Multiple Authentications for a Client

- Multiple authentications for a client, on page 1
- Configure multiple authentications for a client, on page 2
- Verify multiple authentication configurations, on page 9

Multiple authentications for a client

Multiple authentications for a client is a network security feature that

- enables both Layer 2 (L2) and Layer 3 (L3) authentication for wireless client devices
- enhances security by requiring clients to complete multiple types of authentication before connecting, and
- applies only to regular client devices joining a wireless network.

Additional information

- You can enable both L2 and L3 authentication for a given SSID.
- Multiple authentications feature is not supported for guest or specialized client types.

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 Multiple Authentications for a Client feature supports multiple combinations of authentications for clients configured in the WLAN profile.

The table outlines the supported combinations of authentications for clients.

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

Unsupported combinations

The table outlines the combination of authentications on MAC failure that are not supported on a given client:

Authentication Types	Foreign	Anchor	Supported
WPA3-OWE+LWA	Cisco AireOS	Cisco Catalyst 9800 Controller	No
WPA3-SAE+LWA	Cisco AireOS	Cisco Catalyst 9800 Controller	No

Jumbo frame support for RADIUS packets

RADIUS packets are fragmented according to the MTU of the egress interface when you meet all of these conditions.

- The command **ip radius source-interface** is configured under the relevant AAA group server radius group to point to the egress interface.
- The **ip mtu NNN** command is configured on the egress interface.

Note If you set the MTU of the source interface to less than 1500 bytes, additional fragmentation can occur. This may cause packet drops by upstream devices, such as firewalls and load balancers. Authentication failures may result. Verify these configurations during upgrades to prevent these issues.

\

Configure multiple authentications for a client

Configure a WLAN for 802.1X and LWA

Set up a WLAN to enforce strong user authentication with 802.1X and provide local web authentication using the controller interface.

Perform this task when you want to secure WLAN user access with 802.1X credentials and enable local web authentication for guest or additional user workflows.

Before you begin

Confirm that WLAN profiles and the necessary authentication lists are already created or available.

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 the 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**.

The WLAN is now configured to use both 802.1X authentication and local web authentication policies.

Configure a WLAN for 802.1X and LWA (CLI)

Set up a WLAN to enforce strong user authentication with 802.1X and provide local web authentication using the controller interface.

Perform this task when you want to secure WLAN user access with 802.1X credentials and enable local web authentication for guest or additional user workflows.

Before you begin

Confirm that WLAN profiles and the necessary authentication lists are already created or available.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN.

Example:

```
Device(config)# wlan wlan-name wland-id SSID-name
```

- **wlan-name** is the name of the configured WLAN.
- **wlan-id** is the WLAN identifier. The range is one to 512.

- **SSID-name** is the SSID name which can have up to 32 alphanumeric characters.

If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.

Step 3 Enable security authentication list for dot1x security.

Example:

```
Device(config-wlan)# security dot1x authentication-list auth-list-name
```

The configuration is similar for all dot1x security WLANs.

Step 4 Enable web authentication.

Example:

```
Device(config-wlan)# security web-auth
```

Step 5 Enable authentication list for dot1x security.

Example:

```
Device(config-wlan)# security web-auth authentication-list default authenticate-list-name
```

Step 6 Map the parameter map name.

Example:

```
Device(config-wlan)# security web-auth parameter-map parameter-map-name
```

If a parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

Step 7 Enable the WLAN.

Example:

```
Device(config-wlan)# no shutdown
```

The WLAN is now configured to use both 802.1X authentication and local web authentication policies.

Configure WLAN for Preshared Key (PSK) and LWA (GUI)

Set up a WLAN to use both Preshared Key (PSK) and local web authentication via the graphical user interface.

Use this procedure when you want to enforce both PSK and local web authentication for user access to your wireless network.

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**. Next, choose the PSK Format from the **PSK Format** drop-down list. Then, choose 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. Then, choose the authentication list from the **Authentication List** drop-down list.

Step 11 Click **Update & Apply to Device**.

The selected WLAN now enforces both PSK and local web authentication settings

Configure WLAN for Preshared Key (PSK) and LWA (CLI)

Set up a WLAN to use both Preshared Key (PSK) and local web authentication.

Use this procedure when you want to enforce both PSK and local web authentication for user access to your wireless network.

Procedure

	Command or Action	Purpose
Step 1	Enter global configuration mode. **Example:** `Device# configure terminal`	
Step 2	Configure the WLAN. **Example:** `Device(config)# wlan wlan-name wland-id SSID-name`	• **wlan-name** is the name of the configured WLAN. • **wlan-id** is the WLAN identifier. The range is one to 512. • **SSID-name** is the SSID name which can have up to 32 alphanumeric characters. If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.
Step 3	Configure the PSK shared key using the **security wpa psk set-key** *ascii/hex key password* command. **Example:** `Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD`	
Step 4	Disable security AKM for dot1x. **Example:**	

	Command or Action	Purpose
	`Device(config-wlan)# no security wpa akm dot1x`	
Step 5	Configure the PSK support. **Example:** `Device(config-wlan)# security wpa akm psk`	
Step 6	Enable web authentication for WLAN. **Example:** `Device(config-wlan)# security web-auth`	
Step 7	Enable authentication list for dot1x security. **Example:** `Device(config-wlan)# security web-auth authentication-list authenticate-list-name`	
Step 8	Configure the parameter map. **Example:** `(config-wlan)# security web-auth parameter-map parameter-map-name`	If parameter map is not associated with a WLAN, the configuration is considered from the global parameter map.

The selected WLAN now enforces both PSK and local web authentication settings.

Configure WLAN for PSK or iPSK and CWA

Configure WLAN for PSK or iPSK and CWA (GUI)

Configure a WLAN to use either a Pre-Shared Key (PSK) or Identity Pre-Shared Key (iPSK) for authentication, and enable central web authentication for enhanced wireless security.

Use this task to set up secure WLAN access for users and devices, combining key-based authentication with web-based login, using your wireless controller's GUI.

Before you begin

Gather required PSK or iPSK values and authentication lists, as needed.

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**. Then, 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**.

The WLAN is now updated to use PSK or iPSK authentication and central web authentication, combining key-based access with web-based login for network users.

Configure WLAN for PSK or iPSK and CWA (CLI)

Configure a WLAN to use either a Pre-Shared Key (PSK) or Identity Pre-Shared Key (iPSK) for authentication, and enable central web authentication for enhanced wireless security.

Use this task to set up secure WLAN access for users and devices, combining key-based authentication with web-based login, using your wireless controller's CLI.

Before you begin

Gather required PSK or iPSK values and authentication lists, as needed.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the WLAN.

Example:

```
Device(config)# wlan wlan-name wland-id SSID-name
```

- **wlan-name** is the name of the configured WLAN.
- **wlan-id** is the WLAN identifier. The range is one to 512.
- **SSID-name** is the SSID name which can have up to 32 alphanumeric characters.

If you have already created and configured the WLAN, use the **wlan** *wlan-name* command.

Step 3 Disable security AKM for dot1x.

Example:

```
Device(config-wlan)# no security wpa akm dot1x
```

Step 4 Configure the PSK AKM shared key using the **security wpa psk set-key** *ascii/hex key password* command.

Example:

```
Device(config-wlan)# security wpa psk set-key ascii 0 PASSWORD
```

Step 5 Set the MAC filtering parameters.

Example:

```
Device(config-wlan)# mac-filtering auth-list-name
```

The WLAN is now updated to use PSK or iPSK authentication and central web authentication, combining key-based access with web-based login for network users.

Apply a policy profile to a WLAN

Configure and activate a policy profile for a WLAN using CLI.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the default policy profile.

Example:

```
Device(config)# wireless profile policy policy-iot policy-profile-name
```

Step 3 Configure AAA override to apply policies coming from the AAA or ISE servers.

Example:

```
Device(config-wireless-policy)# aaa-override
```

Step 4 Configure NAC in the policy profile.

Example:

```
Device(config-wireless-policy)# nac
```

Step 5 Shutdown the WLAN.

Example:

```
Device(config-wireless-policy)# no shutdown
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-wireless-policy)# end
```

The policy profile is applied to the WLAN and operational.

Verify multiple authentication configurations

Layer 2 authentication

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

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

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------------------------

58ef.68b6.aa60 ewlc1_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.
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 Abbrevations:
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 these commands:

```
Device# show wireless client summary

Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------------------------

58ef.68b6.aa60   ewlc1_ap_1  3     Run    11n(5)   Web Auth      Local
Number of Excluded Clients: 0
```

```
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 Abbrevations:
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_hd1        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]
```