCP port 80 ingress traffic to the supervisor engine by entering the **permit url-redirect** command. The **permit url-redirect** command redirects all TCP port 80 traffic to the supervisor engine.

Any ACL that is mapped to a port/port-VLAN with this access control entry (ACE) redirects all the HTTP/HTTPS protocol packets that match the ACE criteria to the supervisor engine.

If you enable web-based proxy authentication without configuring this ACE, the HTTP/HTTPS packets are not intercepted and authentication is not initiated. The host traffic in this scenario is controlled by the default policy that is configured on the port/VLAN.

Web-based proxy authentication notifies URL redirection through the software when a new host is detected and provides a callback function for the intercepted HTTP packets.

Access Control

Access control is provided by PBACLs. You can use a PBACL to configure the intercept, default, and host-specific ACLs.

PBACLs are mapped to a VLAN. All ports in the VLAN have the default access specified by the PBACL only.



Note

We recommend that you enable web-based proxy authentication on all ports in the VLAN.

Supported HTML Pages for Web-Based Proxy Authentication

This section describes the following HTML pages required to support web-based proxy authentication:

- [Login Page, page 42-5](#)
- [Success Page, page 42-6](#)
- [Login-Fail Page, page 42-6](#)

Login Page

The login page displays at the client in response to the first URL intercept. Web-based proxy authentication supports a customized login page. The customized login page needs the URL (HTTP only) of the login page. The login page contains the following fields:

- Username—character string
- Password—character string
- Radio button with the following options:
 - I have a registered account
 - I have a Guest account
 - I don't have an account



Note

The submit button in the login page points to the HTTPS URL if the switch supports the HTTPS protocol. If HTTPS is not supported, the login page points to the HTTP URL.

A default login page is sent if a customized login page is not specified.

Success Page

The success page is an auto-redirection page that automatically redirects the client browser to the URL that you tried to access initially. The success page is not displayed, it is auto-redirected to the original page.

Login-Fail Page

The login-fail page, which contains information about the authentication failure, allows you to reenter the credentials if an authentication fails. The login-fail page contains all the fields of a login page and information about the authentication failure.

**Note**

An authentication failure can occur if you enter the wrong username/password or if you select the “I don’t have an account” option and the switch does not have default policies configured for this option.

A default login-fail page displays if a customized login-fail page is not specified.

Multiple Hosts Per Port

Web-based proxy authentication authenticates all the hosts (IP addresses) that are seen on the port. The maximum number of hosts supported on a port is 32.

A new web-based proxy authentication state is created for every new host that is seen on the port. If you enable web-based proxy authentication on a port that has multiple DHCP bindings already created, web-based proxy authentication is initialized for all IP addresses.

High Availability

Web-based proxy authentication supports high availability. Only the information from the authenticated hosts is synchronized to the standby supervisor engine. All authenticated hosts remain authenticated upon a switchover. The notification from unauthenticated or authentication in-progress hosts is not synchronized. Web-based proxy authentication initializes these hosts upon a switchover and authentication restarts.

For example, if you entered the credentials and submitted a login page, and the switch sent the credentials to RADIUS and was waiting for a response, if the switchover occurs, the credentials that you entered are lost and the login page is resent to the host when you try to access any URL. You must reenter the credentials.

Host State

The host state determines if the host is granted access to the network. The host states are as follows:

- **Initialize**—Occurs when the IP address of the host is registered with URL redirection for redirecting any HTTP packet from this host to the supervisor engine. After receiving the first HTTP-intercepted packet, the host state changes to the connecting state.
- **Connecting**—Occurs when the login page displays to the client and waits for a response from the client. When the host receives the HTTP POST response, the host state changes to the authenticating state.

- **Authenticating**—Occurs when the host response (HTTP POST message) is processed and you can extract the credentials. The credentials are then authenticated with the external RADIUS server as follows:
 - If the HTTP response fails, the state changes to the Parse-error state. For example, this state could occur if the external login page specified does not conform to the variable/field names that the switch is programmed to process.
 - If the authentication succeeds, the state changes to the Authenticated state. If the authentication fails and the retry count is less than the maximum configured, the state changes to the Authentication-Fail state or the Held state.
- **Authenticated**—Occurs upon a successful authentication. In the Authenticated state, the RADIUS attributes are processed and the policies are applied and returned to the host. No HTTP packets are intercepted and redirected to the supervisor engine. The state changes to the session-timeout state when the session timer expires.
- **Authentication-Fail**—Occurs when RADIUS sends an accept-reject and a Login-Fail page with authentication failure information embedded in it.
- **Parse-Error**—Occurs upon a failure to extract user credentials from the HTTP Post message. A standard login page that is stored internally in the network access device is sent to the client. The state changes to the Authenticating state when the host receives a HTTP Post response.
- **Session-timeout**—Occurs when the session timer expires. The user policies are removed and the state changes to the Initialize state.
- **Held**—Occurs when the authentication retry count exceeds the configured maximum number of retry attempts. No HTTP packets are intercepted. Port initialize and DHCP binding removal removes the Held state designation.

Interaction with Other Features

Web-based proxy authentication interacts with these features as follows:

- **DHCP snooping**—You can enable web-based proxy authentication and DHCP snooping on the same port/VLAN. The default access control list (ACL) for web-based proxy authentication has an ACE that allows DHCP snooping. The creation of DHCP snooping binding triggers web-based proxy authentication.
- **Dynamic ARP inspection (DAI)**—You can enable web-based proxy authentication and DAI on the same port/VLAN. The default ACL requires an ACE to allow ARP inspection. A host has static IP addresses configured. ARP inspection triggers web-based proxy authentication.
- **IP source guard (IPSG)**—You can enable web-based proxy authentication and IPSG on the same port. IPSG uses a PACL for access policy, and web-based proxy authentication uses a PBACL for access policy. The port ACL mode must be in merge mode in order for IPSG to work with web-based proxy authentication.
- **802.1X**—Web-based proxy authentication and 802.1X are independent identity authentication protocols with 802.1X at Layer 2 and web-based proxy authentication at Layer 3. You can enable web-based proxy authentication with 802.1X. When you configure both web-based proxy authentication and 802.1X on a port, the port attempts to authenticate using 802.1X. After successful authentication, it receives policies from RADIUS. If a policy allows all web (HTTP/HTTPS) traffic, then web-based proxy authentication does not occur. The host is not authenticated if the 802.1X policies allow web traffic. If the 802.1X policies do not allow web traffic, then web-based proxy authentication occurs when the host sends the first HTTP/HTTPS packet that is not allowed by the policy. The packet is intercepted by the URL redirect ACE.

- **MAC-Authentication Bypass**—MAC-Authentication Bypass is a Layer 2 authentication that uses a MAC address. There is no actual authentication with MAC-Authentication Bypass. When you configure web-based proxy authentication on an interface that has MAC-Authentication Bypass configured, web-based proxy authentication occurs when the MAC-Authentication Bypass completes. MAC-Authentication Bypass adds the port to a VLAN and gets an IP address using DHCP, which triggers web-based proxy authentication.
- **Port Security**—When you enable port security and web-based proxy authentication on a port, the hosts that are secured by port security are web authenticated.
- **Voice VLAN ID (VVID)**—Web-based proxy authentication and VVID support is restricted to port-VLAN hosts.
- **Guest VLAN**—At the completion of the 802.1X authentication or MAC-Authentication Bypass, a port is added to the guest VLAN based on the 802.1X or the MAC-Authentication Bypass authentication result. The port receives an IP address using DHCP in the guest VLAN. Web-based proxy authentication occurs after the IP address is received.
- **Auth-Fail-VLAN**—You can enable web-based proxy authentication and the authentication-fail VLAN on the same port/VLAN.
- **Network Admission Control (NAC)**—You can enable web-based proxy authentication and NAC LAN port IP on the same port/VLAN. NAC with LAN port IP is independent of web-based proxy authentication; LAN port IP posture validation can happen before web-based proxy authentication.

Default Web-Based Proxy Authentication Configuration

Table 42-1 shows the default web-based proxy authentication configuration settings.

Table 42-1 Web-Based Proxy Authentication Default Configuration

Feature	Default Value
Port access entity (PAE) capability	Authenticator only
Web-based proxy authentication—Global	Disabled
Web-based proxy authentication—Per port	Disabled
Global session timeout	3600 seconds
Quiet timeout	60 seconds
Login attempts	3 attempts

Web-Based Authentication Guidelines and Restrictions

This section provides the guidelines and restrictions for configuring web-based proxy authentication:

- Web-based authentication is not supported on trunk or port-channel interfaces.
- Because PBACL will be mapped to a VLAN, all ports in the VLAN have default access specified by the PBACLs default policy. We recommend that you enable web-based authentication on all the ports in the VLAN.

- Before you enable web-based proxy authentication on a port, you must map a PBAACL with the following ACEs to the VLAN:
 - DHCP snooping
 - ARP inspection
 - Allow DNS
 - Policy config
 - URL Redirect
 - Default policy
- Before you enable web-based proxy authentication on a port, you must enable ARP inspection for the static IP hosts and configure the static ARP inspection rules.

This example shows how to configure a typical ACL with these ACEs:

```
permit dhcp-snooping
permit arp-inspection <ip_addr> <hwaddr>
permit udp any eq dns any [permit DNS]
permit tcp any eq domain any [permit DNS w/TCP]
<Policy configuration>
permit ip group Exception ExpServers
permit ip group Engineer EngServers
permit ip group Manager MgrServers
permit ip group Admin any
permit url-redirect [permit URL redirection]
deny ip any any [Default policy]
```

When the host first comes up, there are no policies configured for the host IP and all host traffic, except for the HTTP traffic that is controlled by the default policy and configured in the PBAACL. The HTTP traffic is redirected to the supervisor engine. Web-based proxy authentication registers this IP with URL redirection when it receives a trigger from DHCP or ARP. The URL redirection module on the supervisor engine receives the packet and passes it to web-based proxy authentication.

After successful authentication, web-based proxy authentication adds the host IP to the groups that are received from RADIUS, expands the PBAACL, and updates the Ternary Content Addressable Memory (TCAM). The host traffic is controlled by the policy configuration. Because the HTTP redirection ACE is at the end, it will not be affected if the host policies are in place. Once the host policies are removed (after the session timeout has been exceeded), the host traffic is again subjected to the default policy and HTTP traffic gets redirected to the supervisor engine.

Configuring Web-Based Proxy Authentication

This section describes how to configure web-based proxy authentication:

- [Enabling or Disabling Web-Based Proxy Authentication Globally, page 42-10](#)
- [Enabling or Disabling Web-Based Proxy Authentication on a Port, page 42-10](#)
- [Initializing Web-Based Proxy Authentication on a Port, page 42-11](#)
- [Configuring the Login Page URL, page 42-11](#)
- [Configuring the Login-Fail Page URL, page 42-12](#)
- [Specifying the Session Timeout Period, page 42-12](#)

- [Specifying the Quiet Period, page 42-12](#)
- [Specifying the Maximum Login Attempts, page 42-13](#)
- [Displaying Web-Based Proxy Authentication Information, page 42-13](#)

Enabling or Disabling Web-Based Proxy Authentication Globally

You must enable web-based proxy authentication for the entire system before you can configure it for the individual ports. After you enable web-based proxy authentication globally, you can configure the individual ports for web-based proxy authentication. To enable web-based proxy authentication for the individual ports, see the “[Enabling or Disabling Web-Based Proxy Authentication on a Port](#)” section on [page 42-10](#).

To enable or disable web-based authentication globally, perform these tasks in privileged mode:

Task	Command
Globally enable web-based proxy authentication.	set web-auth enable
Globally disable web-based proxy authentication.	set web-auth disable

This example shows how to enable web-based proxy authentication globally:

```
Console> (enable) set web-auth enable
enabled web-auth
Console> (enable)
```

This example shows how to disable web-based proxy authentication globally:

```
Console> (enable) set web-auth disable
disabled web-auth
Console> (enable)
```

Enabling or Disabling Web-Based Proxy Authentication on a Port

You can enable web-based proxy authentication for individual ports after you enable web-based proxy authentication globally. To enable web-based proxy authentication globally, see the “[Enabling or Disabling Web-Based Proxy Authentication Globally](#)” section on [page 42-10](#).



Note

If you have disabled web-based proxy authentication globally, web-based proxy authentication on a port may not start but will be stored in the configuration.

To enable or disable web-based authentication on a port, perform these tasks in privileged mode:

Task	Command
Enable web-based proxy authentication on a port.	set port web-auth mod/port enable
Disable web-based proxy authentication on a port.	set port web-auth mod/port disable

This example shows how to enable web-based proxy authentication on a port:

```
Console> (enable) set port web-auth 1/1 enable
web-authentication successfully enabled on Interface 1/1.
Console> (enable)
```

This example shows how to disable web-based proxy authentication on a port:

```
Console> (enable) set port web-auth 1/1 disable
web-authentication successfully disabled on Interface 1/1.
Console> (enable)
```

Initializing Web-Based Proxy Authentication on a Port

When you initialize the port with the **set port web-auth initialize** command, you are returning the port to the first state. In this state, the IP address of the host is registered with URL redirection for redirecting any HTTP packet from this host to the supervisor engine.

If you specify the *ip_addr* argument, web-based proxy authentication is initialized for that host only. If you do not specify the *ip_addr* argument, web-based proxy authentication is initialized for all hosts.

You must enable web-based proxy authentication globally and on the individual port before you can initialize a web-based proxy authentication port for authentication again.

To initialize a web-based proxy authentication port for authentication again, perform this task in privileged mode:

Task	Command
Initialize a web-based proxy authentication port for authentication again.	set port web-auth <i>mod/port initialize</i> [<i>ip_addr</i>]

This example shows how to initialize web-based proxy authentication again for all hosts on a port:

```
Console> (enable) set port web-auth 2/1 initialize
Initialized web-authentication for all hosts on port 2/1.
Console> (enable)
```

This example shows how to initialize web-based proxy authentication again for a specific host:

```
Console> (enable) set port web-auth 2/1 initialize 10.1.1.1
Initialized web-authentication for host 10.1.1.1 on port 2/1.
Console> (enable)
```

Configuring the Login Page URL

When you enter the URL, use the url = **http://string**.

To configure the URL for the login page, perform this task in privileged mode:

Task	Command
Configure the URL for the login page.	set web-auth login-page url <i>url</i>

This example shows how to configure the URL for the login page:

```
Console> (enable) set web-auth login-page url http://proxyauth.cisco.com/login.html
web-auth login-page configured.
Console> (enable)
```

Configuring the Login-Fail Page URL

When you enter the URL, use this format, url = **http://string**.

To configure the URL for the login-fail page, perform this task in privileged mode:

Task	Command
Configure the URL for the login-fail page.	set web-auth login-fail-page url <i>url</i>

This example shows how to configure the URL for the login-fail page:

```
Console> (enable) set web-auth login-fail-page url http://proxyauth.cisco.com/login.html
web-auth login fail page configured.
Console> (enable)
```

Specifying the Session Timeout Period

You can specify the amount of time that this session is valid. After the time has been exceeded, the web-authenticated session is terminated. The RADIUS-supplied session timeout takes precedence over the locally configured value.

To specify the timeout period for the global web-based proxy authentication sessions, perform this task in privileged mode:

Task	Command
Specify the timeout period for the global web-based proxy authentication sessions.	set web-auth session-timeout <i>seconds</i>

This example shows how to specify the timeout period for the global web-based proxy authentication sessions:

```
Console> (enable) set web-auth session-timeout 20
web-authentication session-timeout set to 20 seconds.
Console> (enable)
```

Specifying the Quiet Period

When the authenticator cannot authenticate the host, it remains idle for a set period of time and then tries again. The idle time is determined by the quiet-period value. The default is 60 seconds. You may set the *seconds* value from 0 to 65535 seconds.

To specify the duration of the quiet period, perform this task in privileged mode:

Task	Command
Specify the quiet period.	set web-auth quiet-timeout <i>seconds</i>

This example shows how to specify the quiet period:

```
Console> (enable) set web-auth quiet-timeout 20
web-authentication quiet-timeout set to 20 seconds.
Console> (enable)
```

Specifying the Maximum Login Attempts

You can specify the maximum number of unsuccessful login attempts allowed before blocking the user.

To specify the maximum number of login attempts, perform this task in privileged mode:

Task	Command
Specify the maximum number of login attempts.	set web-auth login-attempts <i>count</i>

This example shows how to specify the maximum number of login attempts:

```
Console> (enable) set web-auth login-attempts
web-authentication max retry count set to <count>
Console> (enable)
```

Displaying Web-Based Proxy Authentication Information

This section describes how you can display the following web-based proxy authentication information:

- [Displaying Summary of Session Information, page 42-13](#)
- [Displaying Per-Port Information, page 42-14](#)

Displaying Summary of Session Information

If you specify the **vlan** *vlan_id* keyword and argument, a summary of information for the specified VLAN is displayed.

In the command output display, the following applies:

- The * indicates the RADIUS assigned value.
- The State field displays the current web-authentication state for the given host.

To display a summary of information about the web-based proxy authentication session, perform this task in normal mode:

Task	Command
Display a summary of information for the web-based proxy authentication session.	show web-auth summary [vlan <i>vlan_id</i>]

This example shows how to display a summary of information about the web-based proxy authentication session:

```

Console> (enable) show web-auth summary
Web-authentication enabled globally
Login-page location url http://proxyauth.cisco.com/login.html
Login-fail-page location url http://proxyauth.cisco.com/loginfail.html
session-timeout : 3600 secs
quiet timeout : 60 secs
Max Login attempt count: 3
-----
IP Address          Interface      Web Auth State
  Session-Timeout  Leftover-Session-Time  VLAN
-----
9.9.150.1           1/1           Authenticated
* 7200              200              100
9.9.150.2           1/2           Authenticating
-                   3600              100
9.9.150.3           1/3           Authentication-fai
3600                -                 100
9.9.160.10          1/4           Held
3600                -                 200
9.9.170.15          1/5           Connecting
300                 3600              -
Console> (enable)

```

This example shows how to display a summary of information about the web-based proxy authentication session for a specific VLAN:

```

Console> (enable) show web-auth summary vlan 100
-----
IP Address          Interface      Web Auth State
  Session-Timeout  Leftover-Session-Time
-----
9.9.150.1           1/1           Authenticated
* 7200              200
9.9.150.2           1/2           Authenticating
3600                -
9.9.150.3           1/3           Held
3600                -
Console> (enable)

```

Displaying Per-Port Information

The **show port web-auth** command displays the following information:

- IP address of the host.
- Current state.
- Session-timeout. The time displayed is the configured timeout if not supplied by RADIUS.
- Leftover session timeout value.

To display information about a web-based proxy authentication port, perform this task in normal mode:

Task	Command
Display information about a web-based proxy authentication port.	show port web-auth <i>mod/port</i>

This example shows how to display information about a web-based proxy authentication port:

```

Console> (enable) show port web-auth 3/48
Port IP-Address Vlan Web-Auth-State
-----
3/48 9.6.7.8 16 AUTHENTICATION_FAIL
Port IP-Address Session-Timeout Session-Timeleft Radius-Rcvd-Timeout
-----
3/48 9.6.7.8 300 300 No
Port IP-Address Policy-Groups
-----
3/48 9.6.7.8

Console> (enable)

```

Displaying Statistics

To display web-based proxy authentication statistics, perform this task in enable mode:

Task	Command
Display web-based proxy authentication statistics.	show web-auth <i>statistics</i>

This example shows how to display web-based proxy authentication statistics:

```

Console> (enable) show web-auth statistics
Total GET Requests received      : 0
Total POST Requests received    : 0
Total responses sent             : 0
Total web auth hosts             : 0
Total successful authentications : 0
Total failed authentications     : 0
Total critical active hosts      : 0
Total web auth Queue Entries    : 0
Total web auth Queue Drops      : 0
Console> (enable)

```

