Local Web Authentication on Converged Access

This document provides information about the global configuration commands that enable the local web authentication on a Wireless LAN controller (WLC). The document also provides information on WLAN configuration commands and global parameter maps.

List of Global Configuration Commands

Use the following commands to enable the local web authentication on the WLC:

Command or Action	Description/Purpose/Example
aaa new-model	Enables the authentication, authorization, and accounting (AAA) access control model.
aaa authentication login *wcm_local* **local**	'wcm_local' is a method which you call under WLAN.
aaa authorization network default *local*	The default authorization is set to local.
aaa authorization credential-download default *local*	Configures the local database to download Extensible Authentication Protocol (EAP) credentials. **Note** You can use **Local. aaa authorization credential-download** command family to download credentials from RADIUS or Lightweight Directory Access Protocol (LDAP).
usernametest **password** *0 test12345*	Enables you to test the username and password for local authentication.

Command or Action	Description/Purpose/Example
parameter-map type webauth global virtual -IP ipv4 192.0.2.1	Enables you to configure the virtual IP address which is required for external and internal Web Authentication. The **Logout** button uses virtual IP Central Web Authentication (CWA). However, it is not mandatory for the **Logout** button to have a virtual IP.
parameter-map type webauth *test_web* • type webauth • Banner c test webauth c	It is a web authentication method in which you need to specify a name to call the web authentication method under the WLAN configuration.
ip http server	Enables the http server. It is required for HTTPS authentication.
ip http authentication local	Log in to GUI using the local authentication.
ip http secure-server	Enables you to access secure web authentication. **Note** To disable secure web authentication, use **no ip http secure-server** command.

Information about Parameter Maps

Global Parameter Maps

Use the following commands to configure the Global Parameter Maps:

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# ?
```

Use the following commands to configure the pre-parameter map for global parameter maps:

Command or Action	Description/Purpose/Example
Banner	Adds extra text on the pages that are generated.
custom-page	Designs login, expired, success, or failure pages that the user can download on the system flash.
Exit	Exits from the parameter map configuration mode.
max-http-conns	Configures maximum number of http connections for each client. It can be configured from 1 to 200, with 20 as the default value.

Command or Action	Description/Purpose/Example
No	Disables a function or to set a default value.
Redirect url	Provides the user with a custom designed page on an external server.
Timeout	Configures an initial timeout session for a user to complete authentication.
Virtual IP	Required for logout page and for external web authentication.
Watch-list	Creates a watch list for the web authentication clients. This is not required for wireless clients.

User Defined Parameter Maps

Use the following commands to configure the User Defined Parameter Maps:

```
Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# ?
```

Use the following commands to configure the pre-parameter map for user defined parameter maps:

Command or Action	Description/Purpose/Example
Banner	Adds extra text on the pages that are generated.
Consent	Displays the terms and conditions that the user needs to accept to enable access.
custom-page	Designs login, expired, success, or failure pages that the user can download on the system flash.
Exit	Exits from the parameter map configuration mode.
max-http-conns	Configures maximum number of http connections for each client. It can be configured from 1 to 200, with 20 as the default value.
No	Disables a function or to set a default value.
Redirect url	Provides the user with a custom designed page on an external server.
Timeout	Configures an initial timeout session for a user to complete authentication.

Command or Action	Description/Purpose/Example
Type	Configures the type of parameter, such as, web authentication, consent, or web consent.

Additional Information on Parameter Maps

The following information is applicable to parameter maps:

- If the parameter-map name that is configured on the WLAN is not valid, global parameter-map configuration is used.
- If user defined parameter name exists, its values are merged with the values that are configured for the global parameter-map. If user defined parameter and global parameters have values configured for a particular field, the user defined parameter map values are used.
- Some of the parameter-map fields such as, ratelimit, needs to be removed from the configuration.
- For custom-pages, the files for login, success, failure, expired needs to be provided before the pages are used.
- If the custom pages are configured, then any banner configuration for the page is ignored.
- Virtual IP address should be configured if web authentication logout page is required or if the external web authentication is done for the logout page.
- The Authentication Bypass functionality is not supported for wireless clients.

WLAN Configuration Commands

Use the following commands to configure WLAN:

```
wlan webauth 11 local_webauth
 client vlan 263                                          -----> client vlan. clients get ip
 from vlan 263
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth                                         ------> set wlan security to
web-auth
 security web-auth authentication-list wcm_local          -------> call the authentication
method from global configuration
 security web-auth parameter-map test_web                 --------> call the webauth method
 type from global configuration
```

Troubleshooting the Configuration

The Access Control Lists are applied to the HTTP server. If web authentication fails to load, verify the following:

```
ip http access-class ##
```