



Multiple Authentications for a Client

- [Information About Multiple Authentications for a Client, on page 1](#)
- [Configuring Multiple Authentications for a Client, on page 2](#)
- [Verifying Multiple Authentication Configurations, on page 8](#)

Information About Multiple Authentications for a Client

Multiple Authentication feature is an extension of Layer 2 and Layer 3 security types supported for client join.



Note You can enable both L2 and L3 authentication for a given SSID.



Note The Multiple Authentication feature is applicable for regular clients only.

Information About Supported Combination of Authentications for a Client

The Multiple Authentications for a Client feature supports multiple combination of authentications for a given client configured in the WLAN profile.

The following table outlines the supported combination of authentications:

Layer 2	Layer 3	Supported
MAB	CWA	Yes
MAB Failure	LWA	Yes
802.1X	CWA	Yes
PSK	CWA	Yes
iPSK + MAB	CWA	Yes
iPSK	LWA	No

MAB Failure + PSK	LWA	No
MAB Failure + PSK	CWA	No

From 16.10.1 onwards, 802.1X configurations on WLAN support web authentication configurations with WPA or WPA2 configuration.

The feature also supports the following AP modes:

- Local
- FlexConnect
- Fabric

Configuring Multiple Authentications for a Client

Configuring WLAN for 802.1X and Local Web Authentication (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Select the required WLAN from the list of WLANs displayed.
- Step 3** Choose **Security > Layer2** tab.
- Step 4** Select the security method from the **Layer 2 Security Mode** drop-down list.
- Step 5** In the **Auth Key Mgmt**, check the **802.1x** check box.
- Step 6** Check the **MAC Filtering** check box to enable the feature.
- Step 7** After MAC Filtering is enabled, from the **Authorization List** drop-down list, choose an option.
- Step 8** Choose **Security > Layer3** tab.
- Step 9** Check the **Web Policy** check box to enable web authentication policy.
- Step 10** From the **Web Auth Parameter Map** and the **Authentication List** drop-down lists, choose an option.
- Step 11** Click **Update & Apply to Device**.
-

Configuring WLAN for 802.1X and Local Web Authentication (CLI)

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.

	Command or Action	Purpose
Step 2	wlan <i>profile-name wlan-id SSID_Name</i> Example: Device(config)# wlan wlan-test 3 ssid-test	Enters WLAN configuration sub-mode. <ul style="list-style-type: none"> • <i>profile-name</i>: Profile name of the configured WLAN. • <i>wlan-id</i>: Wireless LAN identifier. Range is from 1 to 512. • <i>SSID_Name</i>: SSID that can contain 32 alphanumeric characters. Note If you have already configured this command, enter the wlan profile-name command.
Step 3	security dot1x authentication-list <i>auth-list-name</i> Example: Device(config-wlan)# security dot1x authentication-list default	Enables security authentication list for dot1x security. The configuration is similar for all dot1x security WLANs.
Step 4	security web-auth Example: Device(config-wlan)# security web-auth	Enables web authentication.
Step 5	security web-auth authentication-list <i>authenticate-list-name</i> Example: Device(config-wlan)# security web-auth authentication-list default	Enables authentication list for dot1x security.
Step 6	security web-auth parameter-map <i>parameter-map-name</i> Example: Device(config-wlan)# security web-auth parameter-map WLAN1_MAP	Maps the parameter map. Note If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.
Step 7	no shutdown Example: Device(config-wlan)# no shutdown	Enables the WLAN.

Example

```
wlan wlan-test 3 ssid-test
security dot1x authentication-list default
security web-auth
security web-auth authentication-list default
```

```
security web-auth parameter-map WLAN1_MAP
no shutdown
```

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Select the required WLAN.
- Step 3** Choose **Security > Layer2** tab.
- Step 4** Select the security method from the **Layer 2 Security Mode** drop-down list.
- Step 5** In the Auth Key Mgmt, uncheck the **802.1x** check box.
- Step 6** Check the **PSK** check box.
- Step 7** Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.
- Step 8** Choose **Security > Layer3** tab.
- Step 9** Check the **Web Policy** checkbox to enable web authentication policy.
- Step 10** Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.
- Step 11** Click **Update & Apply to Device**.
-

Configuring WLAN for Preshared Key (PSK) and Local Web Authentication

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wlan profile-name wlan-id SSID_Name Example: Device(config)# wlan wlan-test 3 ssid-test	Enters WLAN configuration sub-mode. <ul style="list-style-type: none"> • <i>profile-name</i>- Is the profile name of the configured WLAN. • <i>wlan-id</i> - Is the wireless LAN identifier. Range is from 1 to 512. • <i>SSID_Name</i> - Is the SSID which can contain 32 alphanumeric characters.

	Command or Action	Purpose
		Note If you have already configured this command, enter <code>wlan profile-name</code> command.
Step 3	security wpa psk set-key <i>ascii/hex key password</i> Example: Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD	Configures the PSK shared key.
Step 4	no security wpa akm dot1x Example: Device(config-wlan)# no security wpa akm dot1x	Disables security AKM for dot1x.
Step 5	security wpa akm psk Example: Device(config-wlan)# security wpa akm psk	Configures the PSK support.
Step 6	security web-auth Example: Device(config-wlan)# security web-auth	Enables web authentication for WLAN.
Step 7	security web-auth authentication-list <i>authenticate-list-name</i> Example: Device(config-wlan)# security web-auth authentication-list webauth	Enables authentication list for dot1x security.
Step 8	security web-auth parameter-map <i>parameter-map-name</i> Example: (config-wlan)# security web-auth parameter-map WLAN1_MAP	Configures the parameter map. Note If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Example

```
wlan wlan-test 3 ssid-test
 security wpa psk set-key ascii 0 PASSWORD
 no security wpa akm dot1x
 security wpa akm psk
 security web-auth
 security web-auth authentication-list webauth
 security web-auth parameter-map WLAN1_MAP
```

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** Select the required WLAN.
- Step 3** Choose **Security > Layer2** tab.
- Step 4** Select the security method from the **Layer 2 Security Mode** drop-down list.
- Step 5** In the **Auth Key Mgmt**, uncheck the **802.1x** check box.
- Step 6** Check the **PSK** check box.
- Step 7** Enter the **Pre-Shared Key** and choose the PSK Format from the **PSK Format** drop-down list and the PSK Type from the **PSK Type** drop-down list.
- Step 8** Check the **MAC Filtering** check box to enable the feature.
- Step 9** With MAC Filtering enabled, choose the Authorization List from the **Authorization List** drop-down list.
- Step 10** Choose **Security > Layer3** tab.
- Step 11** Check the **Web Policy** checkbox to enable web authentication policy.
- Step 12** Choose the Web Auth Parameter Map from the **Web Auth Parameter Map** drop-down list and the authentication list from the **Authentication List** drop-down list.
- Step 13** Click **Update & Apply to Device**.
-

Configuring WLAN for PSK or Identity Preshared Key (iPSK) and Central Web Authentication

Configuring WLAN

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# <code>configure terminal</code>	Enters global configuration mode.
Step 2	wlan <i>profile-name</i> <i>wlan-id</i> <i>SSID_Name</i> Example: Device(config)# <code>wlan wlan-test 3 ssid-test</code>	Enters WLAN configuration sub-mode. <ul style="list-style-type: none"> • <i>profile-name</i> - Is the profile name of the configured WLAN. • <i>wlan-id</i> - Is the wireless LAN identifier. Range is from 1 to 512.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • <i>SSID_Name</i> - Is the SSID which can contain 32 alphanumeric characters. <p>Note If you have already configured this command, enter wlan profile-name command.</p>
Step 3	no security wpa akm dot1x Example: Device(config-wlan) # no security wpa akm dot1x	Disables security AKM for dot1x.
Step 4	security wpa psk set-key <i>ascii/hex key password</i> Example: Device(config-wlan) # security wpa psk set-key ascii 0 PASSWORD	Configures the PSK AKM shared key.
Step 5	mac-filtering <i>auth-list-name</i> Example: Device(config-wlan) # mac-filtering test-auth-list	Sets the MAC filtering parameters.

Example

```
wlan wlan-test 3 ssid-test
no security wpa akm dot1x
security wpa psk set-key ascii 0 PASSWORD
mac-filtering test-auth-list
```

Applying Policy Profile to a WLAN**Procedure**

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>policy-profile-name</i> Example: Device(config) # wireless profile policy policy-iot	Configures the default policy profile.

	Command or Action	Purpose
Step 3	aaa-override Example: Device(config-wireless-policy)# aaa-override	Configures AAA override to apply policies coming from the AAA or ISE servers.
Step 4	nac Example: Device(config-wireless-policy)# nac	Configures NAC in the policy profile.
Step 5	no shutdown Example: Device(config-wireless-policy)# no shutdown	Shutdown the WLAN.
Step 6	end Example: Device(config-wireless-policy)# end	Returns to privileged EXEC mode.

Example

```
wireless profile policy policy-iot
aaa-override
nac
no shutdown
```

Verifying Multiple Authentication Configurations

Layer 2 Authentication

After L2 authentication (Dot1x) is complete, the client is moved to *Webauth Pending* state.

To verify the client state after L2 authentication, use the following commands:

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-----
58ef.68b6.aa60  ewlcl_ap_1  3  Webauth Pending  11n(5)  Dot1x  Local
Number of Excluded Clients: 0

Device# show wireless client mac-address <mac_address> detail

Auth Method Status List

Method: Dot1x
Webauth State: Init
Webauth Method: Webauth
Local Policies:
Service Template: IP-Adm-V6-Int-ACL-global (priority 100)
```



```

URL Redirect ACL: IP-Adm-V6-Int-ACL-global
Service Template: IP-Adm-V4-Int-ACL-global (priority 100)
URL Redirect ACL: IP-Adm-V4-Int-ACL-global
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

```

```
Device# show platform software wireless-client chassis active R0
```

ID	MAC Address	WLAN	Client	State
0xa0000003	58ef.68b6.aa60	3		L3 Authentication

```
Device# show platform software wireless-client chassis active F0
```

ID	MAC Address	WLAN	Client	State	AOM ID	Status
0xa0000003	58ef.68b6.aa60	3		L3		Authentication. 730.

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary
```

Client Type Abbreviations:

RG - REGULAR BLE - BLE
HL - HALO LI - LWFL INT

Auth State Abbreviations:

UK - UNKNOWN IP - LEARN IP IV - INVALID
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:

UK - UNKNOWN IN - INIT
LC - LOCAL AN - ANCHOR
FR - FOREIGN MT - MTE
IV - INVALID

EoGRE Abbreviations:

N - NON EOGRE Y - EOGRE

CPP	IF_H	DP	IDX	MAC Address	VLAN	CT	MCVL	AS	MS	E	WLAN	POA
0X49		0XA0000003		58ef.68b6.aa60	50	RG	0	L3	LC	N	wlan-test	0x90000003

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary
```

Vlan	DP	IDX	MAC Address	VLAN	CT	MCVL	AS	MS	E	WLAN	POA
0X49	0xa0000003		58ef.68b6.aa60	50	RG	0	L3	LC	N	wlan-test	0x90000003

Layer 3 Authentication

Once L3 authentication is successful, the client is moved to *Run* state.

To verify the client state after L3 authentication, use the following commands:

```
Device# show wireless client summary
```

Number of Local Clients: 1

MAC Address	AP Name	WLAN	State	Protocol	Method	Role
-------------	---------	------	-------	----------	--------	------

58ef.68b6.aa60	ewlcl_ap_1	3	Run	11n(5)	Web Auth	Local
----------------	------------	---	-----	--------	----------	-------

Number of Excluded Clients: 0

Verifying Multiple Authentication Configurations

```
Device# show wireless client mac-address 58ef.68b6.aa60 detail

Auth Method Status List

Method: Web Auth
Webauth State: Authz
Webauth Method: Webauth
Local Policies:
Service Template: wlan_svc_default-policy-profile_local (priority 254)
Absolute-Timer: 1800
VLAN: 50

Server Policies:

Resultant Policies:
VLAN: 50
Absolute-Timer: 1800
```

```
Device# show platform software wireless-client chassis active R0
```

ID	MAC Address	WLAN	Client State
0xa0000001	58ef.68b6.aa60	3	Run

```
Device# show platform software wireless-client chassis active f0
```

ID	MAC Address	WLAN	Client State	AOM ID.	Status
0xa0000001	58ef.68b6.aa60.	3	Run	11633	Done

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary
```

Client Type Abbreviations:

RG - REGULAR BLE - BLE
HL - HALO LI - LWFL INT

Auth State Abbreviations:

UK - UNKNOWN IP - LEARN IP IV - INVALID
L3 - L3 AUTH RN - RUN

Mobility State Abbreviations:

UK - UNKNOWN IN - INIT
LC - LOCAL AN - ANCHOR
FR - FOREIGN MT - MTE
IV - INVALID

EoGRE Abbreviations:

N - NON EOGRE Y - EOGRE

CPP IF_H	DP IDX	MAC Address	VLAN	CT	MCVL	AS	MS	E	WLAN	POA
0X49	0XA0000003	58ef.68b6.aa60	50	RG	0	RN	LC	N	wlan-test	0x90000003

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath summary
```

Vlan	pal_if_hdl	mac	Input Uidb	Output Uidb
50	0xa0000003	58ef.68b6.aa60	95929	95927

Verifying PSK+Webauth Configuration

```
Device# show wlan summary
```

```
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is NTP, 12:08:32.941 CEST Tue Oct 6 2020
```

Number of WLANs: 1

ID Profile Name SSID Status Security

23 Gladius1-PSKWEBAUTH Gladius1-PSKWEBAUTH UP [WPA2][PSK][AES],[Web Auth]

