IP 盗難

IP 盗難の概要

IP 盗難機能は、すでに別のデバイスに割り当てられている IP アドレスが使用されないようにします。2 つのワイヤレス クライアントが同じ IP アドレスを使用していることがコントローラによって検出された場合、コントローラは、優先順位が低い方のクライアントを IP 盗難者であると宣言し、他方のクライアントが継続できるようにします。ブロックリストが有効になっている場合、そのクライアントが除外リストに登録され、追放されます。

コントローラでは、IP 盗難機能がデフォルトで有効になっています。クライアント（データベース内の新規および既存のクライアント）の優先順位レベルも IP 盗難の報告に使用されます。優先順位レベルは、Dynamic Host Configuration Protocol（DHCP）、Address Resolution Protocol（ARP）、データ収集（クライアントがどの IP アドレスを使用しているかを示す IP データ パケットを調べる）などの学習タイプまたは学習ソースです。有線クライアントは、常に他よりも高い優先順位レベルになります。ワイヤレス クライアントが有線 IP の盗難を試みると、そのクライアントは盗難者であると宣言されます。

IPv4 クライアントの優先順位は次のとおりです。

1. DHCPv4
2. ARP
3. データ パケット

IPv6 クライアントの優先順位は次のとおりです。

1. DHCPv6
2. NDP

3. データ パケット

（注） 静的な有線クライアントは、DHCP よりも優先順位が高くなります。

IP 盗難の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** > **[Client Exclusion Policies]** を選択します。

ステップ 2 [IP Theft or IP Reuse] チェックボックスをオンにします。

ステップ 3 [Apply] をクリックします。

IP 盗難の設定

IP 盗難機能を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless wps client-exclusion ip-theft** 例： `Device(config)# wireless wps client-exclusion ip-theft`	クライアント除外ポリシーを設定します。

IP 盗難除外タイマーの設定

IP 盗難除外タイマーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**exclusionlist timeout** *time-in-seconds* 例： `Device(config-wireless-policy)# exclusionlist timeout 5`	タイムアウトを秒単位で指定します。有効な範囲は 0 ～ 2147483647 です。タイムアウトなしの場合は0を入力します。

IP 盗難設定の確認

IP 盗難機能が有効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless wps summary

Client Exclusion Policy
  Excessive 802.11-association failures   : Enabled
  Excessive 802.11-authentication failures: Enabled
  Excessive 802.1x-authentication         : Enabled
  IP-theft                                : Enabled
  Excessive Web authentication failure    : Enabled
  Cids Shun failure                       : Enabled
  Misconfiguration failure                : Enabled
  Failed Qos Policy                       : Enabled
  Failed Epm                              : Enabled
```

IP 盗難機能に関するその他の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method     Role
-------------------------------------------------------------------------------------
000b.bbb1.0001 SimAP-1                2    Run                11a      None       Local


Number of Excluded Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method
-------------------------------------------------------------------------------------
10da.4320.cce9 charlie2               2    Excluded           11ac     None
```

```
Device# show wireless device-tracking database ip

IP                              VLAN  STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------
  20.20.20.2                     20    Reachable   Local       001e.14cc.cbff
  20.20.20.6                     20    Reachable   IPv4 DHCP   000b.bbb1.0001


Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason               Time Remaining
-------------------------------------------------------------------------------------
10da.4320.cce9                         IP address theft                   59


Device# show wireless exclusionlist client mac 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : IP address theft
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```