Express Wi-Fi by Facebook

Information About Express Wi-Fi by Facebook

Express Wi-Fi by Facebook is a cloud-based, low-cost solution for local entrepreneurs and SMBs in emerging countries to provide Wi-Fi access. Using Express Wi-Fi by Facebook, users can buy data packs and find nearby hotspots.

Facebook provides the software (and sometimes hardware) infrastructure while the ISP or SMB provides internet connectivity and deployments to the subscribers. These service providers provision guest access through a captive portal. This can include both free and paid services including paid internet access with quota enforcement.

Express Wi-Fi by Facebook feature is enabled through a FlexConnect deployment based on the cloud-hosted Cisco Catalyst 9800 Series Wireless Controller where the Cisco AP performs client-related functions such as web authentication, captive portal redirect, matching and accounting of traffic classes and connection to the RADIUS server. This feature also supports FQDN (DNS ACLs) and IP ACLs as well as MAC authentication on the AP. The controller provisions the AP with the required configuration for these tasks.

Note If an AP reboots in standalone mode, the flexconnect URL ACL is not retained. This will cause Express Wi-Fi by Facebook to stop working.

The Express Wi-Fi by Facebook solution comprises the following components:

- Cisco Catalyst 9800 Series Wireless Controller

- Cisco Aironet Wave 2 or Catalyst APs
- Facebook infrastructure

Restrictions for Express Wi-Fi by Facebook

- Express Wi-Fi by Facebook is supported only in a FlexConnect deployment with local switching, local authentication, and local association.
- Express Wi-Fi by Facebook is supported only on Cisco Aironet Wave 2 and Catalyst access points.
- Only three traffic classes are supported.
- The AP supports only three ACLs per client.
- All APs forming a roaming domain should have Layer 2 reachability.
- Up to 64 complex rules and 512 simple rules per ACL are supported, where a simple rule comprises of a destination IP address and port. A complex rule contains more than a destination IP address and port information.
- Only RADIUS CoA messages with the Facebook attribute are supported on the AP.

Enabling Express Wi-Fi by Facebook NAC for Policy Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 On the **Policy** page, click the name of the desired Policy Profile.

Step 3 In the **Edit Policy Profile** window, click the **Advanced** tab.

Step 4 In the **AAA Policy** section, enable the **AAA override** . The AAA Override option of a WLAN enables you to configure the WLAN for identity networking. It enables you to apply VLAN tagging, Quality of Service (QoS), and Access Control Lists (ACLs) to individual clients based on the returned RADIUS attributes from the AAA server.

Step 5 Enable the **NAC State** check box to enable Cisco Network Admission Control (NAC).

Note You can enable NAC state only when AAA override is enabled.

Step 6 From the **NAC Type** drop-down list, select the type of NAC. The default is *XWF*.

Step 7 From the **Policy Name** drop-down list, choose a policy name.

Step 8 From the **Accounting List** drop-down list, choose an accounting list.

Step 9 Enable **Interim Accounting** to maintain a session with NAC.

Step 10 Click **Update & Apply to Device**.

Enabling Accounting RADIUS Server for Flex Profile (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.
Step 2 On the Flex page, click the name of the desired Flex Profile.
Step 3 In the **Edit Flex Profile** window, click the **Local Authentication** tab.
Step 4 Choose the desired server group from the **Local Accounting RADIUS Server Group** drop-down list.
Step 5 Select the **Local Client Roaming** check box.
Step 6 Click **Update & Apply to Device**.

Configuring Captive Portal for Express Wi-Fi by Facebook (GUI)

Procedure

Step 1 Choose **Configuration** > **Security** > **Web Auth**.
Step 2 On the **Web Auth** page, click the name of the desired parameter map.
Step 3 In the **Edit Web Auth Parameter** window, click the **Advanced** tab.
Step 4 In the **Redirect to External Server** section, select the **Express Wi-Fi Key Type** from the drop-down list.
Step 5 Enter the vendor specific key in the **Express Wi-Fi Key** field.
Step 6 Click **Update & Apply to Device**.

Configuring Captive Portal for Express Wi-Fi by Facebook (CLI)

Before you begin

- Configure the URL filter list.
- Configure the IP ACL.

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**parameter-map type webauth** *parameter-map- name* **Example:** `Device(config)# parameter-map type webauth FACEBOOK-MAP`	Creates a parameter map and enters parameter-map webauth configuration mode.
Step 3	**type webauth** **Example:** `Device(config-params-parameter-map)# type webauth`	Configures the webauth type parameter.
Step 4	**redirect for-login** *url-string* **Example:** `Device(config-params-parameter-map)# redirect for-login https://xwfcisco-us.expresswifi.com/customer/captive_portal`	Configures the URL string for redirection during login.
Step 5	**captive-bypass-portal** **Example:** `Device(config-params-parameter-map)# captive-bypass-portal`	Configures captive bypassing.
Step 6	**redirect vendor-specific xwf key 0** *vendor-key* **Example:** `Device(config-params-parameter-map)# redirect vendor-specific xwf key 0 vendor-key`	Configures the URL string for redirection during login.
Step 7	**end** **Example:** `Device(config-params-parameter-map)# end`	Returns to privileged EXEC mode.

Configuring Express Wi-Fi by Facebook Policy on Controller (CLI)

Before you begin

- Enable web authentication and MAC filtering on the WLAN.
- Configure RADIUS proxy server and accounting server.

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *policy-profile-name* **Example:** `Device(config)# wireless profile policy default-policy- profile`	Configures the wireless profile policy.
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	**no central switching** **Example:** `Device(config-wireless-policy)# no central switching`	Disables central switching and enables local switching.
Step 5	**no central association** **Example:** `Device(config-wireless-policy)# no central association`	Disables central association and enables local association for locally switched clients.
Step 6	**no central authentication** **Example:** `Device(config-wireless-policy)# no central authentication`	Disables central authentication and enables local authentication.
Step 7	**nac xwf** **Example:** `Device(config-wireless-policy)# nac xwf`	Configures NAC in the policy profile.
Step 8	**vlan** *vlan-name* **Example:** `Device(config-wireless-policy)# vlan 9`	Configures a VLAN name or VLAN ID.
Step 9	**no shutdown** **Example:**	Enables the profile policy.

	Command or Action	Purpose
	`Device(config-wireless-policy)# no shutdown`	
Step 10	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Configuring RADIUS Server for Accounting and Authentication in FlexConnect Profile (CLI)

Procedure

	Command or Action	Purpose
Step 1	configure terminal **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile-name* **Example:** `Device(config)# wireless profile flex default-flex- profile`	Configures the wireless flex profile and enters wireless flex profile configuration mode.
Step 3	**local-auth radius-server-group** *group-name* **Example:** `Device(config-wireless-flex-profile)# local-auth radius-server-group FB_GROUP`	Configures the authentication server group name.
Step 4	**local-accounting radius-server-group** *group-name* **Example:** `Device(config-wireless-flex-profile)# local-accounting radius-server-group group-name`	Configures the accounting server group name.
Step 5	**local-roaming** **Example:** `Device(config-wireless-flex-profile)# local-roaming`	Enables local roaming.
Step 6	**acl-policy** *policy-name* **Example:**	Configures ACL policy.

	Command or Action	Purpose
	`Device(config-wireless-flex-profile)# acl-policy fbs`	
Step 7	**urlfilter list** *list-name* **Example:** `Device(config-wireless-flex-profile)# urlfilter list fbs`	Applies the URL list to the Flex profile. Here, *list-name* refers to the URL filter list name. The list name must not exceed 32 alphanumeric characters. Note: For a given traffic class, the *list-name* should match the above ACL *policy-name*.
Step 8	**end** **Example:** `Device(config-wireless-flex-profile)# end`	Returns to privileged EXEC mode.

Verifying Express Wi-Fi by Facebook Configurations on Controller

To view ACLs applied on a specific client and the associated AP's MAC address, use the following command:

```
Device# show wireless client mac-address 0102.0304.0506 detail
[...]
Local Roaming Client:
Client ACLs: xwf,fbs
Client State Servers: a03d.6f6b.bebe, cc16.7edc.27d8
```

Verifying Express Wi-Fi by Facebook Configurations on the AP

To view client state, use the following command:

```
Device# show flexconnect client
```

To view all ACLs applied to a specific client, use the following command:

Device# **show client access-list {post-auth | pre-auth} all** *client_mac_address*

```
Device# show client access-list post-auth all 1C:36:BB:10:1B:2C
Post-Auth URL ACLs for Client: 1C:36:BB:10:1B:2C IPv4 ACL: xwf
Fbs
IPv6 ACL:
ACTION  URL-LIST
allow cisco.com
allow yahoo.com
allow google.com
allow xwf.facebook.com
allow xwf-static.xx.fbcdn.net allow cisco-us.expresswifi.com allow xwf-scontent.xx.fbcdn.net
 allow xwfcisco-us.expresswifi.com
Resolved IPs for Client: 1C:36:BB:10:1B:2C HIT-COUNT URL ACTION IP-LIST
xwf
rule 0:
```

```
rule 1:
rule 2:
rule 3:
rule 4:
rule 5:
rule 6:
allow true and ip proto 6 and dst port 22
allow true and ip proto 6 and src port 22
allow true and dst 171.70.168.183 mask 255.255.255.255 allow true and src 171.70.168.183
mask 255.255.255.255 allow true and dst 157.240.22.50 mask 255.255.255.255 allow true and
src 157.240.22.50 mask 255.255.255.255 allow true and src 30.1.1.155 mask 255.255.255.255
and dst
30.1.1.18 mask 255.255.255.255 and ip proto 1
rule 7: allow true and src 30.1.1.18 mask 255.255.255.255 and dst
30.1.1.155 mask 255.255.255.255 and ip proto 1 rule 8: allow true and ip proto 17 rule 9:
allow true and ip proto 17 rule 10: deny all
fbs
rule 0: allow true and dst 31.13.0.0 mask 255.255.0.0
rule 1: allow true and dst 66.220.0.0 mask 255.255.0.0
rule 6: allow true and src 31.13.0.0 mask 255.255.0.0
rule 10: allow true and src 179.60.0.0 mask 255.255.0.0
rule 12: allow true and dst 171.70.168.183 mask 255.255.255.255 rule 14: allow true and ip
 proto 17
        rule 16: deny all
No IPv6 ACL found
```

```
Device# show client access-list pre-auth all 1C:36:BB:10:1B:2C
Pre-Auth URL ACLs for Client: 1C:36:BB:10:1B:2C
IPv4 ACL: xwf
IPv6 ACL:
ACTION  URL-LIST
allow cisco.com
allow yahoo.com
allow google.com
allow xwf.facebook.com
allow xwf-static.xx.fbcdn.net allow cisco-us.expresswifi.com allow xwf-scontent.xx.fbcdn.net
 allow xwfcisco-us.expresswifi.com
Resolved IPs for Client: 1C:36:BB:10:1B:2C HIT-COUNT URL ACTION IP-LIST
xwf
rule 0: allow true and ip proto 6 and dst port 22
rule 1: allow true and ip proto 6 and src port 22
rule 2: allow true and dst 171.70.168.183 mask 255.255.255.255 rule 3: allow true and src
171.70.168.183 mask 255.255.255.255 rule 4: allow true and dst 157.240.22.50 mask
255.255.255.255 rule 5: allow true and src 157.240.22.50 mask 255.255.255.255 rule 6: allow
 true and src 30.1.1.155 mask 255.255.255.255 and dst
30.1.1.18 mask 255.255.255.255 and ip proto 1
rule 7: allow true and src 30.1.1.18 mask 255.255.255.255 and dst
30.1.1.155 mask 255.255.255.255 and ip proto 1 rule 8: allow true and ip proto 17 rule 9:
allow true and ip proto 17 rule 10: deny all
No IPv6 ACL found
Redirect URL for client: 1C:36:BB:10:1B:2C
https://xwfcisco-us.expresswifi.com/customer/captive_portal
```

To view authentication server details applied to a specific client, use the following command where the **wlan_id** ranges from 1 to 15:

Device# **show running-config authentication dot11radio {0 | 1} wlan** *wlan_id*

```
Device# show running-config authentication dot11radio 1 wlan 1
bssid=00:a7:42:f6:4a:8e ssid=aa_namsoo_webauth beacon_period=100
auth=LOCAL AP_OPER_MODE=CONNECTED AP_OPER_MODE from WPA=CONNECTED
AUTH_SERVER[0]=30.1.1.18 AUTH_SERVER_PORT[0]=2812 ACCT_SERVER[0]=30.1.1.18
ACCT_SERVER_PORT[0]=2813 AUTH_SERVER[0]=30.1.1.18 AUTH_SERVER_PORT[0]=2812
ACCT_SERVER[0]=30.1.1.18 ACCT_SERVER_PORT[0]=2813
```

To view client accounting details, use the following command:

Device# **show controller dot11Radio** *{0|1}* **client** *client_mac_address*

```
Device# show client access-list pre-auth redirect-url 1C:36:BB:10:1B:2C
Redirect URL for client: 1C:36:BB:10:1B:2C
https://xwfcisco-us.expresswifi.com/customer/captive_portal
```

To view DCDS (distributed client datastore) or roaming configuration details for an associated client, use the following command:

Device# **show dot11 clients data-store details** *client_mac_address*

```
Device# show dot11 clients data-store details 1C:36:BB:10:1B:2C
First AP Name: APF8B7.E2CC.5D48
Current AP Name: APF8B7.E2CC.5D48
Current AP IP: 30.1.1.169
Current AP BSSID: f8:b7:e2:cd:cb:8e
Current AP SSID: aa_namsoo_webauth
Client VLAN: 1
Client State: 4
Audit Session ID: 3204365612
Accounting Session ID High: 0
Accounting Session ID Low: 0
Client Traffic Class Name: xwf
Client Traffic Class Name: fbs
```