
cnPilot™ Enterprise AP Release Notes

cnPilot E400/e410/e430w/E500/E501S/E502S/e600
System Release 3.6



Introduction

This document provides information for the Cambium Networks cnPilot Enterprise AP system release 3.6.

The information in this document is subject to change without notice. The recommendations, technical data, configurations and statements in this document are believed to be reliable and accurate, but are presented without implied or express warranty. Users must take full responsibility for their applications of any product specified in this document. The information in this document is proprietary to Cambium Networks Ltd.



Note

Hostnames are only allowed to have the following characters 0-9/a-z/A-Z and hyphens. If a previously configured hostname had other characters those characters will be replaced with hyphens.

Supported Platforms

The following table provides details on the supported platforms:

- cnPilot E400 Indoor
- cnPilot e410 Indoor
- cnPilot e430w Indoor wall plate
- cnPilot e600 Indoor
- cnPilot E500 Outdoor
- cnPilot E501S Outdoor
- cnPilot E502S Outdoor



Note

Certain features may not be available on this product line and will be called out explicitly where not applicable.

Features introduced in 3.6 release

The following features are introduced in this release of cnPilot Enterprise AP:

Enhancements in Client Isolation

Earlier, when the client isolation feature was enabled, the communication between the wireless clients within same WLAN and across the WLANs within the same AP was stopped.

Starting with system release 3.6, the user can create exceptions to client isolation by creating Client Isolation Whitelists. The whitelist entries can be automatically learnt gateway entries or the statically added MAC entries.

Configuring a Client Isolation whitelist

You can configure the client isolation whitelist using only the CLI and the configuration using the UI will be implemented in a future release.

To enable Client Isolation functionality:

```
Host (config-wlan-1)# client-isolation
```

```
dynamic          : Enable client isolation network wide
```

```
mac-list         : Enter gateway or wired mac,supported mac formats xx:xx:xx:xx:xx:xx/xx-xx-xx-xx-xx-xx
```

To configure a client isolation whitelist:

```
Host (Config-wlan-1)# client-isolation dynamic
```

```
Host (config-wlan-1)# client-isolation mac list
```

To disable Client Isolation functionality:

```
E400-AFCB56(config-wlan-1)# no client-isolation
dynamic      : Disable network wide isolation (across AP isolation)
mac-list     : Enter gateway or wired mac to delete,supported mac formats xx:xx:xx:xx:xx:xx/xx-
xx-xx-xx-xx-xx
```

To disable a client isolation whitelist:

```
Host(config-wlan-1)# no client-isolation
Host(config-wlan-1)# no client-isolation dynamic
Host(config-wlan-1)# no client-isolation mac-list
```

To view a configured client isolation whitelist:

```
Host(config-wlan-1)# client-isolation mac-list AA:Bb:CC:44:66:77
#show config
wireless wlan 1
ssid bg_client_isolation_test1
no shutdown
vlan 1
security open
band both
dtim-interval 1
max-associated-client 127
client-isolation dynamic
client-isolation mac-list AA:BB:CC:11:22:33
client-isolation mac-list AA:Bb:CC:44:66:77
switchport trunk allowed vlan 1
```

Express Wi-Fi (XWF) Support On Wired Port

The Express Wi-Fi (XWF) is Facebook/Internet.org proprietary standard for Guest Access which works over RADIUS MAC Authentication for controlling guest client state. XWF Lite/XWF-FULL comprises of a server where the actual guest client state is maintained and the server talks to a centralized RADIUS server for sending the client state change messages to the end Access Points.

Usually the RADIUS server is located in the NOC for a given XWF Lite/XWF-FULL installation where it can talk directly to Wi-Fi Access points. The Wi-Fi WLAN is configured with guest-access enabled along with RADIUS based MAC Authentication and the MAC-AUTH-FALLBACK policy. The external page for the guest access configuration points to a XWF Server. It also requires the dynamic authorization to be enabled as the client state changes are dynamically updated by the XWF Server through the centralized RADIUS server to the Wi-Fi Access Points.

The RADIUS responses or the COA update contains Facebook vendor attributes along with quota limits for the given clients.

You can configure this feature in any of the interface (except management port).

To enable this feature:

1. Create a WLAN and configure everything needed for XWF to work with wireless clients.

2. Just one additional config required to extend it to wired port.
Under WLAN > Guest Access > Extend Interface. Enter the interface no here and Save.

Fixed Issues (System Release 3.6)

This section lists the fixed issues in this release of cnPilot Enterprise AP:

Tracking	Product	Description / Workaround
FLCN-2916	All	When managed through Autopilot, the UI did not show the status of Autopilot.
FLCN-3433	All	Redirection of XWF page takes ~80 secs with XWF-Full configuration.
FLCN-3627	All	Missing CNS URL in config causing aurora registration msg send failure.
FLCN-3649	All	COA requests client not found reply a NACK instead of silent drop.
FLCN-3684	All	In wired captive portal, laptop was not getting redirection page after overnight test when the quota got over
FLCN-3711	All	In wired XWF-Full, wired laptops were not getting redirection page and GA_allowed bit was not setting 1.
FLCN-3748	All	The static logout URL for wired GA clients has been fixed.
FLCN-35221	All	The user was not able to access internet until auto splash page was closed on MAC with XWF.

Known Issues (System Release 3.6)

This section lists the known issues in this release of cnPilot Enterprise AP:

Tracking	Product	Description / Workaround
FLCN-2915	All	In Autopilot configuration, a e600 AP cannot upgrade an e410 Access Point. Workaround: Upgrade e410 from its own device UI.
FLCN-3621	All	The status of PPPoE server is always displayed as disconnected when L2TP is enabled. Workaround: None.

Appendix

Supported list of WiFi Features

The following table lists the features that are supported in cnPilot Enterprise AP:

Supported Features	
Controller modes	<ul style="list-style-type: none"> Autonomous Controller-less operations (E.g: roaming) Cloud Managed On-premise virtualized controller
Secure WLAN	<ul style="list-style-type: none"> WPA-TKIP, WPA2 AES, 802.1x 802.11w (Protected Management Frames)
Hotspot 2.0/Passpoint	
Captive Portal/ Guest Access	<ul style="list-style-type: none"> cnMaestro controller Stand-alone AP based Redirection to external radius server Active Directory Integration
Authentication	Secure Web page, RADIUS based 802.1x including EAP-SIM/AKA, EAP-PEAP, EAP-TTLS, and EAP-TLS MAC authentication (local database or External RADIUS server)
Accounting	Supports RADIUS based accounting to multiple AAAs
Scheduled SSID	Turn SSID ON/OFF on a daily/weekly/time of day basis
VLAN	<ul style="list-style-type: none"> Dynamic VLAN assignment from RADIUS server. VLAN per SSID per user, VLAN load balancing
Data Limiting	Dynamic rate limiting of client traffic per SSID & per client
Subscriber QoS	WMM
Client Isolation	
Controller-Less Fast Roaming	<ul style="list-style-type: none"> Yes. 802.11r, Opportunistic Key Caching supports Enhanced roaming Disconnect for sticky clients
ACS: Automatic Channel Selection	Set at start or run periodically
NAT	
DHCP Server	
Firewall	NAT logging
ACL, DNS-ACL	L2, L3 or DNS based access control

Supported Features

Band Steering
Band Balancing

Airtime Fairness

Tunneling	<ul style="list-style-type: none"> • L2TP • L2oGRE • PPPoE
-----------	---

Tools	<ul style="list-style-type: none"> • Packet Capture • Wireless Sniffer • IP Connectivity • Wi-Fi Analyser • Tech Support (Logs)
-------	--

Services

APIs	Presence Locating API
------	-----------------------

Certifications	FCC, ETSI, CE EN 60601-1-2 (Medical EMC) UL2043 Plenum rated
----------------	--

Technical Support

For technical support, see

<http://www.cambiumnetworks.com/support>

Cambium Networks Community Forum

Join the conversation

<http://community.cambiumnetworks.com>