Configuring Local Authentication

Information About Local Web Authentication

Web authentication is a Layer 3 security feature that causes the controller not to allow IP traffic (except DHCP and DNS-related packets) from a particular client until that client has correctly supplied a valid username and password. It is a simple authentication method without the requirement for a supplicant or client utility. Web authentication is typically used by customers who want to deploy a guest-access network. Typical deployments can include hot spot locations such as T-Mobile or Starbucks.

Web authentication does not provide data encryption. Web authentication is typically used as simple guest access for either a hot spot or a campus atmosphere where the only concern is the connectivity.

Web authentication can be performed using:

- Default login window on the controller.
- Modified version of the default login window on the controller.
- A customized login window that you configure on an external web server (external web authentication).
- A customized login window that you download to the controller.

Web Authentication Process

The following process takes place when a user connects to a WLAN configured for web authentication:

- The user opens a web browser and enters a URL, for example, http://www.cisco.com. The client sends out a DNS request for this URL to get the IP address for the destination. The controller bypasses the

DNS request to the DNS server and the DNS server responds back with a DNS reply, which contains the IP address of the destination http://www.cisco.com. This, in turn, is forwarded to the wireless clients.

- The client then tries to open a TCP connection with the destination IP address. It sends out a TCP SYN packet destined to the IP address of http://www.cisco.com.
- The controller has rules configured for the client and hence can act as a proxy for http://www.cisco.com. It sends back a TCP SYN-ACK packet to the client with source as the IP address of http://www.cisco.com. The client sends back a TCP ACK packet in order to complete the three way TCP handshake and the TCP connection is fully established.
- The client sends an HTTP GET packet destined to http://www.cisco.com. The controller intercepts this packet and sends it for redirection handling. The HTTP application gateway prepares a HTML body and sends it back as the reply to the HTTP GET requested by the client. This HTML makes the client go to the default web page URL of the controller, for example, http://<Virtual-Server-IP>/login.html.
- The client closes the TCP connection with the IP address, for example, http://www.cisco.com.
- Now the client wishes to navigate to http://1.1.1.1/login.html. Therefore, the client tries to open a TCP connection with the virtual IP address of the controller. It sends a TCP SYN packet for 1.1.1.1 to the controller.
- The controller responds back with a TCP SYN-ACK and the client sends back a TCP ACK to the WLC in order to complete the handshake.
- The client sends a HTTP GET for /login.html destined to 1.1.1.1 in order to request for the login page.
- This request is allowed based on the web server configured for the controller and the server responds back with the default login page. The client receives the login page on the browser window where the user can log in.

Restrictions for Local Web Authentication

- Sometimes clients are dropped in the IP learn state. To prevent clients from dropping, make sure you enable IP DHCP snooping globally and for the client VLAN.
- Some devices (For example, Ipads) may not redirect to the login page if IP HTTP secure server is used.
- If you have enabled the secure server using the **ip http secure-server** command and then disable it using the **no** form of the command, you need to reboot the controller for the secure server to get deactivated.

Configuring Local Web Authentication

Configuring Local Web Authentication for Local Net Users Using AAA (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login** *local_webauth local*
3. **aaa authorization network** *local_webauth local*
4. **aaa authorization network** *default local*
5. **aaa authorization credential-download default** *local*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `ControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication login** *local_webauth local* **Example:** `ControllerDevice(config)# aaa authentication login local_webauth local`	Sets an authentication method list *local_webauth* to the group type *local*.
Step 3	**aaa authorization network** *local_webauth local* **Example:** `ControllerDevice(config)# aaa authorization network local_webauth local`	Sets an authorization method list *local_webauth* to the group type *local*.
Step 4	**aaa authorization network** *default local* **Example:** `ControllerDevice(config)# aaa authorization network default local`	Sets an authorization method list for local user.
Step 5	**aaa authorization credential-download default** *local* **Example:** `ControllerDevice(config)# aaa authorization credential-download default local`	Sets an authorization method list for use of local credentials.

Configuring Local Web Authentication Using RADIUS Server (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **aaa authentication login** *authentication-list-name* **group** *radius-server-group*
3. **aaa authorization network** *authentication-list-name* **group** *radius-server-group*
4. **aaa group server radius** *radius-server-group*
5. **radius server** *server-name*
6. **address ipv4** *ipv4-address* **auth-port** *auth-port-number***acct-port** *acct-port-number*
7. **key ww-wireless**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `ControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**aaa authentication login** *authentication-list-name* **group** *radius-server-group* **Example:** `ControllerDevice(config)# aaa authentication login webauth_radius group ISE_group`	Sets an authentication method list to the RADIUS server group.
Step 3	**aaa authorization network** *authentication-list-name* **group** *radius-server-group* **Example:** `ControllerDevice(config)# aaa authorization network webauth_radius group ISE_group`	Sets an authorization method list to the RADIUS server group.
Step 4	**aaa group server radius** *radius-server-group* **Example:** `ControllerDevice(config)# aaa group server radius ISE_Group`	Sets an RADIUS server group.
Step 5	**radius server** *server-name* **Example:** `ControllerDevice(config)# radius server ISE`	Sets an RADIUS server.
Step 6	**address ipv4** *ipv4-address* **auth-port** *auth-port-number***acct-port** *acct-port-number* **Example:** `ControllerDevice(config-radius-server)# address ipv4 192.168.154.119 auth-port 1812 acct-port 1813`	Sets an RADIUS server.

	Command or Action	Purpose
Step 7	**key ww-wireless** **Example:** `ControllerDevice(config-radius-server)# key ww-wireless`	Sets an RADIUS server encryption key.

Configuring Local Web Authentication Using RADIUS Server (GUI)

Step 1 Choose **Configuration** > **Security** > **AAA** > **Method Lists** > **Authentication** to open the **Authentication** page.

Step 2 Click **New** to open the **Authentication > New** page.

Step 3 In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for RADIUS server.

Step 4 In the **Type** field, choose **login**.

Step 5 In the **Group Type** field, choose **group**.

Step 6 Select the RADIUS server group from the **Available Server Groups** field.

Step 7 Click **Apply** to save the configuration.
The Authentication method list is displayed in the **Authentication** summary page.

Step 8 Choose **Configuration** > **Security** > **AAA** > **Method Lists** > **Authorization** to open the **Authorization** page.

Step 9 Click **New** to open the **Authorization > New** page.

Step 10 In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for RADIUS server.

Step 11 In the **Type** field, choose **network**.

Step 12 In the **Group Type** field, choose **group**.

Step 13 Select the RADIUS server group from the **Available Server Groups** field.

Step 14 Click **Apply** to save the configuration.
The Authorization method list is displayed in the **Authorization** summary page.

Configuring Guest Users for Local Web Authentication (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **username** *name* { **creation-time** *time* | **privilege** *level* | **password** *encryption-type password*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `ControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**username** *name* { **creation-time** *time* | **privilege** *level* | **password** *encryption-type password* **Example:** `ControllerDevice(config)# user-name viten_webauth creation-time 1368715259 privilege 15 password 0 test12345`	Enters the local database, and establishes a username-based authentication system. Repeat this command for each user. • For name, specify the user ID as one word. Spaces and quotation marks are not allowed. • (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. For encryption-type, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows. • For password, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.

Configuring Guest Users for Local Web Authentication (GUI)

Step 1 Choose **Configuration** > **Security** > **RADIUS** > **Users** to open the **AAA Users** page.

Step 2 In the **User Name** text box, enter the username.
For name, specify the user ID as one word. Spaces and quotation marks are not allowed.

Step 3 In the **Privilege** drop-down list, choose the privilege level the user has after gaining access.
The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access. For encryption-type, enter 0 to specify that an unencrypted password. Enter 7 to specify that a hidden password follows.

Step 4 In the **Password** text box, enter the password the user must enter to gain access to the controller.
The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.

Step 5 In the **Confirm Password** text box, enter the password again.

Step 6 In the **Type** drop-down list, choose the type of user, for example, **network-user**.

Step 7 Check the **Guest User** checkbox.

Step 8 Check the **Set Validity** checkbox (optional).

Step 9 From the **Lifetime** drop-down list, choose the validity period of the user (optional).

Step 10 Click **Apply** to save the configuration.

Configuring a Parameter Map for Local Web Authentication (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **parameter-map type webauth global**
3. **banner** {*file* | *text*}
4. **custom-page**
5. **max-http-conns**
6. **intercept-https-enable**
7. **ratelimit**
8. **redirect**
9. **timeout**
10. **watch-list**
11. **virtual-ip ipv4** *virtual -IP-address*
12. **exit**
13. **no**
14. **parameter-map type webauth** *name* **type** *webauth test*
15. **banner** *bannet-text*
16. **consent email**
17. **custom-page**
18. **max-http-conns**
19. **redirect**
20. **timeout**
21. **type**
22. **exit**
23. **no**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `ControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**parameter-map type webauth global** **Example:** `ControllerDevice(config)# parameter-map type webauth global`	Creates a parameter map and enters parameter-map webauth configuration mode. The specific configuration commands supported for a global parameter map defined with the global keyword differ from the commands supported for a named parameter map defined with the parameter-map-name argument.

Step 3	**banner** {*file* | *text*}
	Example:
	`ControllerDevice(config-params-parameter-map)# banner`
		Displays a banner on the local web-authentication login web page.

Step 4	**custom-page** **Example:** `ControllerDevice(config-params-parameter-map)# custom-page`	Specifies the custom page such as login, expired, success, or failure page.
Step 5	**max-http-conns** **Example:** `ControllerDevice(config-params-parameter-map)# max-http-conns`	Specifies the maximum number of HTTP connections per clients.
Step 6	**intercept-https-enable** **Example:** `ControllerDevice(config-params-parameter-map)# intercept-https-enable`	Specifies to enable intercept of HTTPS traffic.
Step 7	**ratelimit** **Example:** `ControllerDevice(config-params-parameter-map)# ratelimit`	Specifies to rate limit on the number of web authentication sessions.
Step 8	**redirect** **Example:** `ControllerDevice(config-params-parameter-map)# redirect`	Specifies to redirect the URL.
Step 9	**timeout** **Example:** `ControllerDevice(config-params-parameter-map)# timeout`	Specifies to timeout for the initial state of web authentication.

	Command or Action	Purpose
Step 10	**watch-list** **Example:** `ControllerDevice(config-params-parameter-map)#` **`watch-list`**	Specifies the watch list of web authentication clients.
Step 11	**virtual-ip ipv4** *virtual -IP-address* **Example:** `ControllerDevice(config-params-parameter-map)#` **`virtual-ip ipv4 172.16.16.16`**	(Optional) Specifies a virtual IP address for web-based authentication clients. This command is supported in the global parameter map only.
Step 12	**exit** **Example:** `ControllerDevice(config-params-parameter-map)#` **`exit`**	Specifies to exit from **parameter-map params** configuration mode.
Step 13	**no** **Example:** `ControllerDevice(config-params-parameter-map)#` **`no`**	Specifies to negate a command or set its defaults.
Step 14	**parameter-map type webauth** *name* **type** *webauth test* **Example:** `ControllerDevice(config)#` **`parameter-map type webauth user1 type webauth test`**	Specifies parameter map user-defined name for local web-based authentication clients. This command is supported in the global parameter map only.
Step 15	**banner** *bannet-text* **Example:** `ControllerDevice(config-params-parameter-map)#` **`banner`**	(Optional) Displays a banner on the local web-authentication login web page.
Step 16	**consent email** **Example:** `ControllerDevice(config-params-parameter-map)#` **`consent email`**	(Optional) Requests a user's e-mail address on the local web-authentication login web page. This command is supported in named parameter maps only.
Step 17	**custom-page** **Example:** `ControllerDevice(config-params-parameter-map)#` **`custom-page`**	Specifies the custom page such as login, expired, success, or failure page.
Step 18	**max-http-conns** **Example:** `ControllerDevice(config-params-parameter-map)#` **`max-http-conns`**	Specifies the maximum number of HTTP connections per clients.

	Command or Action	Purpose
Step 19	**redirect** **Example:** `ControllerDevice(config-params-parameter-map)# redirect`	Specifies to redirect the URL.
Step 20	**timeout** **Example:** `ControllerDevice(config-params-parameter-map)# timeout`	Specifies to timeout for the initial state of web authentication.
Step 21	**type** **Example:** `ControllerDevice(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16`	(Optional) Specifies the parameter type such as web authentication or consent, or both.
Step 22	**exit** **Example:** `ControllerDevice(config-params-parameter-map)# exit`	Specifies to exit from **parameter-map params** configuration mode.
Step 23	**no** **Example:** `ControllerDevice(config-params-parameter-map)# no`	Specifies to negate a command or set its defaults.

Configuring a Parameter Map and Method List for Local Web Authentication (GUI)

Step 1 Create a global parameter map:

a) Choose **Configuration** > **Security** > **Web Auth** > **Webauth Parameter Map** to open the **Webauth Parameter Map** page.
b) Click the **global** parameter map.
c) In the **Virtual IPv4 Address** text box, enter the virtual IPv4 address.
d) Click **Apply** to save the configuration.

Step 2 Create a new parameter map:

a) Choose **Configuration** > **Security** > **Web Auth** > **Webauth Parameter Map** to open the **Webauth Parameter Map** page.
b) Click **New** to open the **Webauth Parameter Map** page.
c) In the **Parameter-map name**, enter the name for the parameter map.

d) From the **Type - web-auth, consent or both**, choose **webauth**.
e) Click **Apply** to save the configuration.

Step 3 Create authentication method list for local users for local authentication:

a) Choose **Configuration** > **Security** > **AAA** > **Method Lists** > **Authentication** to open the **Authentication** page.
b) Click **New** to open the **Authentication > New** page.
c) In the **Method List name** text box, enter the name for new method list, for example, **local_webauth** for AAA server.
d) In the **Type** field, choose **network**.
e) In the **Group Type** field, choose **local**.
f) Click **Apply** to save the configuration.

Step 4 Create authentication method list for RADIUS authentication:

a) Choose **Configuration** > **Security** > **AAA** > **Method Lists** > **Authentication** to open the **Authentication** page.
b) Click **New** to open the **Authentication > New** page.
c) In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for radius authentication.
d) In the **Type** field, choose **login**.
e) In the **Group Type** field, choose **group**.
f) In the **Groups In This Method** section, select the RADIUS server group, and move it from the **Available Server Groups** area to the **Assigned Server Groups** area.
g) Click **Apply** to save the configuration.

Step 5 Create authorization method list for local users:

a) Choose **Configuration** > **Security** > **AAA** > **Method Lists** > **Authorization** to open the **Authorization** page.
b) Click **New** to open the **Authoriztion > New** page.
c) In the **Method List name** text box, enter the name for new method list, for example, **local_webauth**.
d) In the **Type** field, choose **network**.
e) In the **Group Type** field, choose **local**.
f) Click **Apply** to save the configuration.

Step 6 Create another authorization method list for local authentication:

a) Choose **Configuration** > **Security** > **AAA** > **Method Lists** > **Authorization** to open the **Authorization** page.
b) Click **New** to open the **Authoriztion > New** page.
c) In the **Method List name** text box, enter **default**.
d) In the **Type** field, choose **credential-download**.
e) In the **Group Type** field, choose **local**.
f) Click **Apply** to save the configuration.
g) The **Authorization** page lists the method lists that include default and local web_auth method lists.

Step 7 Create authorization method list for RADIUS authentication:

a) Choose **Configuration** > **Security** > **AAA** > **Method Lists** > **Authorization** to open the **Authorization** page.
b) Click **New** to open the **Authentication > New** page.
c) In the **Method List name** text box, enter the name for new method list, for example, **webauth_radius** for radius authentication.
d) In the **Type** field, choose **network**.
e) In the **Group Type** field, choose **group**.
f) In the **Groups In This Method** section, select the RADIUS server group, and move it from the **Available Server Groups** area to the **Assigned Server Groups** area.

g) Click **Apply** to save the configuration.

Configuring Local Web Authentication on a WLAN (CLI)

SUMMARY STEPS

1. **configure terminal**
2. **wlan** *wlan-name wlan-id ssid/network-name*
3. **client vlan** *vlan-name vlan-id/vlan-name*
4. **no security wpa**
5. **no security wpa akm dot1x**
6. **no security wpa wpa2**
7. **no security wpa wpa2 ciphers aes**
8. **security web-auth**
9. **security web-auth authentication-list** *authentication-list-name*
10. **security web-auth parameter-map** *parameter-map name*
11. **session-timeout** *seconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `ControllerDevice# configure terminal`	Enters global configuration mode.
Step 2	**wlan** *wlan-name wlan-id ssid/network-name* **Example:** `ControllerDevice(config)# wlan user_webauth 7 user_webauth`	Configures WLAN network.
Step 3	**client vlan** *vlan-name vlan-id/vlan-name* **Example:** `ControllerDevice(config-wlan)# client vlan user1`	Enters into VLAN configuration mode.
Step 4	**no security wpa** **Example:** `ControllerDevice(config-wlan)# no security wpa`	Disables WPA or WPA2 support for a WLAN.

	Command or Action	Purpose
Step 5	**no security wpa akm dot1x** **Example:** `ControllerDevice(config-wlan)# no security wpa akm dot1x`	Disables WPA or WPA2 auth key management 802.1x support for a WLAN.
Step 6	**no security wpa wpa2** **Example:** `ControllerDevice(config-wlan)# no security wpa wpa2`	Disables WPA2 support for a WLAN.
Step 7	**no security wpa wpa2 ciphers aes** **Example:** `ControllerDevice(config-wlan)# no security wpa wpa2 ciphers aes`	Disables WPA2 ciphers for a WLAN.
Step 8	**security web-auth** **Example:** `ControllerDevice(config-wlan)#  security web-auth`	Sets the SSID to security web authentication.

Step 9	**security web-auth authentication-list** *authentication-list-name*
	Example:
	`Local web Auth using AAA Server:`
	`ControllerDevice(config-wlan)# security web-auth authentication-list local_webauth`
	`Local web Auth using RADIUS Server:`
	`ControllerDevice(config-wlan)# security web-auth authentication-list webauth_radius`
		Allows you to map the authentication list name from AAA server or RADIUS server within a WLAN.

Step 10	**security web-auth parameter-map** *parameter-map name*
	Example:
	`Using Parameter map from AAA server:`
	`ControllerDevice(config-wlan)# security web-auth parameter-map vit_web`
	`Using Parameter map from RADIUS server:`
	`ControllerDevice(config-wlan)# security web-auth parameter-map webauth_radius`
		Allows you to map the parameter-map name with the web-auth WLAN.

Step 11	**session-timeout** *seconds* **Example:** `ControllerDevice(config-wlan)# session-timeout 1800`	Configures session timeout for clients associated to a WLAN. A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400.

Configuring Local Web Authentication on a WLAN (GUI)

Step 1 Choose **Configuration** > **WLANs** > **New** to open the **WLAN > New** page.

Step 2 Choose **Security** > **Layer 3** in the **WLAN > Edit** page.

Step 3 Check the **Web Policy** checkbox.

Step 4 In the **Webauth Profile** text box, enter the name of the web auth profile, for example, local_webauth or webauth_radius.

Step 5 From the **Webauth Parameter Map** drop-down list, choose the web auth parameter you have created, for example, **test_web**.

Step 6 Click **Apply** to save the configuration.

Note Do not configure the AAA server.

Step 7 Choose **Monitor** > **Clients** to open the **Clients > Detail** page to view the client details for an authenticated user.

Monitoring Local Web Authentication

The following commands can be used to monitor local web authentication configured on the controller.

Table 1: Monitoring Local Web Authentication Command

Command	Purpose
show running-config aaa	Displays the AAA configuration in the running configuration.
show run | section parameter	Displays the section parameter details in the running configuration.
show wireless client mac-address *mac-address* **detail**	Displays detailed information of wireless client based on its MAC address.

Examples: Local Web Authentication Configuration

This example shows how to configure local web authentication for local net users using AAA:

```
ControllerDevice# config terminal
ControllerDevice(config)# aaa authentication login local_webauth local
ControllerDevice(config)# aaa authorization network local_webauth local
ControllerDevice(config)# aaa authorization credential-download default local
ControllerDevice(config)# end
ControllerDevice# show run aaa
```

This example shows how to configure local web authentication for local net users using RADIUS server:

```
ControllerDevice# config terminal
ControllerDevice(config)# aaa authentication login webauth_radius group ISE_group
ControllerDevice(config)# aaa authorization network webauth_radius group ISE_group
ControllerDevice(config)# aaa group server radius ISE_Group
ControllerDevice(config)# radius server ISE
ControllerDevice(config-radius-server)# address ipv4 192.168.154.119 auth-port 1812 acct-port
 1813
ControllerDevice(config-radius-server)# key ww-wireless
ControllerDevice(config-radius-server)# end
ControllerDevice# show run aaa
```

This example shows how to configure guest users for local web authentication:

```
ControllerDevice# config terminal
ControllerDevice(config)# user-name viten_webauth creation-time 1368715259 privilege 15
password 0 test12345
ControllerDevice(config)# end
```

This example shows how to configure parameter map for local web authentication using AAA:

```
ControllerDevice# config terminal
ControllerDevice(config)# parameter-map type webauth global
ControllerDevice(config-params-parameter-map)# virtual-ip ipv4 172.16.16.16
ControllerDevice(config-params-parameter-map)# parameter-map type webauth user1 type webauth
 test
ControllerDevice(config-params-parameter-map)# banner
ControllerDevice(config-params-parameter-map)# end
ControllerDevice# show run aaa
```

This example shows how to configure local web authentication on a WLAN using AAA:

```
ControllerDevice# config terminal
ControllerDevice(config)# wlan user_webauth 7 user_webauth
ControllerDevice(config-wlan)# client vlan user1
ControllerDevice(config-wlan)# no security wpa
ControllerDevice(config-wlan)# no security wpa akm dot1x
ControllerDevice(config-wlan)# no security wpa wpa2
ControllerDevice(config-wlan)# no security wpa wpa2 ciphers aes
ControllerDevice(config-wlan)# security web-auth
ControllerDevice(config-wlan)# security web-auth authentication-list local_webauth
ControllerDevice(config-wlan)# security web-auth parameter-map vit_web
ControllerDevice(config-wlan)# session-timeout 1800
ControllerDevice(config-wlan)# end
ControllerDevice# show run aaa
```

This example shows how to configure local web authentication on a WLAN using RADIUS server:

```
ControllerDevice# config terminal
ControllerDevice(config)# wlan user_webauth 7 user_webauth
ControllerDevice(config-wlan)# client vlan user1
ControllerDevice(config-wlan)# no security wpa
ControllerDevice(config-wlan)# no security wpa akm dot1x
ControllerDevice(config-wlan)# no security wpa wpa2
ControllerDevice(config-wlan)# no security wpa wpa2 ciphers aes
ControllerDevice(config-wlan)# security web-auth
ControllerDevice(config-wlan)# security web-auth authentication-list webauth_radius
ControllerDevice(config-wlan)# security web-auth parameter-map webauth_radius
ControllerDevice(config-wlan)# session-timeout 1800
ControllerDevice(config-wlan)# end
ControllerDevice# show run aaa
```

Additional References for Configuring the Local Web Authentication Configuration

Related Documents

Related Topic	Document Title
Security commands	*Security Command Reference Guide, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*
Local web authentication configuration example	*WLC 5760/3850 Custom WebAuth with Local Authentication Configuration Example*

Standards and RFCs

Standard/RFC	Title
None	—

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature History for Performing Local Web Authentication Configuration

Release	Feature Information
Cisco IOS XE 3.3SE	This feature was introduced.