

E410

取扱説明書



HYTEC INTER Co., Ltd.

第 2 版

ご注意

- 本書の中に含まれる情報は、幣社（ハイテクインター株式会社）の所有するものであり、幣社の同意なしに、全体または一部を複写または転載することは禁止されています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期して作成いたしましたが、万一、ご不審な点や誤り、記載漏れなどのお気づきの点がありましたらご連絡ください。

改版履歴

第 1 版	2017 年 08 月 30 日	新規作成
第 2 版	2021 年 07 月 20 日	改版

ご使用上の注意事項

- 本製品をご使用の際は、取扱説明書に従って正しい取り扱いをしてください。
- 本製品を分解したり改造したりすることは絶対に行わないでください。
- 本製品を直射日光の当たる場所や、温度の高い場所で使用しないでください。本体内部の温度が上がり、故障や火災の原因になることがあります。
- 本製品を暖房器具などのそばに置かないでください。ケーブルの被覆が溶けて感電や故障、火災の原因になることがあります。
- 本製品をほこりや湿気の多い場所、油煙や湯気のあたる場所で使用しないでください。故障や火災の原因になることがあります。
- 本製品を重ねて使用しないでください。故障や火災の原因になることがあります。
- 通気口をふさがないでください。本体内部に熱がこもり、火災の原因になることがあります。
- 通気口の隙間などから液体、金属などの異物を入れないでください。感電や故障の原因になることがあります。
- 本製品の故障、誤動作、不具合、あるいは天災、停電等の外部要因によって、通信などの機会を逸したために生じた損害等の纯粹経済損害につきましては、弊社は一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品は、改良のため予告なしに仕様が変更される可能性があります。あらかじめご了承ください。
- 一般に無線LAN機器は誰でも自由に利用できるため、特定のユーザがチャンネルを独占することがないように、CSMA/CAと言う衝突回避方式を用いて、同じチャンネル上の複数のユーザが互いに譲り合いながら通信を行うようになっています。そのため、ユーザの数が増えたり通信量が増えたりすると実質的な通信速度が低下し、期待した通信速度が得られない場合があります。

目次

1. 製品概要	6
2. 梱包物一覧	6
2.1 E410 梱包物一覧	6
3. ハードウェア	7
4. インストレーション	8
4.1 天井設置	8
4.2 壁設置	8
5. 本マニュアルについて	9
6. システム構成例	10
6.1 ポイントツーポイント	10
6.2 WiFi - AP	10
7. 初期設定	11
7.1 cnMaestro	12
8. ネットワークの運用モード	14
8.1 ポイントツーポイントモードの設定例	14
8.2 WiFi-AP の設定例	19
9. モニタメニューについて	19
10. 設定変更の適用および設定変更の保存	19
11. 設定方法	21
11.1 System	21
11.2 Radio	25
11.3 Wireless LAN(WLAN)	28

11.4 Network	53
12. ファームウェアの管理	69
13. Troubleshoot	71
14. 困った時の対処法	72
15. 製品仕様	78
16. 製品保証	79

1. 製品概要

E410 は、小型軽量の無線 AP です。本製品は WiFi AP の他にポイントツーポイントの無線ブリッジとしても利用可能です。

IEEE802.11a/n/ac に準拠しており屋内外で使用可能な為、様々なソリューションでお使いいただけます。

2. 梱包物一覧

ご使用いただく前に本体と付属品を確認してください。万一、不足の品がありましたら、お手数ですがお買い上げの販売店までご連絡ください。

2.1 E410 の梱包物一覧



#	名称	数量
①		
②	天井設置用ブラケット	1
③	天井設置用プレート	1
④	天井設置用ネジ	4
⑤	壁設置用ネジ&アンカー	4
⑥	ゴム足	4

3. ハードウェア



リセットボタン

底面のリセットボタンを押すことで、機器の初期化(工場出荷モード)が可能です。

初期化・・・15秒長押し 電源LEDが緑から橙色に変わります。

LED

本体正面には、電源、LAN、を確認できる LED があります。



#	LED 表示	状態	表示内容
①	System LED	橙点灯	本体がブートアップ状態。
		緑点灯	ブート成功。 電源が入っていて動作状態。
②	Network LED	緑点灯	E50x が cnMaestro に接続されています。
		橙点灯	E50x が cnMaestro に接続されていません。

* cnMaestroはCambium Networks社のmanagement SWです。

(Cambium Networks社のホームページに登録することでご利用になれます。)

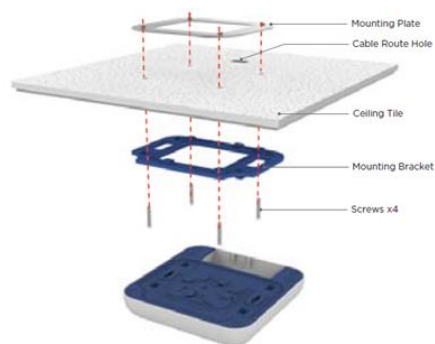
4. インストレーション

本製品には、ポールや壁取り付け用の部品が付属されています。
組み立てや設置の際は、以下の手順に従って作業してください。

4.1 天井設置

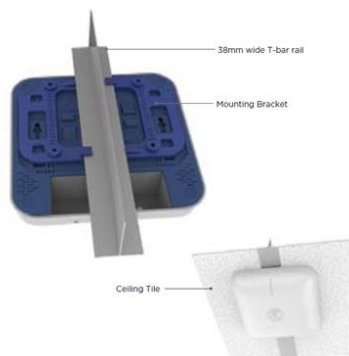
Step 1. ブラケットにクランプを差し込みます。

天井タイルにビス穴を4個開け、ブラケット、タイル、を介してプレート(予めタップが切っている)にねじ込みます。



Step 2. 天井に 38mm(または 24mm, 14mm) T-Bar レールが設置されている場合は、そのレールにはめ込むことも出来ます。

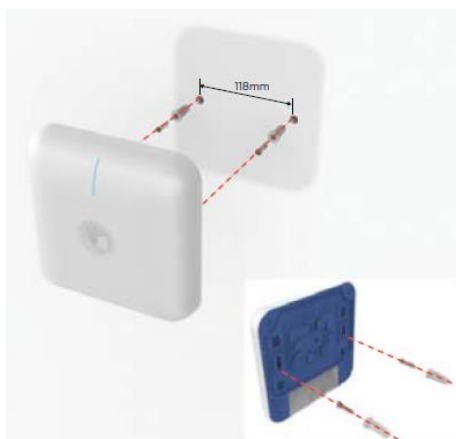
o



4.2 壁設置

Step 1. 壁設置用アンカーを壁に打ち込み、ネジをねじこみます。

Step 2. E410 本体をネジに取り付けてください。



5. 本マニュアルについて

必要な技術と知識

本マニュアルを効率的に使う為には、ネットワークの基本概念と無線接続によるインフラ構築の実用的な知識が必要です。

本マニュアルの表記規則

以下のシンボルが本マニュアルで使われています。



必須ではないが有益な追加情報です。



重要な情報であり注意してください。

略語リスト

略語	詳細
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
GMT	Greenwich Mean Time.
GUI	Graphical User Interface
LED	Light-Emitting Diode
MAC	Media Access Control
MIMO	Multiple Input, Multiple Output

NAT	Network address translation – translation of IP addresses (and ports)
PTP	Point To Point
PTMP	Point To Multi Point
PSK	Pre-Shared Key
QoS	Quality of Service
RSSI	Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
SISO	Simple Input, Simple Output
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2

6. システム構成例

6.1 WiFi – AP

本装置は Mesh-Off の設定で WiFi AP として動作し、複数のスマートフォンや、パソコンと接続が可能です。

周波数は 2.4GHz/5GHz どちらでも選択可能です。

6.2 ポイントツーポイント

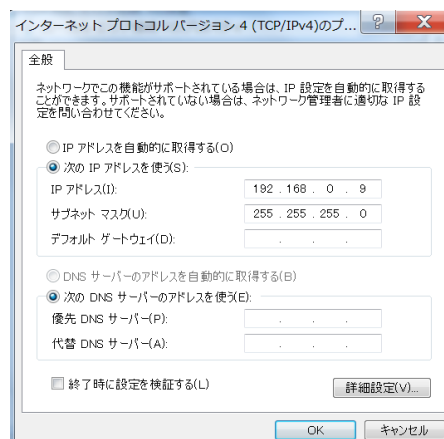
本装置は、アクセスポイントモード(Mesh-Base)とステーションモード(Mesh-Client)を使用することでポイントツーポイント接続が利用できます。周波数は 2.4GHz/5GHz どちらでも選択可能です。

7. 初期設定

本装置の初期設定（出荷時）

IP アドレス : 192.168.0.1
サブネットマスク : 255.255.255.0

WEB ブラウザを使用して本機器に接続するためには、パソコンの IP アドレスを 192.168.0.x、サブネットマスクを 255.255.255.0 に設定します。



PoE インジェクタの Ethernet ポートに Ethernet ケーブルを差し込み、そのケーブルをパソコンの Ethernet ポートに接続します。

WEB ブラウザに初期 IP アドレス 192.168.0.1 を入力すると、ログインページが表示されます。



初期 ID、パスワード

Login : admin

Password : admin

* ご注意： 社内イントラネットに接続した場合、本機器の初期 ip アドレス (192.168.0.x) が他のネットワーク機器と重複する場合があります。その際は、まずネットワークから切り離すようお願いいたします。



初期ログイン時に、使用国の設定を行う必要があります。

設定画面で、**Configure/System** 選択します。

必ず Country-Code に“**JAPAN**”が選択されていることを確認し、最後に”Save”ボタンを押してください。

The screenshot shows a configuration interface with the following fields and values:

- Name: E500-BEA65A
- Location: Tokyo
- Contact: (empty)
- Country-Code: Japan (highlighted with a red box)
- Placement: Indoor (selected), Outdoor (unselected)
- PoE Output: Off
- LED: (checked)

※JAPAN 以外を使用すると、電波法違反となる恐れがあります。

また、屋外使用の場合は Placement を outdoor に選択し”Save”します。屋外で屋内用の周波数を使用すると**法令違反となりますので止めてください。**

Ethernet2 の端子に IP カメラなどを接続する場合は PoE Output を **ON** に設定します。
(802.11af 対応で MAX 56V が出力されます。)

7-1 cnMaestro

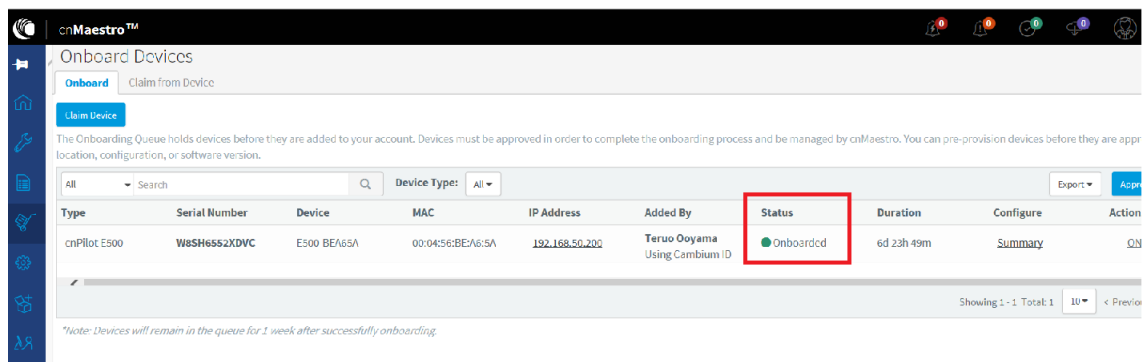
cnMaestroはCambium社のクラウド技術に基づいた次世代ネットワーク管理プラットフォームです。

Onboard Steps

次のステップで、E410をcnMaestroに接続できます。

1. Cambium Remote Managementを有効にします。
2. cnMaestro URLに <https://cloud.cambiumnetworks.com> を入力します。
3. Cambium IDを任意の名前で入力します。(例:HYTEC_SUPER)
4. Onboard Keyに8桁以上の英数字をパスワードとして入力します。
最後に”Save”します。
5. Cambium ホームページに予めお客様のメールアドレス、パスワードを登録しておきます。

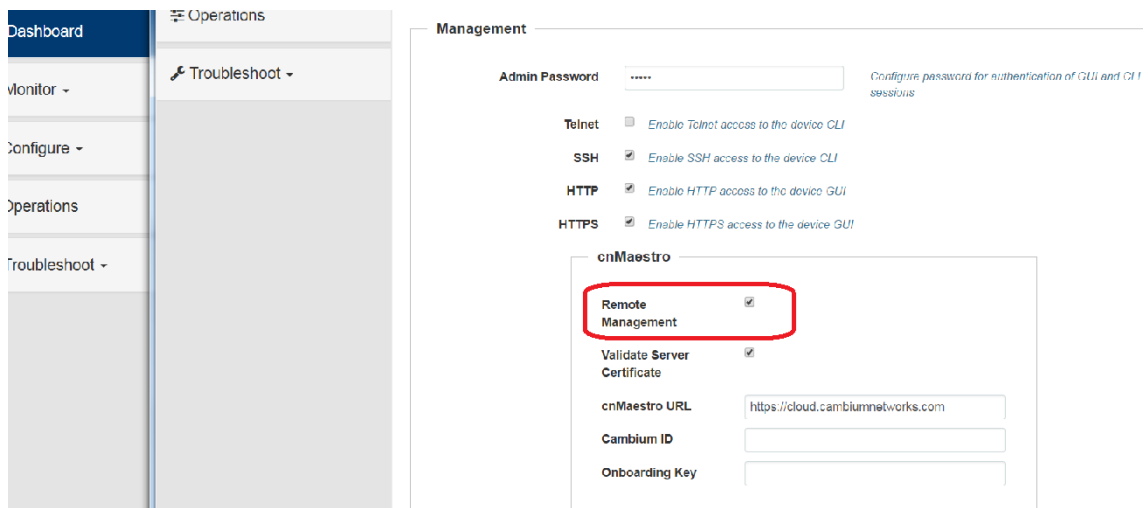
6. <https://cloud.cambiumnetworks.com/>から Create Accountで3項で入力したCambium ID (例:HYTEC_SUPER)を登録し、また、4項で入力した Onboard Keyを入力してアカウントを作成します。
 7. cnMaestro URLで、右上の名前をクリックするとCambium ID (例:HYTEC_SUPER)が現れるのでクリックするとcnMaestro画面が現れます。
 8. 左側の Manage/Dashboard から機器の状態(チャンネル、通信相手情報など)を確認することができます。
- また、Onboard が成功すると機器本体の正面下側にある LED が、橙色から緑色に変わります。



Type	Serial Number	Device	MAC	IP Address	Added By	Status	Duration	Configure	Action
cnPilot E500	W8SH6552XDVC	E500 BEA65A	00:04:56:BEA6:5A	192.168.50.200	Teruo Ooyama Using Cambium ID	Onboarded	6d 23h 49m	Summary	ON

Showing 1 - 1 Total: 1 10 < Previous

*Note: Devices will remain in the queue for 1 week after successfully onboarding.



Management

Admin Password:

Telnet: ☐ Enable Telnet access to the device CLI

SSH: ☒ Enable SSH access to the device CLI

HTTP: ☒ Enable HTTP access to the device GUI

HTTPS: ☒ Enable HTTPS access to the device GUI

cnMaestro

Remote Management: ☒

Validate Server Certificate: ☒

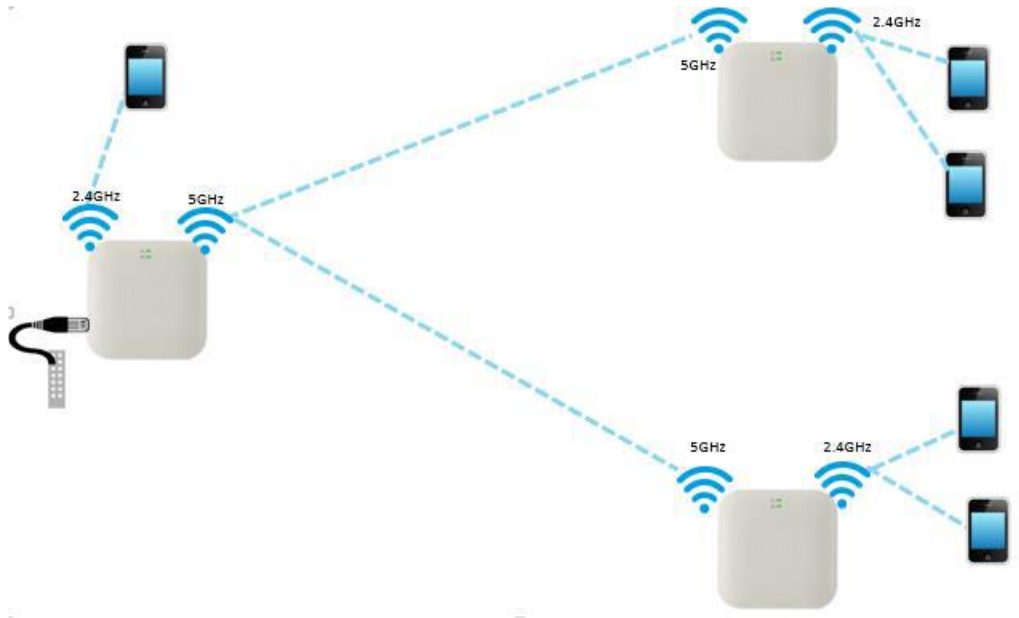
cnMaestro URL:

Cambium ID:

Onboarding Key:

8. ネットワークの運用モード

本製品は、以下のメッシュモードを切り替えることにより、ブリッジや WiFi AP として作動します。



8-1 ポイントツーポイントモードの設定例

まず本製品を二台用意し、一方を親機(Mesh-Base)として設定します。

- ステップ 1: パソコンと本製品を LAN ケーブルで接続して下さい。
(社内ネットワークと切り離すことを推奨します。)
- ステップ 2: パソコンが本製品のサブネットにセットされているかを確認してください。
(例) 192.168.0.150
- ステップ 3: WEB ブラウザを開いて IP アドレスを指定してください。
- ステップ 4: 初期設定 (192.168.0.1/24)
- ステップ 5: 初期パスワードを入力し、Sign In ボタンを押してください。

- ステップ 6: Configure/Radio タブをクリックし、2.4GHz, 5GHz とともに Enable を選択し、Channel、Channel Width、Transmit Power を入力し Save をクリックしてください。
- (2.4GHz は 20MHz のみです。また出力パワーの最大値は、2.4GHz: 16dBm, 5GHz:17dBm です。) Channel で Auto 以外は下の表に沿って設定します。
- (CH36 ~CH64 は 16dBm max.です。)

BW	W52				W53				W56				BW	2.4GHz	
	20MHz		40MHz	80MHz	20MHz		40MHz	80MHz	20MHz		40MHz	80MHz		20MHz	
	Ch.	Freq.			Ch.	Freq.			Ch.	Freq.				Ch.	Freq.
Frequency [MHz]	36	5180	5190	5210	52	5260	5270	5290	100	5500	5510	5530	Freq. [MHz]	1	2412
	40	5200	5190	5210	56	5280	5270	5290	104	5520	5510	5530		2	2417
	44	5220	5230	5210	60	5300	5310	5290	108	5540	5550	5530		3	2422
	48	5240	5230	5210	64	5320	5310	5290	112	5560	5550	5530		4	2427
									116	5580	5590	5610		5	2432
									120	5600	5590	5610		6	2437
									124	5620	5630	5610		7	2442
									128	5640	5630	5610		8	2447
									132	5660	5670	不可		9	2452
									136	5680	5670	不可		10	2457
									140	5700	不可	不可		11	2462
														12	2467
														13	2472

Edit Radio

Radio 1 (2.4GHz)

Radio 2 (5GHz)

Basic

Enhanced Roaming

Radio

Enable ☒ Enable operation of this radio

Channel Auto ▼

Channel Width 20MHz ▼

Transmit Power 16 ▼

Beacon Interval 100

Minimum Unicast rate 1 ▼

Multicast data rate Highest Basic ▼

Airtime Fairness ☐ Enable Airtime Fairness

Candidate Channels All ▼

Mode default ▼

ステップ 7: Configure/WLAN タブをクリックし、Add WLAN で AP 側は Mesh: Base, 任意の SSID 名を入力し、Radio を 2.4GHz または 5GHz を選択して Save をクリックしてください。

The screenshot shows the 'WLAN' configuration page. On the left is a sidebar with navigation items: Monitor, Configure, System, Radio, WLAN (selected), Network, Services, Operations, and Troubleshoot. The main area has a top bar with 'Add WLAN' and 'Edit WLAN' buttons. Below this are tabs for 'Basic', 'Radius Server', 'Usage Limits', and 'Access'. The 'Basic' tab is active, showing the following settings:

Enable	<input checked="" type="checkbox"/>
Mesh	Base
SSID	HYTEC_5
VLAN	1
Security	open
Radios	5GHz

次に本製品のもう一方を無線クライアント(子機)として設定します。

ステップ 1～6 は、親機(Mesh-Base)の初期設定例と同じです。

ステップ 7 Configure/WLAN タブをクリックし、Client 側は Mesh: Client を選択し、同じ SSID、Radio を選択します。
Network/StaticIP で AP とは違う IP アドレスに変更しておきます。

Monitor ▾

Configure ▾

System

Radio

WLAN

Network

Services

Operations

Troubleshoot ▾

Add WLAN

Edit WLAN

HYTEC_5 HYTEC_TEMP

Basic

Basic

Enable ☒

Mesh Client ▾

SSID HYTEC_5

VLAN 1

Security open ▾

Radios 5GHz ▾

Save Cancel





(Client は WLAN の 1 でのみ設定できます。)

ステップ 8

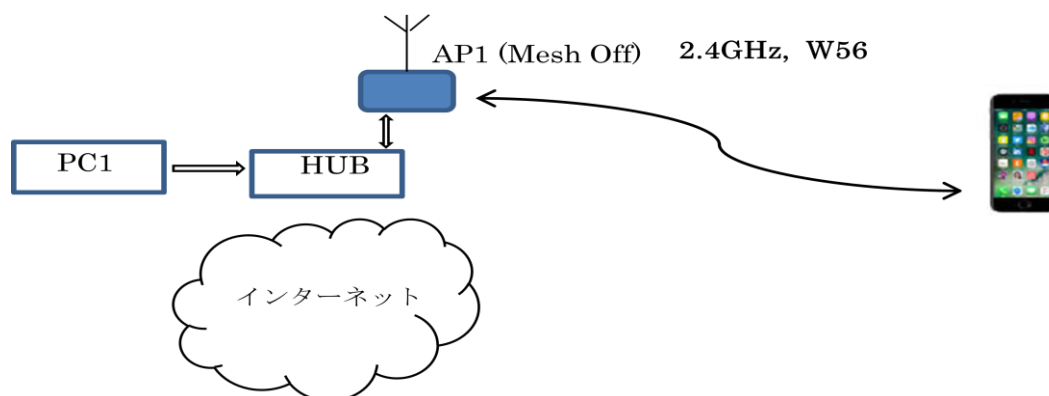
接続を確認するため、Dash Board ページに移動してください。稼働中の周波数が緑色で表示されます。また、通信が確立されている場合は Radio State が”ON”と表示されます。

Ethernet
1000M ETH1

RF Quality
 2.4GHz  5GHz

Radio Info		
Type	2.4GHz	5GHz
WLANS	1	1
Clients	0	0
Channel	6	140
Channel Width	20MHz	20MHz
Power	16	17
MAC Address	00-04-56-BE-B1-50	00-04-56-BE-C4-10
Transmitted packets	0 pkts/sec	0 pkts/sec
Received Packets	0 pkts/sec	0 pkts/sec
Average TX	540 bps	0 bps
Average RX	0 bps	0 bps
Mesh	base	base
Radio State	ON	DFS

8-2 WiFi-AP の設定例



- ステップ 1 本製品は Mesh-Off の設定にします。
- ステップ 2 スマホなどから本製品の SSID に接続します。
- ステップ 3 インターネットに接続する場合等、サーバから IP アドレスが付与される場合は、Configure/Network で IP アドレスを DHCP に設定します。また、必要に応じて Security を設定します。

9. モニタメニューについて

このメニューから、システムの必要な情報が得られます。

wlan0							
SSID	HYTEC_24						
VLAN	1						
Security	open						
Radios	2.4GHz						
Clients	1						
Guest Access	disabled						
RX Bpps	0 bps						
RX Bytes	111169						
RX Packets	260						
RX pps	0						
TX Bpps	1.5 Kbps						
TX Bytes	73248						
TX Packets	379						
TX pps	1						

wlan1							
Wireless Mesh							
MESH-BASE	MESH-CLIENT	IP	BAND	SNR	RSSI	STATUS	
00-04-56-BE-B1-50	00-04-56-BE-B8-30	192.168.50.201	2.4GHz	51	-56	UP	

また、Base (Client)側両方の MAC アドレスや RSSI レベル(受信信号レベル)を得ることが出来ます。

10. 設定変更の適用および設定変更の保存

Save **Configure** の各ページで **Save** ボタンがクリックされると新しい設定が即座に適用されメモリに記憶されます。



パラメータを変更した Web GUI タブごとに **Save** ボタンをクリックする必要があります。

場合によって、Reboot が必要な場合があります。(ファームウェアアップデート時など)

ど)

11. 設定方法

Configure

11-1 System

Parameter	Description	Range	Default
Name	デバイスのホスト名。設定可能な文字数は最大 64 文字。	–	E410-ESN の最後の 3 文字
Location	デバイスの置かれた場所。設定可能な文字数は最大 64 文字。	–	–
Contact	デバイスのコンタクト情報。	–	–
Country-Code	デバイスを運用する国を設定します。許可されているチャネルと送信パワーは国によって変わります。この項目を設定しないと無線は機能しません。必ず Japan を選択してください。	–	–
Placement	cnPilot デバイスは屋内と屋外どちらの運用もサポートします。 Indoor: 選択すると、カントリーコードに対応した屋内用チャネルが有効化します。 Outdoor: 選択すると、カントリーコードに対応した屋外用チャネルが有効化します。	–	Indoor
PoE Output	標準的な 802.3af デバイスや Cambium デバイスの電源供給に対応します。 •Cambium-PoE •802.3af	–	Disabled
LED	運用中に LED を点灯させるため、LED チェックボックスを選択します	–	Enabled
LLDP	L2 ネットワークでデバイスの機能や情報をアドバタイズするための項目です。	–	Enabled

System

Name Hostname of the device (max 64 characters)

Location Location where this device is placed (max 64 characters)

Contact Contact information for the device (max 64 characters)

Country-Code For appropriate regulatory configuration

Placement ☒ Indoor ☐ Outdoor Configure the AP placement details

PoE Output Enable Power-over-Ethernet to an auxiliary device connected to ETH2

LED ☒ Whether the device LEDs should be ON during operation

LLDP ☒ Whether the AP should transmit LLDP packets

Management

Parameter	Description	Range	Default
Admin Password	UI と CLI セッションの認証に使うパスワード	–	admin
Autopilot	未サポートとなります。		
Telnet	デバイス CLI への Telnet アクセスを有効にします。	–	Disabled
SSH	デバイス CLI への SSH アクセスを有効にします。	–	Enabled
SSH Key	SSH キーを使ってデバイスにログインする設定。公開鍵を入力する必要があります。設定すると、AP に秘密鍵を使ってログインする必要があります。CLI と GUI のどちらにも適用されます。	–	Disabled
HTTP	デバイス UI への HTTP アクセスを有効にします。	–	Enabled
HTTP Port	デバイス UI にアクセスするための HTTP ポート番号を設定する項目	1–65535	80
HTTPS	デバイス UI への HTTPS アクセスを有効にします。	–	Enabled
HTTPS Port	デバイス UI にアクセスするための HTTPS ポート番号を設定する項目	1–65535	443
RADIUS Mgmt Auth	ユーザーは、RADIUS 認証を使用して AP へのログインを制御可能です。有効にすると、ユーザーが提供したすべてのクレデンシャルは RADIUS 認証を受けま す。成功した場合、AP の UI へのログインが許可され、CLI と GUI の両方に適用されます。	–	Disabled
RADIUS Server	マネジメント認証のための RADIUS IPv4 サーバを設定する項目です。	–	–
RADIUS Secret	マネジメント認証のための RADIUS shared secret を設定する項目です。	–	–
cnMaestro			
Cambium Remote Mgmt	このデバイスの Cambium Remote Management のためのサポートを有効にします。	–	Enabled
Validate Server Certificate	cnMaestro と cnPilot デバイス間の HTTPs 接続を可能にします。	–	Enabled
cnMaestro URL	IPv4/IPv6/URL を使用しデバイスをオンボードする静的な項目。	–	–
Cambium ID	このデバイスで cnMaestro にログインするのに使用する Cambium ID を設定します。	–	–
Onboarding Key	cnMaestro にデバイスをオンボードするのに使うパスワード	–	–
SNMP			
Enabled	デバイス上で SNMPv2 または SNMPv3 サポートを有効にする項目	–	–
SNMPv2c RO community	SNM v2c 読み取り専用コミュニティストリング	–	–
SNMPv2c	SNM v2c 読み取り/書き込みコミュニティストリング	–	–

RW community			
Trap Receiver IP	SNMPトラップレシーバーIPv4 サーバを設定する項目	–	–
SNMPv3 Username	SNMPv3 のユーザー名を入力します。	–	–
SNMPv3 Password	SNMPv3 のパスワードを入力します。	–	–
Authentication	MDS か SHA から認証タイプを選択します。	–	MDS
Access	RO(読み取り専用)または RW(読み取り・書き込み)からアクセスタイプを選択	–	RO
Encryption	ON または OFF を選択	–	ON

Management

Admin Password Configure password for authentication of GUI and CLI sessions

Autopilot Autopilot Management of APs

Telnet ☐ Enable Telnet access to the device CLI

SSH ☒ Enable SSH access to the device CLI

SSH Key Use SSH keys instead of password for authentication

HTTP ☒ Enable HTTP access to the device GUI

HTTP Port Port No for HTTP access to the device GUI(1-65535)

HTTPS ☒ Enable HTTPS access to the device GUI

HTTPS Port Port No for HTTPS access to the device GUI(1-65535)

RADIUS Mgmt Auth ☒ Enable RADIUS authentication of GUI/CLI sessions

RADIUS Server RADIUS server IP/hostname

RADIUS Secret RADIUS server shared secret

cnMaestro

Remote Management ☒

Validate Server Certificate ☒

cnMaestro URL

Cambium ID

Onboarding Key

SNMP

Enable ☒ Enable/Disable SNMP

SNMPv2c RO community SNMP v2c read-only community string (max 64 characters)

SNMPv2c RW community SNMP v2c read-write community string (max 64 characters)

Trap Receiver IP SNMP trap server ip address

SNMPv3 Username SNMPv3 user name (max 32 characters)

SNMPv3 Password SNMPv3 password (8 to 32 characters)

Authentication

Access

Encryption

Time Settings

Parameter	Description	Range	Default
NTP Server 1	Network Time Protocol Server 1 の名前または IPv4 アドレス	–	–

NTP Server 2	Network Time Protocol Server 2 の名前または IPv4 アドレス	—	—
Time Zone	Time zone は AP が設置された場所から設定可能です。ドロップダウンリストから適切なタイムゾーンを選択し、device clock が実際の時間と同じか確認します。 注意: AP 上に正確な時間を設定することは WLAN Scheduled Access や Syslog 等の機能において重要です。	—	—

Time Settings

NTP Server 1: pool.ntp.org Name or IP address of a Network Time Protocol server

NTP Server 2: in.pool.ntp.org

Time Zone: Asia/Bangkok Configure Timezone

Current System Time: Wed 10 Apr 2019 16:20:49 IST

Event Logging

Parameter	Description	Range	Default
Syslog Server 1	Syslog サーバのホスト名か IPv4/IPv6 アドレスと対応するポート番号	—	514
Syslog Server 2	Syslog サーバのホスト名か IPv4/IPv6 アドレスと対応するポート番号	—	514
Syslog Severity	サーバに転送しなければならないログの深刻度を設定する機能。サポートされるログレベルは RFC に準じる	—	Debug

Event Logging

Syslog Server 1: 10.110.211.97 **Port** 514 Name or IPv4/IPv6 address of syslog server

Syslog Server 2: 10.110.219.10 **Port** 1234

Syslog Severity: Debug (level 7) Specify severity of events forwarded to Syslog servers

Save Cancel

11-2 Radio

Configuring Radio Parameters

Parameter	Description	Range	Default
Radio			
Enable	ラジオのオペレーションを有効化	–	Disabled
Channel	ドロップダウンリストからチャンネルを選択可能です。それらのチャンネルは Configure > System UI にて選択した国に基づきます。	2.4GHz: 1 – 14 5GHz: 36 – 173	
Channel Width	チャンネル幅を選択可能。 2.4GHz: 20MHz のみサポート。 5GHz: 20, 40, 80MHz をサポート。	–	2.4GHz: 20MHz 5GHz: 80MHz
Transmit Power	カバレッジと SLA に基づき、各無線機の送信電力を設定可能です。送信電力の単位は dBm で、範囲は 4～17 ですデフォルト値は AUTO で、無線の送信電力が最大に設定されます。	2.4GHz: 4 – 16 5GHz: 4 – 17 (W56) 4–16 (W53)	Auto
Beacon Interval	2 つの連続した Beacon の間の時間を設定可能です。	50ms – 3400ms	100
Minimum Unicast rate	デバイスのカバーエリアを調節する項目です。高いレートを設定すると範囲は狭くなります。運用上の SLA に基づきこの値を設定可能です。ドロップダウンリストには、レガシーレート、HT レート、VHT レートなど、cnPilot デバイスでアダプタイズされるすべての値が含まれます。	Standard 802.11b と 802.11g データレート	1Mbps
Multicast data rate	マルチキャストトラフィックレートを設定する項目です。cnPilot デバイスに接続されるワイヤレスステーションの種類に応じて変更される。ドロップダウンリストには、highest-basic、lowest-basic、highest-supported があります。	–	2.4GHz に Highest Basic 5GHz に Lowest Basic
Airtime Fairness	Airtime Fairness は、レガシー 11abg クライアントが存在する場合に、11n および 11ac クライアント (HT クライアント) のパフォーマンスを向上させるための AP 上のソリューション。レガシークライアントは、HT クライアント (11n および 11ac クライアント) と比較して、データの送受信に多くのエアタイムを必要とします。このため、HT クライアントの全体的なスループットが低下します。この機能を有効にすると、レガシークライ	–	Disabled

	<p>アントを抑制することで、HT クライアントのパフォーマンスが向上します。</p> <p>高速クライアント(802.11n/802.11ac)と比較して、低速クライアント(802.11a/802.11bg)は、同じサイズのデータを送信するために、より多くのエアタイムを消費し、その結果、高速クライアントのスループットは、より少ない送信機会(より少ないエアタイム)を得るために低下します。この機能を有効にすると、低速のクライアントが多い無線ネットワークにおいて、高速のクライアントのパフォーマンスが向上します。この機能は、遅いクライアントのエアタイムを制御することで実現します。</p>		
Candidate Channels	<p>ユーザーの要求に応じて選択したチャンネルを設定可能です。オプションは操作するバンドによって異なり、以下の通りです。</p> <p>2.4GHz: All, Specific</p> <p>5GHz: All, Specific, Prefer Non-DFS, Prefer DFS</p>	<p>2.4GHz: 1 – 14</p> <p>5GHz: 36 – 173</p>	All
Mode	<p>全ての cnPilot デバイスは 802.11ac Wave 1 または 802.11ac Wave 2 に対応しています。レガシークライアントの中には、期待通りに動作しないものがあります。そのため、このパラメータは、ワイヤレスクライアントに基づいて下位互換性を調整可能です。</p>	<p>2.4GHz: b, bg, n, gn</p> <p>5GHz: a, ac, an, n, n-ac</p>	<p>2.4GHz: 11n mixed mode</p> <p>5GHz: 11ac</p>
Short Guard Interval	cnPilot デバイスのスループットを向上させるための標準的な 802.11 パラメータ	–	Enabled
Off Channel Scan(OCS)			
Enable	ネイバークライアントと AP をキャプチャするため、デバイス上で OCS を有効にする項目	–	–
Dwell-time	チャンネル上にある Wi-Fi デバイスをスキャンするのにかける時間を設定します。	50 – 300	50ms
Auto-RF			
Enable	auto-rf をデバイス上で有効にする項目	–	Disabled
Channel Selection Mode	<p>AutoRF はチャンネル選択において 2 つのモードをサポートします。</p> <ul style="list-style-type: none"> ・干渉ベース ・チャンネル利用ベース 	–	Interference
Channel Hold Mode	自動 RF アルゴリズムによって選択された同じチャンネルを、選択後のチャンネルの品質に関わらず、デバイスが利用するための時間を設定します	5 – 1800	120 Min
Channel Utilization Threshold	自動 rf によるチャンネル選択のトリガーとなる利用率のしきい値を設定します。	20 – 40	25%
Interference Avoidance			
Packet	設定された閾値が満たされたときに、現在のチャンネル	0 – 100	30%

Error Rate Threshold	ルから移動するためのトリガーメカニズム。		
Enhanced Roaming			
Enable	デバイスのエンハンスドローミングを有効にする項目	-	Disabled
Roam SNR threshold	cnPilot 端末は、AP が設定された SNR 以下で見られたときに、AP の認証を解除するトリガーとなります。	1 - 100	15dB

Radio

☒ Enable Enable operation of this radio

Channel: Primary operating channel

Channel Width: Operating width of the channel

Transmit Power: Radio transmit power in dBm (4 to 30, Subject to regulatory limit)

Beacon Interval: Beacon interval in mSec (50 to 3400)

Minimum Unicast rate: Configure the minimum unicast management rate (Mbps)

Multicast data rate: Data-rate to use for transmission of multicast/broadcast packets

Airtime Fairness: ☐ Enable Airtime Fairness

Candidate Channels:

Mode: All modes clients are allowed

☒ Short Guard Interval Enable short guard interval

Off Channel Scan

☐ Enable Enable OCS

Dwell-time: Configure Off Channel-Scan dwelltime in milliseconds (50-300)

Auto RF

☒ Enable Enable Auto RF

Channel Selection Mode: Channel selection done based on interference

Channel Hold Time: Configure channel hold time in minutes (5-1800)

Channel Utilization Threshold: Configure channel utilization threshold in % (20-40)

Interference Avoidance

Packet Error Rate Threshold: Configure packet error rate threshold in % (0-100)

☐ Enable Enable active disconnection of clients with weak signal

Roam SNR threshold: SNR below which clients will be forced to roam (1-100 dB)

11-3 Wireless LAN(WLAN)

Basic

Parameters	Description	Range	Default
Enable	WLAN プロファイルを有効にするオプション。有効にすると、WLAN プロファイルで設定された SSID と各パラメータを含むビーコンがブロードキャストされます	–	–
Mesh	<p>このパラメータは WDS 接続が cnPilot デバイスにおいて確立された場合に必要となります。このパラメータでは 4 つのオプションが利用可能です。</p> <ol style="list-style-type: none"> 1. Base メッシュベースで構成され、通常の AP のように動作する WLAN プロファイル。無線機は起動時にビーコンを行うので、メッシュクライアントとして設定された無線機からその SSID を確認できます。 2. Client mesh-client を設定した WLAN プロファイルは、起動時に利用可能なすべてのチャンネルをスキャンし、接続するメッシュベースの AP を探します。 3. Recovery メッシュリカバリーとして設定された WLAN プロファイルは、接続が成功した後、メッシュリンクの障害を検出すると、事前に設定された SSID をブロードキャストします。これはメッシュベースのデバイス上で排他的に設定する必要があります。メッシュクライアントは、メッシュリンクの障害時にメッシュリカバリー SSID を自動スキャンします。 4. Off WLAN プロファイルでメッシュサポートを無効化します。 	–	OFF(Access Profile Mode)
SSID	ワイヤレスステーションがスキャンして関連付ける固有のネットワーク名	–	–
VLAN	VLAN は、ネットワーク上でワイヤレスステーションのトラフィックと AP のトラフィックを分離するために設定されます。ワイヤレスステーションは、WLAN プロファイルの VLAN フィールドで設定されたサブネットから IP アドレスを取得します。	1 – 4094	1
Security	<p>このパラメータは、選択されたアルゴリズムに基づいて暗号化されるキー値を決定します。cnPilot デバイスでは、以下のセキュリティ方式がサポートされます。</p> <ol style="list-style-type: none"> 1. Open この方法は、ネットワークにレイヤ 2 認証が構築されている場合に適します。cnPilot デバイスにこの設定がされていると、どのワイヤレスステーション 	–	Open

	<p>オンでも接続可能です。</p> <p>2. Osen この方法は、cnPilot デバイスで Passpoint 2.0 が有効になっている場合に多用されます。Passpoint 2.0 が無効になっている場合、このセキュリティはワイヤレスステーションのアソシエーションには影響しません。</p> <p>3. WPA2-Pre-Shared Keys このモードは AES 暗号化でサポートされます。</p> <p>4. WPA2 Enterprise このセキュリティタイプでは、802.1x 認証を使用してワイヤレスステーションを関連付けます。これは、認証方法の中央管理システムです。</p>		
Passphrase	設定されたセキュリティ方式に基づいて鍵を生成するための鍵値となる文字列。	–	12345678
Radios	<p>各 SSID は、配備の要件に応じて送信するように設定可能です。通常のアクセスプロファイルでは、SSID の送信モードを設定できるオプションがあります</p> <ul style="list-style-type: none"> ▪ 2.4GHz and 5GHz ▪ 2.4GHz ▪ 5GHz <p>メッシュ用プロファイルには以下のオプションも有効です</p> <ul style="list-style-type: none"> ▪ 2.4GHz ▪ 5GHz 	–	2.4GHz and 5GHz
VLAN Pooling	<p>このパラメータは、複数のサブネットにクライアントを分散させる場合に必要です。cnPilot デバイスは、導入サイトで利用可能なインフラに基づいて、異なるモードの VLAN プーリングをサポートします。サポートするモードは以下のとおりです。</p> <p>1. Disabled この機能は、この WLAN に対しては無効</p> <p>2. Radius Based このモードをサポートするためには、ユーザは WPA2 Enterprise を設定する必要があります。関連付けの段階では、cnPilot は RADIUS トランザクションからプール名を取得し、端末の VLAN への分散状況に基づいて、cnPilot は適切な VLAN を選択し、端末は cnPilot デバイスによって選択された VLAN に IP アドレスを要求します。</p> <p>3. Static このモードをサポートするためには、ユーザは Configure > Network > VLAN で VLAN プールの詳細を設定する必要があります。アソシエーションフェーズでは、cnPilot がプールを取得し、VLAN 上のワイヤレスステーションの分布状況に基づいて、cnPilot が適切な VLAN を選択し、ワイ</p>	–	Disabled

	ヤレスステーションは cnPilot デバイスが選択した VLAN に IPv4/IPv6 アドレスを要求します。		
Max Clients	1 つの WLAN プロファイルに関連付けることができる端末の最大数を指定します。2.4GHz が 256、5GHz が 128、同時利用が 256 です	1-256	127
Client Isolation	<p>ネットワーク上または AP 上で無線の局間通信を禁止する必要がある場合、この機能を有効にする必要があります。必要に応じて 3 つのオプションを設定可能です。</p> <ol style="list-style-type: none"> 1. Disable このオプションを選択すると、クライアントアイソレーション機能が無効になります。つまり、どの端末も他の端末と通信可能です。 2. Local このオプションを選択すると、クライアントアイソレーション機能が有効化します。このオプションは、同じ AP に接続されたワイヤレスステーションの通信を防止します。 3. Network Wide このオプションを選択すると、クライアントアイソレーション機能が有効になります。同じネットワークに配置されている、異なる AP に接続されたワイヤレスステーション同士の通信を防ぎます。 4. Network Wide Static このオプションを設定すると、ネットワーク上でのクライアント分離機能が有効化します。サブネットを越えてデバイスにアクセスするには、ユーザーがゲートウェイ MAC を設定する必要があります。 注: この項目を選択すると、ユーザーはクライアント隔離 MAC リストに MAC アドレスを追加可能です。最大 64 個の MAC アドレスを追加できます。 	–	Disabled
cnMaestro Managed Roaming	デフォルトで cnPilot デバイスはレイヤ 2 ローミングをサポートしています。このオプションはレイヤ 3 ローミングを可能にします。cnPilot デバイスを cnMaestro に接続することは必須です。レイヤ 3 ローミングはゲストアクセスのみに有効です。	–	Disabled
Hide SSID	Wi-Fi デバイスの基本的なセキュリティモードであり、有効になっていると SSID を表示しません。	–	Disabled
Session Timeout	このフィールドは、ゲストではないワイヤレスステーションに固有のものです。端末が接続すると、セッションタイマーが起動します。セッション時間が経過すると、端末は状況に応じて再認証または再アソシエーションを行う必要があります。デフォルトではこの機能は有効になっています。	60 – 604800	28800
Inactivity	cnPilot デバイスと cnPilot デバイスに関連付けられた	60 –	1800

Timeout	端末との間で通信が行われなくなると、Inactivity タイマーが発生します。タイマーが設定された Inactivity タイムアウト値に達すると、AP はその無線ステーションに認証解除を送信します。デフォルトではこの機能は有効です。	28800	
Drop Multicast Traffic	有効にすると、WLAN に出入りするすべてのマルチキャストをドロップします。	–	Disabled

Basic

Enable ☒

Mesh Mesh Base/Client/Recovery mode

SSID The SSID of this WLAN (upto 32 characters)

VLAN Default VLAN assigned to clients on this WLAN. (1-4094)

Security Set Authentication and encryption type

Passphrase WPA2 Pre-shared Security passphrase or key

Radios Define radio types (2.4GHz, 5GHz) on which this WLAN should be supported

VLAN Pooling Configure VLAN pooling

Max Clients Default maximum Client assigned to this WLAN. (1-256)

Client Isolation When selected, it allows wireless clients connected to the same AP or different APs to communicate with each other in the same VLAN

cnMaestro Managed Roaming ☐ Enable centralized management of roaming for wireless clients through cnMaestro

Hide SSID ☐ Do not broadcast SSID in beacons

Session Timeout Session time in seconds (60 to 604800)

Inactivity Timeout Inactivity time in seconds (60 to 28800)

Drop Multicast Traffic ☐ Drop the send/receive of multicast traffic

Advanced

Parameters	Description	Range	Default																														
WLAN > Basic > Advanced																																	
UAPSD	この機能を有効にすると、cnPilot デバイスは WMM Power Save / UAPSD をサポートします。この機能は、VOIP 通話やライブビデオストリーミングなどのアプリケーションを使用する際に必要です。この機能は、トラフィックの優先順位付けに役立ちます。以下は cnPilot デバイスが従うデフォルトのトラフィック優先順位です	-	Disabled																														
<table><tr><th>Priority</th><th>802.1D Priority (= UP)</th><th>802.1D Designation</th><th>Access Category</th><th>WMM Designation</th></tr><tr><td rowspan="7">lowest <div>↓</div> highest</td><td>1</td><td>BK</td><td rowspan="2">AC_BK</td><td rowspan="2">Background</td></tr><tr><td>2</td><td>-</td></tr><tr><td>0</td><td>BE</td><td rowspan="2">AC_BE</td><td rowspan="2">Best Effort</td></tr><tr><td>3</td><td>EE</td></tr><tr><td>4</td><td>CL</td><td rowspan="2">AC_VI</td><td rowspan="2">Video</td></tr><tr><td>5</td><td>VI</td></tr><tr><td>6</td><td>VO</td><td rowspan="2">AC_VO</td><td rowspan="2">Voice</td></tr><tr><td>7</td><td>NC</td></tr></table>				Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation	lowest <div>↓</div> highest	1	BK	AC_BK	Background	2	-	0	BE	AC_BE	Best Effort	3	EE	4	CL	AC_VI	Video	5	VI	6	VO	AC_VO	Voice	7	NC
Priority	802.1D Priority (= UP)	802.1D Designation	Access Category	WMM Designation																													
lowest <div>↓</div> highest	1	BK	AC_BK	Background																													
	2	-																															
	0	BE	AC_BE	Best Effort																													
	3	EE																															
	4	CL	AC_VI	Video																													
	5	VI																															
	6	VO	AC_VO	Voice																													
7	NC																																
QBSS	有効にすると、QBSS IE が管理フレームに追加さ	-	Disabled																														

DTIM interval	<p>れます。この IE は、スマートワイヤレスステーションが接続のためより良い AP を決定できるように、AP によるチャネル使用率の情報を提供します。ステーション数、チャネル使用率、利用可能なアドミッション容量がこの IE で得られる情報です。このパラメータは、パワーセーブに対応したモバイルステーションがインフラに組み込まれている場合に重要な役割を果たします。このフィールドを有効にすると、ブロードキャストおよびマルチキャストフレームの送信を制御します。</p>	1-255	1
Monitored Host			
Host	この機能は、バックボーンネットワークが遮断されている場合に必要です。cnPilot デバイスは、このパラメータに設定されたホスト名/IP の到達性を監視し、WLAN の状態を変更します	-	Disabled
Interval	設定された監視ホストに対する keep-alive メカニズムの状態に基づいて、ネットワークの健全性を監視する頻度。	60-3600 Sec	300
Attempts	状態を決定するための、keep-alive メカニズムのパケット数	1-20	1
DNS Logging Host	この機能は、WLAN プロファイルに接続された端末がアクセスしたウェブサイトの監視を管理者が要求した場合に必要となります。	-	Disabled
Connecton Logging Host	有効にすると、WLAN に関連付けられた端末によってアクセスされたすべての TCP 接続を供給します。	-	Disabled
Band Steering	この機能を有効にすると、ワイヤレスステーションが 5GHz 帯に接続するように誘導されます。cnPilot デバイスでは 3 つのモードがサポートされており、設置や端末の種類に応じて選択可能です。以下は、ワイヤレスステーションを 5GHz 帯に強制的に接続させるモードの順番です <ul style="list-style-type: none"> Low Normal Aggressive 	-	Disabled
Proxy ARP	無線ネットワークでの ARP フラッドを回避するための規定。有効にすると、AP は、その AP に接続されている無線ステーションの ARP 要求に応答します。IPv4 インフラのための機能です。	-	Enable
Proxy ND	無線ネットワークでの ARP フラッドを回避するための規定。有効にすると、AP は、その AP に接続されている無線ステーションの ARP 要求に応答します。これは、IPv6 インフラのための機能です	-	Disabled
Unicast DHCP Insert	DHCP のオファーと ACK/NACK パケットをユニキャストパケットとして端末に送信する機能。	-	Enabled
DHCP	有効にすると、AP に関連付けられたワイヤレスステーションから生成された DHCP パケットに	-	Disabled

Option 82 Option 82 パラメータが付加されます。オプション 82 では、サーキット ID とリモート ID を付加できます。サーキット ID とリモート ID の両方で、以下のパラメータを選択可能です。

- Hostname
- AP MAC
- BSSID
- SSID
- VLAN ID
- Site ID
- Custom
- All

Tunnel このオプションは、ユーザーのトラフィックが L2TP Disabled
Mode または L2GRE を使用して DMZ ネットワークに
トンネリングされる場合に有効です。

Fast- Roaming Protocol	<p>Wi-Fi ネットワークで音声アプリケーションをサポートするための重要な点の 1 つは、QoS とは別に、クライアントが AP 間でいかに早く接続を移動できるかということです。通話の切断を避けるためには、この時間を 150 ミリ秒以下にする必要があります。これは、WPA2-PSK セキュリティメカニズムを使用している場合には容易に達成可能です。しかし、エンタープライズ環境では、より強固なセキュリティ (WPA2-Enterprise で提供されるもの) が必要です。WPA2-Enterprise では、クライアントは AAA サーバと複数のフレームを交換するため、AAA サーバの場所によってはローミング時間が 700 ミリ秒以上になります。</p> <p>次のうちからひとつを選択します</p> <ol style="list-style-type: none"> 1. OK このローミング方式は、ローミング問題にスケーラビリティを持たせるための独自のソリューション。この方法では、クライアントが新しい AP に移動するたびに AAA サーバで認証を行う必要がありません。 2. 802.11r これは高速ローミングのための IEEE 規格で、クライアントがターゲットの AP にローミングする前に、新しい AP との最初のハンドシェイクが行われるという新しい概念のローミングを導入しており、これを Fast Transition (FT) と呼びます。2 種類の FT ローミングモードがサポートされます。 <ul style="list-style-type: none"> ▪ Over-the-Air デフォルトでは無効 	–	Disabled
------------------------------	---	---	----------

	<ul style="list-style-type: none"> Over-the-DS 		
Re-association Timeout	クライアントから AP への再接続試行がタイムアウトするまでの秒数を指定します。FT ローミングが有効な場合にのみ適用されます	1-100	20
RRM(802.11k)	AP は、近隣の AP の SSID 名 (複数の AP に設定された SSID) を 11k クライアントに送信します。以下のパラメータを有効にする必要があります。 <ul style="list-style-type: none"> Enable OCS Enable RRM Support for WPA2 authentication method 	-	Disabled
PMF(802.11w)	802.11w は、PMF (Protected Management Frames) サービスとも呼ばれ、管理フレームの暗号化を定義します。管理フレームが暗号化されていないと、無線接続が DoS 攻撃を受けやすくなり、管理フレームを使ってやり取りされる重要な情報を盗聴者から守ることができません。	<ul style="list-style-type: none"> Optional Mandatory Disabled 	-
SA Query	正規の 802.11w クライアントは、SA クエリ再試行時間と呼ばれる事前に設定された時間 (ミリ秒) 内に、セキュリティアソシエーション (SA) クエリ応答フレームで応答する必要があります	100-500	100ms
Association Comeback Time	この値は、アソシエーションレスポンスにアソシエーションカムバックタイム情報要素として含まれる。AP は設定された間隔でアソシエーションを拒否します。	1-20	1 sec

Advanced

UAPSD ☐ Enable UAPSD

QoS ☐ Enable QoS load element

DTIM interval Number of beacons (1-255)

Monitored Host

Host IP Address or Hostname that should be reachable for this WLAN to be active

Interval Duration in seconds (60-3600)

Attempts Number of attempts to check the reachability of monitored host (1-20)

DNS Logging Host Port Syslog server where all client DNS requests will be logged

Connection Logging Host Port Syslog server where all client connection requests will be logged

Band Steering Steer dual-band capable clients towards 5GHz radio

Proxy ARP ☒ Respond to ARP requests automatically on behalf of clients

Proxy ND ☐ Respond to IPv6 ND requests automatically on behalf of clients

Unicast DHCP ☒ Convert DHCP-OFFER and DHCP-ACK to unicast before forwarding to clients

Insert DHCP Option 82 ☐ Enable DHCP Option 82

Tunnel Mode ☒ Enable tunneling of WLAN traffic over configured tunnel

Fast-Roaming Protocol ☐ OKC ☐ 802.11r Configure roaming protocol

RRM (802.11k) ☐ Enable Radio Resource Measurements (802.11k)

PMF (802.11w)

Save Cancel

Guest Access

Parameters	Description	Range	Default
WLAN > Guest Access			
Enable	ゲストアクセス機能を有効にします	–	Disabled
Access Policy	4 種類のアクセスタイプが利用可能。 1. Clickthrough このモードでは認証メカニズム無しでユーザーがデータにアクセス可能。ユーザーは接続し利用規約に同意すればインターネットに接続できます。 2. RADIUS このモードが選択されると、ユーザーはユーザーネームとパスワードを入力する必要があり、それらは認証のため RADIUS サーバにリダイレクトされます。成功すると、ユーザーはデータにアクセス可能となります。 3. LDAP このモードが選択されると、ユーザーはユーザーネームとパスワードを入力する必要があり、それらは認証のため LDAP サーバにリダイレクトされます。成功すると、ユーザーはデータにアクセス可能となります。 4. Local Guest Account ユーザーは、デバイス上でユーザーネームとパスワードを設定する必要があります。このユーザーネームとパスワードは、認証とデータアクセスを成功させるためにリダイレクトページで入力する必要があります。	–	Clickthrough
Redirect Mode	リダイレクション URL の HTTP または HTTPS モードを設定するのに役立ちます。 1. HTTP AP は HTTP POSTUAL を接続しているクライアントに送信し、http://<事前に規定した URL>という形式になる。 2. HTTPS AP は HTTP POSTUAL を接続に成功しているクライアントに送信し、http://<事前に規定した URL>という形式になります。	–	HTTP
Hotspot DNS Name	DNS サーバに追加され、cnPilot の IP アドレスに解決可能なフレンドリーなホスト名を設定可能。–	–	–

Title	度設定されたこのパラメータは、ワイヤレス テーションに提供されるリダイレクト URL の IP アド レスに置き換えられます。 スプラッシュページのタイトルを設定可能。このパ ラメータで設定されたテキストはリダイレクシ ョンページに表示されます。テキストは太字で表 されます。	Up to 255 characters	Welcome To Cambium Powred Hotspot
Contents	スプラッシュページのコンテンツを設定可能。リダ イレクションページのタイトルの下に設定したテキ ストが表示されます	Up to 255 characters	Please enter username and password to get Web Access
Terms	Terms and Agreement に同意するときのスプラッ シュページに表示されるテキストを設定します。	Up to 255 characters	–
Logo	http(s)://<IP アドレス>/logo.png に設定したロゴ画 像を表示する。PNG と JPEG フォーマットに対応。	–	–
Background Image	http(s)://<IP アドレス>/backgroundimage.png に設 定した背景画像を表示します。PNG と JPEG フ ォーマットに対応。	–	–
Success Action	captive portal service へログイン成功後のリダイ レクション URL を設定する項目です。3 種類のリダ イレクション URL を設定可能。 1. Internal Logout Page ログイン成功後、ワイヤレスクライアントは AP にホストされたログアウトページにリダイレクト されます。 2. Redirect user to External URL ここでは、デバイスのリダイレクション URL パ ラメータに設定された URL にユーザーはリダ イレクトされます。 3. Redirect user to Original URL ここでは、以前ユーザーが captive portal 認証 に成功した URL にリダイレクトされます。	–	Internal Logout page
Redirect user to External URL	ログイン成功後のリダイレクション URL を設定、AP や端末の情報を URL に付加可能です。 ▪ Prefix Query Strings in Redirect URL このオプションはデフォルトで選択されていま す。次の情報がリダイレクション URL に追加 されます。 SSID	–	–

	AP MAC NAS ID AP ID Client MAC Redirection URL User can provide either HTTP or HTTPS URL ユーザーは、キャプティブポータル認証が成功する前にアクセスしていた URL にリダイレクトされます。リダイレクト URL には、デフォルトで有効になっている Prefix Query Strings というパラメータがあり、詳細は以下のとおりです。 <ul style="list-style-type: none"> Prefix Query Strings in Redirect URL このオプションはデフォルトで選択されています。次の情報がリダイレクション URL に追加されます。 SSID AP MAC NAS ID AP IP Client MAC 		
Success message	ゲストアクセス認証が成功したときに表示されるテキストを設定するための規定。この設定は、Success Action モードが Internal Logout Page の場合にのみ適用されます。	-	-
Redirect	<ul style="list-style-type: none"> 有効にすると、HTTP URLs のみがゲストアクセスログインページにリダイレクトされます。 無効にすると、HTTP と HTTPS URLs がゲストアクセスログインページにリダイレクトされます。 	-	-
Redirect User Page	このフィールドに設定された IPv4/IPv6 アドレスは、ゲストアクセスセッションのログアウト URL として使用されます。設定した IPv4/IPv6 アドレスは、インターネットに接続できないようにします。	-	1.1.1.1
Proxy Redirection Port	プロキシサーバを有効にするためのプロキシポートを設定可能。これにより、プロキシポートでアクセスした URL がログインページにリダイレクトされます。	1 - 65535	-
Session Timeout	クォータが持続する場合に、クライアントがインターネットへのアクセスを許可される時間であり、その後、AP は認証解除を送信します。ワイヤレスステーションは、セッションタイムアウト後にゲストアクセス認証を受けなければなりません。	60 - 2592000	1800
Inactivity	接続されているがデータトラフィックがない無線ス	60 -	1800

Timeout	セッションを切断するためのタイムアウト期間を設定するための規定。AP は、端末からデータが受信されないとタイマーを開始し、タイマーが 0 になると切断します。	2592000	
MAC Authentication Fallback	サポートされているタイプの MAC アドレス認証が失敗した場合に、ワイヤレスステーションがゲストアクセスのログインページにリダイレクトされる仕組みです。	–	Disabled
Extend Interface	イーサネットインタフェース上でゲストアクセスをサポートする項目	–	Disabled
Whitelist	IPv4/IPv6 または URL を設定してトラフィックを迂回させることで、ユーザーがゲストアクセス認証なしでこれらの IP または URL にアクセスできるようにする機能。	–	–
Captive Portal bypass User Agent	ブラウザのユーザーエージェントに基づいて、設定された特定のブラウザに自動ポップアップを制限する機能	–	–

Basic	Radius Server	Guest Access	Usage Limits	Scheduled Access	Access	Passpoint
<p>Enable <input type="checkbox"/></p> <p>Portal Mode <input checked="" type="radio"/> Internal Access Point <input type="radio"/> External Hotspot <input type="radio"/> cnMaestro</p> <p>Access Policy <input checked="" type="radio"/> Clickthrough <i>Splash-page where users accept terms & conditions to get on the network</i> <input type="radio"/> Radius <i>Splash-page with username & password, authenticated with a RADIUS server</i> <input type="radio"/> LDAP <i>Redirect users to a login page for authentication by a LDAP server</i> <input type="radio"/> Local Guest Account <i>Redirect users to a login page for authentication by local guest user account</i></p> <p>Redirect Mode <input checked="" type="radio"/> HTTP <i>Use HTTP URLs for redirection</i> <input type="radio"/> HTTPS <i>Use HTTPS URLs for redirection</i></p> <p>Redirect Hostname <input type="text"/> <small>Redirect Hostname for the splash page (up to 255 chars)</small></p> <p>Title <input type="text"/> <small>Title text in splash page (up to 255 chars)</small></p> <p>Contents <input type="text"/> <small>Main contents of the splash page (up to 255 chars)</small></p> <p>Terms <input type="text"/> <small>Terms & conditions displayed in the splash page (up to 255 chars)</small></p> <p>Logo <input type="text" value="Eg: http://domain.com/logo.png"/> <small>Logo to be displayed on the splash page</small></p> <p>Background Image <input type="text" value="Eg: http://domain.com/backgroundImage.jpg"/> <small>Background image to be displayed on the splash page</small></p> <p>Success Action <input checked="" type="radio"/> Internal Logout Page <input type="radio"/> Redirect user to External URL <input type="radio"/> Redirect user to Original URL</p> <p>Success message <input type="text"/></p> <p>Redirect <input checked="" type="checkbox"/> HTTP-only <i>Enable redirection for HTTP packets only</i></p> <p>Redirect User Page <input type="text" value="1.1.1.1"/> <small>Configure IP address for redirecting user to guest portal splash page</small></p> <p>Proxy Redirection Port <input type="text"/> <small>Port number(1 to 65535)</small></p> <p>Session Timeout <input type="text" value="28800"/> <small>Session time in seconds (60 to 2592000)</small></p> <p>Inactivity Timeout <input type="text" value="1800"/> <small>Inactivity time in seconds (60 to 2592000)</small></p> <p>MAC Authentication Fallback <input type="checkbox"/> <i>Use guest-access only as fallback for clients failing MAC-authentication</i></p> <p>Extend Interface <input type="text"/> <small>Configure the interface which is extended for guest access</small></p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p>						

Add Whitelist
Captive Portal bypass User Agent

IP Address or Domain Name

IP Address Domain Name	Action
No white list available	

1 / 1
10 items per page

WLAN > Guest Access > External Hotspot

Parameters	Description	Range	Default
WLAN > Guest Access > External Hotspot			
Address Policy	<p>エンドユーザー用に 4 種類のアクセスタイプが用意されています。</p> <ol style="list-style-type: none"> Clickthrough このモードでは、ユーザーは認証メカニズムなしでデータにアクセス可能。接続して利用規約に同意すれば、すぐにインターネットにアクセスできます。 Radius ユーザーは、ユーザー名とパスワードを入力する必要があり、その情報は RADIUS サーバーに転送されて認証されます。認証に成功すると、ユーザーはデータにアクセスできるようになります。 LDAP ユーザーは、ユーザー名とパスワードを入力し、LDAP サーバーにリダイレクトされて認証されます。認証に成功すると、ユーザーにデータへのアクセスが提供されます。 	–	Clickthrough

	<p>4. Local Guest Account ユーザーはデバイス上で ユーザー名とパスワードを設定 する必要があり、認証とデータアクセ スを成功させるためには、リダイレ クトページでその情報を提供する 必要があります。</p>		
LDAP Server baseDN	サーバがユーザーを検索するポイント を設定する項目	-	-
LDAP Server adminDN	LDAP/AD サーバの検索を成功させる ために、LDAP サーバと結合するアド ミン・ドメインを設定するための項目	-	-
LDAP Server Admin Password	ドメインコンポーネントで定義されたす べての組織単位を検索するために、 LDAP/AD サーバの管理者パスワード を設定する項目	-	-
Redirect Mode	<p>リダイレクション URL の HTTP または HTTPS モードを設定する項目</p> <p>1. HTTP AP は関係したクライアントに HTTP POSTUAL を送信します。</p> <p>2. HTTPS AP は HTTPS POSTUAL を関連 付けに成功したクライアントに送信 する。https://<事前に設定済の URL>という形式になります。</p>	-	HTTP
Redirect Hostname	DNS サーバに追加され、cnPilot IP ア ドレスをリゾルブ可能なフレンドリーホ スト名を設定可能です。このパラメータ を設定すると、ワイヤレスステーシ ョンに提供されるリダイレクト URL の IP アドレスに置き換えられます。	-	-
WISPr Clients External Server Login	WISPr で取得したゲストアクセスポータ ルの URL のリダイレクトを可能にする 項目	-	Disabled
External Page URL	ゲストアクセスが認証されていないワ イヤレスステーションに表示される ランディング/ログインページを設定可 能。	-	-
External Portal Post Through cnMaestro	これは、HTTPS が外部のゲストアクセ スポータルでのみサポートされている 場合に必要です。このオプションを有 効にすると、証明書は最小限に抑える ことができます。証明書は cnMaestro	-	Disabled

	On-Premises にのみインストールする必要があります。		
External Portal Type	<p>cnPilot デバイスでは 2 種類のポータルタイプがサポートされています。</p> <ol style="list-style-type: none"> Standard このモードを選択すると、全てのサードパーティベンダーのゲストアクセスが承認され、cnPilot デバイスに統合されます。 XWF このモードは Facebook Express Wi-Fi デプロイメント用に選択されます。 	–	Standard
XWF Key	これは、XWF のバージョンに関わらず、XWF ポータルモードが選択されている場合に適用されます。	–	–
XWF Token	URL エンコードフォーマットの XWF アクセストークン	–	–
XWF SSE Server Timeout	XWF ポータルモードが選択されている場合に適用されます。XWF SSE サーバのタイムアウトを設定するための規定です。	5–1800	60
Success Action	<p>キャプティブポータルサービスへのログイン成功後のリダイレクト URL を設定する機能。リダイレクト URL には、以下の 3 つのモードがあります。</p> <ol style="list-style-type: none"> Internal Logout Page ログインに成功後、ワイヤレスクライアントは AP にホストされたログアウトページにリダイレクトされます。 Redirect user to External URL ここでは、デバイス上のリダイレクション URL パラメータで設定された URL にユーザーはリダイレクトされます。 Redirect user to Original URL ここでは、captive portal authentication が成功する前にユーザーがアクセスしていた URL にリダイレクトされます。 	–	Internal Logout Page
Redirect user to	ログイン成功後のリダイレクション URL	–	–

External URL	<p>を設定し、AP や端末の情報を URL に付加することができます。</p> <ul style="list-style-type: none"> Prefix Query Strings in Redirect URL このオプションはデフォルトで選択されています。リダイレクション URL に以下の情報が追加されます SSID AP MAC NAS ID AP IP Client MAC Redirection URL ユーザーは HTTP と HTTPS URL のどちらも供給可能です。 		
Redirection user to Original URL	<p>ユーザーは、キャプティブポータル認証が成功する前にユーザーがアクセスしていた URL にリダイレクトされます。リダイレクト URL の Prefix Query Strings は、デフォルトで有効になっており、詳細は以下のとおりです。</p> <ul style="list-style-type: none"> Prefix Query Strings in Redirect URL このオプションはデフォルトで選択されており、リダイレクション URL に以下の情報が追加されます。 SSID AP MAC NAS ID AP IP Client MAC 	–	–
Success message	<p>ゲストアクセス認証が成功したときに表示されるテキストを設定するための規定。この設定は、Success Action モードが Internal Logout Page の場合にのみ適用されます。</p>	–	–
Redirection URL Query String	<p>“Prefix Query Strings in Redirect URL” が選択されている場合、リダイレクション URL に以下の情報が追加されます。</p> <ul style="list-style-type: none"> Client IP RSSI 	–	Disabled

	<ul style="list-style-type: none"> AP Location 		
Redirect	<ul style="list-style-type: none"> 有効の場合、HTTP URL のみゲストアクセスログインページにリダイレクトされます。 無効の場合、HTTP と HTTPS URL のどちらもゲストアクセスログインページにリダイレクトされます。 	–	Enabled
Redirect User Page	このフィールドに設定された IP アドレスは、ゲストアクセスセッションのログアウト／切断／キャプティブポータル URL へのリダイレクトとして使用されます。設定した IP アドレスは、インターネットに接続できないようにします。	–	1.1.1.1
Proxy Redirection Port	プロキシサーバを有効にするためのプロキシポートを設定可能。これにより、プロキシポートでアクセスした URL をログインページにリダイレクトできます。	1 – 65535	–
Session Timeout	クォータが持続する場合に、クライアントがインターネットへのアクセスを許可される時間であり、その後、AP は認証解除を送信します。端末は、セッションタイムアウト後にゲストアクセス認証を受ける必要があります。	60–2592000	1800
Inactivity Timeout	接続されていてもデータトラフィックのない無線ステーションを切断するための、タイムアウト期間を設定するための項目。AP は、無線ステーションからデータが受信されないとタイマーを開始し、タイマーが 0 になると切断します。	60–2592000	1800
MAC Authentication Fallback	MAC アドレス認証に失敗した場合、端末がゲストアクセスのログインページにリダイレクトされる仕組み。	–	Disabled
Extend Interface	イーサネットインタフェースにおいてゲストアクセスをサポートする項目	–	Disabled
Traffic Class 1	これは XWF ポータルタイプにのみ適用されます。このトラフィッククラスには、リダイレクション、ログイン、および支払いが成功した場合の XWF に関連する IP および URL が含まれます。	–	–
Traffic Class 2	XWF ポータルタイプ専用の項目。このトラフィッククラスには、ゲストアクセス認証なしでアクセス可能なホワイトリストの IP/URL が含まれます。	–	–

Internet	XWF ポータルタイプにのみ適用される項目。このトラフィッククラスには、ゲストアクセスの認証に成功した後にアクセス可能なホワイトリストの IP/URL が含まれます。	–	–
Whitelist	トラフィックをバイパスする IP または URL を設定して、ユーザーがゲストアクセス認証なしでそれらの IP または URL にアクセスできるようにします。このパラメータは、標準ポータルタイプで有効です。	–	–
Captive Portal bypass User Agent	ブラウザのユーザーエージェントに基づいて設定された、特定のブラウザに自動ポップアップを制限するための項目。標準ポータルタイプで有効です。	–	–

Basic Radius Server Guest Access Usage Limits Scheduled Access Access **Passpoint**

Enable ☒

Portal Mode ☐ Internal Access Point ☒ External Hotspot ☐ cnMaestro

Access Policy ☐ Clickthrough Splash-page where users accept terms & conditions to get on the network
☒ Radius Splash-page with username & password, authenticated with a RADIUS server
☐ LDAP Redirect users to a login page for authentication by a LDAP server
☐ Local Guest Account Redirect users to a login page for authentication by local guest user account

Redirect Mode ☒ HTTP Use HTTP URLs for redirection
☐ HTTPS Use HTTPS URLs for redirection

Redirect Hostname
Redirect Hostname for the splash page (up to 255 chars)

WISPr Clients External Server Login ☐

External Page URL
Eg: http://external.com/login.html
 URL of external splash page

External Portal Post Through cnMaestro ☐

External Portal Type External Portal Type Standard/XWF

Success Action ☒ Internal Logout Page ☐ Redirect user to External URL ☐ Redirect user to Original URL

Success message

Redirection URL Query String ☐ Client IP Include IP of client in the redirection url query strings
☐ RSSI Include rssi value of client in the redirection url query strings
☐ AP Location Include AP Location in the redirection url query strings

Redirect ☒ HTTP-only Enable redirection for HTTP packets only

Redirect User Page
Configure IP address for redirecting user to guest portal splash page

Proxy Redirection Port
Port number(1 to 65535)

Session Timeout
Session time in seconds (60 to 2592000)

Inactivity Timeout
Inactivity time in seconds (60 to 2592000)

MAC Authentication Fallback ☐ Use guest-access only as fallback for clients failing MAC-authentication

Extend Interface
Configure the interface which is extended for guest access

Traffic Class 1 Traffic Class 2 Internet

Name

Policy

IP Address | Subnet | Domain Name Action

Traffic Class 1 not available

1 1 10 Items per page

Add Whitelist Captive Portal bypass User Agent

IP Address or Domain Name

IP Address | Domain Name Action

No white list available

1 1 10 Items per page

WLAN > Guest Access > cnMaestro

Parameters	Description	Range	Default
WLAN > Guest Access > cnMaestro			
Guest Portal Name	CnMaestro 上でホストされている Guest Access プロファイルの名前を設定する項目	–	–
Redirect	有効の場合、HTTP URL のみが Guest Access ログインページにリダイレクトされます。 無効の場合、HTTP と HTTPS URL の両方が Guest Access ログインページにリダイレクトされます。	–	Enabled
Redirect User Page	このフィールドに設定された IP アドレスは、ゲストアクセスセッションのログアウト URL として使用されます。設定した IP アドレスは、インターネットに接続できないようにしてください。	–	1.1.1.1
Proxy Redirection Port	プロキシサーバを有効にするためのプロキシポートを設定可能。これにより、プロキシポートでアクセスした URL をログインページにリダイレクトすることができます。	1 – 65535	1800
Inactivity Timeout	接続されていてもデータトラフィックがない無線ステーションを切断するための、タイムアウト期間を設定するための項目。AP は、無線ステーションからデータが受信されないとタイマーを開始し、タイマーが 0 になると切断します。	60 – 2592000	1800
MAC Authentication Fallback	MAC アドレス認証に失敗した場合、端末がゲストアクセスのログインページにリダイレクトされる仕組み	–	Disabled
Extend Interface	イーサネットインタフェースにおいてゲストアクセスをサポートする項目	–	Disabled
Whitelist	トラフィックをバイパスする IP または URL を設定して、ユーザーがゲストアクセス認証なしでそれらの IP または URL にアクセスできるようにします。このパラメータは、標準ポータルタイプで有効です。	–	–
Captive Portal bypass Use Agent	ブラウザのユーザーエージェントに基づいて設定された、特定のブラウザに自動ポップアップを制限するための項目。標準ポータルタイプで有効です。	–	–

Basic

Radius Server

Guest Access

Usage Limits

Scheduled Access

Access

Passpoint

Enable

☒

Portal Mode

☐ Internal Access Point ☐ External Hotspot ☒ cnMaestro

Guest Portal Name

Guest Portal Name which is hosted on cnMaestro

Redirect

☒ HTTP-only Enable redirection for HTTP packets only

Redirect User Page

Configure IP address for redirecting user to guest portal splash page

Proxy Redirection Port

Port number(1 to 65535)

Inactivity Timeout

Inactivity time in seconds (60 to 2592000)

MAC Authentication Fallback

☐ Use guest-access only as fallback for clients failing MAC-authentication

Extend Interface

Configure the interface which is extended for guest access

Save

Cancel

Add Whitelist

Captive Portal bypass User Agent

IP Address or Domain Name

Save

IP Address | Domain Name

Action

No white list available

1

/ 1

10

items per page

Usage Limits

Parameters	Description	Range	Default
Rate Limit per Client	クライアントごとのスループットを制限する機能。クライアントごとのデフォルトの許容スループットは無制限で、802.11 プロトコルで許容される最大値です。SSID 上の各クライアントとの間のトラフィックは、WLAN Configuration 内の Usage-limits で利用可能な Client Rate Limit を設定することで、どちらの方向にもレートを制限することができます。これは、公共のホットスポットのように、バックホールが限られていて、ネットワーク管理者が 1 つのクライアントが利用可能なすべての帯域を独占しないようにしたい場合に有用です。	–	0 [Unlimited]
Rate Limit per WLAN	WLAN に関連する無線ステーションの数に関係なく、WLAN 全体で制限する機能。GUI の WLAN Configuration セクションで使用制限を設定することにより、SSID 上のすべてのアップストリーム/ダウンストリームトラフィック(すべてのワイヤレスクライアントにわたって集約される)は、どちらの方向にもレートを制限することができます。これは、複数の SSID が使用されている場合に便利で、1 つは企業用、もう 1 つはゲスト用となっています。ネットワーク管理者は、ゲスト用 VLAN のトラフィックが常にスロットルされ、企業用 WLAN に影響を与えないようにすることができます。	–	0 [Unlimited]

Basic
Radius Server
Guest Access
Usage Limits
Scheduled Access
Access
Passpoint

Rate Limit per Client
Upstream:
Kbps
Downstream:
Kbps

Rate Limit per WLAN
Upstream:
Kbps
Downstream:
Kbps

Save
Cancel

Scheduled Access

Parameters	Description	Range	Default
Scheduled Access	選択した時間帯に Wi-Fi サービスを利用できるようにする機能。cnPilot では、全日または週の特定の日に Wi-Fi サービスを利用できるようにすることができます。時間の単位は hours (時間) です。	00:00 Hrs. – 23:59 Hrs.	Disabled

Basic	Radius Server	Guest Access	Usage Limits	Scheduled Access	Access	Passpoint
<div> <div>Sunday</div> <div>Start Time</div> <div>End Time</div> <div>HH:MM format</div> </div>						
<div> <div>Monday</div> <div>Start Time</div> <div>End Time</div> <div>HH:MM format</div> </div>						
<div> <div>Tuesday</div> <div>Start Time</div> <div>End Time</div> <div>HH:MM format</div> </div>						
<div> <div>Wednesday</div> <div>Start Time</div> <div>End Time</div> <div>HH:MM format</div> </div>						
<div> <div>Thursday</div> <div>Start Time</div> <div>End Time</div> <div>HH:MM format</div> </div>						
<div> <div>Friday</div> <div>Start Time</div> <div>End Time</div> <div>HH:MM format</div> </div>						
<div> <div>Saturday</div> <div>Start Time</div> <div>End Time</div> <div>HH:MM format</div> </div>						
<div> <div>Save</div> <div>Cancel</div> </div>						

Access

Parameters	Description	Range	Default
ACL			
Precedence	ACL ルールのインデックスを設定する機能。設定された優先順位の値に基づいてパケットが検証され処理されます。	1-256	1
Policy	トラフィックを許可、拒否またはルートするかどうかの設定	Allow/ Deny/ Route	Deny
Direction	設定された ACL のルールを、任意の方向または特定の方向に適用するための規定。	—	—
Type	cnPilot デバイスは、3 つのレイヤの ACL をサポートします。ルールの設定は以下。 <ul style="list-style-type: none"> MAC IP このタイプは IPv4 ベースの IP ACL IP6 このタイプは IPv6 ベースの IP ACL Proto このタイプは IPv4 でサポートされているプロトコル用 Proto6 このタイプは IPv6 でサポートされているプロトコル用 	—	IP
Source	このオプションは、ACL タイプが IPv4/IPv6 アドレスに設		

IP/Mask	定されている場合に使用可能。このフィールドでは、ルールを単一の IPv4/IPv6 アドレスに適用するのか、IPv4/IPv6 アドレスの範囲に適用するのかを設定可能。		
Destination IP/Mask	このオプションは、ACL タイプが IPv4/IPv6 アドレスに設定されている場合に使用可能。このフィールドでは、ルールを単一の IPv4/IPv6 アドレスに適用するのか、IPv4/IPv6 アドレスの範囲に適用するのかを設定可能。	-	-
Source MAC/Mask	このオプションは、ACL タイプが MAC アドレスに設定されている場合に使用可能。このフィールドでは、ルールを単一のデバイスの MAC アドレスに適用するのか、MAC アドレスの範囲に適用するのかを設定可能。	-	-
Destination MAC/Mask	このオプションは、ACL タイプが MAC アドレスに設定されている場合に使用可能。このフィールドでは、ルールを単一のデバイスの MAC アドレスに適用するのか、MAC アドレスの範囲に適用するのかを設定可能。	-	-
Protocol	このオプションは、ACL タイプを proto/proto6 として選択した場合に利用可能。ユーザーは以下のプロトコルを選択できます。 <ul style="list-style-type: none"> • TCP • UDP • ICMP • Any 	-	TCP
Source Port	プロトコルとポートの組み合わせで ACL を適用する機能。	-	-
Destination Port	プロトコルとポートの終着点で ACL を適用する機能。		
Description	管理者がわかりやすいように、ACL ルールごとにテキスト文字列を追加することができます。	-	-
DNS-ACL			
Precedence	ACL ルールのインデックスを設定する機能。設定された優先順位の値に基づいてパケットが検証され、処理されます。	-	1
Action	トラフィックを許可または拒否する設定	-	Deny
Domain	ドメイン名を設定し、設定された Action に基づいてルールが適用される	-	-
MAC Authentication			
MAC Authenticat ion Policy	cnPilot は複数の MAC 認証方法をサポートする。以下にそれぞれのモードの詳細を示します。 1. Permit リストアップされた端末の MAC アドレスは、AP へのアソシエートが許可される。 2. Deny ユーザーが MAC アドレスを設定した場合、それらの端末はアソシエートを拒否し、リストされていない MAC アドレスは許可されます。		

	<p>3. Radius 無線認証のたびに、cnPilot が radius request を送信し、radius accept を受信すると、端末の接続が許可されます。</p> <p>4. cnMaestro このオプションは、管理者が MAC 認証ポリシーを集中管理したい場合に適します。無線認証のたびに、AP は cnMaestro に接続を許可するか拒否するかのクエリを送信する。コンフィギュレーションに基づき、ワイヤレスステーションは許可または拒否されます。</p>		
--	---	--	--

Dual stack 有効時の IP ACL の動作

IPv4 ACL Rule	IPv6 ACL Rule	Remark
No rule	No rule	All IPv4 and IPv6 allowed
IPv4 permit rule	No rule	All IPv6 packets dropped
No rule	IPv6 rule	All IPv4 packets dropped
IPv4 permit rule	IPv6 permit rule	All IPv4 and IPv6 allowed

DNS-ACL

Precedence
1

Action
Deny

Domain

Save

Precedence	Policy	Domain Name	Action
No Rules available			

1

10

Items per page

MAC Authentication

MAC Authentication Policy
Deny

MAC

Description

Save

MAC Address	Action	Description
No MAC Address available		

1

10

Items per page

11-4 Network

IPv4 network VLAN

IPv4 Parameters

Parameter	Description	Range	Default
Edit	ユーザーがコンフィグレーションの閲覧・更新を行う VLAN インタフェースを選択する機能。	–	VLAN1
Address	選択したインタフェースの IPv4 アドレス設定モードを設定する機能。以下の 2 つのモードをサポートします 1. DHCP cnPilot デバイスが DHCP サーバから IPv4 アドレスを取得しようとするデフォルトモード 2. Static IP 選択した VLAN の IPv4 アドレスとネットマスクをユーザーが明示的に設定する必要があります。	–	DHCP
NAT	このオプションは、ローカルの DHCP サーバを定義している場合に適しています。このオプションを選択すると、端末かサーバフィックは、デフォルトゲートウェイのインタフェース IP に NAT されます。		Disabled
Zeroconf IP	Zeroconf IP を有効にすることを推奨します。このインタフェースは VLAN1 設定部でのみ利用可能です。VLAN1 がイーサネットインタフェースで許可されていない場合、この IP にはアクセスできません。	–	Enabled
DHCP Relay Agent	このオプションは、DHCP サーバが、DHCP IP を要求しているクライアントとは異なる VLAN でホストされている場合に有効です。このオプションを有効にすると、DHCP パケットにオプション 82 が付加されます。以下の情報を設定可能です。 1. DHCP Option 82 Circuit ID <ul style="list-style-type: none"> Hostname APMAC BSSID SSID Custom 2. DHCP Option 82 Remote ID <ul style="list-style-type: none"> Hostname APMAC BSSID SSID Custom 	–	Disabled
Request Option All	この設定では、cnPilot AP が以下を学習するインタフェースを決定します。	–	Enabled on

	<ul style="list-style-type: none"> IPv4 デフォルトゲートウェイ オプション 43 や 15 のような DHCP クライアントオプション (コントローラーディスカバリーのようなコントローラーホスト名/IPv4 アドレス) DNS Servers Domain Name 		VLAN1
--	---	--	-------

Routing & DNS > IPv4 parameters

Parameters	Description	Range	Default
Default Gateway	デフォルトゲートウェイを設定するための規定です。これが指定された場合、cnPilot デバイスはこのゲートウェイを最優先でインストールします。	–	–
DNS Server	cnPilot デバイスにスタティック DNS サーバを設定します。DNS サーバは最大 2 台まで設定可能です。	–	–
Domain Name	ドメイン名を設定するための規定です。これがされた場合、cnPilot デバイスはこのドメイン名を最優先でインストールします。	–	–
DNS Proxy	このパラメータが有効な場合、cnPilot デバイスは DNS プロキシサーバとして動作します。	–	Disabled

Routing & DNS

IPv4

Default Gateway	<input type="text"/>	<i>IP address of default gateway</i>
DNS Server 1	<input type="text"/>	<i>Primary Domain Name Server</i>
DNS Server 2	<input type="text"/>	<i>Secondary Domain Name Server</i>
Domain Name	<input type="text"/>	<i>Domain name</i>
DNS Proxy	<input type="checkbox"/>	<i>DNS Proxy</i>

IPv6

Save

Cancel

Routes

Parameters	Description	Range	Default
Gateway Source Precedence	cnPilot デバイスが複数の方法で学習した場合に、デフォルトゲートウェイと DNS サーバを優先的に使用するための設定です。デフォルトは Static, DHCP, PPPoE の順です。	–	Static
Add Multiple Route Entries	<p>ユーザーはスタティックルートを設定することができます。スタティックルートの設定に必要なパラメータは以下の通りです。</p> <ul style="list-style-type: none"> ▪ Destination IP ▪ Mask ▪ Gateway 	–	–
Port Forwarding	<p>この機能はワイヤレスステーションが NAT の背後にある場合に必要です。ユーザーはこの機能を使用して、ワイヤレスステーションでホストされているサービスにアクセスできます。NAT の背後にあるワイヤレスステーションでホストされているサービスにアクセスするには、以下の設定パラメータが必要です。</p> <ul style="list-style-type: none"> ▪ Port ▪ IP Address ▪ Type 	–	–

VLAN

Routes

Ethernet Ports

Security

DHCP

Tunnel

PPPoE

VLAN Pool

Gateway Source Precedence

IPv4

IPv6

STATIC
DHCP
PPPoE

STATIC
AUTO-CONFIG/DHCP

Save

Save

Add Multiple Route Entries - IPv4

Destination IP

Mask

Gateway

Save

xxx.xxx.xxx.xxx

xxx.xxx.xxx.xxx

xxx.xxx.xxx.xxx

Destination IP

Mask

Gateway

Action

No routes available

1

10 items per page

Add Multiple Route Entries - IPv6

Destination IP/prefix

Gateway

Save

Destination IP

Gateway

Action

No routes available

1

10 items per page

Port Forwarding

Port

IP Address

Type

Save

TCP

Port

IP Address

Protocol

Action

No rules available

1

10 items per page

Ethernet Ports

Parameters	Description	Range	Default
Ethernet	<p>cnPilot デバイスの Ethernet ポートは、以下のモードで動作するように設定されています。</p> <ol style="list-style-type: none"> 1. Access Single VLAN このモードではシングル VLAN トラフィックが許可されます。 2. Trunk Multiple VLANs このモードでは複数 VLAN がサポートされます。 3. Tunnel Mode L2GRE トンネルを有効にする項目です。デバイスのイーサネット 2 ポートにのみ適用可能です。 	–	Access
ACL			
Precedence	ACL ルールのインデックスを設定する機能です。パケットは設定された優先順位の値に基づいて検証され、処理されます。	1-256	1
Policy	トラフィックを許可するか拒否するかの設定	Deny/Permit	Deny
Direction	設定された ACL のルールを、任意の方向または特定の方向に適用するための項目。	–	in
Type	<p>cnPilot デバイスは、3 つのレイヤの ACL をサポートしており、ルールの設定は以下のようになります。</p> <ul style="list-style-type: none"> ・ IP ・ MAC ・ Proto 	–	IP
Source IP/Mask	このオプションは、ACL タイプが IP アドレスに設定されている場合に利用できます。このフィールドでは、ルールを単一の IP アドレスに適用するのか、複数の IP アドレスに適用するのかを設定できます。	–	–
Destination IP/Mask	このオプションは、ACL タイプが IP アドレスに設定されている場合に使用できます。このフィールドでは、ルールを単一の IP アドレスに適用するか、複数の IP アドレスに適用するかを設定できます。	–	–
Source MAC/Mask	このオプションは、ACL タイプが MAC アドレスに設定されている場合に使用できます。このフィールドでは、ルールを単一のデバイスの MAC アドレスに適用するのか、MAC アドレスの範囲に適用するのかを設定できます。	–	–
Destination MAC/Mask	このオプションは、ACL タイプが MAC アドレスに設定されている場合に使用できます。この		

	フィールドでは、ルールを単一のデバイスの MAC アドレスに適用するのか、MAC アドレスの範囲に適用するのかを設定できます。		
Protocol	このオプションは、ACL タイプを proto として選択した場合に利用できます。ユーザーは以下のプロトコルを選択できます。 <ul style="list-style-type: none"> ・ TCP ・ UDP ・ ICMP ・ Any 	－	TCP
Source Port	プロトコルとポートの組み合わせで ACL を適用する機能	－	－
Destination Port	プロトコルとポートの組み合わせで ACL を適用する機能。	－	－
Description	管理者がわかりやすいように、ACL ルールごとにテキスト文字列を追加することができます。	－	－

VLAN Routes **Ethernet Ports** Security DHCP Tunnel PPPoE VLAN Pool

Eth1 Eth2

ETH1 Access Single VLAN

Access Mode VLAN
1

Save Cancel

ACL

Precedence 1 Policy Deny Direction In

Type IP Source IP/Mask Destination IP/Mask

Description

Save

Preced...	Policy	Directi...	Type	Rule	Description	Action
No Rules available						

1 / 1 10 items per page

IPv6 network VLAN

IPv6 parameters

Parameters	Description	Range	Default
Address	選択したインタフェースの IPv6 アドレス設定モードを設定する機能。5 つのモードをサポートしています。 <ul style="list-style-type: none"> Disabled Autoconfig Static Stateless DHCPv6 Stateful DHCPv6 		AUtoConfig
Request Option All	この設定では、cnPilot AP が以下を学習するインタフェースを決定します。 IPv6 default gateway オプション 52 や 24 のような DHCP クライアントオプション(コントローラーディスカバリーのようなコントローラーホスト名/IPv6 アドレス)	–	Enabled on VLAN1

The screenshot shows the 'VLAN' configuration page with tabs for VLAN, Routes, Ethernet Ports, Security, DHCP, Tunnel, PPPoE, and VLAN Pool. The 'VLAN' tab is active, showing 'Edit VLAN 1' and a 'Delete this interface' button. A red box highlights the 'IPv6' configuration section, which includes an 'Address' dropdown set to 'AutoConfig', a 'Request Option All' checkbox, and a checked option 'Use IPv6 Gateway, DNS, DHCPv6 options received on this interface'. Other sections like 'IPv4' and 'General' are visible but not highlighted.

Routes

Parameters	Description	Range	Default
Gateway Source Precedence	cnPilot デバイスが複数の方法で学習した場合に、デフォルトゲートウェイと DNS サーバを優先するための機能です。デフォルトは Static と AUTO-CONFIG/DHCP の順です。	–	Static
Add Multiple Route Entries	ユーザーはスタティックルートを設定することができます。スタティックルートの設定に必要なパラメータは以下の通りです。 <ul style="list-style-type: none"> Destination IP/prefix Gateway 	–	–

VLAN

Routes

Ethernet Ports

Security

DHCP

Tunnel

PPPoE

VLAN Pool

Gateway Source Precedence

IPv4

IPv6

STATIC
DHCP
PPPoE

STATIC
AUTO-CONFIG/DHCP

Save

Save

Add Multiple Route Entries - IPv4

Destination IP

Mask

Gateway

Save

xxx.xxx.xxx.xxx

xxx.xxx.xxx.xxx

xxx.xxx.xxx.xxx

Destination IP

Mask

Gateway

Action

No routes available

1

10 items per page

Add Multiple Route Entries - IPv6

Destination IP/prefix

Gateway

Save

Destination IP

Gateway

Action

No routes available

1

10 items per page

Port Forwarding

Port

IP Address

Type

Save

TCP

Port

IP Address

Protocol

Action

No rules available

1

10 items per page

Ethernet Ports

Parameters	Description	Range	Default
Ethernet	<p>cnPilot デバイスの Ethernet ポートは、以下のモードで動作するように設定されています。</p> <ol style="list-style-type: none"> 1. Access Single VLAN このモードでは、シングル VLAN が許可されます。 2. Trunk Multiple VLAN このモードでは複数 VLAN がサポートされます。 	–	Access
ACL			
Precedence	ACL ルールのインデックスを設定する機能です。パケットは設定された優先順位の値に基づいて検証され、処理されます。	1–256	1
Policy	トラフィックを許可および拒否するよう設定する項目	Deny/ Permit	Deny
Direction	設定された ACL のルールを、任意の方向または特定の方向に適用するための規定。	–	In
Type	<p>cnPilot デバイスは、3 つのレイヤの ACL をサポートしています。ルールの設定は以下のようになります。</p> <ul style="list-style-type: none"> ・ IP6 ・ MAC ・ Proto6 	–	IP
Source IP/Mask	このオプションは、ACL タイプが IP アドレスに設定されている場合に使用できます。このフィールドでは、ルールを単一の IP アドレスに適用するか、複数の IP アドレスに適用するかを設定できます。	–	–
Destination IP/Mask	このオプションは、ACL タイプが IP アドレスに設定されている場合に利用できます。このフィールドでは、ルールを単一の IP アドレスに適用するのか、複数の IP アドレスに適用するかを設定できます。	–	–
Source MAC/Mask	このオプションは、ACL タイプが MAC アドレスに設定されている場合に使用できます。このフィールドでは、ルールを単一のデバイスの MAC アドレスに適用するのか、MAC アドレスの範囲に適用するかを設定できます。	–	–
Destination MAC/Mask	このオプションは、ACL タイプが MAC アドレスに設定されている場合に使用できます。このフィールドでは、ルールを単一のデバイスの MAC アドレスに適用するのか、MAC アドレスの範囲に適用するかを設定できます。	–	–
Protocol	<p>このオプションは、ACL タイプを proto として選択した場合に利用できます。以下のプロトコルを選択できます。</p> <ul style="list-style-type: none"> ・ TCP 	–	TCP

	<ul style="list-style-type: none"> UDP ICMP Any 		
Source Port	プロトコルとポートの組み合わせで ACL を適用する機能。	-	-
Destination Port	プロトコルとポートの組み合わせで ACL を適用する機能。	-	-
Description	管理者がわかりやすいように、ACL ルールごとにテキスト文字列を追加することができます。	-	-

The screenshot shows the 'Ethernet Ports' configuration page. Under the 'Eth1' tab, the 'Access Mode' is set to 'Access Single VLAN' with 'VLAN 1' selected. Below this, the 'ACL' section is active. It contains fields for 'Precedence' (1), 'Policy' (Deny), 'Direction' (In), 'Type' (IP6, highlighted with a red box), 'Source IP/Mask', and 'Destination IP/Mask'. A 'Description' field is also present. At the bottom, there is a table with columns: Preced., Policy, Direction, Type, Rule, Description, and Action. The table is currently empty, displaying 'No Rules available'. Navigation controls at the bottom right show '1 / 1' items and '10 items per page'.

General

Parameters	Description	Range	Default
Management Access	CLI (Telnet、SSH)、GUI (HTTP、HTTPS)、SNMP のすべてのモードでデバイスのアクセスを制限する機能を提供します。ユーザーは以下のようにデバイスのアクセス制	-	Allow from both

	限を設定できます。 <ul style="list-style-type: none"> ▪ Block ▪ Allow from Wired ▪ Allow from both wired and wireless 		Wired and Wireless
--	---	--	--------------------

The screenshot shows the 'VLAN' configuration page. At the top, there are tabs for 'VLAN', 'Routes', 'Ethernet Ports', 'Security', 'DHCP', 'Tunnel', 'PPPoE', and 'VLAN Pool'. The 'VLAN' tab is active. Below the tabs, there's a section for 'VLAN' with an 'Edit' dropdown set to 'VLAN 1' and a 'Delete this interface' button. To the right is an 'Add new L3 Interface' button. Below these are sections for 'IPv4', 'IPv6', and 'General'. The 'General' section is highlighted with a red rectangle. It contains a 'Management Access' dropdown menu currently set to 'Allow from both Wired & Wireless', and a note 'CLI/GUI/SNMP access via this interface'.

Security

Parameters	Description	Range	Default
DoS Protection	cnPilot デバイスには、有線ネットワーク上の DoS 攻撃を検知する機能が内蔵されています。cnPilot デバイスが検知する攻撃は、以下の通りです。 <ul style="list-style-type: none"> ▪ IP Spoof ▪ Smurf Attack ▪ IP Spoof Log ▪ ICMP Fragment 	–	Disabled
Rogue AP			
Detection	cnPilot デバイスは、cnMaestro と連携して、Rogue AP を検出する機能を備えています。この機能を有効にすると、すべてのネイバー情報が cnMaestro に共有され、ネットワーク内の Rogue AP が報告されます。	–	Disabled

VLAN	Routes	Ethernet Ports	Security	DHCP	Tunnel	PPPoE	VLAN Pool
------	--------	----------------	----------	------	--------	-------	-----------

DoS Protection

☐ IP Spoof *Enable IP spoof attack protection(Checks whether spoofed IP address is reachable before accept)*
☐ Smurf Attack *Enable SMURF attack protection(Do not respond to broadcast ICMP)*
☐ IP Spoof Log *Enable IP spoof log messages(Log unroutable source addresses)*
☐ ICMP Fragment *Enable fragmented ping attack protection(Drop fragmented ICMP packets)*

Rogue AP

Detection ☐ Enable rogue AP detection

DHCP

Parameters	Description	Range	Default
Edit	cnPilot デバイスで複数のプールが定義されている場合、DHCP プールを選択する機能		
Address Range	ユーザーは、ドロップダウンボックスから選択した DHCP プールの開始アドレスと終了アドレスを設定できます。	–	–
Default Router	ドロップダウンボックスから選択した DHCP プールのネクストホップを設定する機能	–	–
Domain Name	ドロップダウンボックスから選択した DHCP プールのドメイン名を設定するための項目	–	–
DNS Address	ドロップダウンボックスから選択した DHCP プールに DNS サーバを設定するための項目です。	–	–
Network	ドロップダウンボックスから選択した DHCP プールのネットワーク ID を設定するための項目です。	–	–
Lease	ドロップダウンボックスから選択した DHCP プールのリースを設定するための項目です。	–	–
Add Bind List			
	DHCP プールを設定すると、ユーザーは定義されたアドレスプールから MAC と IP をバインドすることができ、ワイヤレスステーションが接続するたびに同じ IP アドレスを取得できるようになります。IP アドレスの割り当てには以下のパラメータが必要です。 <ul style="list-style-type: none"> MAC Address IP Address 	–	–

VLAN Routes Ethernet Ports Security **DHCP** Tunnel PPPoE VLAN Pool

Edit [Delete this Pool](#) [Create Pool](#)

Address Range Start End IP address range to be assigned to clients

Default Router Default router IP

Domain Name Domain Name

DNS Address Primary Secondary Domain name for the client

Network IP Mask Subnet number and mask of the DHCP address pool

Lease 1 Hours Minutes Lease time (days.hours:minutes)

[Save](#) [Cancel](#)

Add Bind List

MAC Address xx:xx:xx:xx:xx:xx **IP Address** xxx.xxx.xxx.xxx [Save](#)

MAC Address	IP Address	Action
No bind list available		

1 / 1 10 items per page

PPPoE

Parameters	Description	Range	Default
Enable	PPPoE クライアントを有効にする機能	–	Disable
VLAN	PPPoE クライアントが IP アドレスを取得すべき VLAN ID を設定できます。	–	–
Service Name	PPPoE サービス名を設定します	–	–
Authentication info	PPPoE 認証に必要な認証情報を設定するための項目です。	–	–
MTU	Maximum Transmission Unit	500–1492	1430
TCP MSS Clamping	PPPoE エンドポイントを設定します。IP かエンドポイントのホスト名のどちらも対応しています	–	Enabled
Management Access	有効にすると、ユーザーは UI か SSH で PPPoE IP を使いアクセスできます	–	Disabled

VLAN Routes Ethernet Ports Security DHCP Tunnel **PPPoE** VLAN Pool

Enable ☐

VLAN Vlan ID assigned to PPPoE

Service Name Configure pppoe service-name parameters

Authentication Info Max 64 characters

MTU Configure mtu for pppoe connection (500-1492 bytes)

TCP-MSS Clamping ☒ Enable tcp mss clamping for pppoe connection

Management Access ☐ Enable CLI/GUI/SNMP access via this interface

VLAN Pool

Parameter	Description	Range	Default
VLAN Pool Name	VLAN リストのフレンドリーネームを設定する	–	–
VLAN ID List	それぞれの VLAN プール名のための VLAN ID リスト。シングルまたは複数の VLAN ID を設定可能。複数 VLAN ID はコンマかハイフンで仕切ることができます	–	–

VLAN Routes Ethernet Ports Security DHCP Tunnel PPPoE **VLAN Pool**

VLAN Pool Name Vlan Pool Name

VLAN ID List 1-4094

VLAN Pool Name VLAN ID List A...

No list available

12. ファームウェアの管理



アップデートの最中は、絶対に電源を切らないでください。

Operations > Firmware Upgrade を開きます

「ファイルを選択」をクリックし、ダウンロードすべきimage fileを選択します

Upgrade Firmwareをクリックします

Save

System

Operations > Systems

System の Reboot、また工場出荷モードに設定可能です。

System

Reboot
Download Tech Support
Disconnect All Clients
Flash LEDs
10
Flash LED (1-120) seconds
Factory Default

Configuration

Operations > Configuration

工場出荷モードに戻す前に現状の設定を吸い出し、保存することができます。

Export をクリックすれば、PC 内のダウンロードに格納され、工場出荷モード後に Import で元の設定に戻すことが出来ます。元の構成を有効にするには必ず Reboot が必要です。

13. Troubleshoot

Packet Capture:

Administratorがある特定のインタフェースで全てのパケットをキャプチャすることができます。ネットワークのアドレス、プロトコルタイプが表示されます。

特定のMAC address, IP address, port numberなどを指定してパケットにフィルタをかけることができます。パケット数も制限できるので画面からはみ出ることがありません。

イーサネットインタフェースでキャプチャされたパケットは、デバイスの物理インタフェースで送信受信されているパケットです。

WLANインタフェースパケットは、特定のWLAN上のデータパケットです。それらは無線インタフェースでブリッジされています。

Troubleshoot > Packet Capture

Troubleshoot / Packet Capture

Interface :

Ethernet

Ex : 1

Source IP & Destination IP:

Source IP

Destination IP

Source MAC & Destination MAC:

Source MAC

Destination MAC

Direction :

Both

Count :

Ex : 100

Filter :

Ex : icmp[icmptype] == 8

NOTE: Packet capture is aborted after 60 seconds, if the count has not reached.
Summary will not be available when aborted.

Start Capture

Packet Capture Result

Logs and Events:

システムは、クライアントに関連した認証から構成変更まで機器上のどんな行為に関するイベントメッセージも生成します。

1. あとで表示とフィルタリングできるようcnMaestro にフォワードします。
2. コマンドラインの ‘show logging’ でみるができます。
3. syslog serversに送信されます

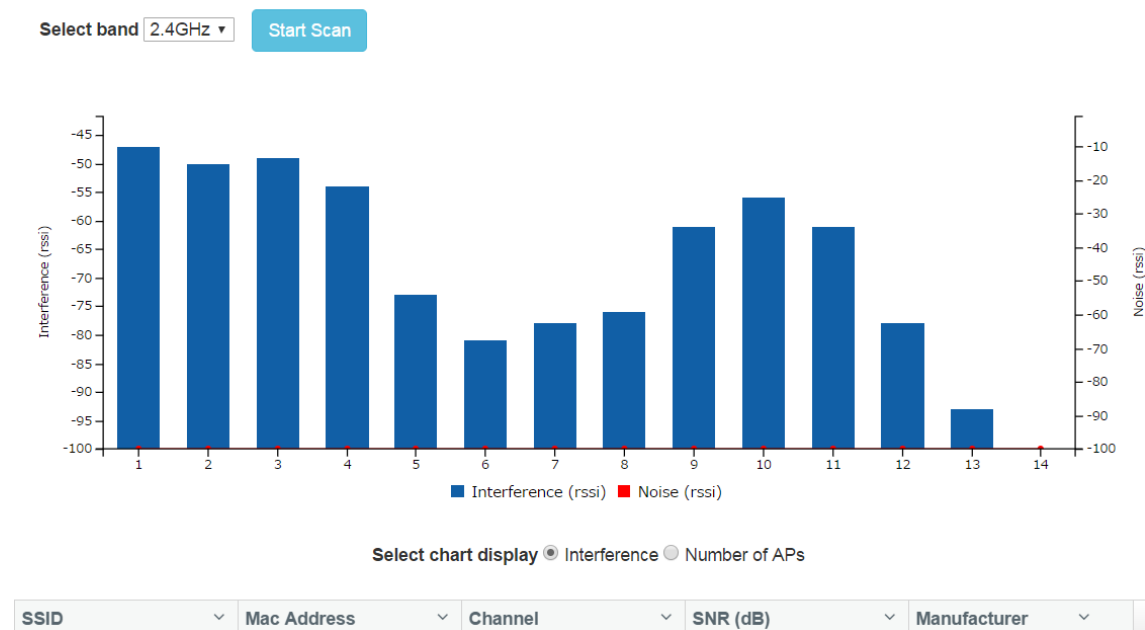
Connectivity:

相手方無線機器の IP アドレスに ping を打ち、応答を確認できます。

WiFi Analyzer

2.4GHz または 5GHz を選択し、“Start Scan”をクリックします。

近傍の無線機器の SSID や製造元が表示されます。



14. 困ったときの対処法

項目

- ① 機器本体の IP アドレスがわからなくなった場合
- ② 有線 LAN で機器本体と通信ができない場合
- ③ 端末から SSID が見えない場合(アクセスポイントモード時)
- ④ 端末から SSID は見えるが接続できない場合(アクセスポイントモード時)
- ⑤ ポイントツーポイント、ポイントツーマルチポイント接続ができない場合
- ⑥ 期待した通信速度が得られない場合
- ⑦ 通信が切れやすい場合

① 機器本体の IP アドレスがわからなくなった場合

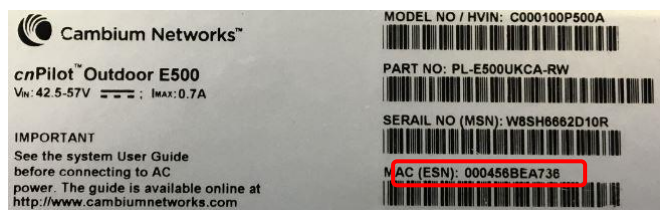
1) 方法 1

LAN 端子の近くにあるリセットボタンを長押しすることで、IP アドレスは初期状態の 192.168.0.1 に戻ります。

この方法を用いると現在設定されている各種設定値も全て初期化されます。

2) 方法 2

通常使用する IP アドレスとは別に、機器毎に固有の IP アドレスがあります。IP アドレスは 169.254.xxx.yyy になります。xxx と yyy の値は本体の MAC アドレスによって決まります。例えば、16 進数表記の MAC アドレスの下 4 桁が A7 36 の場合は、10 進数表記では 167 と 54 になるので、IP アドレスは、169.254.167.54 となります。MAC アドレスは機器本体裏面のシールに記載されています。



② 有線 LAN で機器本体と通信ができない場合

1) 機器本体前面の LED は点灯していますか。

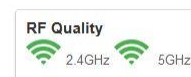
- a) 電源投入後しばらくして 2 つの LED が橙色もしくは緑色で点灯する場合は正常に立ち上がっています。

- b) LED が点滅している場合は機器本体の異常です。8 ページに記載の方法で初期化を行っても点滅状態が続く場合は故障が考えられます。
 - c) LED が点灯しない場合は、PoE 電源と LAN ケーブルが正しく接続されているか確認してください。それでも症状が変わらない場合は、PoE 電源または LAN ケーブルを交換し、問題部分の切り分けを行ってください。
- 2) パソコン側の LAN の設定が機器本体の IP アドレスに接続できるようになっていますか。
18 ページに記載されているパソコン側の IP アドレスおよびサブネットマスクが機器本体と同じネットワークの範囲になっているか確認してください。
 - 3) ブラウザを立ち上げ直すことで接続できるようになりますか。
ブラウザが以前に接続した時のキャッシュを読み込んでしまう場合があります。立ち上げ直すことで正常に機器本体へアクセスできるようになる場合があります。

③ 端末から SSID が見えない場合(アクセスポイントモード時)

スマートフォンや PC 等の端末で本体の SSID を検索しても見つからない場合は次の項目の確認を行ってください。

- 1) Dashboard 画面の右上の扇型の WiFi のマークが緑色になっていますか。



2.4GHz 帯のみをイネーブルにしている場合は 2.4GHz のマークのみ緑色になります。イネーブルにしているバンドのマークが緑色にならない場合は **Configure > Radio** の設定がイネーブルになっていないか、**Configure > WLAN** の設定がイネーブルになっていないことが考えられます。



- 2) SSID が見えない設定になっていませんか。
Configuration > WLAN で **Hide SSID** の設定にイネーブルになっていると、SSID は見えなくなります。
- 3) ポイントツーポイントモードの Client 設定になっていませんか。
Configuration > WLAN で **Mesh** が **Client** になっていると、SSID を送出しません。Mesh のモードがアクセスポイントである **off** の設定になっていることを確認してください。

- 4) 5GHz 帯は立ち上がるまで時間がかかります。

5GHz 帯は電源立ち上げ後、同じ周波数をレーダーが使用していないか 1 分間ほど検知するため、2.4GHz 帯に比べ 1 分ほど立ち上がりが遅くなります。

④ 端末から SSID は見えるが接続できない場合(アクセスポイントモード時)

スマートフォンや PC 等の端末で SSID を検索し、機器本体の SSID が見つかったとしても接続ができない場合は次の項目の確認を行ってください。

- 1) パスワードの要求があり、パスワードを入力しても受け付けられない。

Configuration > WLAN の Passphrase に正しいパスワードを入力し Save ボタンをクリックしてください。なお、一度セットしたパスワードは読み出すことができません。

- 2) 本体の設定が Base モードになっている。

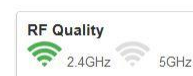
アクセスポイントモードではなく、ポイントツーポイントモードの親局設定である Mesh Base に設定されていると、スマートフォンや PC から SSID は見えますが接続することができません。Configuration > WLAN の Mesh が off になっていることを確認してください。

- 3) サーバが DHCP モードになっていますか。

本機器をルータモードではなく通常モードで使用する場合、端末の IP アドレスは本機器に有線 LAN で接続されるサーバから配られます。サーバが DHCP に対応していない状態の場合はスマートフォンや PC 等の端末が IP アドレスをもらえず待ち状態となります。なお、端末の IP アドレスが手動設定の場合はこの問題はありません。

⑤ ポイントツーポイント、ポイントツーマルチポイント接続ができない場合

- 1) Dashboard 画面の右上の扇型の WiFi のマークが緑色になっていますか。



通常では、親機(Base)と子機(Client)の Dashboard 画面の 2.4GHz もしくは 5GHz のマークが緑色になります。緑色にならない場合は Configure > Radio の設定がイネーブルになっていないか、Configure > WLAN の設定がイネーブルになっていないことが考えられます。



- 2) Base と Client で SSID、暗号化パスワードが一致していますか。

SSIDを確認し、暗号化を行っている場合は Base と Client で同じパスワードを再度入力してください。

- 3) 5GHz 帯は立ち上がるまで時間がかかります。

5GHz 帯は電源立ち上げ後、同じ周波数をレーダーが使用していないか 1 分間ほど検知するため、2.4GHz 帯に比べ 1 分ほど立ち上がりが遅くなります。

⑥ 期待した通信速度が得られない場合

- 1) 他の無線 LAN からの干渉により、実効速度が低下します。

無線 LAN はだれでも自由に使用できるため、同じチャンネルを使用する他の無線 LAN が近くにあると互いに干渉するようになります。無線 LAN は他局が電波を出しているときは送信を待つようになるため、他局が多くなればなるほど待ち時間が長くなり、通信の平均速度は低下します。特に 2.4GHz 帯は使用ユーザが多いこと、同じ周波数帯を別の用途でも使用するため、干渉の影響が高くなります。2.4GHz 帯で同じ周波数帯を使用する機器には次のようなものがあります。

- a) 電子レンジ
- b) 工業用加熱機器や医療用電気メス
- c) アマチュア無線
- d) Bluetooth

- 2) 見通しの悪い場所に機器が設置されている。

2.4GHz も 5GHz も電波は光と同じように直進性が高いため、見通しの悪いところには電波が飛びにくくなります。十分に見通しのとれた場所に設置する必要があります。

また植物の葉は電波を吸収しやすいため、木が茂っている環境では電波の飛びが悪くなります。無線の伝搬路上に植物がある場合は、春になって木が茂ってくると通信速度の低下もしくは通信断となることがあります。

- 3) 機器の設置場所によっては通信速度が低下します。

無線の伝搬路は機器間の直線上で伝わる直接波の他に地面や建物で反射する反射波が存在します。反射波は直接波よりも伝搬路が長くなるため、遅れて受信側に到達します。電波は波であり高くなる山と低くなる谷が繰り返され、直接波の山と遅れた反射波の山がちょうど重なる場合は互いに強め合いますが、直接波の山と反射波の谷が重なる場合は互いに打ち消し合うようになり、受信側で受ける電波は弱くなります。そのため、見通しが良く、距離も問題ない場合でも期待した通信速度が得られないことがあります。

その場合は、機器の取り付け位置を上下方向、左右方向また機器自体を左右に振りながら受信レベルが高くなることを探します。数十 cm 程度の移動でも改善が見込めます。

⑦ 通信が切れやすい場合

- 1) 他の無線機器類からの干渉により、通信断が発生します。

無線 LAN はだれでも自由に使用できることと、同じ周波数帯を他の用途でも使用しているため干渉の影響で速度低下や通信断が発生しやすくなります。

a) 2.4GHz 帯無線 LAN

電子レンジと同じ周波数帯であるため、電子レンジの近くで 2.4GHz 帯無線 LAN を使用すると、電子レンジが動作しているときは通信断が発生しやすくなります。

工業用加熱機器や医療用加熱機器、アマチュア無線でも同じ周波数帯を使用しているため非定期的に通信断が発生する可能性があります。

対策としては、指向性のある無線 LAN 機器を使用すること、途中で中継を行うこと 5GHz 帯無線 LAN を使用することなどがあります。

b) 5GHz 帯無線 LAN

5GHz 帯無線 LAN の周波数幅は 2.4GHz 帯無線 LAN の約 3 倍あるため、無線 LAN 同士による干渉の影響はすくなくなり、電子レンジのような加熱機器の影響は受けませんが、次の無線機器からの影響を受けます。

・ レーダー

この周波数帯はレーダーに優先権があるため、レーダーの信号を受信した場合は直ちに通信を止めて他の周波数へ移らなければなりません。また移動先の周波数では 1 分間レーダー検知を行わなければならないため、その間は通信断となります。なお、レーダーの周波数や運用時間は公開されていないことが多いため、事前に回避策をとることができません。

・ 無人移動体画像伝送システム

ドローン等に搭載したカメラの映像を伝送するシステムで、無線 LAN のように他の電波を受信した場合は通信を見合わせるキャリアセンス機能はないため、この電波が出ているときは干渉を受け続けることになります。

この無線システムでは 5650MHz 以上を使用するため、5500MHz から 5650MHz の範囲の周波数を使用することで回避できます。

- ・ アマチュア無線

最近はこの周波数帯を用いてドローンに搭載したカメラの映像を伝送するアマチュア局が増えてきたため干渉を受けやすくなってきています。この無線システムも 5650MHz 以上を使用するため、5500MHz から 5650MHz の範囲の周波数を使用することで回避できます。

2) 障害物の影響により、通信断が発生します。

周波数が高い 2.4GHz や 5GHz の電波は光と同じように直進性が高く、テレビやラジオの電波のように障害物の裏側へ回り込むいわゆる回折の効果が期待できないため、伝搬路が自動車等で一時的に遮断されると、その間は通信が停止してしまいます。そのため、無線機器はトラックや建設機械等の影響を受けない環境に設置する必要があります。

15. 製品仕様

製品型番	E410
無線 LAN インタフェース	IEEE802.11(b, g, a, n, ac)
有線 LAN インタフェース	RJ-45(10/100/1000BASE-TX) x1 ポート
アンテナ部	2.4GHz, 5GHz 共用 MIMO 内蔵
セキュリティ	WPA2(802.11i)、WPA2 Enterprise(802.1x/EAP)
プロトコル	DHCP、SNMP、NTP、HTTP、HTTPS
変調技術	OFDM
変調方式	OFDM: 16/64/256QAM、QPSK、BPSK
周波数帯	2.4GHz, 5.1- 5.7GHz
最大通信速度	802.11n: 300Mbps
最大通信速度	802.11ac: 860Mbps
チャンネル数	最大 13 チャンネル (2.4GHz)
SSID 登録数	16
無線動作モード	Mesh-Base、Mesh-Client、Mesh-Off
最大同時接続 クライアント数	2.4GHz: 256, 5GHz: 127
最大送信出力	16dBm (2.4GHz), 13dBm (5GHz)
アンテナ利得	4dBi (2.4GHz), 4.29dBi(5GHz)
受信感度	-90dBm ~ (帯域幅による)
管理機能	HTTP/HTTPS、SNMP(read only) v2c/v3
電源	AC 100~240V 50/60Hz(PoE アダプタ) ※別売り (弊社取り扱い製品) の PoE アダプタをご使用ください
最大消費電力	8W typ. 13W max.
動作温度	0 ~ +50°C
動作湿度	0 ~ 95%(結露なきこと)
保存温度	-40 ~ +70°C
保存湿度	0 ~ 95%(結露なきこと)
寸法	(W)170mm x (D)70mm x (H)41mm(突起部含まず)
重量(本体のみ)	384g
取り付け方法	天井・壁面
認定	工事設計認証番号: 003-170155 CE Marking、RoHS
製品保証期間	1 年間
付属品	天井設置用ブラケット、プレート各 1 個 天井設置用ネジ 4 個 ゴム足 4 個 壁設置用ねじ&アンカー 各 2 本

16. 製品保証

◆ 故障かなと思われた場合には、弊社カスタマサポートまでご連絡ください。

- 1) 修理を依頼される前に今一度、この取扱説明書をご確認ください。
- 2) 本製品の保証期間内の自然故障につきましては無償修理させていただきます。
- 3) 故障の内容により、修理ではなく同等品との交換にさせて頂く事があります。
- 4) 弊社への送料はお客様の負担とさせていただきますのでご了承ください。

初期不良保証期間：

ご購入日より 3ヶ月間 (弊社での状態確認作業後、交換機器発送による対応)

製品保証期間：

ご購入日より 1年間 (お預かりによる修理、または交換対応)

◆ 保証期間内であっても、以下の場合は有償修理とさせていただきます。
(修理できない場合もあります)

- 1) 使用上の誤り、お客様による修理や改造による故障、損傷
- 2) 自然災害、公害、異常電圧その他外部に起因する故障、損傷
- 3) 本製品に水漏れ・結露などによる腐食が発見された場合

◆ 保証期間を過ぎますと有償修理となりますのでご注意ください。

◆ 本製品に起因する損害や機会の損失については補償致しません。

◆ 修理期間中における代替品の貸し出しは、基本的に行っておりません。別途、有償サポート契約にて対応させて頂いております。有償サポートにつきましてはお買い上げの販売店にご相談ください。

◆ 本製品の保証は日本国内での使用においてのみ有効です。

製品に関するご質問・お問い合わせ先

ハイテクインター株式会社

カスタマサポート

TEL 0570-060030

MAIL support@hytec.co.jp

受付時間 平日 9:00～17:00

HYTEC INTER Co., Ltd.