

H3C Wireless製品

FAQ

New H3C Technologies Co., Ltd.
<https://www.h3c.com/>

ドキュメントバージョン: 6W100-20200907

Copyright © 2021, New H3C Technologies Co., Ltd. およびそのライセンス供給会社が著作権所有。

New H3C Technologies Co., Ltdの書面による事前の同意なしに、このマニュアルのいかなる部分も、いかなる形式または手段によっても複製または配布することはできません。

商標

New H3C Technologies Co., Ltdの商標を除き、本書に記載されている商標は、それぞれの所有者に帰属します。

通知

このドキュメントの情報は、予告なしに変更されることがあります。記述、情報、および推奨事項を含む、このドキュメントのすべての内容は正確であることに万全を期していますが、明示または黙示を問わず、いかなる種類の保証をおこなうものではありません。H3Cは、ここに含まれる技術的または編集上の誤りまたは脱落について責任を負わないものとします。

環境保護

この製品は、環境保護要件に準拠するように設計されています。この製品の保管、使用、および廃棄は、適用される国内法および規制を満たしている必要があります。

序文

このガイドでは、H3C 製品のFAQについて説明します。この序文には、ドキュメントに関する次のトピックが含まれています:

- 対象読者。
- 表記法。
- ドキュメントへのフィードバック。

対象読者

このドキュメントの対象読者は次のとおりです:

- ネットワーク計画者。
- フィールドテクニカルサポートおよびサービスエンジニア。
- Cloudnetを使用するネットワーク管理者。

表記法

次の情報は、ドキュメントで使用されている表記法について説明しています。





コマンド規則

表記法	説明
太字	太字 のテキストは、示されている文字の通りに入力するコマンドとキーワードを表します。
<i>イタリック</i>	<i>イタリック</i> のテキストは、示されている文字の通りに入力するコマンドとキーワードを表しません。
[]	角括弧は、オプションの構文の選択肢(キーワードまたは引数)を囲みます。
{ x y ... }	中括弧は、垂直バーで区切られた必要な構文の選択肢のセットを囲み、そこから1つを選択します。
[x y ...]	角括弧は、縦棒で区切られたオプションの構文の選択肢のセットを囲み、そこから1つまたは何も選択しません。
{ x y ... } *	アスタリスクでマークされた中括弧は、垂直バーで区切られた必要な構文の選択肢のセットを囲み、そこから少なくとも1つを選択します。
[x y ...] *	アスタリスクでマークされた角括弧は、垂直バーで区切られたオプションの構文の選択肢を囲み、そこから1つの選択肢、複数の選択肢、または何も選択しません。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1~n回入力できます。
#	シャープ(#)記号で始まる行はコメントです。













GUIの規則

表記法	説明
太字	ウインドウ名、ボタン名、フィールド名、およびメニュー項目は太字で表示されます。例えば、 New User ウィンドウを開いて OK をクリックします。
>	マルチレベルメニューは山括弧で区切られています。例えば、 File > Create > Folder 。

記号

表記法	説明
 警告！	理解または従わないと怪我につながる可能性のある重要な情報に注意を喚起する警告。
 注意:	重要な情報に注意を喚起する警告。理解または従わないと、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性があります。
 重要:	重要な情報に注意を喚起する警告。
注意:	追加情報または補足情報を含む警告。
 ヒント:	役立つ情報を提供する警告。

ネットワークポロジアイコン

表記法	説明
	ルーター、スイッチ、ファイアウォールなどの一般的なネットワークデバイスを表します。
	ルーターやレイヤー3スイッチなどのルーティング対応デバイスを表します。
	レイヤー2またはレイヤー3スイッチなどの汎用スイッチ、またはレイヤー2転送およびその他のレイヤー2機能をサポートするルーターを表します。
	統合有線WLANスイッチ上のアクセスコントローラ、統合有線WLANモジュール、またはアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向性信号を表します。
	指向性信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、負荷分散デバイスなどのセキュリティ製品を表します。
	ファイアウォール、負荷分散、NetStream、SSL VPN、IPS、ACGモジュールなどのセキュリティモジュールを表します。

このドキュメントで提供される例

このドキュメントの例では、ハードウェアモデル、構成、またはソフトウェアバージョンがデバイスとは異なるデバイスを使用している場合があります。例で示されるポート番号、サンプル出力、スクリーンショット、およびその他の情報は、デバイスにあるものとは異なる場合があります。

ドキュメントへのフィードバック

製品マニュアルに関するご意見は、info@h3c.comまで電子メールでお寄せください。
ご感想をお寄せいただければ幸いです。

内容

Q1 APのACへの登録はVLAN 1が必須ですか？	7
Q2 WLANで802.1x認証でRADIUS認証を利用する際に、エラーが発生しました。チェックすべき項目は何ですか？ ..	9
Q3-Q5の無線制御の方法の事前解説.....	10
Q3 特定のSSIDにアクセスできる時間帯を制御することができますか。.....	13
Q4 特定のSSIDを無線の電波に含ませる時間帯を制御することができますか。.....	20
Q5 無線の電波を送受信できる時間帯を制御することができますか。.....	21
Q6 特定のユーザーのPCのWiFiのMACアドレスを指定してアクセスを拒否するように設定する方法は？	23

Q1 APのACへの登録はVLAN 1が必須ですか？

A: APとAC間の制御通信はVLAN 1が使われます。VLAN 1の定義は以下のように、ap-group定義の中にvlan 1という記述を指定してください。

```
#
Wlan ap-group default-group
remote-configuration enable
vlan 1
vlan 2
ap-model WA538-JP
radio 1
radio enable
service-template 1 vlan 2
radio 2
radio enable
service-template 1 vlan 2
radio 3
radio enable
service-template 2 vlan 2
gigabitethernet 1
Port link-type trunk
Port trunk permit vlan 1 2
Port trunk pvid vlan 1
gigabitethernet 2
Port link-type trunk
Port trunk permit vlan 1 2
Port trunk pvid vlan 1
```

無線テンプレート(SSID,暗号化)を設定

```
#例えばWPA2/CCMP
wlan service-template 1
client forwarding-location ap
ssid H3C_WIFI_01
vlan 2
akm mode psk
preshared-key pass-phrase cipher
$c$3$yvVSH20fC4gGPUa1RCXdVUaYhPwUI8r9PuBb
cipher-suite ccmp
security-ie rsn
service-template enable
#
```

```
#認証なし
wlan service-template 2
client forwarding-location ap
ssid 00000japan
vlan 2
service-template enable
#
```

DHCP Server (AP管理用)

```
dhcp enable
#
dhcp server ip-pool MGT
gateway-list 172.16.1.254
network 172.16.1.0 mask
255.255.255.0
dns-list 8.8.8.8
#
interface Vlan-interface1
ip address 172.16.1.1 255.255.255.0
dhcp server apply ip-pool MGT
#
```

DHCP Server (クライアント用)

```
dhcp server ip-pool client
gateway-list 192.168.1.1
network 192.168.1.0 mask 255.255.255.0
dns-list 8.8.8.8
#
interface Vlan-interface2
ip address 192.168.1.1 255.255.255.0
dhcp server apply ip-pool client
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan 2
port trunk pvid vlan 1
#
dhcp enable
dhcp server forbidden-ip 192.168.1.1 192.168.1.9
```


Q2 WLANで802.1x認証でRADIUS認証を利用する際に、エラーが発生しました。チェックすべき項目は何ですか？

A: 例えば以下のようなエラーが発生した場合、ファイアウォールでポート1812、1813がブロックされていないか確認してください。

“AAA processed accounting-start request and return 8.”

```
%Feb 24 12:26:44:384 2021 L3-025-A01A DOT1X/6/DOT1X_WLAN_LOGOFF: -  
Username=host/sGIGA-s-UserMAC=d8c0-a699-7af5-BSSID=1019-65c2-1c91-SSID=sGIGA-  
s-APName=AP-02
```

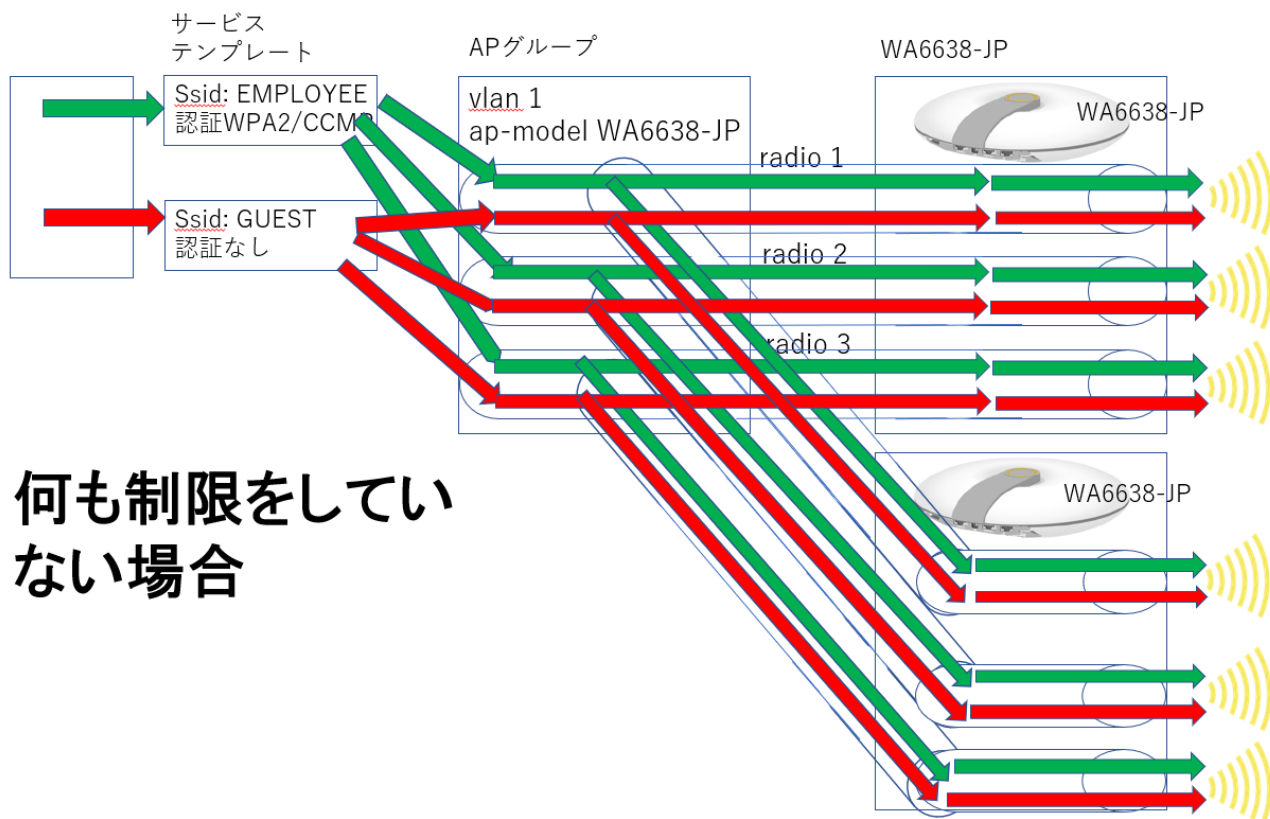
5-A02A-02-RadioID=1-VLANID=411; Session for an 802.1X user was terminated.Reason:AAA processed accounting-start request and return 8.

ちなみに、RADIUS設定は以下のようなものでした:

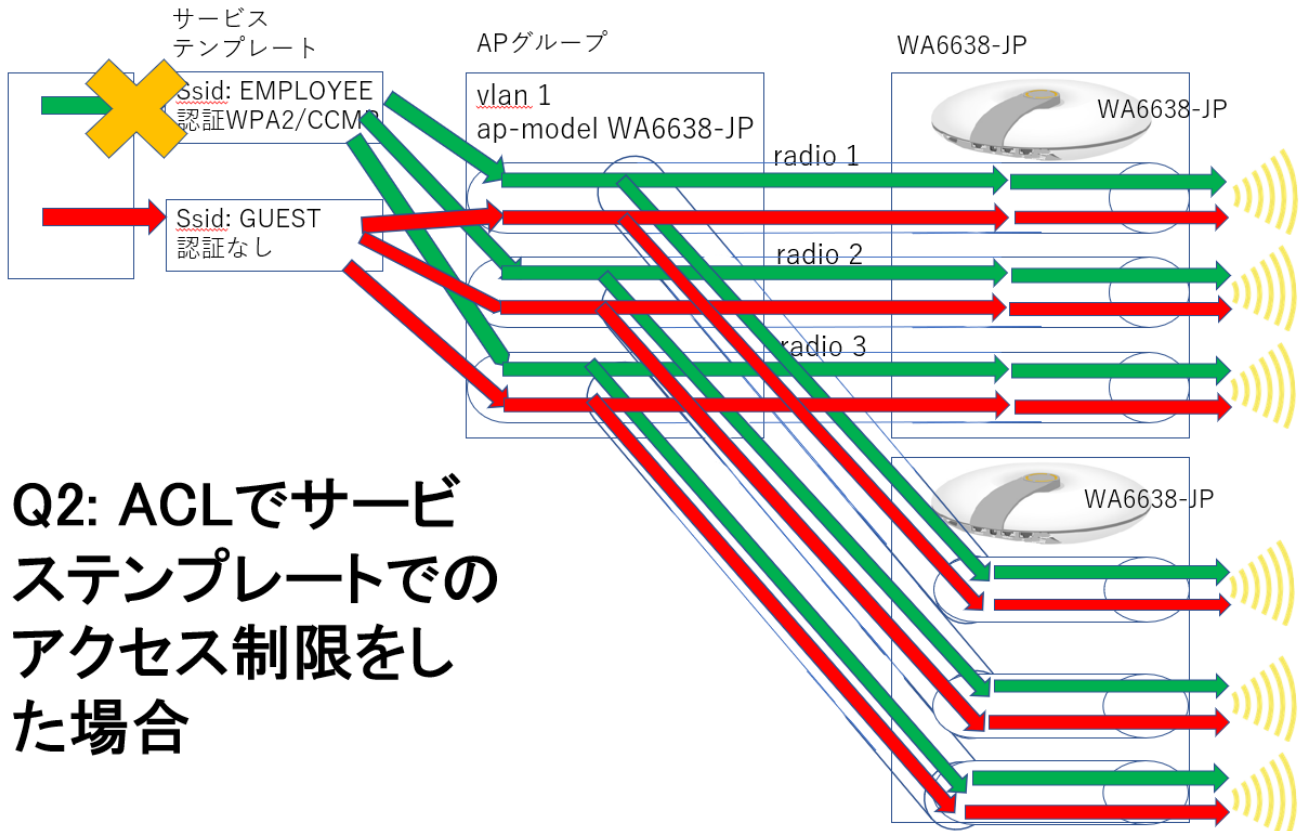
```
-----  
RADIUS scheme name: dot1x_radius  
Index: 1  
Primary authentication server:  
Host name: Not Configured  
IP : 111.108.213.1 Port: 1812  
VPN : Not configured  
State: Active (duration: 2 weeks, 6 days, 0 hours, 16 minutes, 34 seconds)  
Test profile: Not configured  
Weight: 0  
Primary accounting server:  
Host name: Not Configured  
IP : 111.108.213.1 Port: 1813  
VPN : Not configured  
State: Blocked  
Most recent blocked period: 2021/02/24 12:43:33 - now  
Weight: 0  
Second authentication server:  
Host name: Not Configured  
IP : 111.108.213.2 Port: 1812  
VPN : Not configured  
State: Active (duration: 2 weeks, 6 days, 0 hours, 16 minutes, 34 seconds)  
Test profile: Not configured  
Weight: 0  
Second accounting server:  
Host name: Not Configured  
IP : 111.108.213.2 Port: 1813  
VPN : Not configured  
State: Blocked  
Most recent blocked period: 2021/02/24 12:43:42 - now  
Weight: 0  
Accounting-On function : Disabled
```

Q3-Q5の無線制御の方法の事前解説

無線の制限をしていない状態

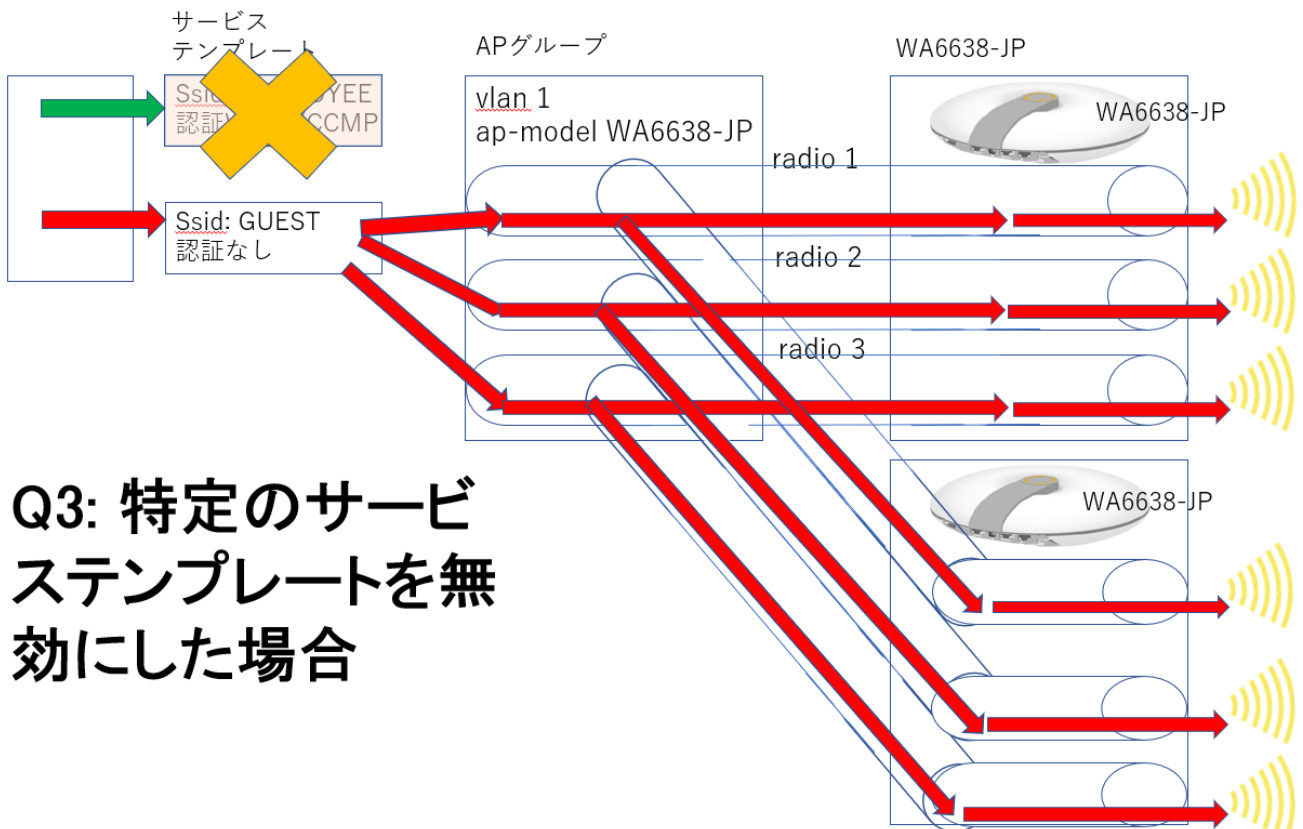


ACLを利用したアクセス制御



Q2: ACLでサービス
ステンプレートでの
アクセス制限をし
た場合

サービステンプレートを利用した無線制限



Q3: 特定のサービ
ステンプレートを無
効にした場合

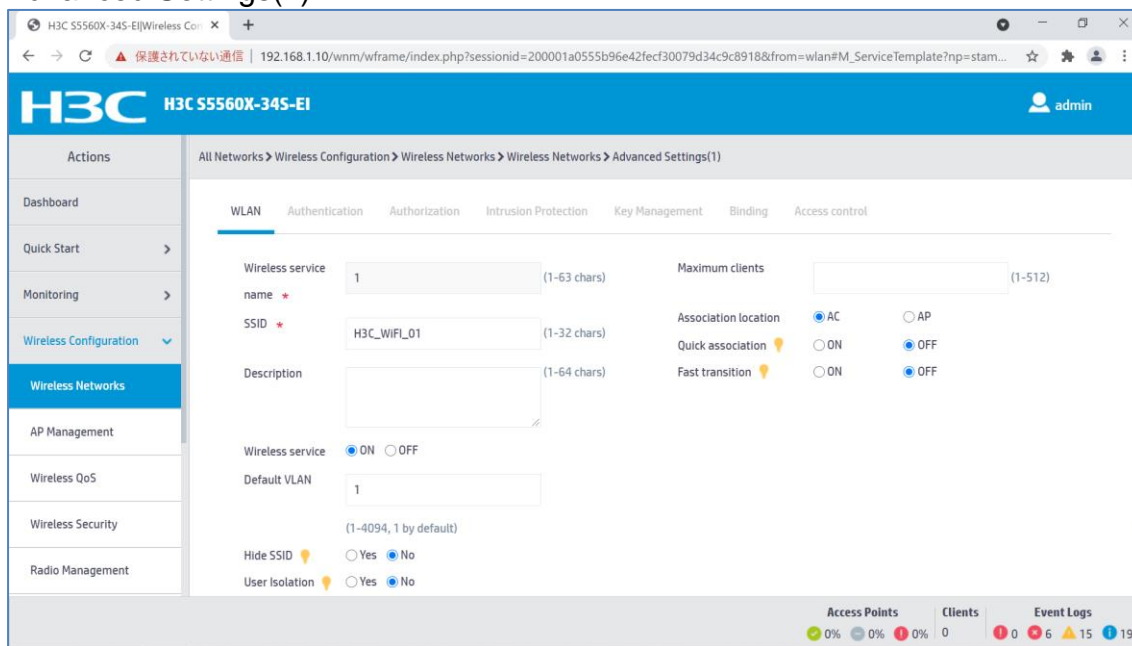
Q3 特定のSSIDにアクセスできる時間帯を制御することができますか。

解決策

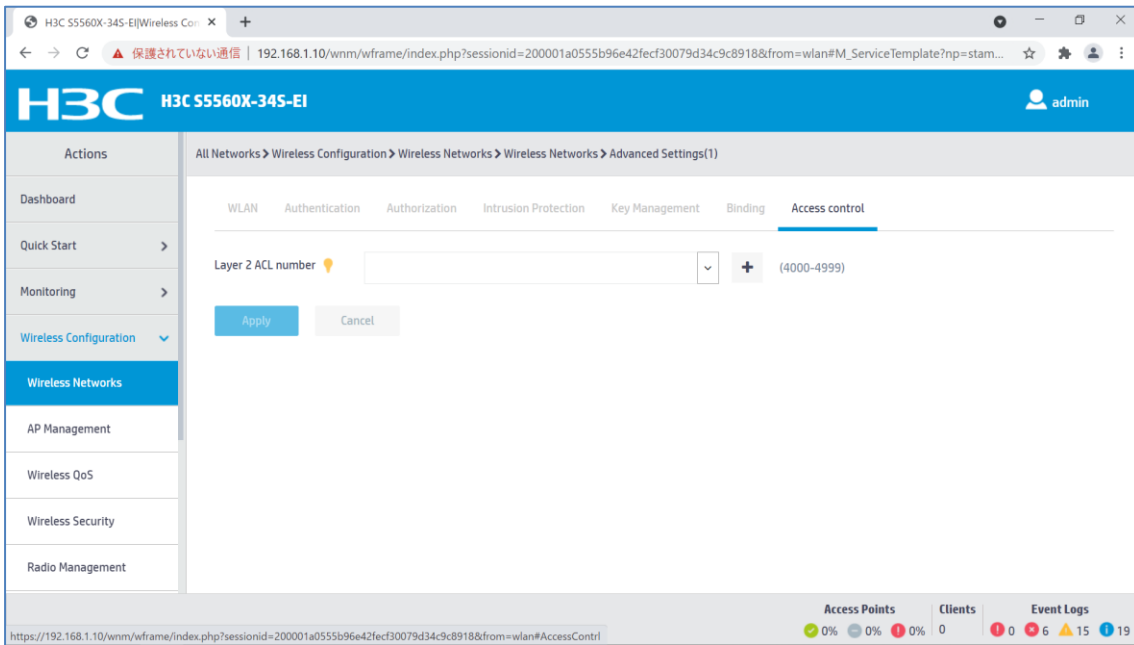
WLANのSSIDの設定の編集でAccess Controlのタブからtime rangeを設定するACLを作成します。ただし、アクセスできなくなる時間前に接続されているクライアントは、アクセスできなくなる時間を過ぎてもそのままアクセス出来ませんが、一旦切断を解除すると再度接続することはできません。

手順

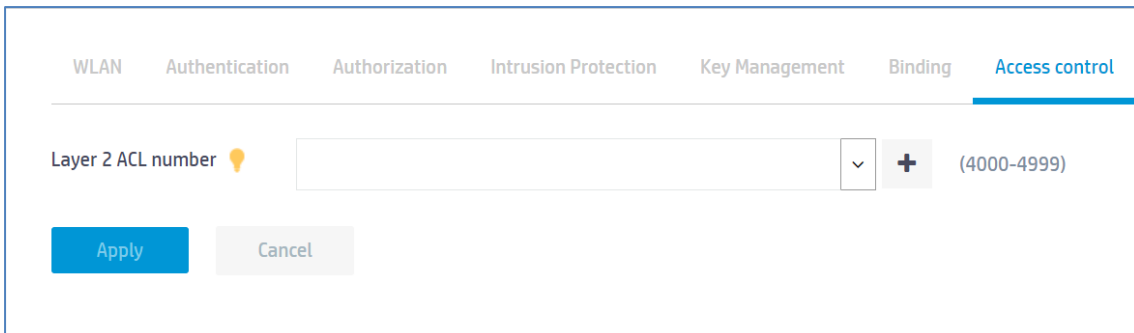
1. All Networks > Wireless Configuration > Wireless Networks > Wireless Networks > Advanced Settings(1)



2. Access ControlタブでLayer 2 ACL numberに4000から4999までの数字を入力し、+をクリックします。



3. このポップアップメニューではEthernet frame header ACLのみ選択できますので、Applyをクリックします。



New ACL
✕

ACL type

IPv4 ACL
 IPv6 ACL
 Ethernet frame header ACL
 User defined ACL

Apply
Cancel

4. ActionをPermit(接続できる時間帯を指定する場合)かDeny(接続できない時間帯を指定する場合)を選択します。例えば、朝9:00から夕方17:00のみアクセスできるとするとPermitを選択します。そして、time range設定行の+をクリックします。

New Rule For Ethernet Frame Header ACL
✕

ACL (4000-4999 or 1-63 chars)

Rule ID * (0-65534) Auto numbered

Description (1-127 chars)

Action * Permit Deny

Match criteria

- Source MAC address/mask 💡
- Destination MAC address/mask
- CoS (802.1p priority)
- DSAP and SSAP fields in LLC encapsulation
- Protocols in the Ethernet frame header

Time range +

Counting

- Count the number of times this rule has been matched
- Continue to add next rule

Apply
Cancel

4. Description(オプション)を入力し、Applyをクリックします。

New Ethernet Frame Header ACL ✕

ACL * (4000-4999 or 1-63 chars)

Rule match order Config Auto

Rule numbering step (1-20)

Description (1-127 chars)

Continue to add rule

5. New Time Rangeで例えば、月曜から金曜までの朝9:00から夕方17:00までという時間帯を入力して、Applyをクリックします。

New Time Range ✕

Name * (1-32 chars)

Periodic time range

Start Time(hh:mm)	End Time(hh:mm)	Sun	Mon	Tue	Wed	Thu	Fri	Sat
09:00	17:00	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Absolute time range

Start Time(hh:mm)	Start Date(YYYY-MM-DD)	End Time(hh:mm)	End Date(YYYY-MM-DD)
hh:mm	YYYY-MM-DD	hh:mm	YYYY-MM-DD

6. Time rangeの設定ができましたので、Applyをクリックします。


New Rule For Ethernet Frame Header ACL ✕

ACL (4000-4999 or 1-63 chars)

Rule ID * (0-65534) Auto numbered

Description (1-127 chars)

Action * Permit Deny

Match criteria Source MAC address/mask 
 Destination MAC address/mask
 CoS (802.1p priority)
 DSAP and SSAP fields in LLC encapsulation
 Protocols in the Ethernet frame header


Time range ✕ +

Counting Count the number of times this rule has been matched
 Continue to add next rule

7. 前のメニューに戻りますので、このACL ruleをApplyします。

All Networks > Wireless Configuration > Wireless Networks > Wireless Networks > Advanced Settings(1)

WLAN Authentication Authorization Intrusion Protection Key Management Binding **Access control**

Layer 2 ACL number  + (4000-4999)

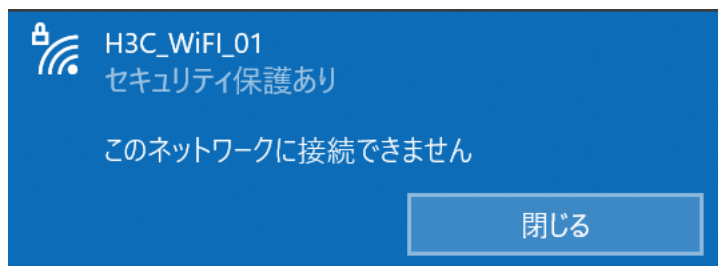
8. 動作確認をしました。

朝9:00前にSSIDにアクセスすると、以下のように「このネットワークにアクセスできません」というメッセージで接続できないことが分かります(このACLは、無線は出たままで、アクセスできる時間帯を制御します)。

```
<H3C>display clock
```

```
08:59:25.251 UTC Wed 03/31/20121
```

```
<H3C>
```



朝9:00を過ぎるとこのSSIDに接続できるようになりました。

```
<H3C>display clock
```

```
09:00:00.143 UTC Tue 03/31/2021
```

```
<H3C>%Mar 31 09:01:29:372 2021 H3C
```

```
STAMGR/6/STAMGR_CLIENT_ONLINE: Client c8e2-6535-5d0e went online from BSS 1019-65c2-48a0 vlan 1 with SSID H3C_WiFi_01 on AP 1019-65c2-48a0 Radio ID 1. State changed to Run.
```

```
%Mar 31 09:01:30:101 2021 H3C
```

```
STAMGR/6/STAMGR_CLIENT_SNOOPING: Detected client IP change: Client MAC: c8e2-6535-5d0e, IP: 192.168.1.13, -NA-, -NA-, -NA-, Username: -NA-, AP name: 1019-65c2-48a0, Radio ID: 1, Channel number: 52, SSID: H3C_WiFi_01, BSSID: 1019-65c2-48a0.
```



補足

GUIで設定したACLはコマンドでは以下のように設定されます。

#

```
wlan service-template 1
```

```
ssid H3C_WiFi_01
```

```
akm mode psk
```

```
preshared-key pass-phrase cipher
```

```
$c$3$+5hDJ7T8AFmbrws+1u5DJnN684C8qmw5xuezOT2sbTbtoQ==
```

```
cipher-suite ccmp
```

```
security-ie rsn
```

```
access-control acl 4000
```

```
service-template enable
```

#

#

```
time-range "work time range settings" 09:00 to 17:00 working-day
```

#

```
acl mac 4000
```

```
description work time range settings
```

```
rule 0 permit time-range "work time range settings"
```

#

Q4 特定のSSIDを無線の電波に含ませる時間帯を制御することができますか。

解決策

公共の施設などで、セキュリティ強化のために夜間の時間帯には特定のSSID(ゲスト用)を電波に乗せないようにするためには、GUIではできませんので、CLIコマンドで行う必要があります。

仮定

電波に乗せる時間帯を、朝9時から夜17時まで制限するものとした例を以下に示します。

手順

1. SSIDを無効にするコマンドをスケジュールjobとして定義します。

```
[WX1840X] scheduler job radio_disable
[WX1840X-job-radio_disable] command 1 system-view
[WX1840X-job-radio_disable] command 2 wlan service-template 1
[WX1840X-job-radio_disable] command 3 undo service-template enable
[WX1840X-job-radio_disable] quit
```

2. 毎日夜17時にSSIDを無効にするコマンドを実行します。

```
[WX1840X] scheduler schedule stop_radio
[WX1840X-schedule-stop_radio] job radio_disable
[WX1840X-schedule-stop_radio] time repeating at 17:00
[WX1840X-schedule-stop_radio] quit
```

3. SSIDを有効にするコマンドをスケジュールjobとして定義します。

```
[WX1840X] scheduler job radio_enable
[WX1840X-job-radio_enable] command 1 system-view
[WX1840X-job-radio_enable] command 2 wlan service-template 1
[WX1840X-job-radio_enable] command 3 service-template enable
[WX1840X-job-radio_enable] quit
```

4. 毎日朝9時にSSIDを有効にするコマンドを実行します。

```
[WX1840X] scheduler schedule start_radio
[WX1840X-schedule-stop_radio] job radio_enable
[WX1840X-schedule-stop_radio] time repeating at 09:00
[WX1840X-schedule-stop_radio] quit
```

Q5 無線の電波を送受信できる時間帯を制御することができますか。

解決策

公共の施設などで、電力節約とセキュリティ強化のために夜間の時間帯には電波を出さないようにするためには、GUIではできませんので、CLIコマンドで行う必要があります。

仮定

無線を出す時間帯を、朝9時から夜17時まで制限するものとした例を以下に示します。

手順

1. 無線インタフェースを無効にするコマンドをスケジュールjobとして定義します。

```
[WX1840X] scheduler job radio_disable
[WX1840X-job-radio_disable] command 1 system-view
[WX1840X-job-radio_disable] command 2 wlan ap-group default-group
[WX1840X-job-radio_disable] command 3 ap-model WA6638-JP
[WX1840X-job-radio_disable] command 4 radio 1
[WX1840X-job-radio_disable] command 5 radio disable
[WX1840X-job-radio_disable] command 6 radio 2
[WX1840X-job-radio_disable] command 7 radio disable
[WX1840X-job-radio_disable] command 8 radio 3
[WX1840X-job-radio_disable] command 9 radio disable
#(オプション)以下はAPのLEDを消灯させるコマンドです
[WX1840X-job-radio_disable] command 10 led-mode quiet
[WX1840X-job-radio_disable] quit
```

2. 毎日夜17時に無線インタフェースを無効にするコマンドを実行します。

```
[WX1840X] scheduler schedule stop_radio
[WX1840X-schedule-stop_radio] job radio_disable
[WX1840X-schedule-stop_radio] time repeating at 17:00
[WX1840X-schedule-stop_radio] quit
```

3. 無線インタフェースを有効にするコマンドをスケジュールjobとして定義します。

```
[WX1840X] scheduler job radio_enable
[WX1840X-job-radio_enable] command 1 system-view
[WX1840X-job-radio_enable] command 2 wlan ap-group default-group
[WX1840X-job-radio_enable] command 3 ap-model WA6638-JP
[WX1840X-job-radio_enable] command 4 radio 1
[WX1840X-job-radio_enable] command 5 radio enable
[WX1840X-job-radio_enable] command 6 radio 2
[WX1840X-job-radio_enable] command 7 radio enable
```

```
[WX1840X-job-radio_enable] command 8 radio 3
[WX1840X-job-radio_enable] command 9 radio enable
#(オプション)以下はAPのLEDを通常点灯させるコマンドです
[WX1840X-job-radio_enable] command 10 led-mode normal
[WX1840X-job-radio_enable] quit
```

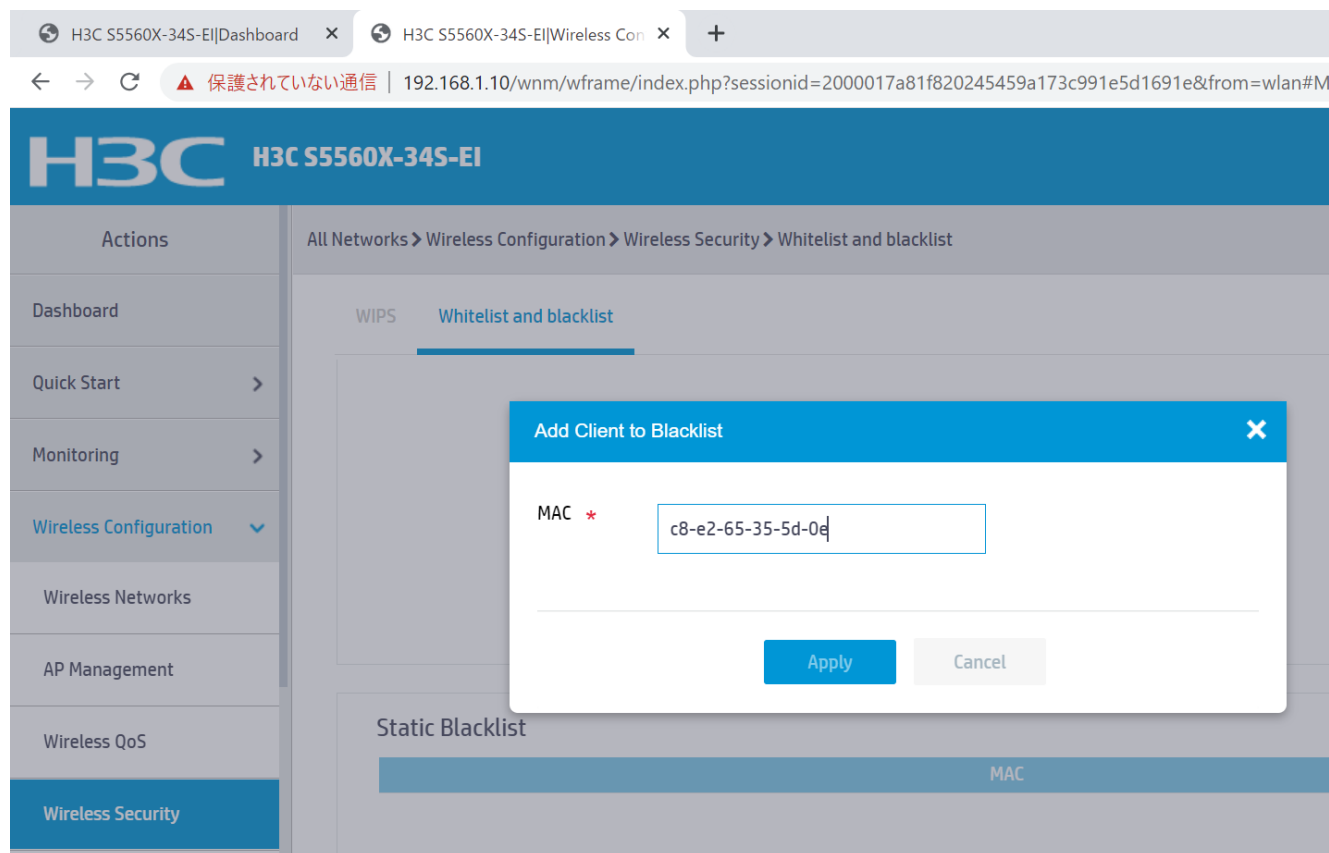
4. 毎日朝9時に無線インタフェースを有効にするコマンドを実行します。

```
[WX1840X] scheduler schedule start_radio
[WX1840X-schedule-stop_radio] job radio_enable
[WX1840X-schedule-stop_radio] time repeating at 09:00
[WX1840X-schedule-stop_radio] quit
```

Q6 特定のユーザーのPCのWiFiのMACアドレスを指定してアクセスを拒否するように設定する方法は？

解決策

以下のように、APのAll Networks > Wireless Configuration > Wireless Security > Whitelist and blacklistで拒否したいWiFiのMACアドレスを指定します。



コマンドでは以下のようになります：

```
[AC] wlan whitelist mac-address c8e2-6535-5d0e  
[AC] wlan static-blacklist mac-address c8e2-6535-3344
```

ちなみに、この例ではPCのWiFiのMACアドレスは以下のようになっております。

Wireless LAN adapter Wi-Fi:

```
接続固有の DNS サフィックス . . . . . :  
説明 . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz  
物理アドレス . . . . . : C8-E2-65-35-5D-0E
```


1. ホワイトリストを検索します。
 - クライアントの MAC アドレスがホワイトリストのどのエントリとも一致しない場合、クライアントは拒否されます。
 - 一致する場合、クライアントは許可されます。
2. **ホワイトリストエントリが存在しない場合は、静的および動的ブラックリストを検索します。**
 - クライアントの MAC アドレスがいずれかのブラックリストのエントリと一致する場合、クライアントは拒否されます。
 - **一致するものがない場合、またはブラックリストエントリが存在しない場合、クライアントは許可されます。**

ACで設定された静的ブラックリストとホワイトリストは、ACに接続されているすべてのAPIに適用され、動的ブラックリストは、攻撃パケットを受信したAPIに適用されます。