

# eWLC 9800 Local WebAuth with Custom Pages using the WebAuth Bundle

Download the Wireless Lan Controller Web Authentication Bundle - 16.10.1  
(WLC\_WEBAUTH\_BUNDLE\_1.0.zip) from Cisco.com:

<https://software.cisco.com/download/home/286316412/type/282791507/release/16.10.1>

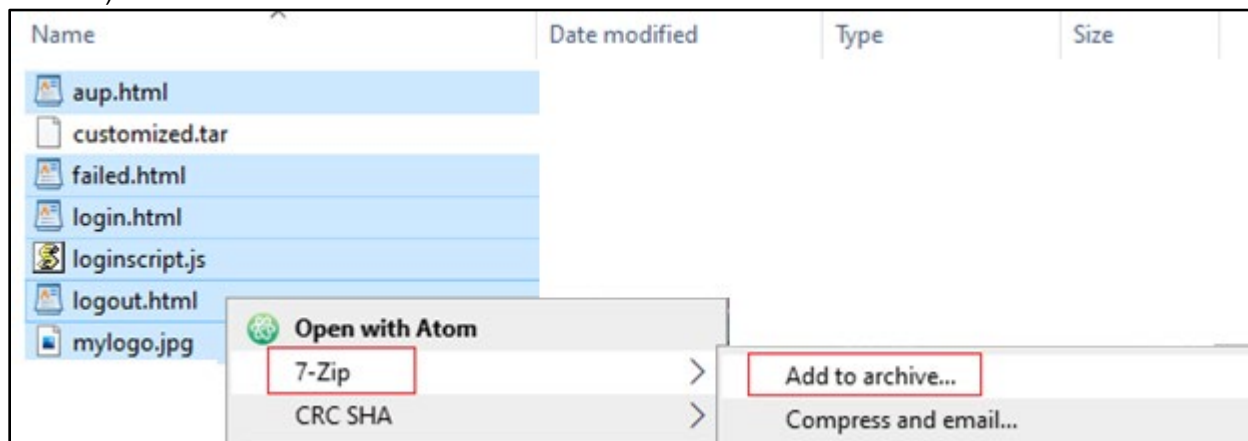
(it is the same for all 9800) in my tests, I used the file that I downloaded from the 9800-40 and used it for 9800-L and virtual 9800-CL

Now, unzip that folder.

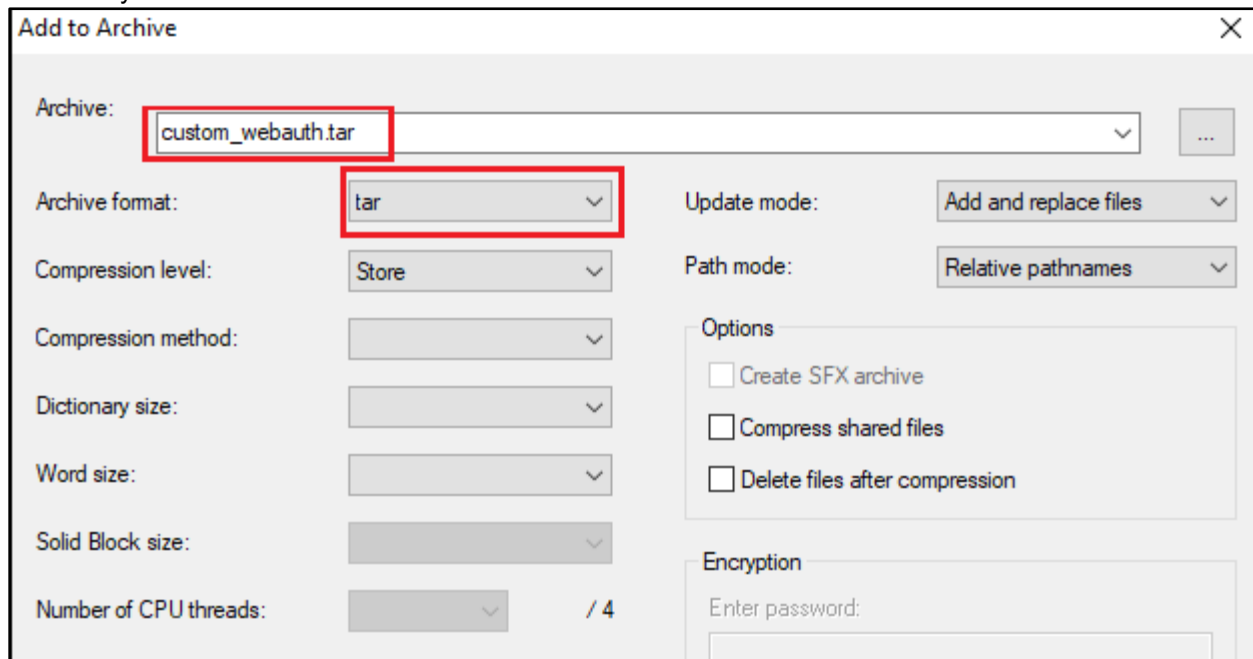
if you want to change everything, open each html file and edit them as you want, and you can upload the logo also, the file names are not important, you can call them anything you want.

After that, delete the login.tar file because we're going to generate a new one.

Select all the files and right mouse click and select 7-Zip (assuming you have the free 7-Zip program installed) and choose Add to archive...



Give it any name and choose tar as the Archive format:



The image shows a dialog box titled "Add to Archive" with a close button (X) in the top right corner. The dialog contains several settings for creating an archive:

- Archive:** A text field containing "custom\_webauth.tar" is highlighted with a red box.
- Archive format:** A dropdown menu showing "tar" is highlighted with a red box.
- Update mode:** A dropdown menu showing "Add and replace files".
- Path mode:** A dropdown menu showing "Relative pathnames".
- Compression level:** A dropdown menu showing "Store".
- Compression method:** A dropdown menu.
- Dictionary size:** A dropdown menu.
- Word size:** A dropdown menu.
- Solid Block size:** A dropdown menu.
- Number of CPU threads:** A dropdown menu showing "/ 4".
- Options:** A section with three unchecked checkboxes: "Create SFX archive", "Compress shared files", and "Delete files after compression".
- Encryption:** A section with a label "Enter password:" and an empty text input field.

Then go to the 9800  
Administration > Management > Backup & Restore >  
change the file type to Web Auth Bundle  
and upload just that .tar file

Cisco Catalyst 9800-L Wireless Controller 17.3.1

Administration > Management > Backup & Restore

**Config File Management**

Copy	To Device
File Type	Web Auth Bundle
Transfer Mode	HTTP
Source File Path*	Select File customized.tar

Download File

Cisco Catalyst 9800-L Wireless Controller 17.3.1

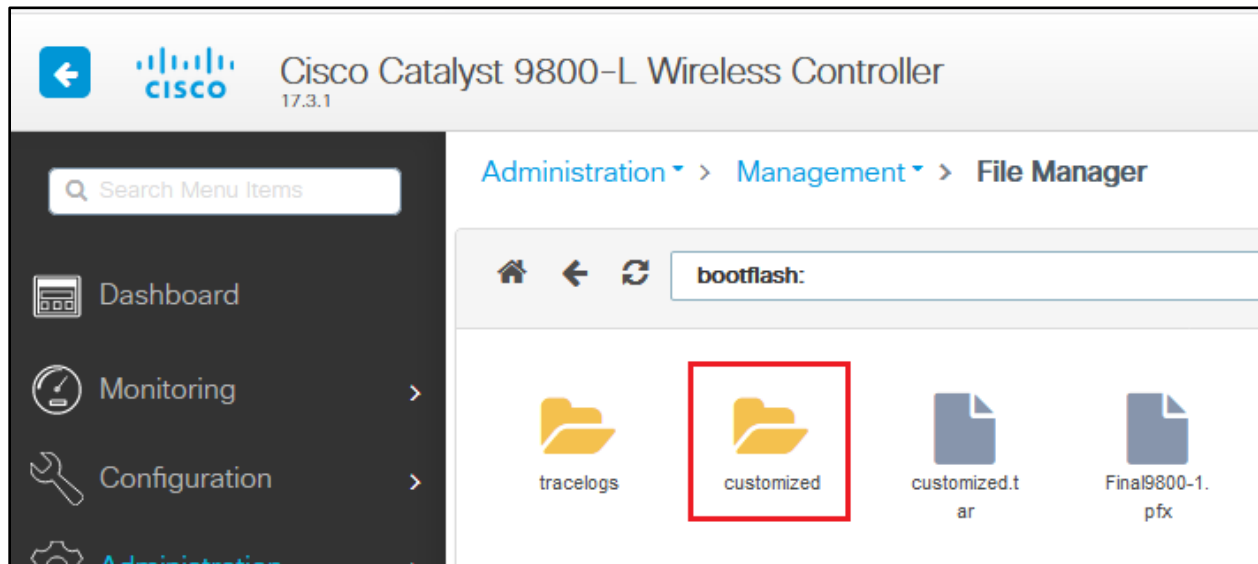
Administration > Management > Backup & Restore

**Config File Management**

Copy	To Device
File Type	Web Auth Bundle
Transfer Mode	HTTP
Source File Path*	Select File customized.tar ✓

DownloadFile

By default, the 9800 will create a folder inside the bootflash and will call it whatever you called your .tar file and all the files will be in that folder:



If you have HA setup then you need to run 17.3 code (or future releases) because of this enhancement bug:

CSCvr05309: copy webauth tar bundle to standby bootflash also incase of HA setup

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvr05309>

To check on both HA (Active and Standby), assuming we uploaded a file called customized.tar

```
9800-1#show bootflash: | s customized
```

```
9800-1#show stby-bootflash: | s customized
```

```
9800-1#show bootflash: | s customized
1313      161280 Oct 08 2020 16:17:15.0000000000 +00:00 customized.tar
1314        4096 Oct 08 2020 16:17:15.0000000000 +00:00 customized
1315        2595 Oct 08 2020 16:17:15.0000000000 +00:00 customized/aup.html
1316         327 Oct 08 2020 16:17:15.0000000000 +00:00 customized/failed.html
1317        4071 Oct 08 2020 16:17:15.0000000000 +00:00 customized/login.html
1318         318 Oct 08 2020 16:17:15.0000000000 +00:00 customized/loginscript.js
1319        1116 Oct 08 2020 16:17:15.0000000000 +00:00 customized/logout.html
1320       147245 Oct 08 2020 16:17:15.0000000000 +00:00 customized/mylogo.jpg
9800-1#
9800-1#
9800-1#show stby
9800-1#show stby-bootfl
9800-1#show stby-bootflash: | s customized
1154      161280 Oct 08 2020 16:17:15.0000000000 +00:00 customized.tar
1234        4096 Oct 08 2020 16:17:16.0000000000 +00:00 customized
1235        2595 Oct 08 2020 16:17:16.0000000000 +00:00 customized/aup.html
1236         327 Oct 08 2020 16:17:16.0000000000 +00:00 customized/failed.html
1237        4071 Oct 08 2020 16:17:16.0000000000 +00:00 customized/login.html
1238         318 Oct 08 2020 16:17:16.0000000000 +00:00 customized/loginscript.js
1239        1116 Oct 08 2020 16:17:16.0000000000 +00:00 customized/logout.html
1240       147245 Oct 08 2020 16:17:16.0000000000 +00:00 customized/mylogo.jpg
9800-1#
9800-1#
9800-1#
```

Note: the files that have been uploaded manually will not be synced to the HA Standby.

## success.html file

Do i need success.html file because the bundle has no such a file?

No, you don't need that file to make this works, but if you need that, you can simply create one and add it to the .tar file and upload that tar file to the 9800 eWLC.

Next step: create new Parameter Map

Edit Web Auth Parameter

General Advanced **All below settings are optional**

Parameter-map name

Banner Type  None  Banner Text  Banner Title  File Name

Maximum HTTP connections

Init-State Timeout(secs)

Type

Captive Bypass Portal

Disable Success Window

Disable Logout Window

Disable Cisco Logo

Sleeping Client Status

Sleeping Client Timeout (minutes)

When checking "Disable Success Window" this is to disable the 9800 default success page and not the success.html file page "if you used it" so if you use both, the guest will see dual success pages, one from the 9800 "the default one" and second one is from the success.html file.

Even if you disable all success pages (Disable Success Window and no success.html used) the mobile devices will see success page like below while PCs will see it for a second and will go away.

Example from iPhone:

captive.apple.com

Local WebAuth Customized

< >

Log In Done

Success

## Edit Web Auth Parameter

General

**Advanced**

### Redirect to external server

Redirect for log-in

Redirect On-Success

Redirect On-Failure

Redirect Append for AP MAC Address

Redirect Append for Client MAC Address

Redirect Append for WLAN SSID

Portal IPV4 Address

Portal IPV6 Address

Express WiFi Key Type

### Customized page

Login Failed Page

bootflash:/customized/ 


Login Page

bootflash:/customized/ 

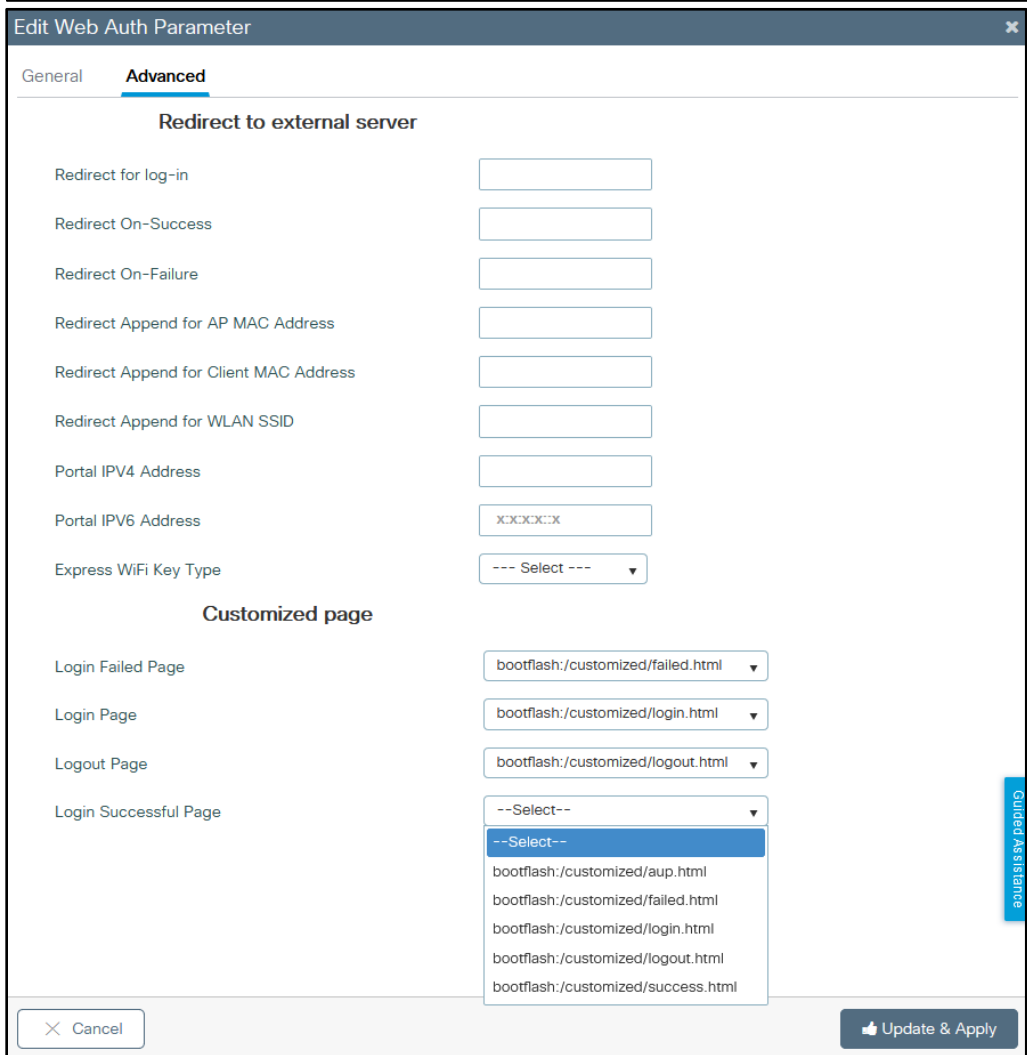
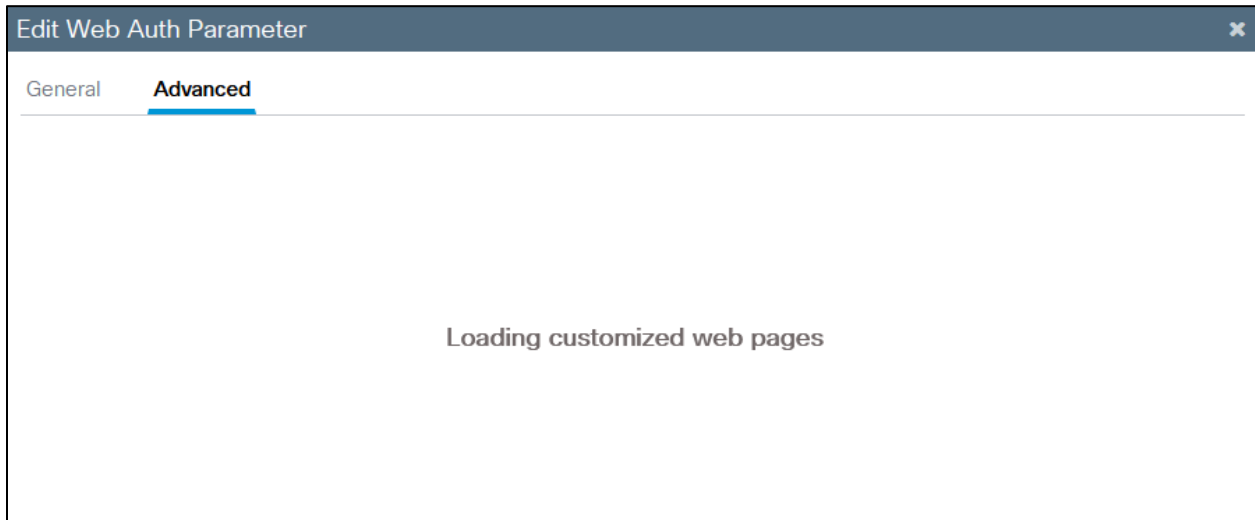
Logout Page

bootflash:/customized/ 

Login Successful Page

If you click on the blue icon beside any page, the 9800 will try to load that and you can choose the pages as below





We will use the WLAN to authenticate the guests from local 9800 guest accounts first and from ISE (RADIUS Server) second.  
(we don't need to enable or configure AAA "third tab here" or add preauth ACL)

Edit WLAN

General **Security** Advanced Add To Policy Tags

Layer2 **Layer3** AAA

Web Policy

Web Auth Parameter Map With-Custom-Bundle ▼

Authentication List default ▼ ⓘ

*For Local Login Method List to work, please make sure the configuration 'aaa authorization network default local' exists on the device*

<< Hide

On Mac Filter Failure

Splash Web Redirect  DISABLED

**Preauthentication ACL**

IPv4 None ▼

IPv6 None ▼

**Sample config for ISE or any RADIUS Server:**

```
radius server ISE
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
timeout 5
retransmit 3
automate-tester username dummy probe-on
key XXXXXXXXXXXX
exit
aaa group server radius RADIUS-GROUP
server name ISE
exit
aaa authentication dot1x ISE-Method group RADIUS-GROUP
aaa authorization network ISE-Method group RADIUS-GROUP
aaa accounting identity default start-stop group RADIUS-GROUP
aaa authentication webauth default local group RADIUS-GROUP
end
```

Note: as you can see in the last cli command, I'm checking local users first then ISE.

If you want to add local Guest users:

The screenshot shows a web-based configuration interface for adding a guest user. The breadcrumb navigation at the top reads "Configuration > Security > Guest User". Below this, there are two buttons: "+ Add" (highlighted with a red box) and "Delete". The main content area is titled "Add Guest User" and is divided into two columns: "General" and "Lifetime".

General		Lifetime	
User Name*	guest22	Years*	1
Password*	••••••	Months*	0
	<input type="checkbox"/> Generate password	Days*	0
Confirm Password*	••••••	Hours*	0
Description*	Guest 22	Mins*	0
AAA Attribute list	Enter/Select		
No. of Simultaneous User Logins*	0		
	<i>Enter 0 for unlimited users</i>		

At the bottom of the form, there are two buttons: "Cancel" and "Apply to Device".

Testing with local 9800 guest accounts: "from iPhone"

🔒 lwa.  
Local WebAuth Customized

< > **Log In** **Cancel**

---

**Welcome to TestCompany**

The TestCompany provides Internet access at no charge in selected areas for guests with portable computers or devices capable of receiving wireless signals. You will be able to access the Internet from your wireless device when sitting within range of an access point. Guests are expected to use the wireless access in a legal and responsible manner. By using this wireless access network, the user acknowledges that he/she is subject to, and agrees to abide by all laws, and all state and federal rules and regulations applicable to Internet use.

**Terms and Conditions of Use**

Guests will need a notebook/laptop computer or other device equipped with a wireless card that supports the WiFi standard.  
The TestCompany assumes no responsibility for the safety of equipment.


**Security Considerations**

Wireless access is by nature an insecure medium. As with most guest wireless

Please enter your username/password

**Username**

**Password**



# Testing with guests configured within ISE: "from PC"

ⓘ You must log in to this network before you can access the Internet.

**Welcome to TestCompany**

**Accessing TestCompany Public Network From Your Wireless Device**

The TestCompany provides Internet access at no charge in selected areas for guests with portable computers or devices capable of receiving wireless signals. You will be able to access the Internet from your wireless device when sitting within range of an access point. Guests are expected to use the wireless access in a legal and responsible manner. By using the wireless access network, the user acknowledges that he/she is subject to, and agrees to abide by all laws, and all state and federal rules and regulations applicable to Internet use.

**Terms and Conditions of Use**

Guests will need a notebook/laptop computer or other device equipped with a wireless card that supports the IEEE 802.11 standard. The TestCompany assumes no responsibility for the safety of equipment.

**Security Considerations**

Wireless access is by nature an insecure medium. As with most guest wireless networks, any information being sent or received over the TestCompany wireless network could potentially be intercepted by another wireless user. Caution and informed wireless users should not transmit their credit card information, passwords and any other sensitive personal information while using a wireless "hot spot".

Access using the TestCompany wireless network is acknowledged that there can be no expectation of privacy when using the wireless network. Users assume all associated risks and agree to hold harmless the TestCompany and its employees for any personal information (e.g. credit cards) that is compromised, or for any damage caused to user's hardware or software due to electric surges, security issues or consequences caused by viruses or hacking. All wireless access users should have up-to-date virus protection on their personal laptop computers or wireless devices.

**Please enter your username/password**

Username test

Password \*\*\*\*

[I Agree with Policy Above](#)

