WebAuth Bundle for Cisco IOS XE Version 3.6.0 for Cisco WLC 5760 and Catalyst 3850 Series Readme

7/2/2014

This document supports the release of WebAuth bundle, which can be installed along with the Cisco IOS XE Version 3.6.0 for the Cisco WLC 5760 and Catalyst 3850 series.

1 Contents

1 Contents 1

2 Prerequisites for WebAuth Testing 2

3 WebAuth Configuration 2

3.1 Local WebAuth using Local User Database 2
3.1.1 Local WebAuth – Local Net Users 2

3.2 Local WebAuth Configuration Example (Using CLI) 9

3.3 Local WebAuth Using RADIUS Authentication 10

3.4 Additional Information on Parameter-Maps 14

3.5 Custom Local WebAuth Configuration Example 15

3.6 Custom External WebAuth Configuration Example 17

3.7 Local Webauth – Caveats 23

3.8 Useful debugs and show commands 23

3.9 WebAuth Logout 23
3.9.1 Login Page 24
3.9.2 Success-Logout Page 24

3.10 WebAuth Custom HTML Pages 25
3.10.1 Custom Consent Parameter-Map Configuration Example 25

3.11 WebAuth Custom Pages on External Server 26
3.11.1 External WebAuth with Custom Consent Page with Email Option 26

3.12 Downloading Web Authentication Tar Bundle 26
3.12.1 Downloading Web Authentication Tar Bundle (CLI) 26
3.12.2 Downloading Web Authentication Tar Bundle (GUI 27
3.12.3 Integrating Customized Web Authentication Pages into a Parameter Map (CLI) 29
3.12.4 Linking Image in Custom Pages 30
3.12.5 WebAuth Page Behavior When Upgraded from CiscoIOS XE Version 3.3 to 3.6 31

4 How to Use WebAuth Bundle 31

5 Obtaining Documentation, Obtaining Support, and Security Guidelines 31

2 Prerequisites for WebAuth Testing

Before You Begin

Before configuring and customizing Webauth, please ensure the following conditions are fulfilled:

1. Your Personal Computer (PC) gets an IP address on an open SSID
2. Your PC is able to ping the default gateway
3. Your PC identifies and locates the DNS-server (ipconfig/all)
4. Your PC is able to resolve names (with `nslookup <variable name>`)
5. Your PC is able to access the internet

Note

- To force the Webauth user to re-authenticate during testing from the CLI, enter the following command:
  `show wireless client summary`
  `wireless client mac-address <mac> deauthenticate`
- To force the Webauth user to re-authenticate during testing from the GUI, navigate to: **Monitor > Clients > Choose client > Remove**
  - The MAC address of the user is visible on the PC (ipconfig/all) and depending on the connection, in the WLC GUI (**monitor > clients**) or in the **`show client summary`** command from WLC CLI.

3 WebAuth Configuration

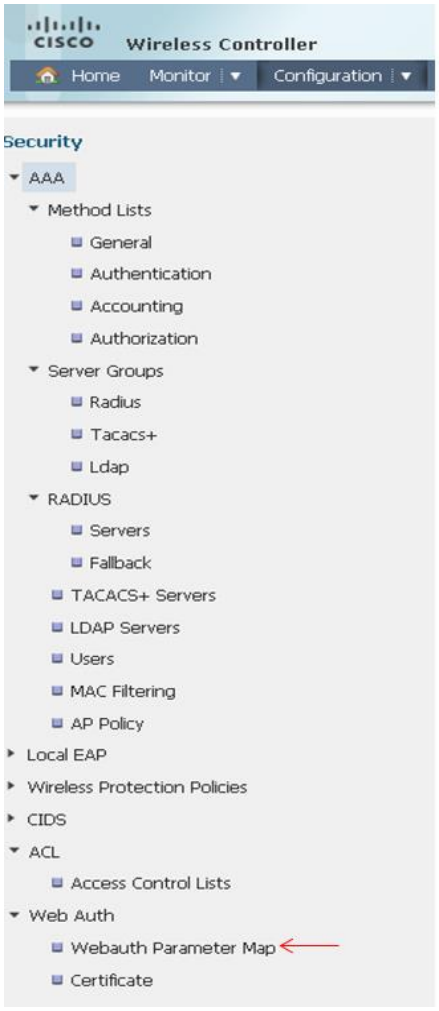
3.1 Local WebAuth using Local User Database

3.1.1 Local WebAuth – Local Net Users

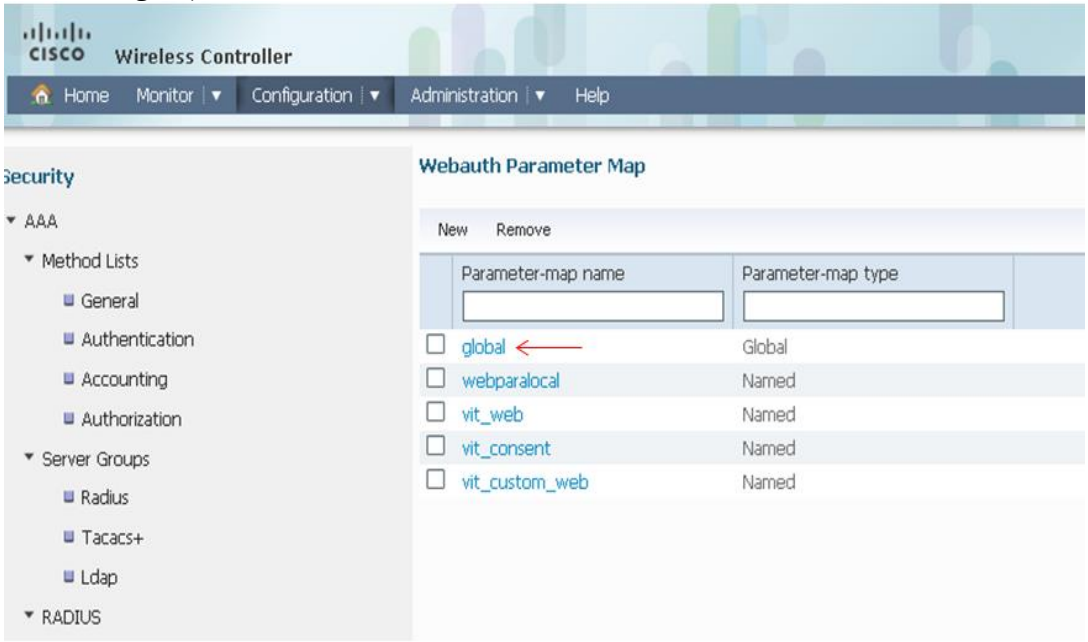
Using GUI

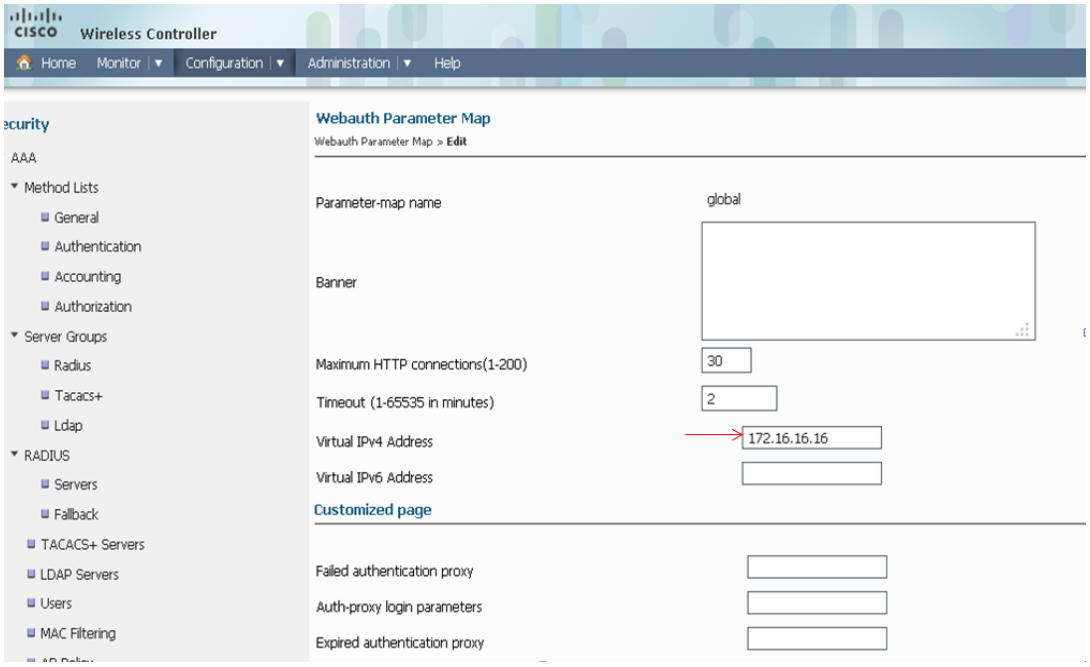
To define the Global Parameter Map where the virtual IP address is defined, complete these steps:

Step 1: Navigate to **Configuration > Security > Web Auth > Webauth Parameter Map**

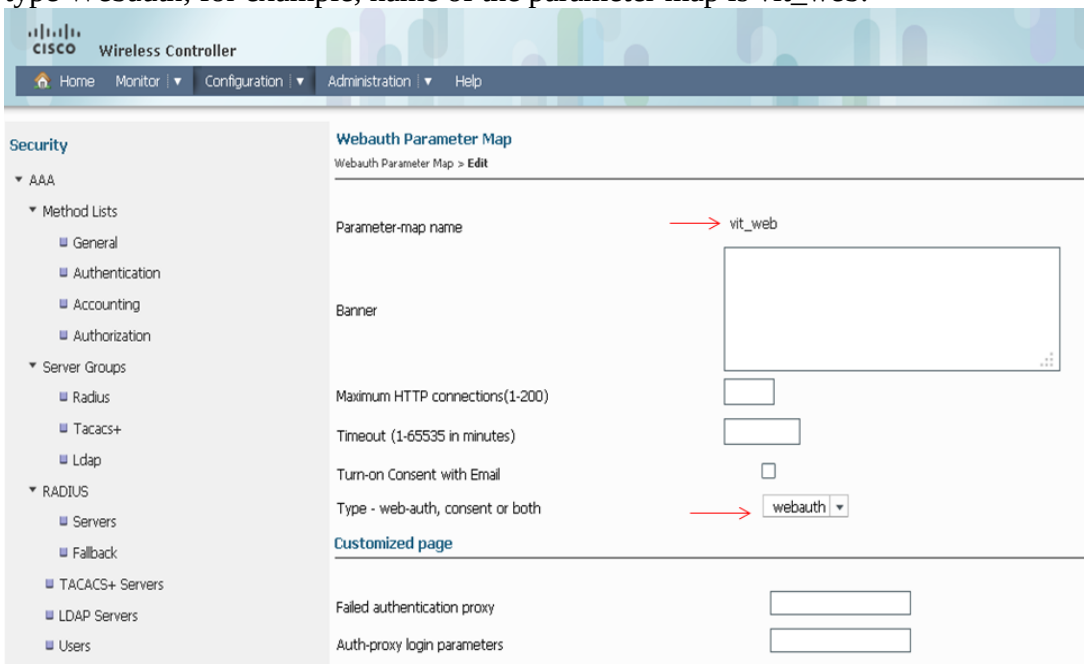


Step 2: Click the **global** parameter map and define the virtual IPv4 address (described in the next figure).

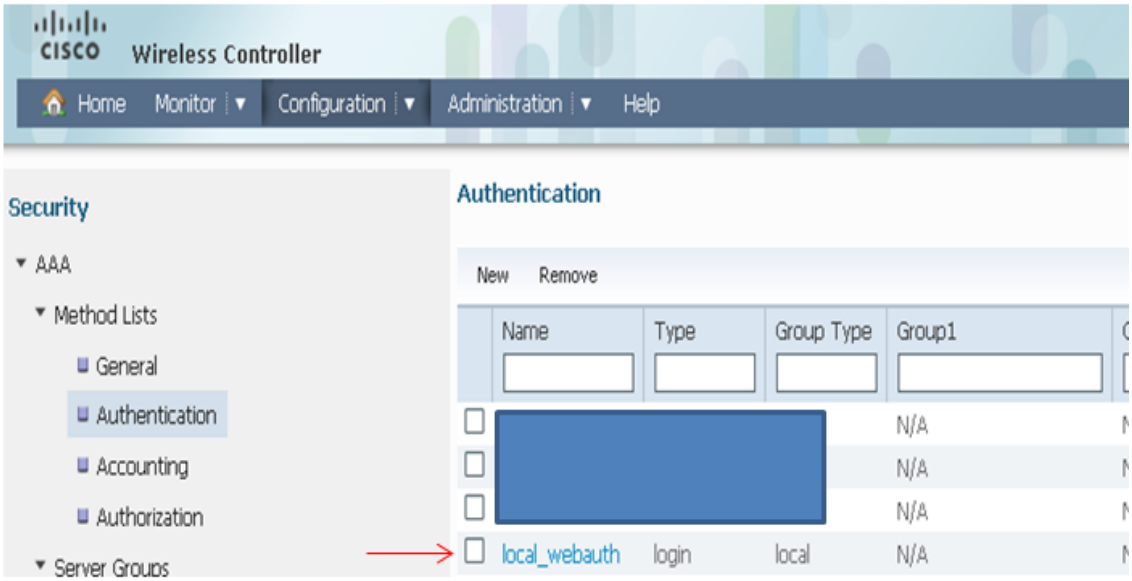




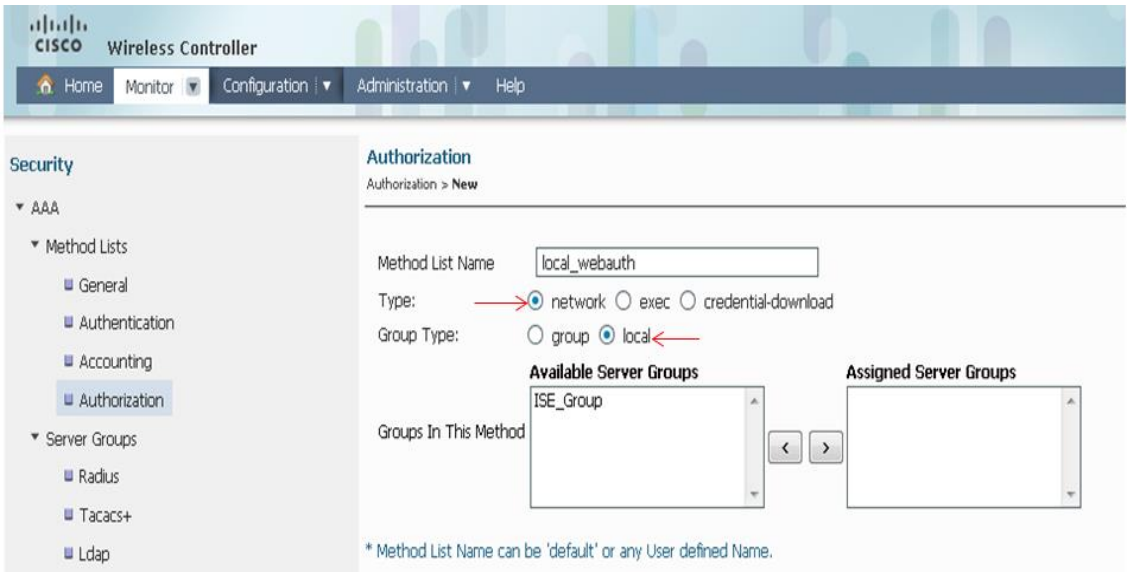
Step 3: Navigate back to the Parameter map tab and create a new parameter map of type Webauth; for example, name of the parameter map is vit_web.



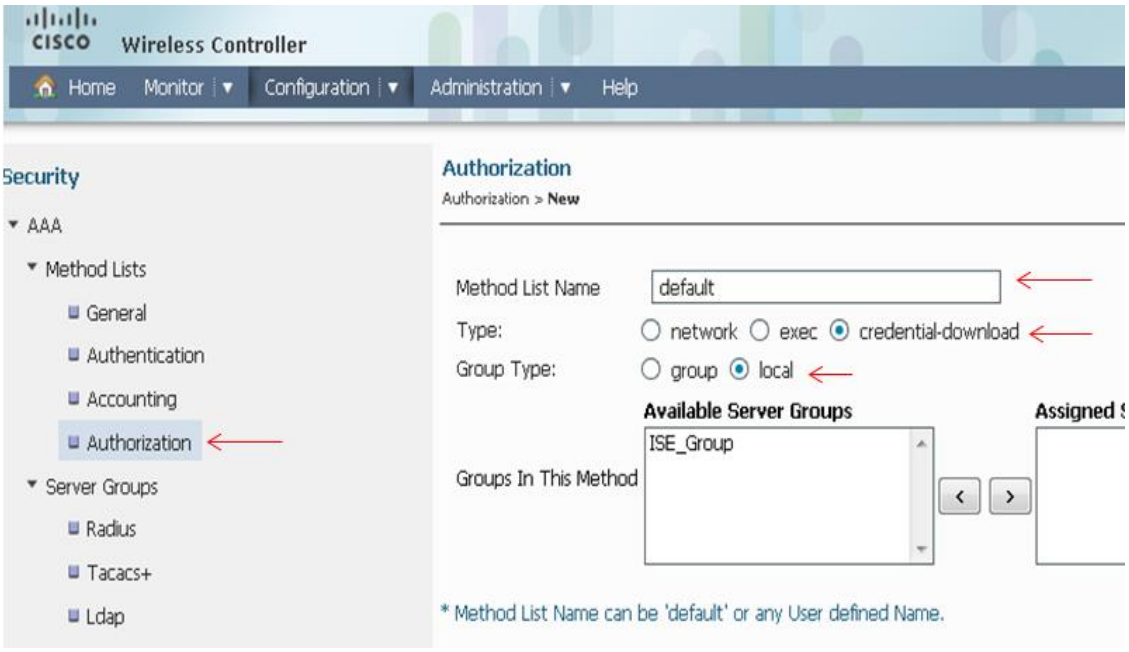
Step 4: Create a method list for local authentication and authorization; for example, local_webauth.



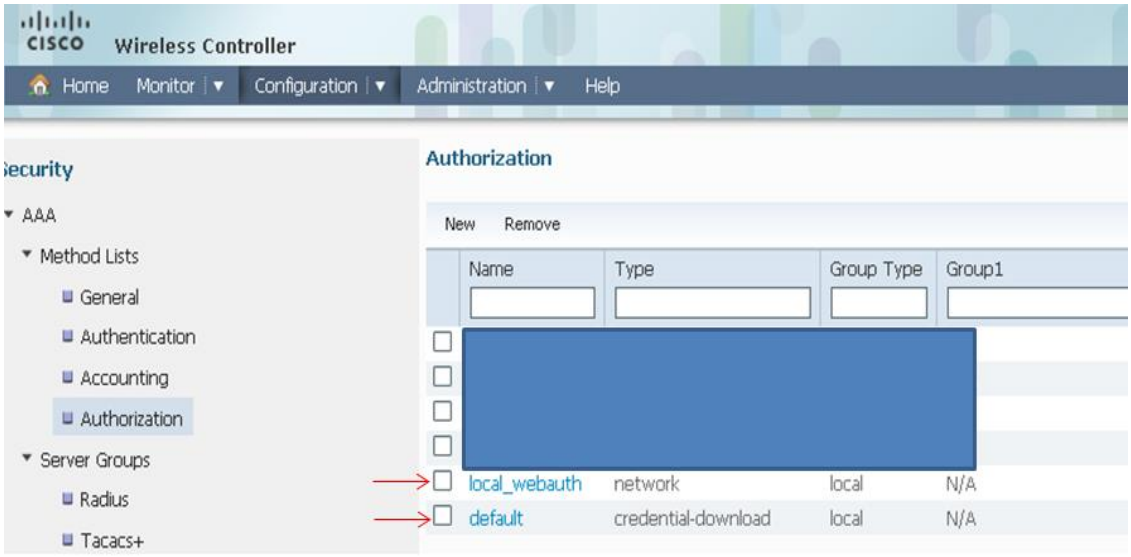
Step 5: For the authorization method list, create a new method list named local_webauth. Select **network** for Type and **local** for Group Type**.**



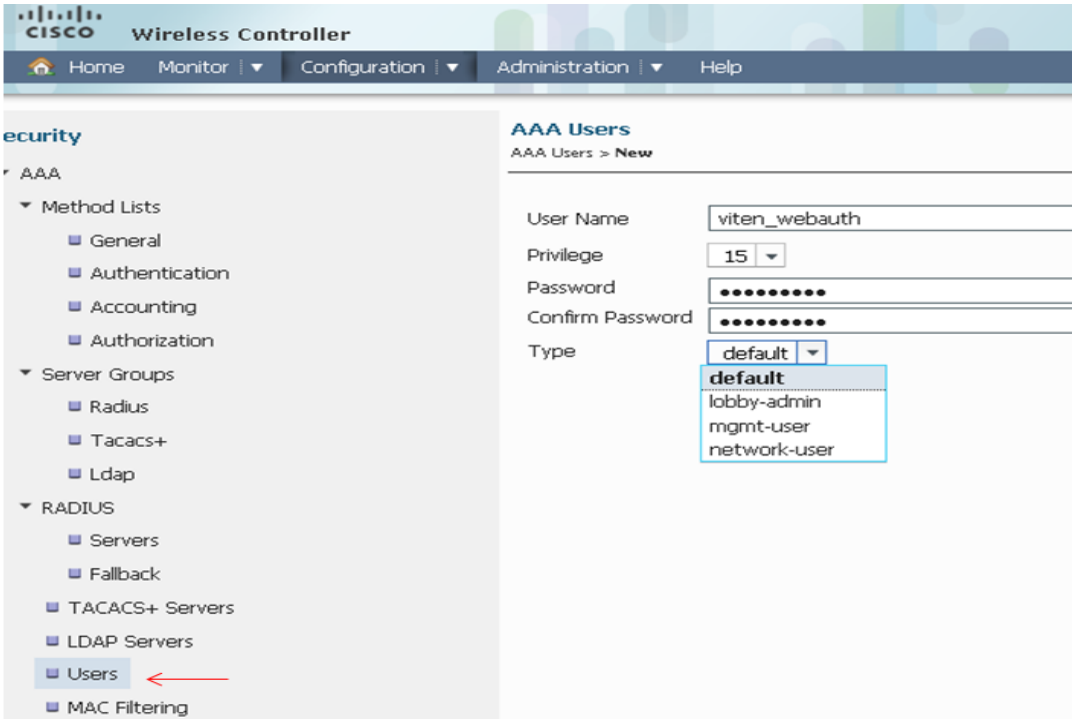
Step 6: You would need another authorization method list for using local net users for authentication. Create a method list called **default**, select **credential-download** as the **Type** and **local** as the **Group Type**.



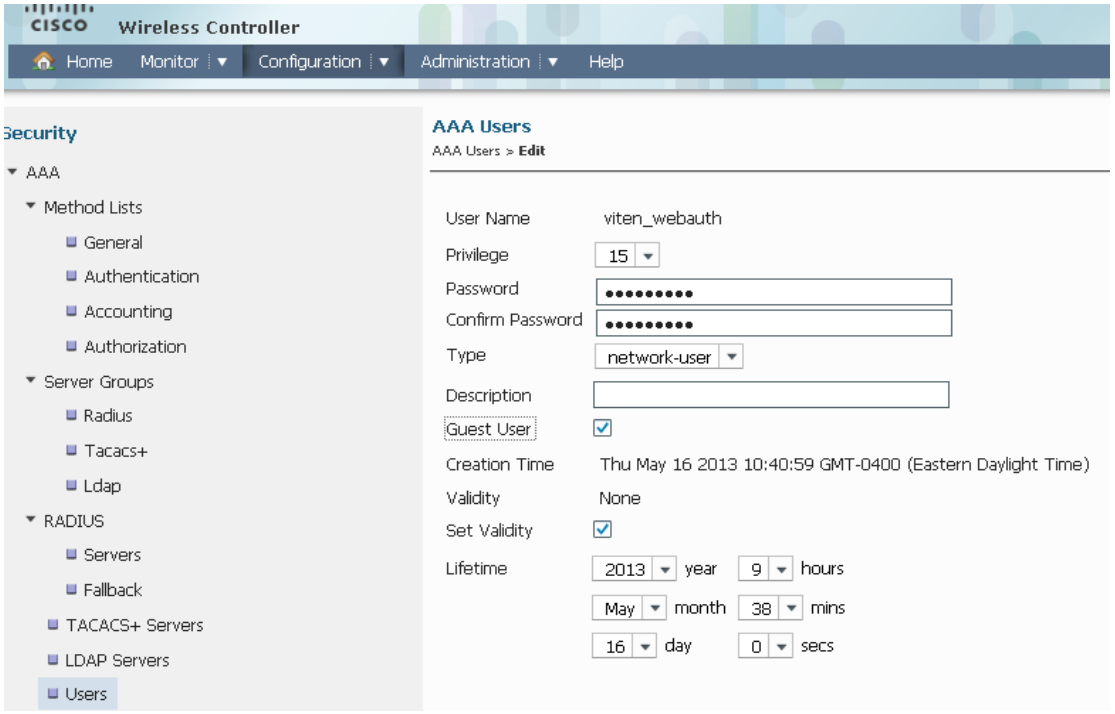
Step 7: The **Authorization** summary page lists the Method List added, in this case — **default** and **local_webauth.**



Step 8: Create local net users by navigating to **Configuration > Security > RADIUS > Users** and enter the **username, privilege, password and type** (example: network-user)



Step 9: When you select the **network-user** as the **Type,** an additional option of **Guest User** is displayed.

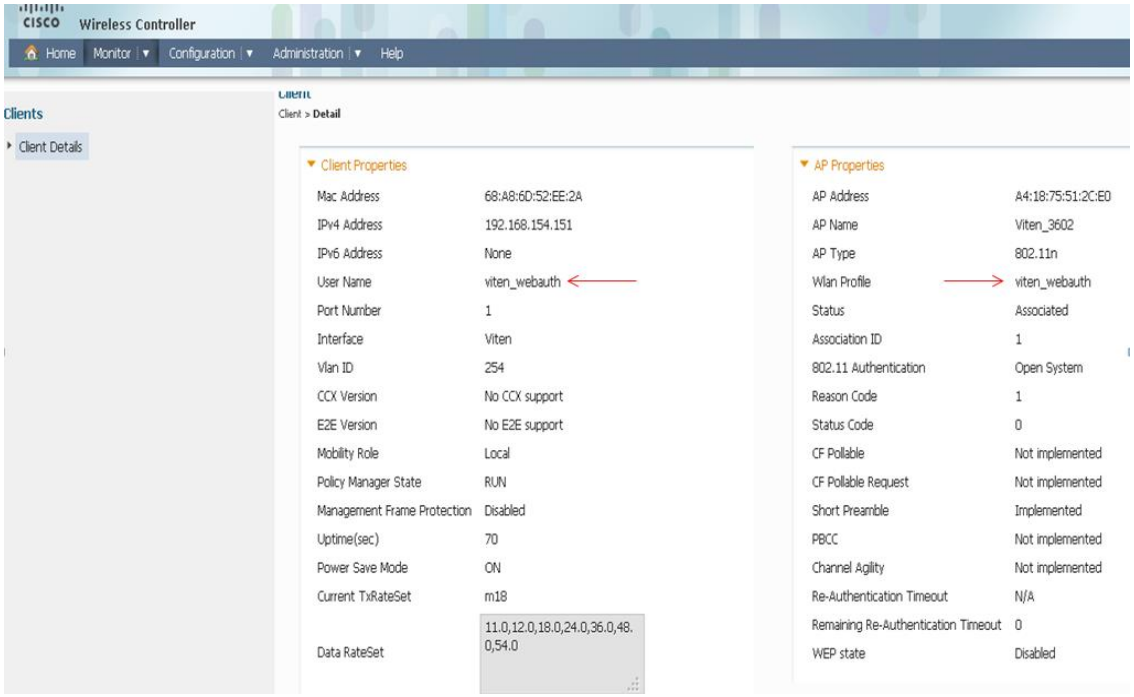


Step 10: Navigate to **Configuration > WLANS > New**

Step 11: Set the interface and enable the WLAN. Navigate to the Security tab and disable Layer 2 security. Navigate to Layer 3 security tab, enable **Web Policy** and enter the name

of the **Webauth Profile** (example: local_webauth) and select the **Webauth Parameter Map** (example: vit_web). Click A**pply**.

Step 12: Navigate to **Client > Detail** to view the client details for an authenticated user.



Configure Http Server

Use the following command to configure Http server:

```
!
ip http server
no ip http secure-server
```

required if https need to be configured

Check/ Enable Other Configuration

Use the following command to check/enable other configuration:

ip device tracking

3.2 Local WebAuth Configuration Example (Using CLI)

- AAA Part
  - **aaa authentication login** *local_webauth* **local**
  - **aaa authorization network** *local_webauth* **local**
  - **aaa authorization network** *default* **local**
  - **aaa authorization credential-download** *default* **local**

Syntax	Description
aaa authentication login *local_webauth* local	Authentication method list for login.
aaa authorization network *local_webauth* local	Authorization method list for the network.
aaa authorization network *default* local	Authorization method list for local user.
aaa authorization credential-download *default* local	Authorization method list for use of local credentials.

- Parameter-Map
  - **parameter-map type webauth** *global*

    virtual-ip ipv4 *172.16.16.16*
  - **parameter-map type webauth** *vit_web*

    type webauth

    banner

Syntax	Description
parameter-map type webauth *global* virtual-ip ipv4 *172.16.16.16*	Global parameter map is used to define the virtual IP address.

`parameter-map type webauth vit_web`
`type webauth`
`banner`
	Named parameter map (example: vit_web) with the Type set as Webauth.

Note

The above example is a simple configuration example. There are other options for the field type such as consent, webconsent and so on.

- WLAN Configuration

```
wlan viten_webauth 7 viten_webauth
 client vlan Viten
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list local_webauth
 security web-auth parameter-map vit_web
 session-timeout 1800
 no shutdown
```

Syntax	Description
`security web-auth`	Set the SSID to security **web-auth**
`security web-auth authentication-list local_webauth`	Call the method list.
`security web-auth parameter-map vit_web`	Call the parameter map.

Note

To add network users to the switch for local authentication, enter 123 as both username and password.

3.3 Local WebAuth Using RADIUS Authentication

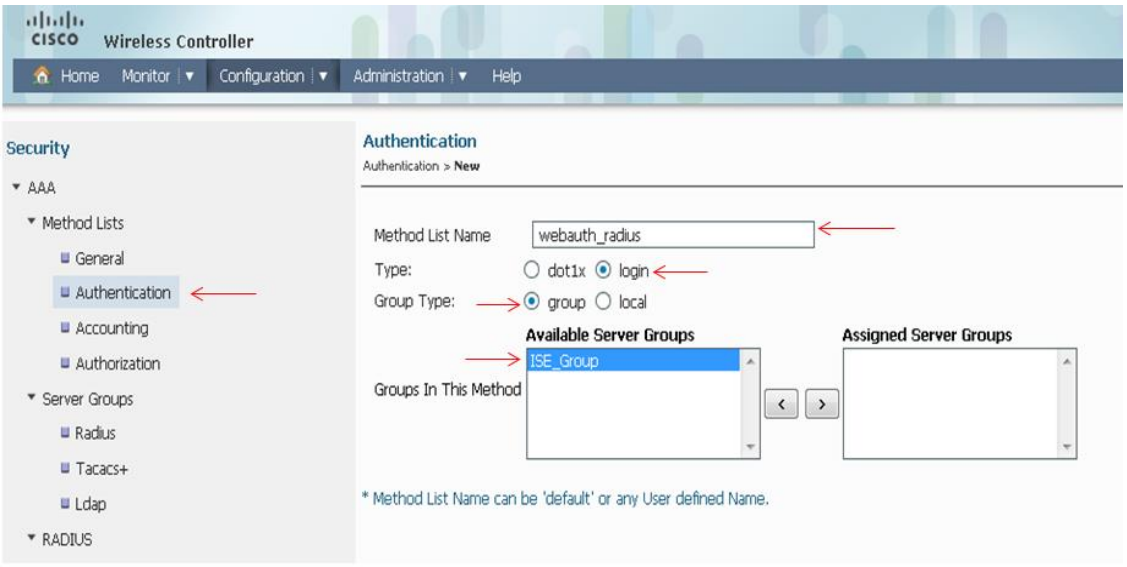
Using GUI

The only difference between the local Webauth, local authentication, and local Webauth using RADIUS authentication is the authentication and authorization method list.

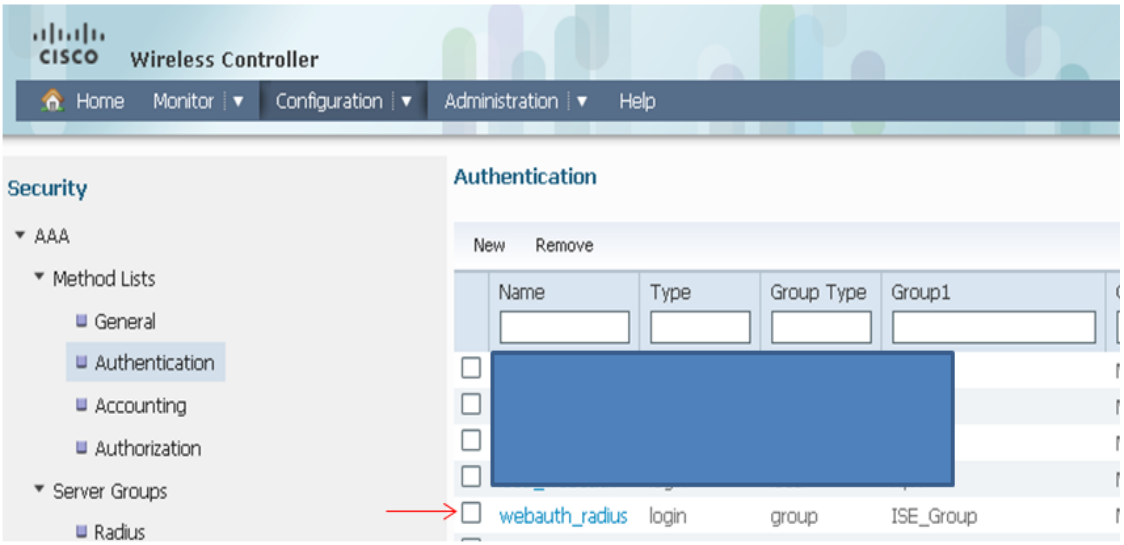
- Create a new authentication method list and point it to the RADIUS server group.
- Create a new authorization method list and point it to the RADIUS server group.

To create a new authentication method list such as webauth_radius, complete these steps:

Step 1: Navigate to **Configuration > Security > AAA > Method List > Authentication > New** and select **login** as the **Type** (which is used for Webauth), and **group** as the **Group Type.** Select the RADIUS server group (example: ISE_Group).

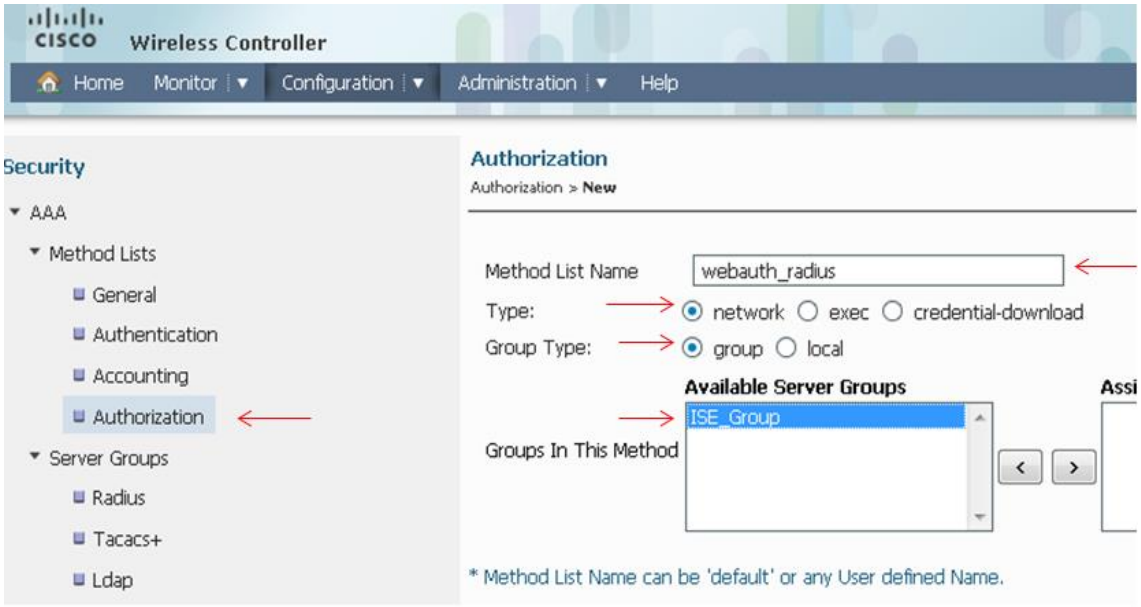


Step 2: You can view the Authentication Method list in the **Authentication** summary page.

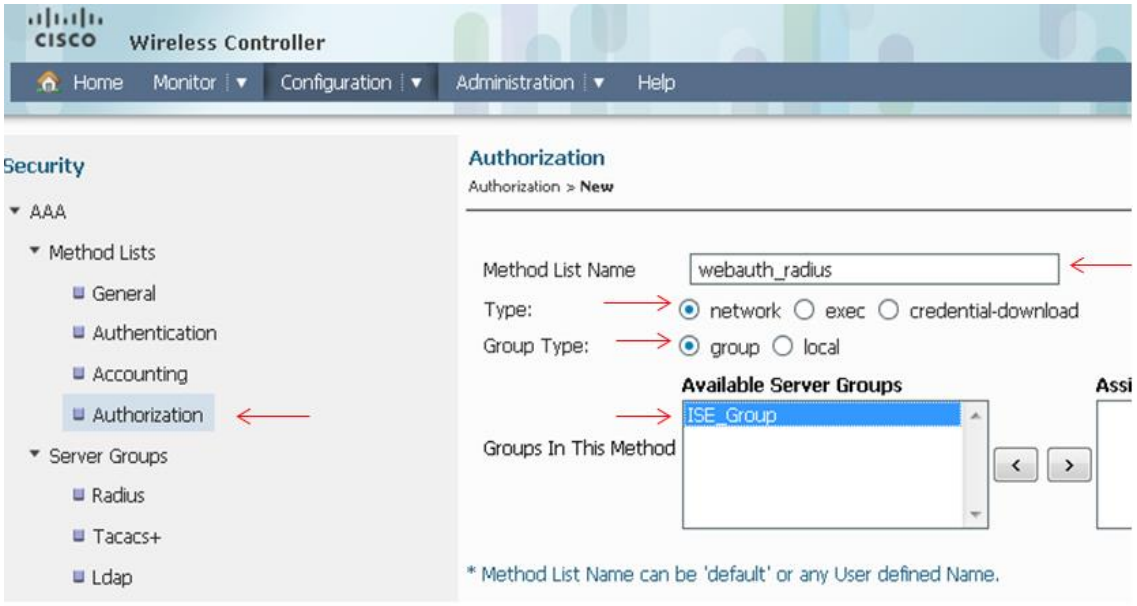


To create a new authorization method list such as webauth_radius, complete these steps:

Step 1: Navigate to **Configuration > Security > AAA > Method List > Authorization > New** and select **network** as the **Type** and **group** as the **Group Type**. Select the RADIUS server group (example: ISE_Group).



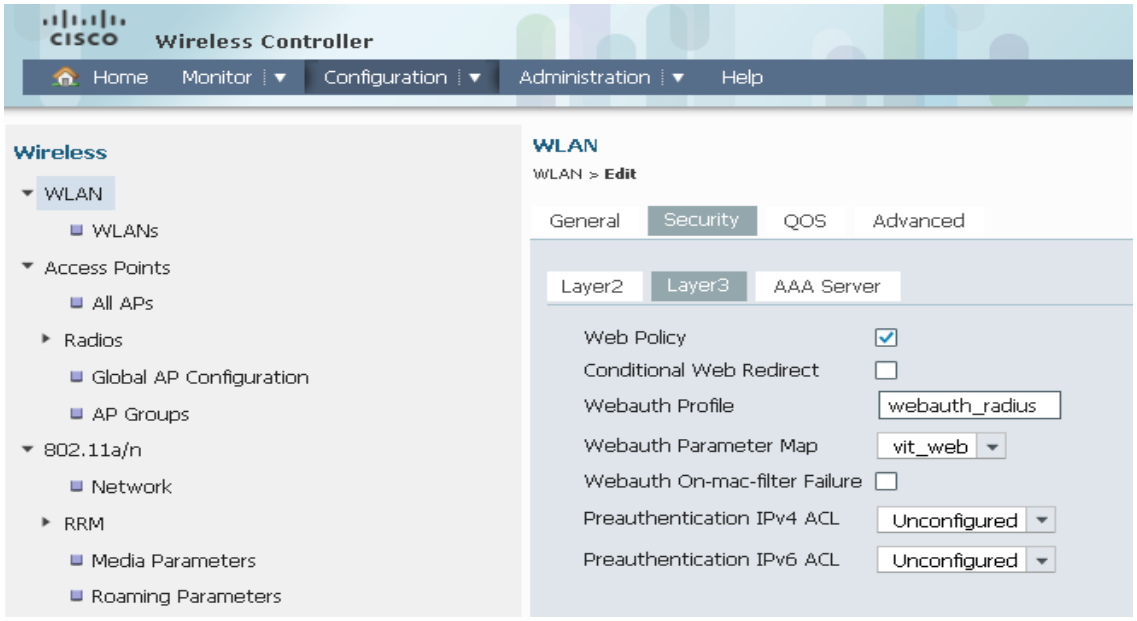
Step 2: You can view the Authorization Method list in the **Authorization** summary page.



WLAN Configuration

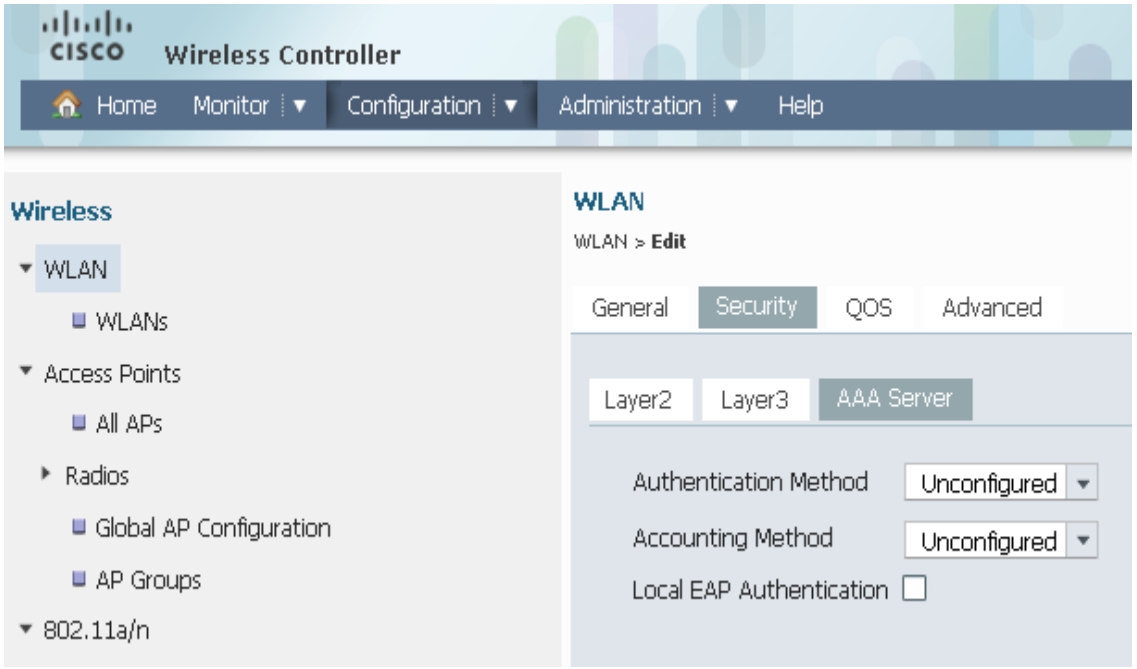
To configure WLAN complete these steps:

Step 1: Select the appropriate Webauth parameter map and enter the method list which uses the RADIUS server group for authentication and authorization (example: webauth_radius)



Note

Leave the AAA server unconfigured.



Using CLI

- AAA part
  - **aaa authentication login** *webauth_radius* **group** *ISE_Group*
  - **aaa authorization network** *webauth_radius* **group** *ISE_Group*
  - **aaa group server radius** *ISE_Group*

    server name ISE
  - **radius server ISE**

    address ipv4 *192.168.154.119* **auth-port 1812 acct-port 1813**

    key ww-wireless

Syntax	Description
`aaa authentication login` *webauth_radius* `group` *ISE_Group*	Authentication method list for the login.
`aaa authorization network` *webauth_radius* `group` *ISE_Group*	Authorization method list for the network.
`aaa group server radius` *ISE_Group*	Radius server group definition.
`server name ISE`	Radius server name.
`radius server ISE`	Defines Radius server **ISE**

3.4 Additional Information on Parameter-Maps

Global Parameter-Map

```
(config)#parameter-map type webauth global

3850(config-params-parameter-map)#?
```

Pre Parameter-Map Params Commands	Description
banner	Banner file or text.
custom-page	Custom-page - login, expired, success or failure page.
exit	Exits from parameter-map params configuration mode.
max-http-conns	Maximum number of HTTP connections per clients.
intercept-https-enable	Enable intercept of https traffic

no	Negates a command or set its defaults.
ratelimit	Rate limit on number of Webauth sessions.
redirect	Redirects the URL.
timeout	Timeout for the initial state of Webauth.
virtual-ip	Virtual IP address.
watch-list	Watch list of Webauth clients.

User Defined Named Parameter-Map

```
3850(config)#parameter-map type webauth test
3850(config-params-parameter-map)#?
```

Pre Parameter-Map Params Commands	**Description**
banner	Banner file or text.
consent	Consent parameters
custom-page	Custom-page - login, expired, success or failure page.
exit	Exits from the parameter-map params configuration mode.
max-http-conns	Maximum number of HTTP connections per client.
no	Negates a command or set its defaults.
redirect	Redirects the URL.
timeout	Timeout for the initial state of Webauth.
type	Type of parameter - web-auth, consent or both.

3.5 Custom Local WebAuth Configuration Example

- AAA Part
  - **aaa authentication login** *local_webauth* **local**
  - **aaa authorization network** *local_webauth* **local**
  - **aaa authorization network** *default* **local**
  - **aaa authorization credential-download** *default* **local**

Syntax	**Description**
`aaa authentication login local_webauth local`	Authentication method list for login.
`aaa authorization network local_webauth`	Authorization method list for

`local`	the network.
`aaa authorization network default local`	Authorization method list for the local user.
`aaa authorization credential-download default local`	Authorization method list for use of local credentials.

- Parameter-Map
    - **parameter-map type webauth** *global*

      virtual-ip ipv4 *172.16.16.16*
    - **parameter-map type webauth** *vit_custom_web*

      type webauth

      timeout init-state min *5*

Syntax	Description
`parameter-map type webauth global` `virtual-ip ipv4 172.16.16.16`	Global parameter map used to define the virtual IP address.
`timeout init-state min 5`	Timeout for entering credentials.

```
custom-page login device flash:/custom_webauth/webauth_login.html
custom-page success device flash:/custom_webauth/webauth_success.html
custom-page failure device flash:/custom_webauth/webauth_failure.html
custom-page login expired device
flash:/custom_webauth/webauth_expired.html

banner text ^C Custom Webauth ^C
```

#Named parameter map (example: vit_custom_web) with type webauth.

- WLAN Configuration

```
wlan viten_webauth 8 viten_custom_webauth
 client vlan 263
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list local_webauth
 security web-auth parameter-map vit_custom_web
 session-timeout 1800
 no shutdown
```

Syntax	Description

`security web-auth`	Sets the SSID to security web-auth.
`security web-auth authentication-list local_webauth`	Calls the method list for authentication.
`security web-auth parameter-map vit_custom_web`	Calls the security parameter map.

Note

You can use the **`copy tftp: flash:`** command to copy the custom pages locally to the flash memory.

3.6 Custom External WebAuth Configuration Example

- AAA Part

Adding External RADIUS Server

For the purpose of the example, ISE is used:

- **`radius server ISE`**

  `address ipv4` *`192.168.154.119`* **`auth-port 1812 acct-port 1813`**

  `key Cisco123`

- **`aaa group server radius`** *`rad_ise`*

  `server name ISE`

Syntax	Description

`radius server ISE`
`address ipv4 192.168.154.119 auth-port 1812 acct-port 1813`
`key Cisco123`
	Defines the external RADIUS server.

`aaa group server radius rad_ise` `server name ISE`	Defines the AAA RADIUS group and specifies the RADIUS server to be used.

Creating Authentication Method Lists

- **`aaa authentication login`** *`external_ise`* **`group`** *`rad_ise`*

  #Authentication method list (example: external_ise) which calls the RADIUS group server (example: rad_ise).

Creating Authorization Method Lists

- **`aaa authorization network`** *`external_webauth`* **`group`** *`rad_ise`*

  #Authorization method list (example: external_webauth) which points to the RADIUS server group (example: rad_ise).

- Parameter-Map
    - **parameter-map type webauth** *global*

      virtual-ip ipv4 *172.16.16.16*

    - **parameter-map type webauth** *vit_custom_external*

      type webauth

      redirect for-login *https://192.168.154.119:8443/guestportal/portals/external_webauth/portal.jsp*

      redirect portal ipv4 *192.168.154.119*

      banner text ^C Custom Webauth External ^C

Syntax	Description
parameter-map type webauth *global* virtual-ip ipv4 *172.16.16.16*	Global parameter map used to define the virtual IP address.
parameter-map type webauth *vit_custom_external* type webauth redirect for-login *https://192.168.154.119:8443/guestportal/portals/external_webauth/portal.jsp*	ISE custom guest portal.
redirect portal ipv4 *192.168.154.119*	Redirects to ISE.
banner text ^C Custom Webauth External ^C	Named parameter map.

Note

- Optionally you could also mention the redirect on-success and redirect on-failure pages defined under the parameter-map.

  redirect on-success url

  redirect on-failure url

- It is recommended that you disable the **Telnet/HTTP** access and only allow secure **SSH/HTTPS** access to devices.

- Pre Authentication Access Control List (ACL)

```
ip access-lists extended preauth_ise
 permit udp any eq bootps any
 permit udp any any eq bootpc
 permit udp any eq bootpc any
```

```
permit udp any any eq domain
permit udp any eq domain any

permit ip any host 192.168.154.119
permit ip host 192.168.154.119 any
```

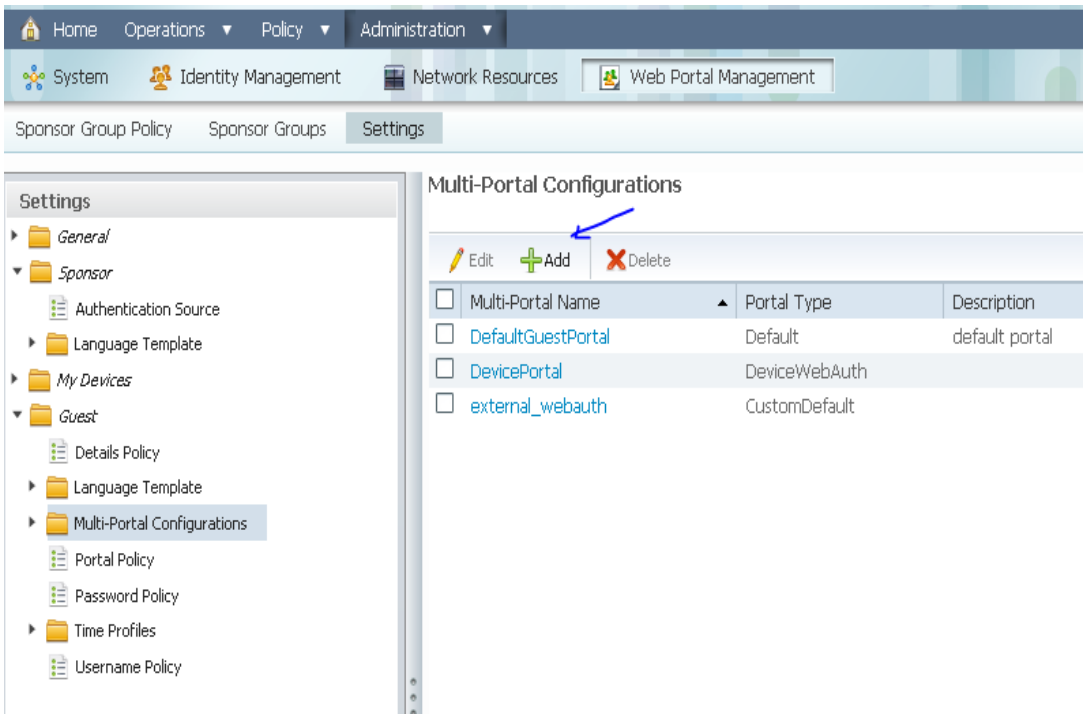
Syntax	Description
ip access-lists extended *preauth_ise* permit udp any eq bootps any permit udp any any eq bootpc permit udp any eq bootpc any	Allows DHCP.
permit udp any any eq domain permit udp any eq domain any	Allows DNS.
permit ip any host *192.168.154.119* permit ip host *192.168.154.119* any	Allows access to and back from the ISE.

- WLAN Configuration

```
wlan viten_webauth 9 viten_custom_external
 client vlan 254
 ip access-group web preauth_ise
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 security web-auth authentication-list external_ise
 security web-auth parameter-map vit_custom_external
 session-timeout 1800
 no shutdown
```

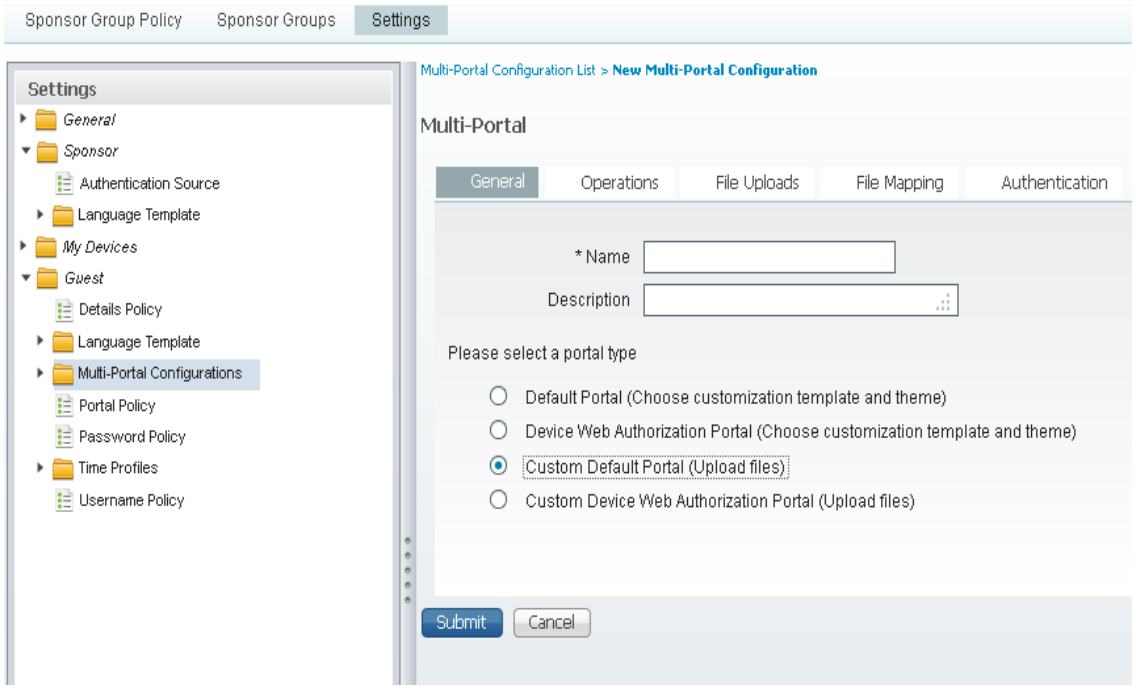
Syntax	Description
ip access-group web *preauth_ise*	Pre-authentication for the ACL.
security web-auth	Sets the SSID to security **web-auth.**
security web-auth authentication-list *external_ise*	Calls the method list for authentication.
security web-auth parameter-map *vit_custom_external*	Calls the security parameter map.

- ISE Custom Guest Portal Screenshots

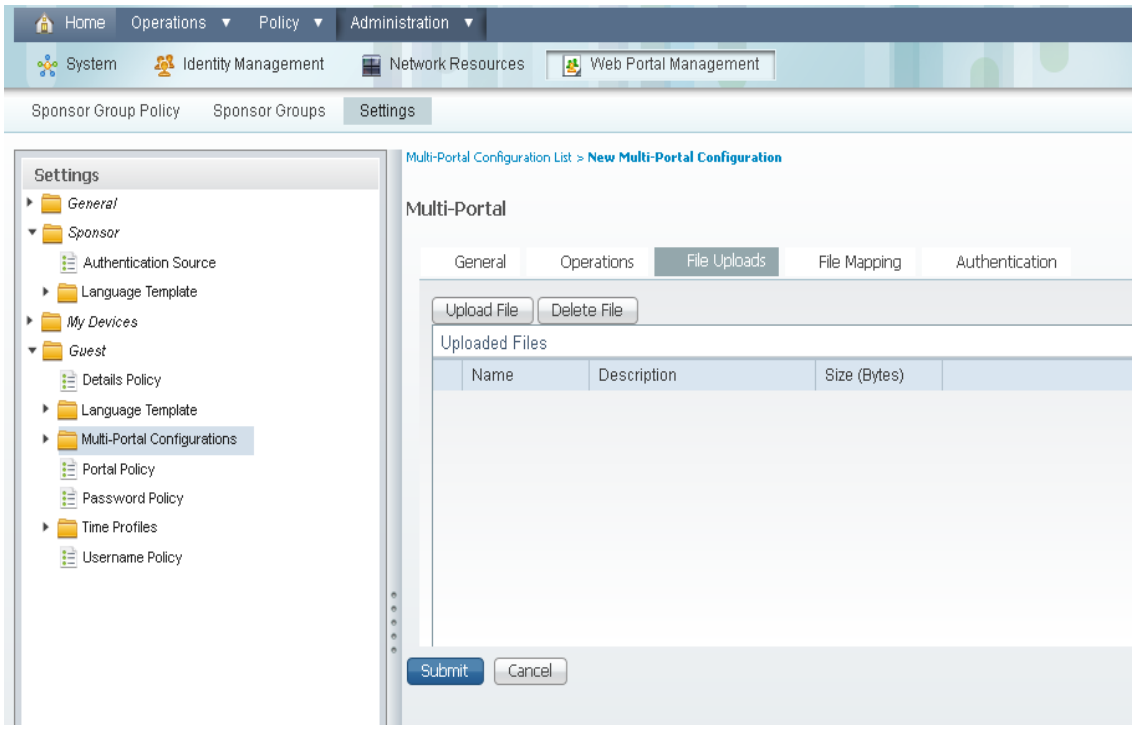


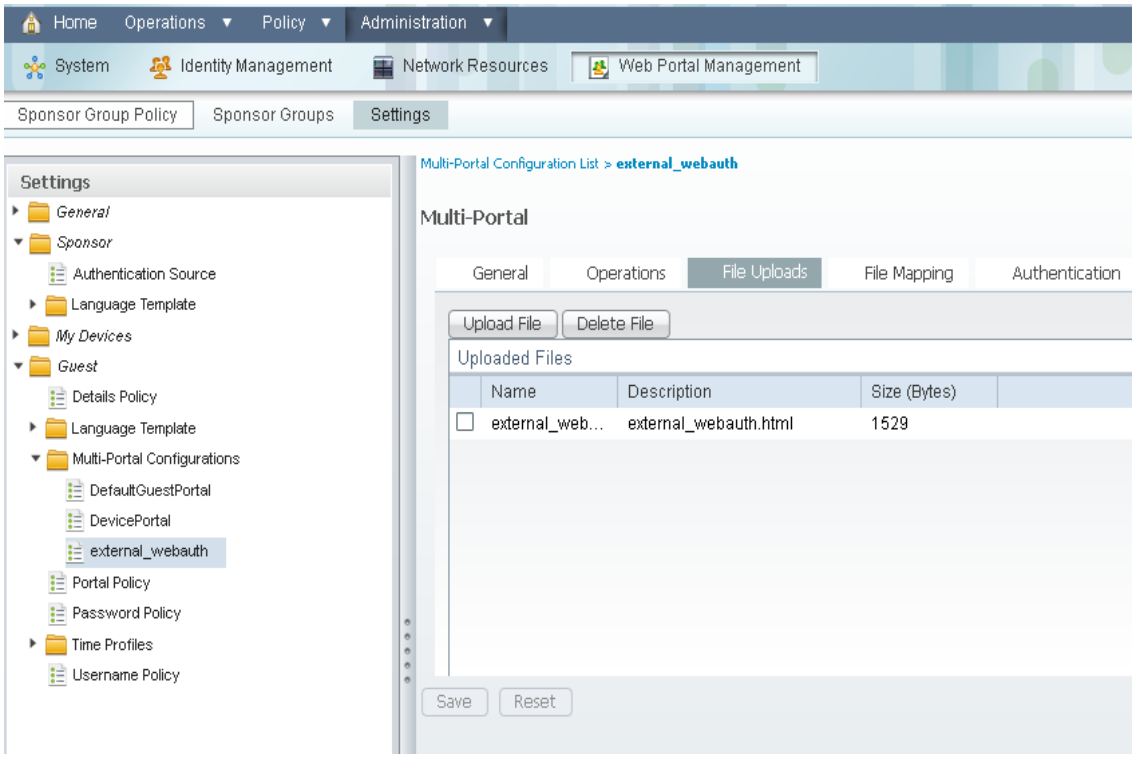
To add a custom default portal called **external_webauth,** complete these steps:

Step 1: Click **Add** and select **Custom Default Portal**

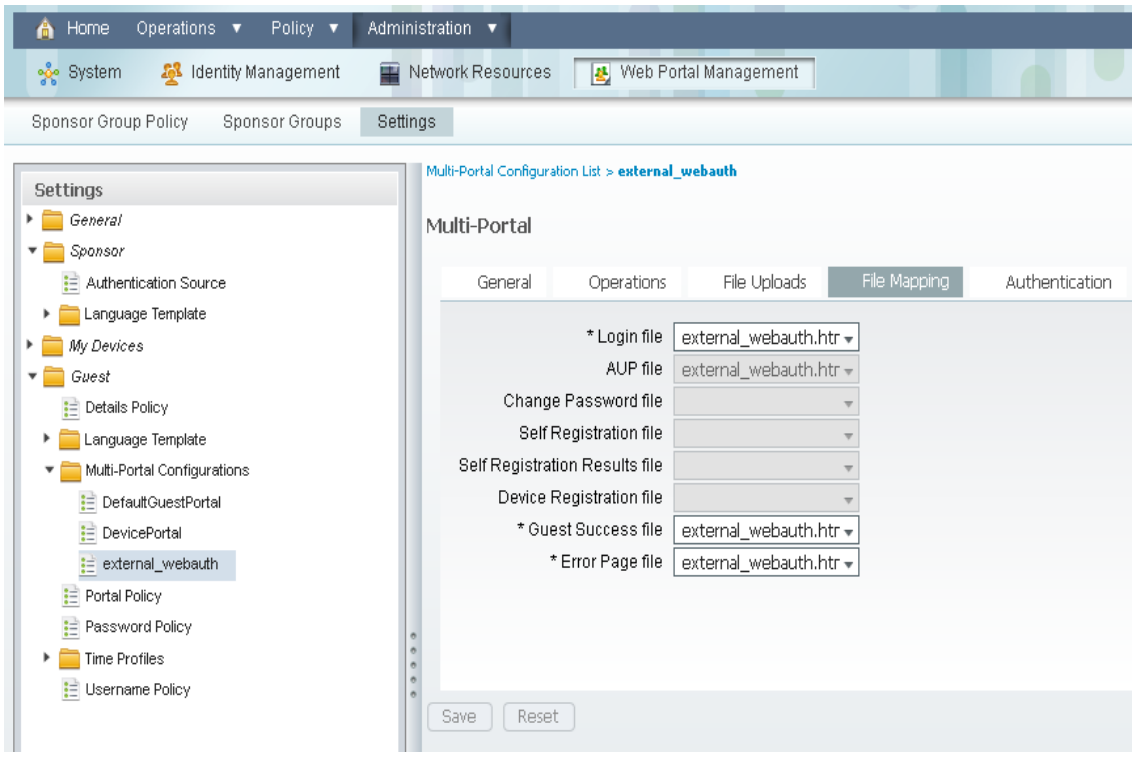


Step 2: Upload the login, success and failure pages. In this example the login page external_webauth.hmtl is used.

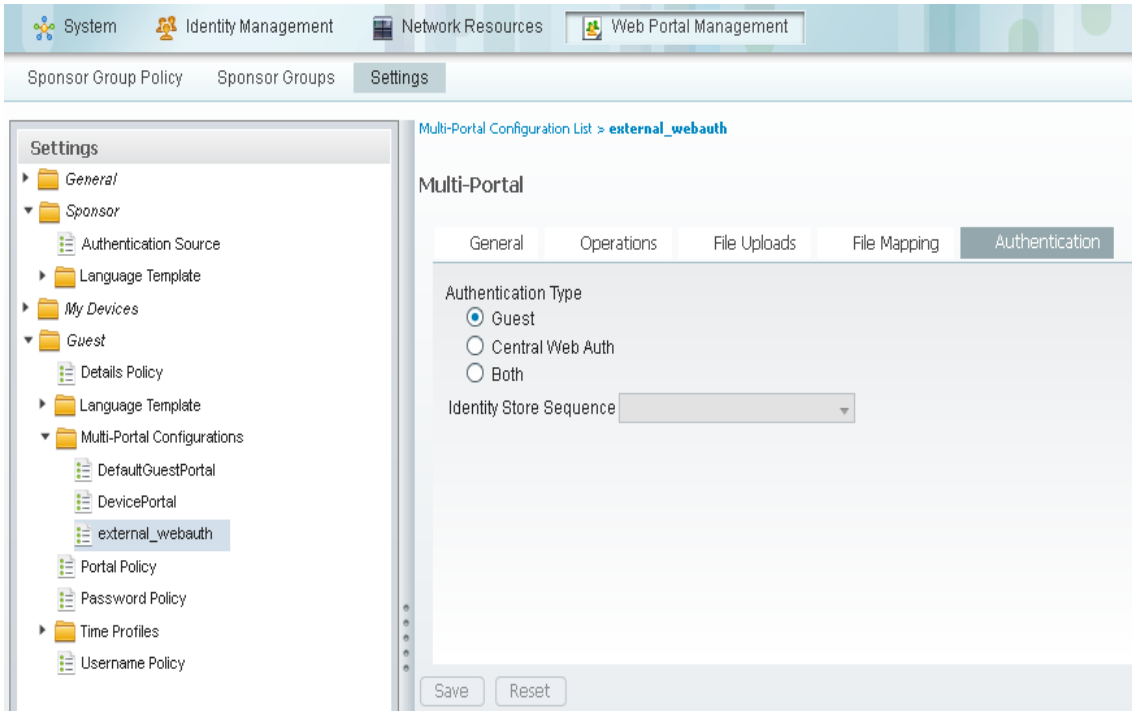




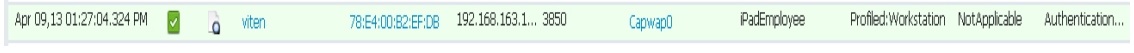
Step 3: In File Mapping tab, map the uploaded HTML pages (In this example, external_webauth.html that was uploaded in the previous step is mapped against the Login file, AUP file, Guest Success file, and Error page file).



Step 4: Click the Authentication tab and select the Authentication type required.



Step 5: The following screenshot shows the status of the authenticated user in the ISE Authentication success log page. The authorization policy returns an access-accept.



Note

See the following URLs for more information about guest portal configuration on the ISE:

http://www.cisco.com/en/US/docs/security/ise/1.0.4/user_guide/ise10_guest_pol.pdf
http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_guest_pol.pdf
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byoddg.html

3.7 Local Webauth – Caveats

- Sometimes clients may get stuck in the IP learn state. Make sure that IP DHCP snooping is enabled globally and also for the client VLAN.
- iPads may not redirect to the login page if the **`ip http secure-server`** command is used.

3.8 Useful debugs and show commands

```
debug ip device tracking obj-create
debug ip device tracking obj-destroy
debug aaa authentication
debug radius authentication
debug client mac-address <mac>
debug ip admissions [command family]

show run aaa
show run | section parameter
show wireless client mac-address <mac> detail
Debug ip http all
```

3.9 WebAuth Logout

The virtual IP address must not exist on the subnet or switch. Once the credentials are authenticated successfully, the user is shown the success-logout page. This is always generated by the switch, regardless of the custom page configuration.

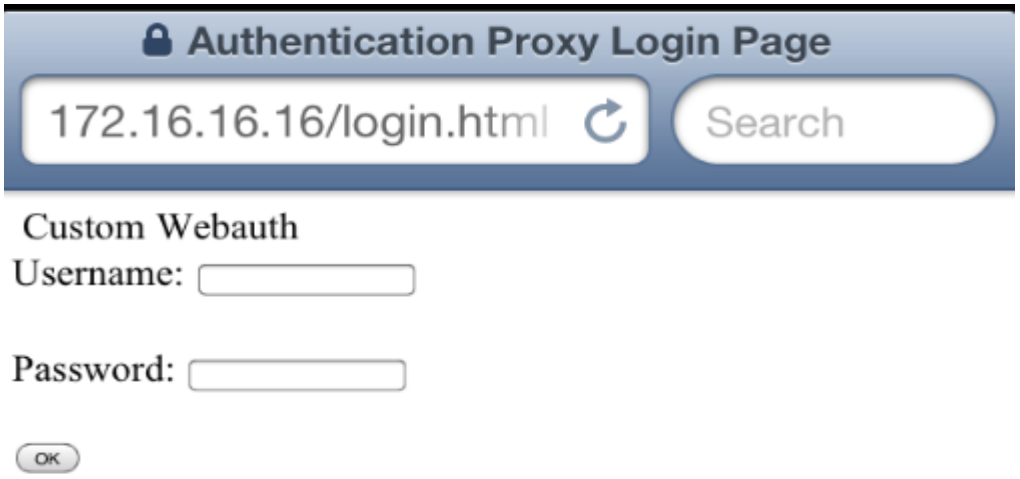
The success-logout page contains two links and an input button. The **HERE** link opens the initial URL in a new window or tab. The **logout** link sends a **GET** request to the virtual IP which is intercepted by the switch, and you are logged out of the session.

Clicking the input button closes the window. This in turn, causes the javascript from the parent window (the login page) to either open the original URL or to open the URL that was assigned by the success-logout page (the final URL as shown in the debug command output).

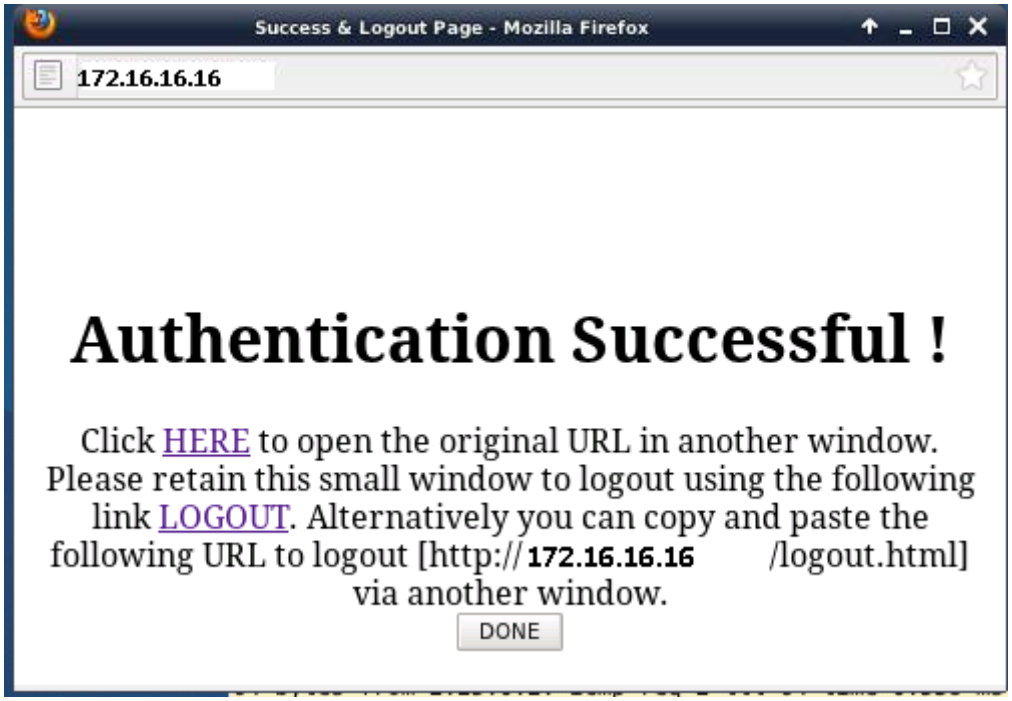
```
debug ip admission page
!
07:02:29: WA-PAGE : Gi1/0/10    [10.0.0.1  ] Send webauth logout page
07:02:29: WA-PAGE : Gi1/0/10    [10.0.0.1  ] initial url
[http://2.25.0.2/image.gif]
```

```
07:02:29: WA-PAGE : Gi1/0/10    [10.0.0.1   ] logout url
[http://100.100.100.100/logout.html]
07:02:29: WA-PAGE : Gi1/0/10    [10.0.0.1   ] final url
[http://10.0.0.2/image.gif]
```

3.9.1 Login Page



3.9.2 Success-Logout Page



3.10 WebAuth Custom HTML Pages

The Custom page in Webauth allows customers to use their own HTML page for Webauth login, success, and failure pages instead of the default page. Customers can use the example HTML code given below as per their requirement and see the code in the 3850 switch and 5760 controller by downloading the HTML file to the flash memory.

```
!
conf t
parameter-map type webauth global
 virtual-ip ipv4 172.16.16.16
!
parameter-map type WEBAUTH
 type webauth
 custom-page login device flash:webauth_login.html
 custom-page login expired device flash:webauth_expire.html
 custom-page failure device flash:webauth_fail.html
 custom-page success device flash:webauth_success.html
!
```

Example of Copying HTML File to Flash

```
3850 #$/10.0.0.100/WebAuth/loginusername.html flash:login.html
Destination filename [login.html]?
Accessing tftp://10.0.0.100/WebAuth/loginusername.html...
Loading WebAuth/loginusername.html from 10.0.0.100 (via Vlan136): !
[OK - 1222 bytes]
```

Example to Check the Content of Flash

```
3850 #sh flash:
-#- --length-- ---------date/time--------- path
1     109405 Feb 03 2012 11:15:44 +00:00 bellFpga03_0a.hex
2     1222 Jul 03 2013 19:47:55 +00:00 login.html
3     782 Jul 03 2013 19:48:35 +00:00 loginsucess.html
```

3.10.1 Custom Consent Parameter-Map Configuration Example

Users can be allowed without authentication by just clicking the accept button in the consent login HTML page. To configure the parameter type as consent, use the below code:

```
parameter-map type webauth webparalocal
type consent
custom-page login device flash:webauth_consent.html
custom-page success device flash: webauth_success.html
custom-page failure device flash:webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

3.11 WebAuth Custom Pages on External Server

For a Webauth page to work on the external Webauth server, the HTML is similar to the custom webauth HTML pages, except that the form *action* specifies the virtual IP address so that the post is sent to the switch and not to the external server.

The success-logout page has the final URL set to the success page on the external server. Therefore, when the user clicks the **DONE** button on this page, the browser fetches the success page from the external server.

```
!
conf t
parameter-map type webauth global
 timeout init-state min 5
 virtual-ip ipv4 172.16.16.16
parameter-map type webauth WEBAUTH_CONSENT
 type webauth
 redirect portal ipv4 10.0.98.34
 redirect for-login http://10.0.98.34/~iwilson/login.html
 redirect on-success http://10.0.98.34/~iwilson/success.html
 redirect on-failure http://10.0.98.34/~iwilson/failure.html
```

3.11.1 External WebAuth with Custom Consent Page with Email Option

```
parameter-map type webauth webparalocal
 type consent
consent email
 redirect for-login http://10.0.128.50/webauth/webauth_consent.html
 redirect on-success http://10.0.128.50/webauth/webauth_success.html
 redirect on-failure http://10.0.128.50/webauth/webauth_failure.html
 redirect portal ipv4 10.0.128.50
```

In this example, the virtual IP should be same on HTML and switch configuration.

```
parameter-map type webauth global
virtual-ip ipv4 172.16.16.16
```

3.12 Downloading Web Authentication Tar Bundle

You can download a tar bundle using the CLI or the GUI.

3.12.1 Downloading Web Authentication Tar Bundle (CLI)

You can download a tar bundle (.tar) containing all personalized files from the FTP or TFTP server.

- **archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY>**

Syntax	Description
`archive tar /xtract <transfer mode> ://<IP> /<location>/<login filename> < DIRECTORY>`	Specifies to download a tar bundle (.tar) from the FTP or TFTP server.

Example

```
Controller# archive tar /xtract tftp://9.1.0.100/user1/login.tar  flash2
Controller# show flash:
59    4096 Jan 08 2014 13:19:33.0000000000 +00:00 flash
60    2574 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/aup.html
61    4082 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/login.html
62    70123 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/yourlogo.jpg
63    344 Jan 08 2014 13:19:51.0000000000 +00:00 flash2/failed.html
64    1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/logout.html
64    1653 Jan 08 2014 13:19:52.0000000000 +00:00 flash2/expired.html
```

3.12.2 Downloading Web Authentication Tar Bundle (GUI

Step 1: Select **Configuration** > **Commands** > **Download File** to open the Download File in the Controller GUI page.

Step 2: Select Webauth Bundle from the **File Type** drop-down list.

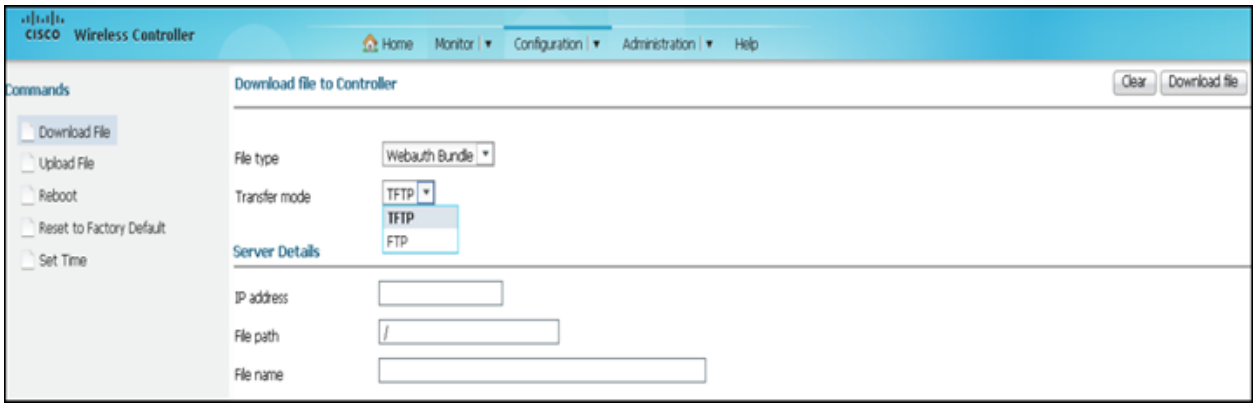
Step 3: From the **Transfer Mode** drop-down list, choose one of the following options:

- TFTP
- FTP

Step 4: Enter the IP address of the server in the **IP Address** field.

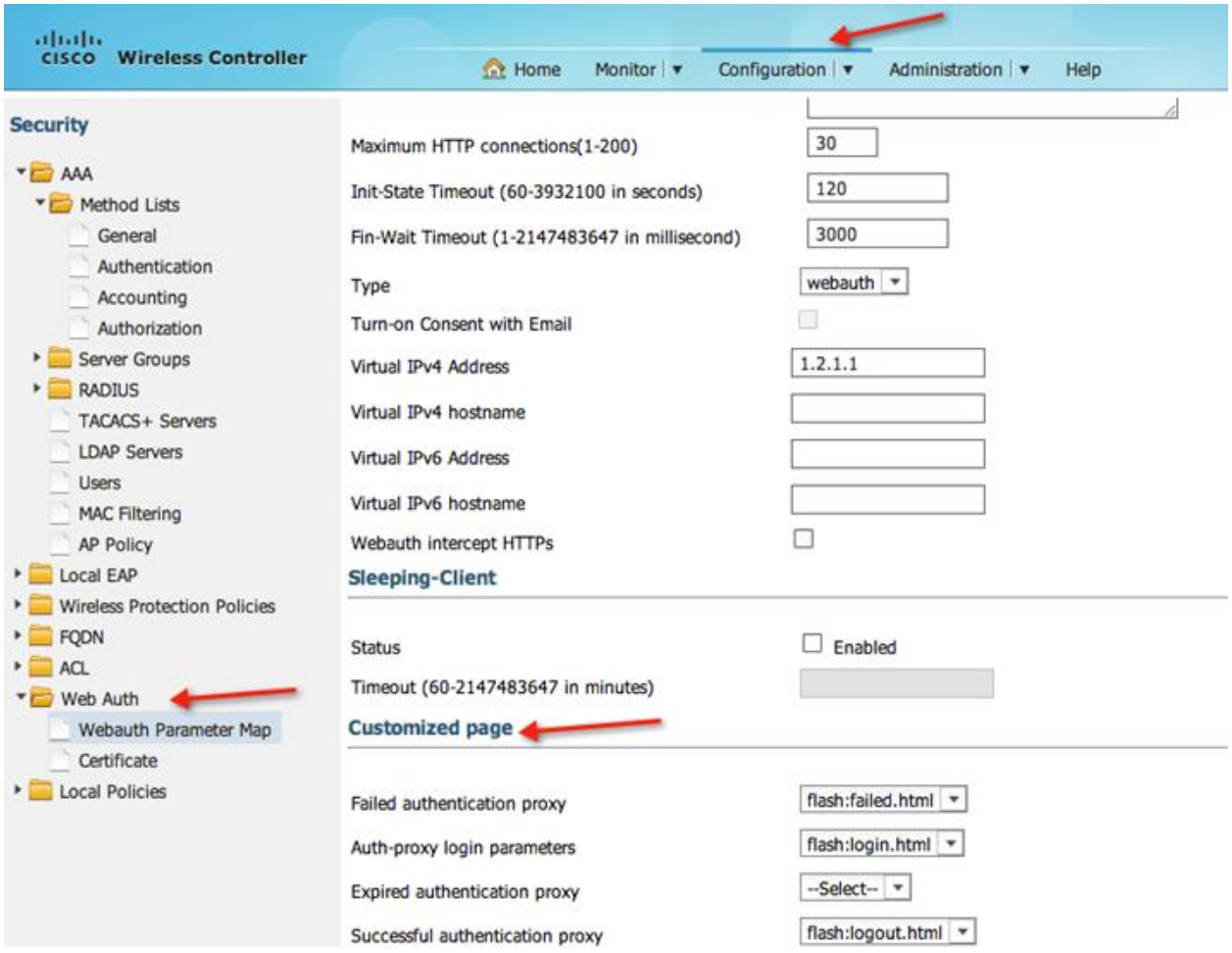
Step 5: Enter the directory path of the software in the **File Path** field,.

Step 6: enter the name of the controller software file (*filename.aes*) in the **File Name** field box.



Note: You can specify a path for downloading the tar file to different folder when using the CLI method only. It is not available in the GUI method.

The downloaded file is listed as a parameter map.



3.12.3 Integrating Customized Web Authentication Pages into a Parameter Map (CLI)

By configuring the personalized pages into a parameter map, you can configure all the personalized paged together at one time. This minimizes the need of configuring all the four custom pages separately. You can configure any page separately, the others pages use the default configurations.

- **configure terminal**
- **parameter-map type webauth name type webauth**
- **custom-page login device flash:flash2/login.html**
- **custom-page success device flash: flash2/logout.html**
- **custom-page failure device flash: flash2/failed.html**
- **end**

  Ensure you download loginscript.js to the flash.
- **show parameter-map type webauth name name**

  The tar file which contain the custom logout should refer to loginscript.js in its html

  <script language="javascript" src = "/loginscript.js"></script>

Syntax	Description
configure terminal **Example:** `Controller# configure terminal`	Enters global configuration mode.
parameter-map type webauth *name* **type** *webauth* **Example:** `Controller(config)# parameter-map type webauth WEB type webauth`	Creates a parameter map.
custom-page login device flash:flash2/login.html **Example:** `Controller(config-params-parameter-map)# custom-page login device flash:flash2/login.html`	Configures the personalized pages into a parameter map
custom-page success device flash: flash2/logout.html **Example:** `Controller(config-params-parameter-map)# custom-page success device flash: flash2/logout.html`	Configures the personalized pages into a parameter map.
end **Example:** `Controller(config)# end`	Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

show parameter-map type webauth name *name*
Example:
`Controller# show parameter-map type webauth name WEB`
`Parameter Map Name : WEB`
	Displays the user defined parameter map.

Type : webauth Custom Page: Auth-proxy login : flash: flash2/login.html Auth-proxy Init State time : 120 sec Auth-proxy Fin Wait time : 3000 milliseconds Webauth max-http connection : 30 Webauth logout-window : Enabled Consent Email : Disabled	

3.12.4 Linking Image in Custom Pages

In custom pages, you can also send back images.

In releases earlier to software release 3E, the custom page had to contain the link to the image as an entire path, in the form of: <img src="http://<ip-addresss>/flash:web_auth_image.jpg" alt="name">. The IP address is the management IP address of the controller.

- img src="./flash:web_auth_image.jpg" alt="name”>
- <img src="./flash:web_auth_image.jpg" alt="name”>

Syntax	Description
<img src="./flash:web_auth_image.jpg" alt="name”> **Example:** Controller# **<img src="./flash:web_auth_image.jpg" alt="name”>**	Specifies link image to the custom page. The virtual IP address is automatically used as a source. The logical link implies that you define the virtual IP address in the global parameter map. **Note**:You can still define the full path of the image (with controller IP address). In such case, the IP address is either the management IP or the virtual IP (if configured).

3.12.5 WebAuth Page Behavior When Upgraded from CiscoIOS XE Version 3.3 to 3.6

After you upgrade to Cisco IOS XE Release 3.6E, the WebAuth success page behavior is different from the behavior seen in Cisco IOS XE Release 3.3.X SE. After a successful authentication on the WebAuth login page, the original requested URL opens in a pop-up window and not on the parent page. It is recommended to upgrade the WebAuth Tar Bundle in the same format as used by AireOS Wireless LAN Controllers, a sample of which is available on CCO.

4 How to Use WebAuth Bundle

The HTML files such as login, logout, expired, and failed, are grouped in separate folders–custom consent, custom webauth, custom webconsent, and external webauth page–in the Webauth bundle provided and can be customized for your requirement.

Table: WEBAUTH_BUNDLE Categorization

Folder	HTML Files Available
Custom Consent	• consent.html • failed.html • logout.html
Custom Webauth	• login.html • failed.html • logout.html

5 Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html