

AireOS のある ISE ワイヤレス CWA とホットスポット フローおよび次世代 WLC を設定する

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[統合 5508 WLC の設定](#)

[グローバル設定](#)

[ゲストのサービス セット 識別子 \(SSID \) の設定 :](#)

[リダイレクト ACL の設定](#)

[HTTPS リダイレクト](#)

[アグレッシブ フェールオーバー](#)

[キャプティブ バイパス](#)

[コンバージド 3850 NGWC の設定](#)

[グローバル設定](#)

[SSID 設定](#)

[リダイレクト ACL 設定](#)

[コマンドライン インターフェイス \(CLI \) 設定](#)

[ISE の設定](#)

[一般的な ISE 設定タスク](#)

[使用例1 : すべてのユーザ接続でゲスト認証を使用するCWA](#)

[使用例2 : デバイス登録を使用したCWAが1日1回ゲスト認証を実施する。](#)

[使用例3:HostSpotポータル](#)

[確認](#)

[使用例 1](#)

[使用例 2](#)

[使用例 3](#)

[AireOS での FlexConnect ローカル スイッチング](#)

[外部/アンカー シナリオ](#)

[トラブルシューティング](#)

[AireOS と コンバージド アクセス WLC の両方での一般的な障害状態](#)

[AireOS WLC](#)

[NGWC](#)

[ISE](#)

[関連情報](#)

概要

このドキュメントでは、Cisco AireOSと次世代ワイヤレスLANコントローラ(NGWC)を使用してIdentity Services Engine(ISE)に3つのゲストケースを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Wireless LAN Controller (統合およびコンバインド アクセス)
- Identity Services Engine (ISE)

使用するコンポーネント

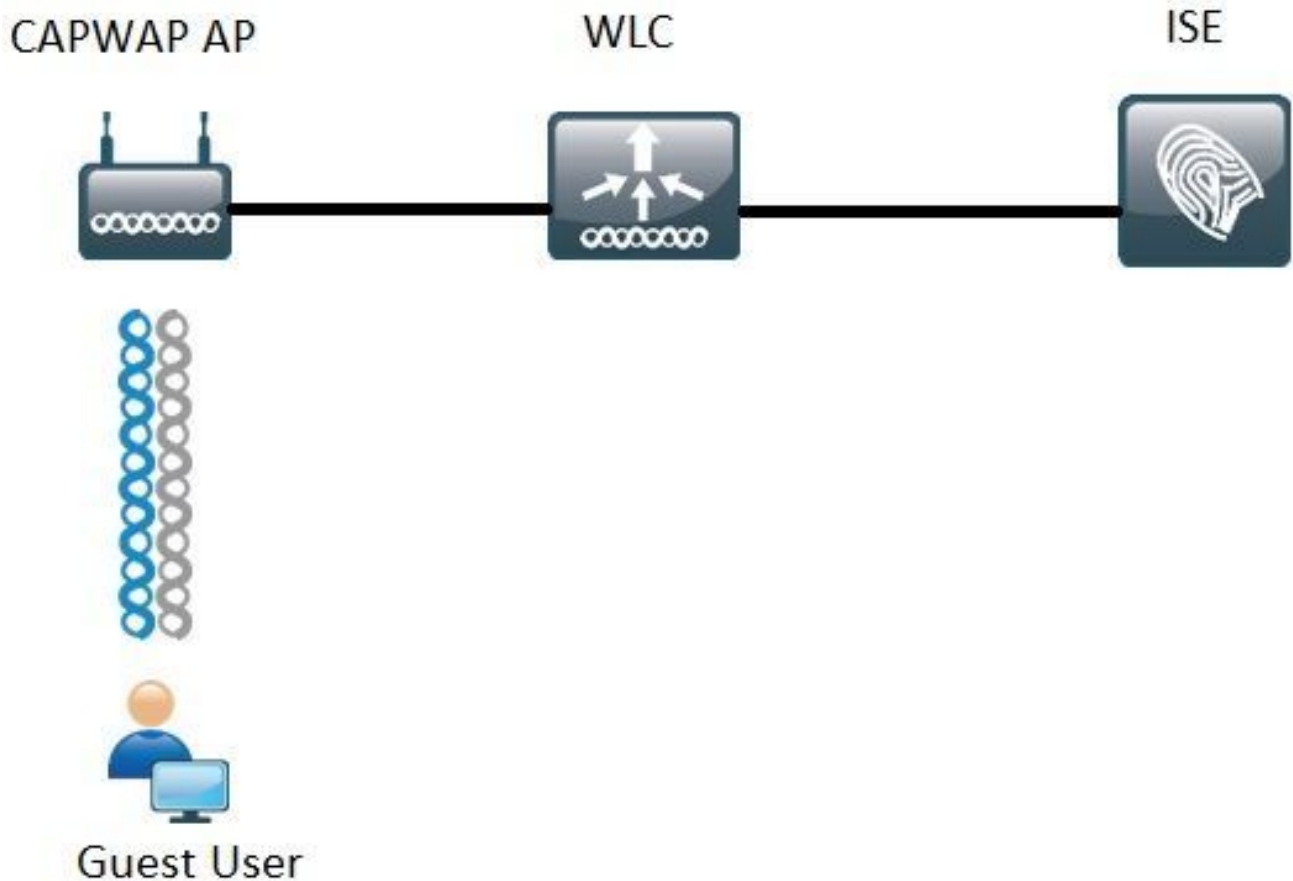
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine バージョン 2.1
- Cisco Wireless LAN Controller 5508 8.0.121.0
- Next Generation Wireless Controller(NGWC)catalyst 3850(WS-C3850-24P)(03.06.04.E)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



このドキュメントで説明している手順は、ISE で任意のゲスト フローをサポートするための、統合 WLC とコンバージド アクセス WLC の両方での一般的な設定を示しています。

統合 5508 WLC の設定

ISE で設定される使用例に関係なく、WLC の観点から、最初は、認証およびアカウントिंगサーバとして ISE を指し示し、MAC フィルタリングが有効になっている Open SSID (と AAA オーバーライドおよび RADIUS NAC) に接続するワイヤレス エンドポイントを設定します。これにより、ISE のゲスト ポータルへのリダイレクトを正常に実行するために、ISE が WLC に必要な属性をダイナミックにプッシュできるようになります。

グローバル設定

1. ISEを認証およびアカウントिंगサーバとしてグローバルに追加します。
 - [Security] > [AAA] > [Authentication] の順に選択し、[New] をクリックします。



- ISE サーバの IP と共有秘密を入力します。
- [Server Status] と [Support for RFC 3676] (認可変更 (CoA) のサポート) がどちらも [Enabled] に設定されていることを確認します。
- デフォルトのサーバタイムアウトでは、AireOS WLCは2秒です。ネットワークの特性 (異なる場所での遅延、ISE、およびWLC) に応じて、サーバのタイムアウトを少なくとも5秒に増やして、不要なフェールオーバーイベントを回避することが有益な場合があります。
- [Apply] をクリックします。
- 設定するポリシー サービス ノード (PSN) が複数ある場合は、追加のサーバ エントリを作成します。

注：この特定の設定例には、2つのISEインスタンスが含まれています

- [Security] > [AAA] > [RADIUS] > [Accounting] の順に選択し、[New] をクリックします。
- ISE サーバの IP と共有秘密を入力します。
- [Server Status] が [Enabled] に設定されていることを確認します。
- 必要に応じて、サーバ タイムアウトを増やします (デフォルトは 2 秒) 。

2.フォールバック設定。

統合環境では、サーバ タイムアウトがトリガーされると、WLC は次の設定済みのサーバに移動します。ここで、「次」は、WLAN の順番です。他に使用できるものがない場合、WLC はグローバル サーバリスト内の次のものを選択します。SSID (プライマリ、セカンダリ) で複数のサーバが設定されている場合、フェールオーバーが発生すると、WLCはデフォルトで、プライマリサーバがオンラインに戻っていても、認証 (または) アカウンティングトラフィックをセカンダリインスタンスに永続的に送信し続けます。

この動作を軽減するには、フォールバックを有効にします。[Security] > [AAA] > [RADIUS] > [Fallback] の順に選択します。デフォルトの動作はオフです。サーバ ダウン イベントから回復する唯一の方法では、管理者による操作 (サーバの管理ステータスをグローバルにバウンスする) が必要です。

フォールバックの有効化には、次の 2 つのオプションがあります。

- [Passive] : パッシブ モードでは、サーバが WLC 認証要求に応答しない場合、WLC はサーバ

を非アクティブ キューに移して、タイマーを設定します ([Interval in Sec] オプション)。タイマーが期限切れになると、WLC は、サーバの実際ステータスに関係なく、サーバをアクティブ キューに移します。認証要求がタイムアウトする (つまり、サーバがまだダウンしている) と、サーバ エントリは再び非アクティブ キューに移され、タイマーが再び設定されます。サーバが正常に応答すると、サーバはアクティブ キューに入れられたままになります。ここで設定できる値の範囲は 180 ~ 3600 秒です。

- **[Active]** : アクティブ モードでは、サーバが WLC 認証要求に応答しない場合、WLC はサーバをデッドとしてマークし、非アクティブ サーバ プールにサーバを移して、そのサーバが応答するまでの定期的なプローブ メッセージの送信を開始します。サーバが応答すると、WLC はデッド サーバをアクティブ プールに移して、プローブ メッセージの送信を停止します。このモードでは、WLC により、ユーザ名と秒単位のプローブ間隔 (180 ~ 3600) の入力を求められます。

注:WLCプローブでは、認証の成功は必要ありません。成功した認証と失敗した認証のどちらも、サーバをアクティブ キューに移すために十分なサーバの応答とみなされます。

ゲストのサービス セット識別子 (SSID) の設定 :

- [WLANs] タブに移動し、[Create New] オプションの下の [Go] をクリックします。



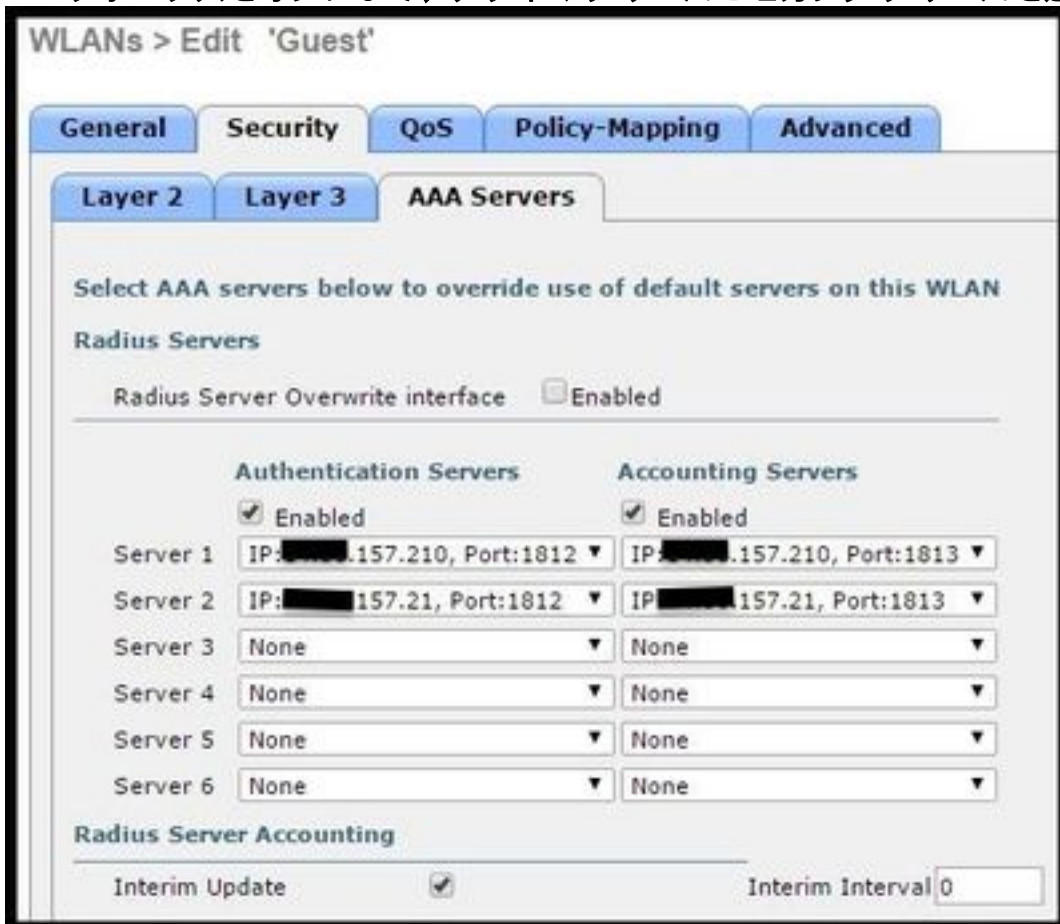
- プロファイル名と SSID 名を入力します。[Apply] をクリックします。
- [General] タブで、使用するインターフェイスまたはインターフェイス グループ (ゲスト VLAN) を選択します。



- [Security] > [Layer 2] > [Layer 2 Security] の順に選択し、[None] を選択して、[Mac Filtering] チェックボックスをオンにします。



- [AAA Servers] タブで、[Authentication Servers] と [Accounting Servers] の [Enabled] チェックボックスをオンにして、プライマリ サーバとセカンダリ サーバを選択します。



- 暫定アップデート：これはオプションの設定であり、このフローにメリットを追加するものではありません。これを有効にするには、WLCで8.x以降のコードを実行する必要があります

Disabled：この機能は完全に無効になっています。

0間隔で有効：クライアントのMobile Station Control Block(MSCB)エントリに変更があるたびに、WLCはISEにアカウントिंगアップデートを送信します(IPv4またはIPv6アドレスの割り当てまたは変更、クライアントローミングイベント) 追加の定期的なアップデートは送信されません

設定された暫定インターバルで有効：このモードでは、WLCはクライアントのMSCBエントリの変更時にISEに通知を送信し、また設定されたインターバルで（変更に関係なく）追加の定期的なアカウント通知を送信します。

- [Advanced] タブで、[Allow AAA Override] をオンにして、[NAC state] の下の [RADIUS NAC] を選択します。これにより、WLC は、ISE から取得したすべての属性値ペア (AVP) を適用します。
- [SSID general] タブに移動し、SSID ステータスの [Enabled] チェックボックスをオンにします。

WLANs > Edit 'Guest'

The screenshot shows the configuration page for a WLAN named 'Guest'. The 'Advanced' tab is selected. The configuration includes:

- Profile Name: Guest
- Type: WLAN
- SSID: Guest
- Status: Enabled

- [Apply] をクリックして変更を適用します。

リダイレクト ACL の設定

このACLはISEによって参照され、どのトラフィックがリダイレクトされ、どのトラフィックが通過を許可されるかを決定します。

- [Security] タブ > [Access Control Lists] の順に選択し、[New] をクリックします。
- 次の図は ACL の例です。

The screenshot shows the configuration page for an Access Control List named 'Guest_Redirect'. The 'General' tab is selected. The configuration includes:

- Access List Name: Guest_Redirect
- Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

このACLは、TCPポート8443を介したDNSサービスおよびISEノードとの間のアクセスを許可する必要があります。一番下は暗黙の deny になっています。これは、他のトラフィックが ISE のゲスト ポータル URL にリダイレクトされることを意味します。

HTTPS リダイレクト

この機能は AireOS 8.0.x 以降でサポートされていますが、デフォルトではオフになっています。HTTPS サポートを有効にするには、[WLC Management] > [HTTP-HTTPS] > [HTTPS Redirection] の順に選択して [Enabled] に設定するか、CLI で次のコマンドを適用します。

```
(Cisco Controller) >config network web-auth https-redirect enable
```

HTTPS リダイレクトを有効にした後の証明書の警告

https-redirectを有効にすると、リダイレクト中に証明書信頼の問題が発生する可能性があります。この問題は、コントローラに有効なチェーン証明書がある場合でも、またこの証明書がサードパーティの信頼できる認証局によって署名されている場合でも発生します。その原因は、WLC にインストールされている証明書が仮想インターフェイスのホスト名または IP アドレスに対して発行されることにあります。クライアントが<https://cisco.com>を試行すると、ブラウザは cisco.com に証明書が発行されることを想定します。しかし、WLC がクライアントによって発行された GET を代行受信するには、まず、WLC が、SSL ハンドシェイク フェーズで仮想インターフェイス証明書を提示する HTTPS セッションを確立する必要があります。これにより、SSL ハンドシェイク中に提示された証明書が、クライアントがアクセスしようとしている元の Web サイト (WLC の仮想インターフェイスホスト名ではなく cisco.com) に発行されていないため、ブラウザに警告が表示されます。異なるブラウザで異なる証明書エラーメッセージが表示される場合がありますが、すべて同じ問題に関連しています。

アグレッシブ フェールオーバー

この機能は、AireOS WLC ではデフォルトで有効になっています。アグレッシブ フェールオーバーが有効になっている場合、あるクライアントが RADIUS タイムアウト イベントの影響を受けると、WLC は AAA サーバを応答不能としてマークし、それを次の設定済み AAA サーバに移します。

この機能が無効になっている場合は、少なくとも 3 つのクライアント セッションで RADIUS タイムアウト イベントが発生したときのみ、WLC が次のサーバにフェールオーバーします。この機能は、次のコマンドで無効にできます (このコマンドではリブートは必要ありません)。

```
(Cisco Controller) >config radius aggressive-failover disable
```

この機能の現在のステータスを確認するには、次のコマンドを使用します。

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

キャプティブ バイパス

キャプティブ ポータルを検出してログオン ページを自動起動するキャプティブ ネットワーク アシスタント (CNA) メカニズムをサポートしているエンドポイントは、通常、制御されたウィンドウ内の擬似ブラウザによってこれを実行しますが、他のエンドポイントは、完全機能のブラウザを起動して、これをトリガーします。CNA が擬似ブラウザを起動するエンドポイントの場合、フローが中断される可能性があります ISE キャプティブポータルにリダイレクトされます。これは通常、Apple iOS デバイスに影響し、特にデバイス登録、VLAN DHCP リリース、コンプライアンスチェックを必要とするフローに悪影響を与えます。

使用中のフローの複雑さに応じて、キャプティブバイパスを有効にすることを推奨できます。このようなシナリオでは、WLC は CNA ポータルの検出メカニズムを無視し、クライアントはリダイレクトプロセスを開始するためにブラウザを開く必要があります。

次のコマンドで、この機能のステータスを確認します。

```
(Cisco Controlller) >show network summary

Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

この機能を有効にするには、次のコマンドを入力します。

```
(Cisco Controlller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
```

You must reset system for this setting to take effect.

WLC は、変更を有効にするためにリセット システム (再起動) が必要であることをユーザに警告します。

この時点では、show network summary コマンドにより機能が有効になっていることが示されますが、変更を有効にするには WLC を再起動する必要があります。

コンバージド 3850 NGWC の設定

グローバル設定

1. ISEを認証およびアカウントिंगサーバとしてグローバルに追加する

- [Configuration] > [Security] > [RADIUS] > [Servers] の順に選択し、[New] をクリックします。
- 環境条件を反映した ISE サーバの IP アドレス、共有秘密、サーバ タイムアウト、および再試行回数を入力します。
- [Support for RFC 3570] (CoA のサポート) が [Enabled] になっていることを確認します。
- この手順を繰り返してセカンダリ サーバ エントリを追加します。

RADIUS Servers

Radius Servers > **New**

Server Name

Server IP Address

Shared Secret

Confirm Shared Secret

Auth Port (0-65535)

Acct Port (0-65535)

Server Timeout (1-1000)secs

Retry Count (0-100)

Support for RFC 3576 ▾

2. ISEのサーバグループの作成

- [Configuration] > [Security] > [Server Groups] の順に選択し、[New] をクリックします。
- グループに名前を割り当て、[Dead-time] の値を分単位で入力します。これは、コントローラがサーバをアクティブサーバのリストに移す前に非アクティブキューで保持する時間です。
- [Available Servers] リストのサーバを [Assigned Servers] 欄に追加します。

Radius Server Group

Radius Server Group > **New**

Name

MAC-delimiter ▾

MAC-filtering ▾

Dead-time (0-1440) in minutes

Group Type

Servers In This Group

Available Servers	Assigned Servers
<input type="text"/>	ISE2 ISE1

3. Dot1xをグローバルに有効にする

- [Configuration] > [AAA] > [Method Lists] > [General] の順に選択し、[Dot1x system Auth Control] をオンにします。

General

Dot1x System Auth Control

Local Authentication

Local Authorization

4. 方式リストの設定

- [Configuration] > [AAA] > [Method Lists] > [Authentication] の順に選択し、新しいメソッドリストを作成します。この使用例の場合は、タイプを Dot1x とし、ISE_Group グループ (前の手順で作成したグループ) を追加して、[Apply] をクリックします。

Authentication
Authentication > New

Method List Name:

Type: dot1x login

Group Type: group local

Fallback to local:

Groups In This Method:

Available Server Groups:

Assigned Server Groups:

- アカウンティング ([Configuration] > [AAA] > [Method Lists] > [accounting]) と認可 ([Configuration] > [AAA] > [Method Lists] > [Authorization]) について、同じ手順を実行します。次のように表示されるはずです

Accounting
Accounting > New

Method List Name:

Type: dot1x exec identity network commands

Groups In This Method:

Available Server Groups:

Assigned Server Groups:

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

Available Server Groups:

Assigned Server Groups:

Groups In This Method:

5. 許可MACフィルタメソッドを作成します。

これは、後で、SSID 設定から呼び出されます。

- [Configuration] > [AAA] > [Method Lists] > [Authorization] の順に選択し、[New] をクリックします。
- ドメイン リスト名を入力します。[Type] で [network]、[Group Type] で [group] を選択します。
- ISE_Group を [Assigned Server Groups] フィールドに追加します。

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

Available Server Groups:

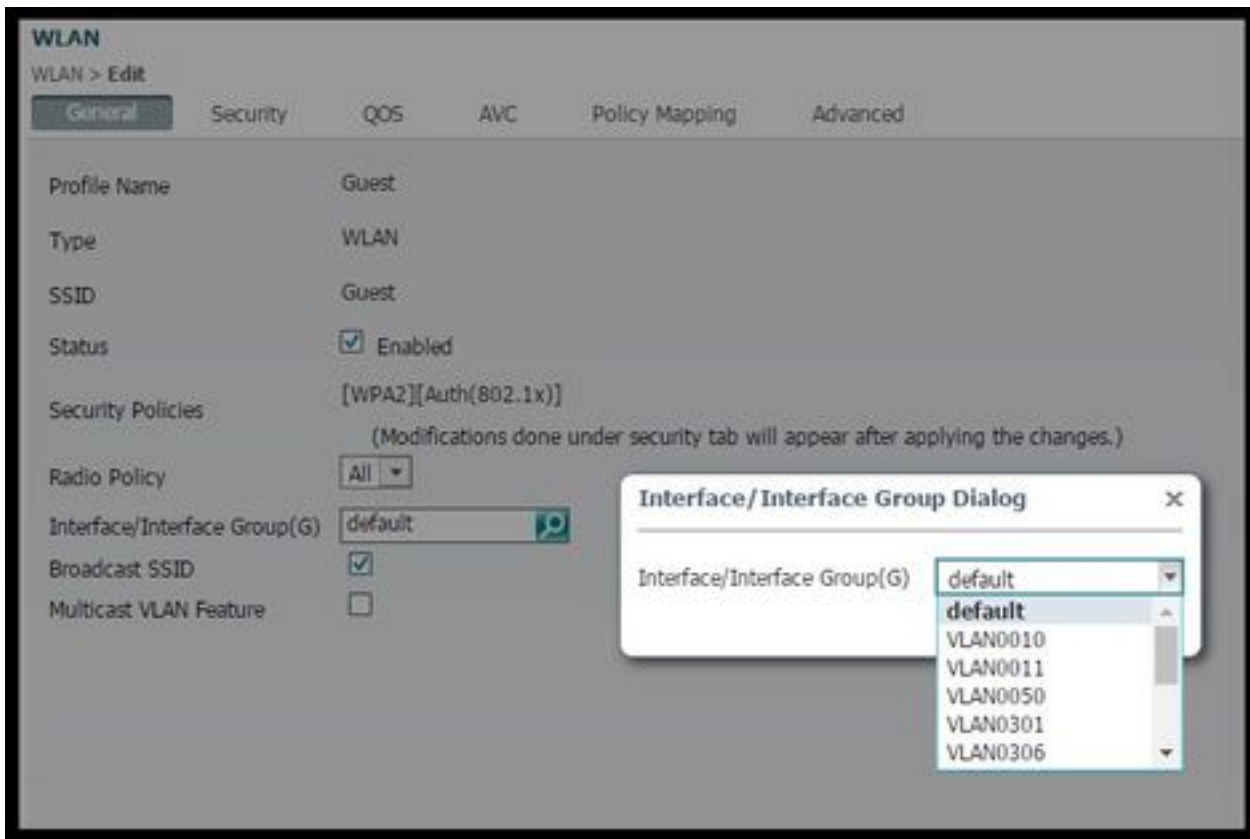
Assigned Server Groups:

Groups In This Method:

SSID 設定

1. ゲストSSIDの作成

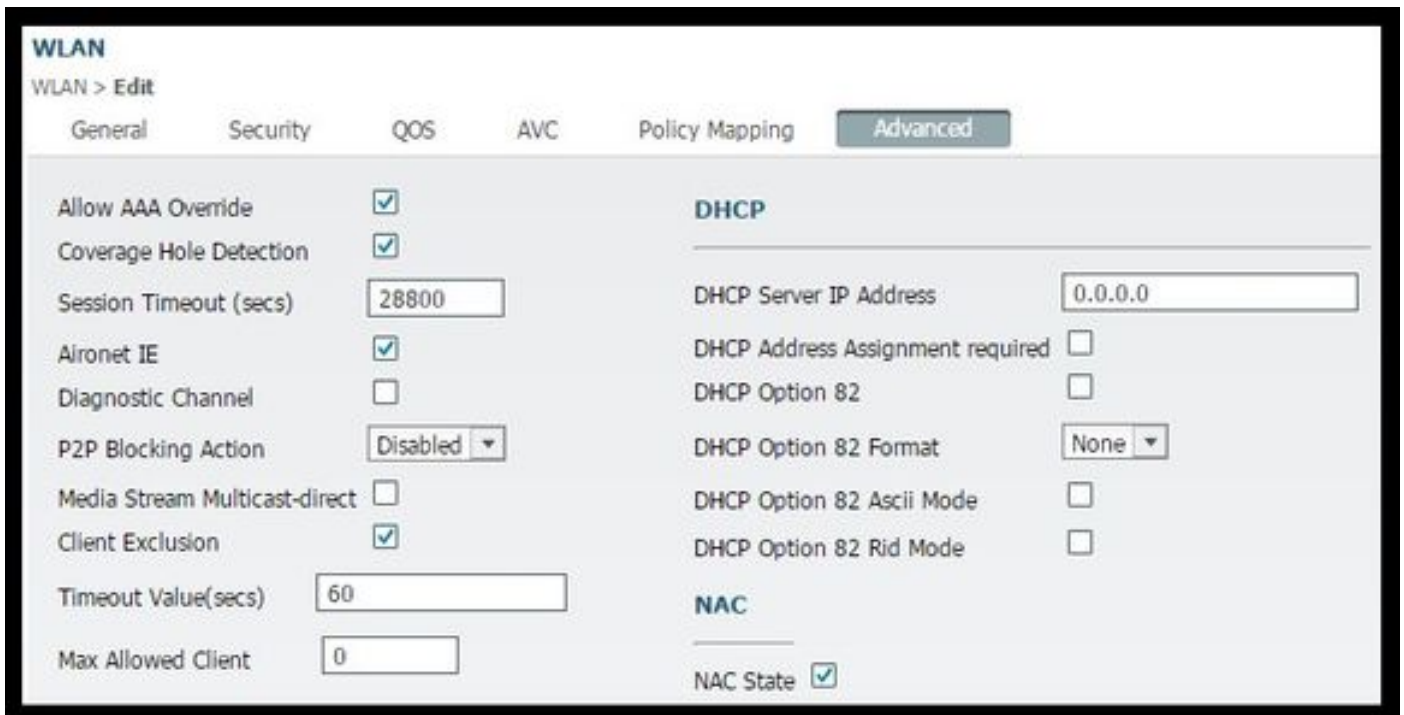
- [Configuration] > [Wireless] > [WLANs] の順に選択し、[New] をクリックします。
- WLAN ID、SSID、およびプロファイル名を入力し、[Apply] をクリックします。
- [Interface/Interface Group] の SSID 設定で、ゲスト VLAN レイヤ 3 インターフェイスを選択します。



- [Security] > [Layer 2] の順に選択し、[None] を選択して、[Mac Filtering] の横に、前に設定した MAC フィルタ メソッド リスト名 (MacFilterMethod) を入力します。
- [Security] > [AAA Server] タブの順に選択し、適切な認証メソッドリスト (ISE_Method) と アカウンティング メソッド リスト (ISE_Method) を選択します。



- [Advanced] タブで、[Allow AAA Override] と [NAC state] をオンにします。残りの設定は、各導入要件 (セッションタイムアウト、クライアント除外、Aironet拡張機能のサポート) に従って調整する必要があります。



- [General] タブに移動し、[Status] を [Enabled] に設定します。[Apply] をクリックします。

リダイレクト ACL 設定

この ACL は、後で ISE によって、初期 MAB 要求に応答してアクセスを承認するときに参照されます。NGWCは、これを使用して、リダイレクトするトラフィックと許可する必要があるトラフィックを決定します。

- [configuration] > [security] > [ACL] > [Access Control Lists] の順に選択し、[Add New] をクリックします。
- [Extended] を選択し、ACL 名を入力します。
- 次の図は、一般的なリダイレクト ACL の例を示しています。

Access Control Lists
ACLs > ACL detail

Details :

Name: Guest_Redirect
Type: IPv4 Extended

Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
10	deny	icmp	any	any	-	-
20	deny	udp	any	any	-	eq 67
30	deny	udp	any	any	-	eq 68
40	deny	udp	any	any	-	eq 53
50	deny	tcp	any	157.210	-	eq 8443
60	deny	tcp	any	157.21	-	eq 8443
70	permit	tcp	any	any	-	eq 80
80	permit	tcp	any	any	-	eq 443

注:10行目はオプションです。これは、通常、トラブルシューティングのために追加されま

す。このACLは、DHCPおよびDNSサービスへのアクセスと、ISEサーバポートTCP 8443 (ACEの拒否) へのアクセスを許可する必要があります。HTTPトラフィックとHTTPSトラフィックはリダイレクトされます (許可 ACE)。

コマンドライン インターフェイス (CLI) 設定

前の手順で説明したすべての設定は、CLI を使用して適用することもできます。

802.1x のグローバルな有効化

```
dot1x system-auth-control
```

グローバル AAA 設定

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
!
aaa group server radius ISE_Group
  server name ISE2
  server name ISE1
  deadtime 10
  mac-delimiter colon
!
```

WLAN 設定

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
no security wpa
```

```
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

リダイレクト ACL の例

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
 10 deny icmp any any
 20 deny udp any any eq bootps
 30 deny udp any any eq bootpc
 40 deny udp any any eq domain
 50 deny tcp any host 172.16.157.210 eq 8443
 60 deny tcp any host 172.16.157.21 eq 8443
 70 permit tcp any any eq www
 80 permit tcp any any eq 443
```

HTTP と HTTPS のサポート

```
3850#show run | inc http
ip http server
ip http secure-server
```

注:HTTP経由でWLCへのアクセスを制限するためにACLを適用すると、リダイレクションに影響します。

ISE の設定

ここでは、このドキュメントに示されているすべての使用例をサポートするために必要な ISE の設定について説明します。

一般的な ISE 設定タスク

1. ISE にログインし、[Administration] > [Network Resources] > [Network Devices] の順に選択して、[Add] をクリックします。
2. WLC に関連付けられた名前と WLC の IP アドレスを入力します。
3. [RADIUS Authentication Settings] チェックボックスをオンにして、WLC 側で設定されている共有秘密を入力します。次に、[Submit] をクリックします。

Network Devices List > Cisco_5508

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

4. [Policy] > [Authentication] に移動し、[MAB] で[Edit] をクリックし、[Use: Internal Endpoints] で[If user is not found] オプションが[Continue] に設定されていることを確認します (デフォルトで設定されている必要があります)。

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based

MAB : If Wired_MAB OR Wireless_MAB Allow Protocols: Default Network Access and

Default : Use

Internal Endpoints

Identity Source

Options

If authentication failed

If user not found

If process failed

Note: For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

Dot1X : If Wireless_802.1X Allow Protocols: Default Network Access

使用例1：すべてのユーザ接続でゲスト認証を使用するCWA

フローの概要

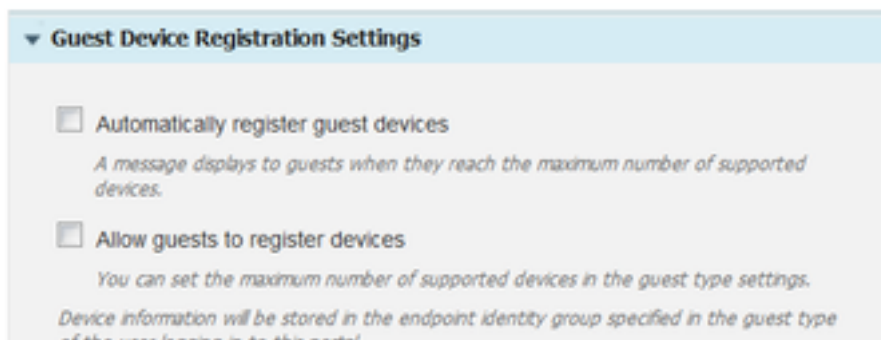
1. ワイヤレス ユーザはゲスト SSID に接続します。

2. WLCは、AAAサーバとしてISE上のMACアドレスに基づいてエンドポイントを認証します。
3. ISEは、url-redirectおよびurl-redirect-aclの2つの属性値ペア(AVP)を使用して戻り、access-acceptを返します。WLCがこのAVPをエンドポイントセッションに適用すると、端末はDHCP-Requiredに移行し、IPアドレスを取得するとCENTRAL_WEB_AUTHにとどまります。この手順では、WLCは、クライアントのHTTP/HTTPSトラフィックのリダイレクトを開始する準備ができています。
4. エンドユーザがWebブラウザを開き、HTTPまたはHTTPSトラフィックが生成されると、WLCはユーザをISEゲストポータルにリダイレクトします。
5. ユーザがゲストポータルに移動すると、ゲストクレデンシャル(この使用例の場合はスポンサーが作成)の入力を求められます。
6. ISEはクレデンシャルの検証時にAUPページを表示し、クライアントが承認すると、ダイナミックCoAタイプのRe-authenticateがWLCに送信されます。
7. WLCは、モバイル端末に認証解除を発行せずに、MACフィルタリング認証を再処理します。これは、エンドポイントに対してシームレスである必要があります。
8. 再認証イベントが発生すると、ISEは認可ポリシーを再評価し、以前に成功したゲスト認証イベントがあったため、今回はエンドポイントにアクセス許可が与えられます。

このプロセスは、ユーザがSSIDに接続するたびに繰り返されます。

コンフィギュレーション

1. ISEに移動し、[Work Centers] > [Guest Access] > [Configure] > [Guest Portals]の順に選択して、[Sponsored Guest Portal]を選択(または新しいポータルタイプのスポンサー承認型ゲストを作成)します。
2. [Guest Device Registration Settings]で、すべてのオプションをオフにして、[Save]をクリックします。



3. [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles]に移動します。
。[Add]をクリックします。

4.このプロファイルは、最初のMac認証バイパス(MAB)要求への応答として、Redirect-URLおよびRedirect-URL-ACLをWLCにプッシュされます。

- [Web Redirection (CWA, MDM, NSP, CPP)] チェックボックスをオンにして、[Centralized Web Auth]を選択したら、[ACL]フィールドにリダイレクトACL名を入力し、[Value]から[Sponsored Guest Portal (default)](または以前の手順で作成した他の特定のポータル)を選択します。

プロファイルは、次の図に示すように表示される必要があります。次に[Save]をクリックします。
。

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

 Web Redirection (CWA, MDM, NSP, CPP) ⓘ

 ACL

 Value
 Display Certificates Renewal Message

 Static IP/Host name/FQDN

ページの下部にある [Attribute Details] には、WLC にプッシュされる属性値ペア (AVP) が表示されます。

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-ac=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
```

5. [Policy] > [Authorization] に移動し、新しいルールを挿入します。このルールは、WLCからの初期MAC認証要求に応答してリダイレクトプロセスをトリガーします(この場合は **Wireless_Guest_Redirect**と呼ばれます)。

6. [Conditions] で[Select Existing Condition from Library] を選択し、[condition name] で [Compound condition] を選択します。「**Wireless_MAB**」という定義済みの複合条件を選択します。

注：この条件は、WLCから発信されたアクセス要求で予期される2つのRADIUS属性で構成されます (NAS-Port-Type= IEEE 802.11 <すべてのワイヤレス要求に存在>およびService-Type = Call Check<。これはMAC認証バイパスに対する特定の要求を示します>)。

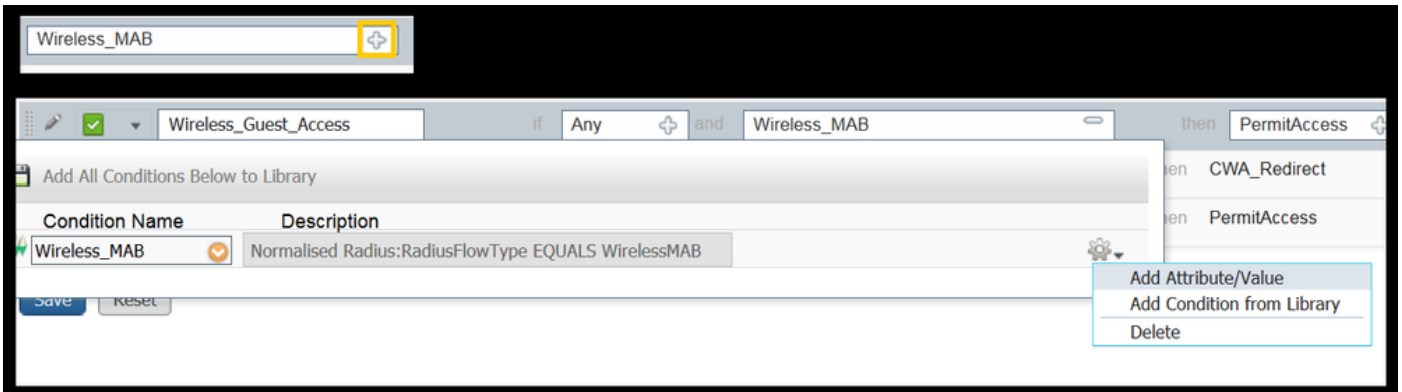
7.結果で、[Standard] > [CWA_Redirect] (前の手順で作成した認可プロファイル) を選択します。次に [Done] をクリックし、[Save] をクリックします。

Wireless_Guest_Redirect if Wireless_MAB then CWA_Redirect Edit

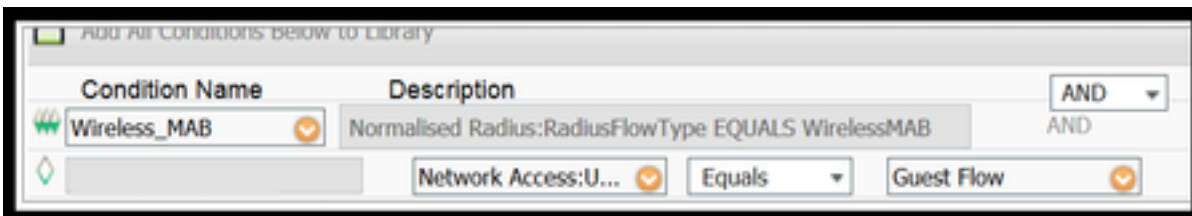
8. **CWA_Redirect**ルールの最後に移動し、[Edit] の横にある矢印をクリックします。次に [duplicate above] を選択します。

9.セッションがISEのCoA (この場合はWireless_Guest_Access) で再認証されると、エンドポイントが照合するポリシーであるため、名前を変更します。

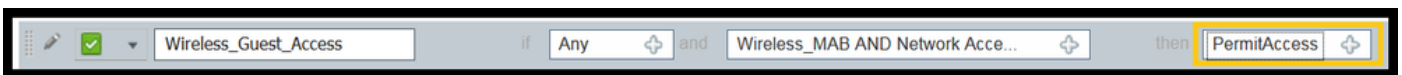
10. [Wireless_MAB] 複合条件の横にある[+] 記号をクリックして条件を展開し、[Wireless_MAB] 条件の最後で[Add Attribute/Value] をクリックします。



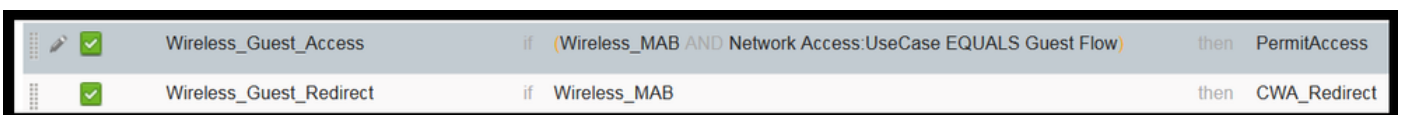
11. [Select Attribute]で、[Network Access] > [UseCase Equals Guest flow] を選択します。



12. [Permissions] で[PermitAccess] を選択します。次に [Done] をクリックし、[Save] をクリックします。



2つのポリシーは次のようになります。



使用例2：デバイス登録を使用したCWAが1日1回ゲスト認証を実施する。

フローの概要

1. ワイヤレス ユーザはゲスト SSID に接続します。
2. WLCは、AAAサーバとしてISE上のMACアドレスに基づいてエンドポイントを認証します。
3. ISE は、2つの属性値ペア (AVP) (url-redirect と url-redirect-acl) とともにアクセス承認を返します。
4. WLCがこのAVPをエンドポイントセッションに適用すると、端末はDHCP-Requiredに移行し、IPアドレスを取得するとCENTRAL_WEB_AUTHにとどまります。この手順では、WLCは、クライアントのHTTP/HTTPSトラフィックのリダイレクトを開始する準備ができています。
5. エンドユーザがWebブラウザを開き、HTTPまたはHTTPSトラフィックが生成されると、WLCはユーザをISEゲストポータルにリダイレクトします。

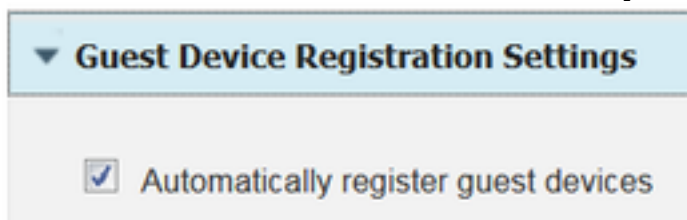
6. ユーザがゲスト ポータルに移動すると、スポンサーが作成したクレデンシャルの入力を求められます。
7. クレデンシャルの検証時に、ISE は、このエンドポイントを特定の (事前設定済みの) エンドポイント アイデンティティ グループ (デバイス登録) に追加します。
8. AUP ページが表示され、クライアントが承認すると、ダイナミック CoA タイプの Re-authenticate が WLC に送信されます。
9. WLC は、モバイル端末に認証解除を発行せずに、MAC フィルタリング認証を再処理します。これは、エンドポイントに対してシームレスである必要があります。
10. 再認証イベントが発生すると、ISE は認可ポリシーを再評価します。今回は、エンドポイントが適切なエンドポイント アイデンティティ グループのメンバーであるため、ISE は制限なしのアクセス承認を返します。
11. エンドポイントは手順 6 で登録されているため、ユーザは、そのユーザが ISE から手動で削除されるか、エンドポイント消去ポリシーによって基準を満たすエンドポイントのフラッシュが実行されるまで、戻るたびにネットワークで許可されます。

このラボのシナリオでは、認証は 1 日に 1 回実行されます。再認証トリガーは、使用されたエンドポイント アイデンティティ グループのすべてのエンドポイントを毎日削除するエンドポイント消去ポリシーです。

注：最後のAUP承認からの経過時間に基づいて、ゲスト認証イベントを適用できます。1日に1回（たとえば4時間ごと）以上の頻度でゲストログオンを強制する必要がある場合は、このオプションを選択できます。

コンフィギュレーション

1. ISE で、[Work Centers] > [Guest Access] > [Configure] > [Guest Portals] の順に選択して、[Sponsored Guest Portal] を選択 (または新しいポータル タイプのスポンサー承認型ゲストを作成) します。
2. [Guest Device Registration Settings] で、[Automatically register guest devices] オプションがオンになっていることを確認します。[Save] をクリックします。



3. [Work center] > [Guest Access] > [Configure] > [Guest Types] に移動するか、ポータルの[Guest Device Registration Settings]で指定されたショートカットをクリックします。

▼ Guest Device Registration Settings

Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers > Guest Access > Configure > Guest Types](#)

4. スポンサーユーザがゲストアカウントを作成すると、そのアカウントにゲストタイプが割り当てられます。個々のゲストタイプには、異なるエンドポイントIDグループに属する登録済みエンドポイントを含めることができます。デバイスを追加する必要があるエンドポイントIDグループを割り当てるには、スポンサーがこれらのゲストユーザに使用するゲストタイプを選択します(この使用例はWeekly (デフォルト) に基づいています)。

5. ゲストタイプにログインしたら、[Login Options] のドロップダウンメニューから[Endpoint Identity group for guest device registration] を選択します

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

6. [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。
。[Add] をクリックします。

7. このプロファイルは、最初のMac認証バイパス(MAB)要求への応答として、Redirect-URLおよびRedirect-URL-ACLをWLCにプッシュされます。

- [Web Redirection (CWA, MDM, NSP, CPP)] チェックボックスをオンにして、[Centralized Web Auth] を選択したら、[ACL] フィールドにリダイレクト ACL 名を入力し、[Value] から、このフロー用に作成したポータル ([CWA_DeviceRegistration]) を選択します。

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Centralized Web Auth ACL Value

8. [Policy] > [Authorization] に移動し、新しいルールを挿入します。このルールは、WLCからの初期MAC認証要求に応答してリダイレクトプロセスをトリガーします(この場合は **Wireless_Guest_Redirect** と呼ばれます)。

9. [Conditions] で [Select Existing Condition from Library] を選択し、[condition name] で [Compound condition] を選択します。「**Wireless_MAB**」という定義済みの複合条件を選択します。

10. [Results] で、[Standard] > [CWA_DeviceRegistration] (前のステップで作成した認可プロファイル) を選択します。次に [Done] をクリックし、[Save] をクリックします。

Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

11. 上記のポリシーを複製し、名前を変更します。これは、再認証イベント (**Wireless_Guest_Access** と呼ばれます) から戻った後にエンドポイントがヒットするポリシーです。

12. [Identity Group Details] ボックスで、[Endpoint Identity Group] を選択し、[Guest Type(GuestEndpoints)]で参照したグループを選択します。

13. [Results] で [PermitAccess] を選択します。[Done] をクリックし、[Save] をクリックして変更内容を保存します。

Wireless_Guest_Access if GuestEndpoints AND Wireless_MAB then PermitAccess
 Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

14. GuestEndpointグループを毎日消去するエンドポイント消去ポリシーを作成します。

- [Administration] > [Identity management] > [Settings] > [Endpoint Purge] の順に選択します。
- [Purge] ルールには、[Elapsed Time]が30日より長い場合にGuestEndpointsの削除をトリガーするルールがデフォルトで存在する必要があります。
- GuestEndpoints の既存のポリシーを変更するか、新しいポリシーを作成します (デフォルトのポリシーが削除されている場合)。消去ポリシーは毎日定義された時間に実行されることに注意してください。


この使用例の場合、条件は、経過日が 1 日未満の GuestEndpoints のメンバーです。

使用例3:HostSpotポータル

フローの概要

1. ワイヤレス ユーザはゲスト SSID に接続します。
2. WLC は、ISE を AAA サーバとして使用し、MAC アドレスに基づいてエンドポイントを確認します。
3. ISEは、url-redirectとurl-redirect-aclの2つの属性値ペア(AVP)を使用してaccess-acceptを返します。
4. WLC がこの AVP をエンドポイント セッションに適用すると、端末は DHCP-Required に移行し、IP アドレスを取得すると CENTRAL_WEB_AUTH にとどまります。この手順では、WLC は、クライアントの HTTP/HTTPS トラフィックをリダイレクトする準備ができています。
5. エンドユーザが Web ブラウザを開き、HTTP または HTTPS トラフィックが生成されると、WLC はユーザを ISE ホットスポット ポータルにリダイレクトします。
6. このポータルで、ユーザは、アクセプタブル ユース ポリシーを受け入れるように求められます。
7. ISE は、エンドポイント MAC アドレス (エンドポイント ID) を設定済みのエンドポイント アイデンティティ グループに追加します。
8. 要求を処理するポリシー サービス ノード (PSN) は、ダイナミック CoA タイプの **Admin-Reset** を WLC に発行します。
9. WLC は、着信 CoA の処理を完了すると、認証解除をクライアントに発行します (クライアントの復帰に要する時間は接続が失われる)。
10. クライアントが再接続すると、新しいセッションが作成されるため、ISE 側ではセッションの継続性はありません。これは、認証が新しいスレッドとして処理されることを意味します。
11. エンドポイントが設定済みのエンドポイント アイデンティティ グループに追加され、エンドポイントがそのグループのメンバーであるかどうかを確認する認証ポリシーが存在するため、新しい認証はこのポリシーに適合します。その結果、ゲスト ネットワークへのフルアクセスが可能になります。
12. エンドポイントの消去ポリシーの結果としてエンドポイントIDオブジェクトがISEデータベースから消去されない限り、ユーザはAUPを再度受け入れる必要はありません。

コンフィギュレーション

1. これらのデバイスを登録時に移すための新しいエンドポイント アイデンティティ グループを作成します。[Work Centers] > [Guest Access] > [Identity Groups] > [Endpoint Identity Groups] に移動し、 Add .
- グループ名を入力します (この使用例の場合は HotSpot_Endpoints)。説明を追加します。親グループは不要です。

Endpoint Identity Group List > HotSpot_Endpoints

Endpoint Identity Group

* Name

Description

Parent Group

2. [Work Centers] > [Guest Access] > [Configure] > [Guest Portals] に移動し、[Hotspot Portal (default)] を選択します。

3. [Portal Settings]を展開し、[Endpoint Identity Group]で[Endpoint Identity Group] の下の [HotSpot_Endpoints] グループを選択します。これにより、登録されたデバイスが指定されたグループに送信されます。

Endpoint

Identity *Configure endpoint identity groups at:*
group: * [Work Centers](#) > [Guest Access](#) > [Identity Groups](#)

4. [Save] をクリックして変更内容を保存します。

5. WLCから発信されたMAB認証時にホットスポットポータルを呼び出す認可プロファイルを作成します。

- [Policy] > [Policy elements] > [Results] > [authorization] > [Authorization Profiles] の順に選択し、**認証プロファイル (HotSpotRedirect)** を作成します。
- [Web redirection (CWA, MDM, NSP, CPP)] **チェックボックスをオンにして**、[Hot Spot] を選択したら、[ACL] フィールドにリダイレクト ACL 名 (Guest_Redirect) を入力し、[Value] から適切なポータル ([Hotspot Portal (default)]) を選択します。

Add New Standard Profile

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Hot Spot: ACL: Value:

Static IP/Host name/FQDN

Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = url-redirect-ad=Guest_Redirect
 cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. WLCからの最初のMAB要求時にHotSpotRedirect結果をトリガーする認可ポリシーを作成します。

- [Policy] > [Authorization] の順に選択し、新しいルールを挿入します。このルールは、WLCからの初期MAC認証要求に応答してリダイレクトプロセスをトリガーします(この場合は **Wireless_HotSpot_Redirect** と呼ばれます)。
- [Conditions] で [Select Existing Condition from Library] を選択し、[condition name] で [Compound condition] を選択します。
- 表示される画面で、[Standard] > [HotSpotRedirect] (以前の手順で作成した認可プロファイル) の順に選択します。次に [Done] をクリックし、[Save] をクリックします。

7. 2番目の認可ポリシーを作成します。

- 上記のポリシーを複製します。これは、再認証イベント (「Wireless_HotSpot_Access」という名前) から戻った後にエンドポイントが照会するポリシーであるため、名前を変更します。
- [Identity Group Details] ボックスで [Endpoint Identity Group] を選択し、以前の手順で作成したグループ (HotSpot_Endpoints) を選択します。
- 表示される画面で、[PermitAccess] を選択します。[Done] をクリックし、[Save] をクリックして変更内容を保存します。

<input checked="" type="checkbox"/>	Wireless_HotSpot_Access	if HotSpot_Endpoints AND Wireless_MAB	then PermitAccess
<input checked="" type="checkbox"/>	Wireless_HotSpot_Redirect	if Wireless_MAB	then HotSpotRedirect

8. [経過時間(Elapsed time)]が5日を超えるエンドポイントをクリアするページポリシーを設定します。

- [Administration] > [Identity Management] > [Settings] > [Endpoint Purge] の順に選択し、[Purge] で新しい消去ポリシーを作成します。
- [Identity Group Details] ボックスで [Endpoint Identity Group] > [HotSpot_Endpoints] の順に選択します。

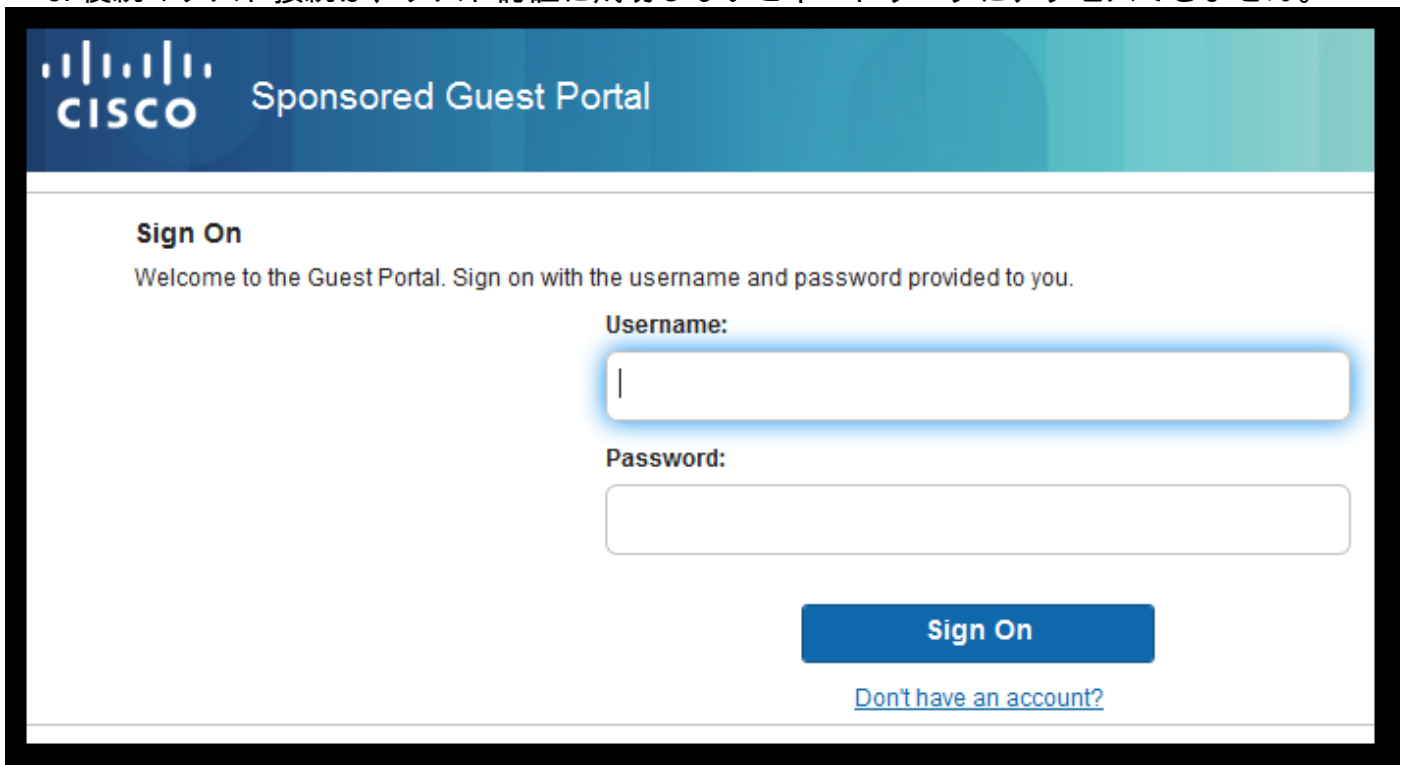
- [conditions] で、[Create New Condition (Advanced Option)] をクリックします。
- [Select Attribute]で、[ENDPOINTPURGE : ElapsedDays GREATER THAN 5 days] を選択します。

HotSpot_Endpoints_PurgeRule if HotSpot_Endpoints AND ENDPOINTPURGE:ElapsedDays GREATER THAN 5

確認

使用例 1

1. ユーザはゲスト SSID に接続します。
2. ユーザがブラウザを開き、HTTP トラフィックが生成されると、すぐにゲスト ポータルが表示されます。
3. ゲスト ユーザが AUP を認証し、承認すると、成功ページが表示されます。
4. Re-authenticate CoA が送信されます (クライアントには透過的)。
5. エンドポイント セッションが再認証され、ネットワークへのフル アクセスが可能になります。
6. 後続のゲスト接続は、ゲスト認証に成功しないとネットワークにアクセスできません。



The screenshot shows a web portal with a blue header containing the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". Below the password field is a blue "Sign On" button and a link that says "Don't have an account?".



Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Success

You now have Internet access through this network.

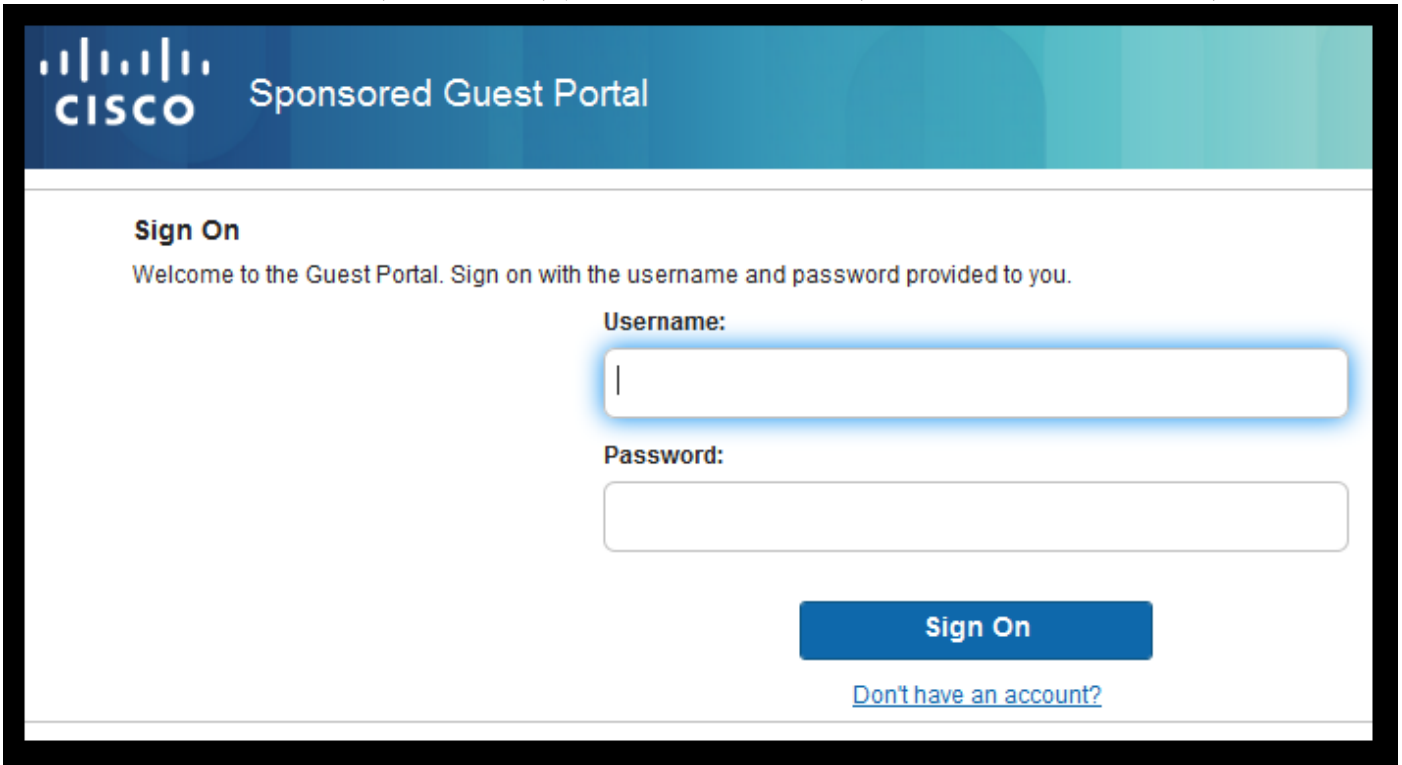
ISE からのフローの RADIUS ライブ ログ :

1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Accounting Start
1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Re-Authentication Event
	68:7F:74:72:18:2E					← CoA Event
1001	68:7F:74:72:18:2E					← Guest Authentication Event
68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	← Initial MAB request

使用例 2

1. ユーザはゲスト SSID に接続します。
2. ユーザがブラウザを開き、HTTP トラフィックが生成されると、すぐにゲスト ポータルが表示されます。

3. ゲスト ユーザが AUP を認証し、承認すると、デバイスが登録されます。
4. 成功ページが表示され、Re-authenticate CoA が送信されます (クライアントには透過的)。
5. エンドポイント セッションが再認証され、ネットワークへのフル アクセスが可能になります。
6. 後続のゲスト接続は、エンドポイントが設定済みのエンドポイント アイデンティティ グループのメンバーであり続ける限り、ゲスト認証を実施することなく許可されます。



The image shows a screenshot of the Cisco Sponsored Guest Portal. At the top left, there is the Cisco logo and the text "Sponsored Guest Portal". Below this, the heading "Sign On" is displayed. A welcome message reads: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". The "Username:" field is currently empty and has a blue highlight. Below the "Password:" field is a blue "Sign On" button. At the bottom right, there is a link that says "Don't have an account?".



Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

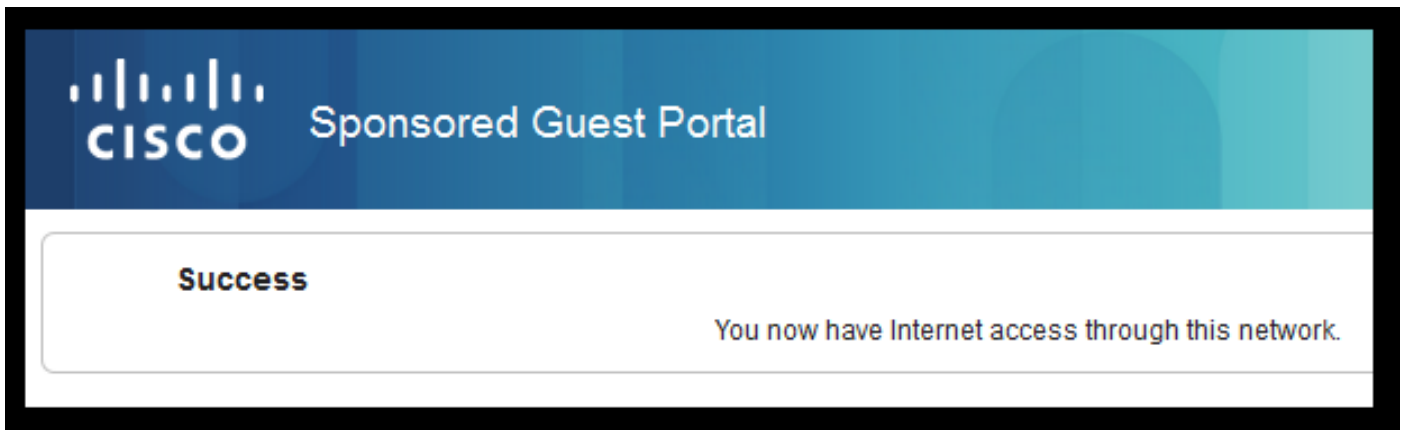


Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue



ISE からのフローの RADIUS ライブ ログ :

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
●		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	
✓		68.7F:74.72:1...	68.7F:74.72:...	PermitAccess	GuestEndpoints
✓		hfr592	68.7F:74.72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
✓			68.7F:74.72:...		
✓		hfr592	68.7F:74.72:...		GuestType_Contractor (default)
✓		68.7F:74.72:1...	68.7F:74.72:...	CWA_DeviceRegistration	Profiled

Accounting Start
Subsequent MAB request(no redirect to guest portal)
Re-Authentication Event
CoA Reauth Event
Guest Authentication and Device Registration
Initial MAB request

使用例 3

1. ユーザはゲスト SSID に接続します。
2. ユーザがブラウザを開き、HTTP トラフィックが生成されると、すぐに AUP ページが表示されます。
3. ゲスト ユーザが AUP を承認すると、デバイスが登録されます。
4. 成功ページが表示され、Admin-Reset CoA が送信されます (クライアントには透過的)。
5. エンドポイントがネットワークに再接続し、フルアクセスが可能になります。
6. 後続のゲスト接続は、エンドポイントが設定済みのエンドポイントアイデンティティグループのメンバーであり続ける限り、AUP 承認を実施することなく許可されます (設定内容が異なる場合)。



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



Connection Successful

You have successfully connected to the network.

AireOS での FlexConnect ローカル スイッチング

FlexConnect ローカル スイッチングが設定されている場合、ネットワーク管理者は次のことを確認する必要があります。

- リダイレクト ACL が FlexConnect ACL として設定されてる。
- AP 自体で [FlexConnect] タブ > [External WebAuthentication ACLs] > [Policies] の順に選択し、リダイレクト ACL を選択して [Apply] をクリックするか、

All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 301 **VLAN Mappings**

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

External WebAuthentication ACLs

Local Split ACLs

Central DHCP Processing

Layer2 ACLs

Policies

Policy ACL CWA_Redirect ▾

Add

Policy Access Control Lists

CWA_Redirect ▾

FlexConnect グループが属する ポリシー ACL を追加する ([Wireless] > [FlexConnect Groups] の順に選択し、目的のグループを選択して、[ACL Mapping] > [Policies] の順に選択し、リダイレクト ACL を選択して [Add] をクリックする) ことにより、リダイレクト ACL が適用されている。

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

Policies

Policy ACL CWA_Redirect ▾

Add

Policy Access Control Lists

CWA_Redirect ▾

TOR_Redirect ▾

ポリシー ACL を追加すると、WLC が、設定済みの ACL を FlexConnect グループの AP メンバープッシュします。これを実行しないと、Web リダイレクトに関する問題が発生します。

外部/アンカー シナリオ

自動アンカー (外部アンカー) シナリオでは、次の点を強調することが重要です。

- リダイレクト ACL は、外部 WLC とアンカー WLC の両方で定義する必要があります (アンカーでのみ実施される場合でも) 。
- レイヤ 2 認証は、常に、外部 WLC によって処理されます。ISE と 外部 WLC の間ですべての RADIUS 認証およびアカウントिंगトラフィックが発生するため、これは設計フェーズで (トラブルシューティング用にも) 非常に重要になります。
- リダイレクト AVP がクライアント セッションに適用されると、外部 WLC は、モビリティ ハンドオフ メッセージにより、アンカーでのクライアント セッションを更新します。
- この時点で、アンカー WLC は、事前設定されたリダイレクト-ACL を使用してリダイレクトを実施しはじめます。
- アンカーと外部の両方からISE (同じ認証イベントを参照) に対するアカウントिंग更新を回避するには、アンカーWLC SSIDでアカウントिंगを完全にオフにする必要があります。
- URL ベースの ACL は、外部/アンカー シナリオではサポートされません。

トラブルシューティング

AireOS と コンバージド アクセス WLC の両方での一般的な障害状態

1. クライアントがゲスト SSID に参加できない

`show client detailed xx:xx:xx:xx:xx:xx`は、クライアントがSTARTでスタックしていることを示します。通常、これはAAAサーバから返される属性をWLCが適用できないことを示すインジケータです。

ISE によってプッシュされるリダイレクト ACL 名が、WLC で事前定義されている ACL の名前と正確に一致することを確認してください。

ISEがWLCにプッシュするように設定されているその他の属性 (VLAN ID、インターフェイス名、Airespace-ACL) にも同じ原則が適用されます。その後、クライアントはDHCP、次にCENTRAL_WEB_AUTHに移行する必要があります。

2. リダイレクト AVP はクライアントのセッションに適用されているが、リダイレクトが機能しない

クライアントのポリシーマネージャの状態がCENTRAL_WEB_AUTHであり、有効なIPアドレスがSSID用に設定されたダイナミックインターフェイスにアラインされていること、およびリダイレクトACL属性とURLリダイレクト属性がクライアントのセッションに適用されていることを確認します。

リダイレクト ACL

AireOS WLCでは、リダイレクトACLは、リダイレクトしてはならないトラフィックを明示的に許可する必要があります。たとえば、DNSやISEはTCPポート8443で双方向に許可され、暗黙のdeny ip any anyは残りのトラフィックがリダイレクトされるトリガーとなります。

コンバージド アクセスでは、ロジックが逆になります。拒否 ACE によってリダイレクトがバイ

パスされ、許可 ACE によってリダイレクトがトリガーされます。このため、TCP ポート 80 および 443 を明示的に許可することをお勧めします。

ポート 8443 を介したゲスト VLAN から ISE へのアクセスを確認します。設定の観点からはすべてが適切であると思われる場合、作業を進展させるための最も簡単な方法は、クライアントのワイヤレスアダプタの背後でキャプチャを取得し、リダイレクトがどこで破綻しているかを確認することです。

- DNS 解決は行われますか。
- 要求されたページに対する TCP 3 ウェイ ハンドシェイクは完了していますか。
- クライアントが GET を開始した後に WLC がリダイレクト アクションを返しますか。
- 8443 を介した ISE に対する TCP 3 ウェイ ハンドシェイクは完了していますか。

3. ISE がゲスト フローの最後で VLAN 変更をプッシュした後にクライアントがネットワークにアクセスできない

フローの開始時にクライアントが IP アドレスを取得すると (Pre Redirect 状態)、ゲスト認証の実行後に VLAN 変更がプッシュされた場合 (CoA 再認証の後)、ゲスト フローで DHCP リリース/更新を実施 (ポスチャ エージェントなし) する唯一の方法は、モバイル デバイスでは動作しない Java アプレットを使用するものです。

その結果、VLAN Y の IP アドレスにより VLAN X でクライアントがブラックホール化したままになります。ソリューションを計画する際には、この点を考慮する必要があります。

4. リダイレクト時にゲスト クライアントのブラウザに「HTTP 500 Internal error, Radius session not found」というメッセージが表示される

これは、通常、ISE でセッションが失われた (セッションが終了した) ことを示しています。この問題の最も一般的な原因は、外部/アンカーが導入されたときにアンカー WLC で設定されたアカウントティングです。この問題を解決するには、アンカーでアカウントティングを無効にして、認証とアカウントティングが外部で処理される状態を維持します。

5. ISEのHotSpotポータルでAUPを受け入れた後、クライアントが切断され、切断されたままになるか、別のSSIDに接続されます。

これは、このフロー(CoA Admin Reset)に含まれるDynamic Change of Authorization(CoA)によりWLCがワイヤレスステーションに対して認証解除を発行するため、ホットスポットで発生する可能性があります。大半のワイヤレスエンドポイントは、認証解除が発生した後に問題なくSSIDに戻りますが、場合によっては、クライアントが、認証解除イベントに応答して別の優先SSIDに接続します。元のSSIDを維持するか別の使用可能な(優先)SSIDに接続するかはワイヤレスクライアントに委ねられるため、この問題を回避するためにISEまたはWLCからできることはありません。

この場合、ワイヤレスユーザは手動でホットスポットSSIDに接続する必要があります。

AireOS WLC

```
(Cisco Controller) >debug client
```

debug client により、クライアント ステート マシンの変更に関係する一連のコンポーネントをデバッグするように設定されます。

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

```
Debug Flags Enabled:
```

```
  dhcp packet enabled.  
  dot11 mobile enabled.  
  dot11 state enabled  
  dot1x events enabled.  
  dot1x states enabled.  
  mobility client handoff enabled.  
  pem events enabled.  
  pem state enabled.  
  802.11r event debug enabled.  
  802.11w event debug enabled.  
  CCKM client debug enabled.
```

AAA コンポーネントのデバッグ

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

これは、MABまたはDot1X SSIDを介して接続するユーザの数に応じて、リソースに影響を与える可能性があります。 DEBUG レベルのこれらのコンポーネントは、WLC と ISE 間の AAA トランザクションを記録し、RADIUS パケットを画面に表示します。

これは、ISEが予期された属性を配信できない場合、またはWLCがそれらを正しく処理しない場合に重要です。

Web 認証リダイレクト

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

これは、WLC がリダイレクトを正常にトリガーしていることを確認するために使用できます。次に、デバッグからのリダイレクトの例を示します。

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430  
  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is  
HTTP/1.1 200 OK  
Location:  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-0050
```

NGWC

debug client により、クライアント ステート マシンの変更に関係する一連のコンポーネントをデバッグするように設定されます。

```
3850#debug client mac-address <client MAC>
```

このコンポーネントにより、RADIUS パケット (認証とアカウントリング) が画面に表示されます。これは、ISEが適切なAVPを提供していることを確認し、CoAが正しく送信および処理されていることを確認する必要がある場合に便利です。

```
3850#debug radius
```

これにより、ワイヤレス クライアントが関係するすべての AAA 移行 (認証、認可、およびアカウントリング) が実行されます。これは、WLC が AVP を正しく解析してクライアント セッションに適用することを確認するために重要です。

```
3850#debug aaa wireless all
```

NGWC でリダイレクトに関する問題が発生している可能性がある場合には、これを有効にすることができます。

```
3850#debug epm plugin redirect all
```

```
3850#debug ip http transactions
```

```
3850#debug ip http url
```

ISE

RADIUS ライブ ログ

初期 MAB 要求が ISE で正しく処理されていることと、ISE が予期される属性をプッシュすることを確認します。[Operations] > [RADIUS] > [Live logs] の順に選択し、[Endpoint ID] でクライアント MAC を使用して出力をフィルタリングします。認証イベントを見つけたら、クリックして詳細情報を表示し、承認の一部としてプッシュされた結果を確認します。



Result

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

TCPDump

この機能は、ISE と WLC の間の RADIUS パケット交換を詳細に調べる必要がある場合に使用できます。これにより、WLC側でデバッグを有効にしなくても、ISEが正しい属性をaccess-acceptで送信することを証明できます。TCPDump によるキャプチャを開始するには、[Operations] > [Troubleshoot] > [Diagnostic Tools] > [General Tools] > [TCPDump] の順に選択します。

次に、TCPDump を使用してキャプチャした正しいフローの例を示します。

Source	Destination	Protocol	Length	Info
154.5	157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
157.13	154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
154.5	157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
157.13	154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
157.13	154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
154.5	157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
154.5	157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
157.13	154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

次の図には、初期 MAB 要求 (上記のスクリーンショットの 2 番目のパケット) に応答して送信された AVP が示されています。

RADIUS Protocol

```
Code: Access-Accept (2)
Packet identifier: 0x0 (0)
Length: 401
Authenticator: f1eaaffcfaa240270b885a9ba8ccd06d
[This is a response to a request in frame 1]
[Time from request: 0.214509000 seconds]
Attribute Value Pairs
  AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC
  AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...
  AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...
  AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect
  AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)
    VSA: l=189 t=Cisco-AVPair(1): url-
```

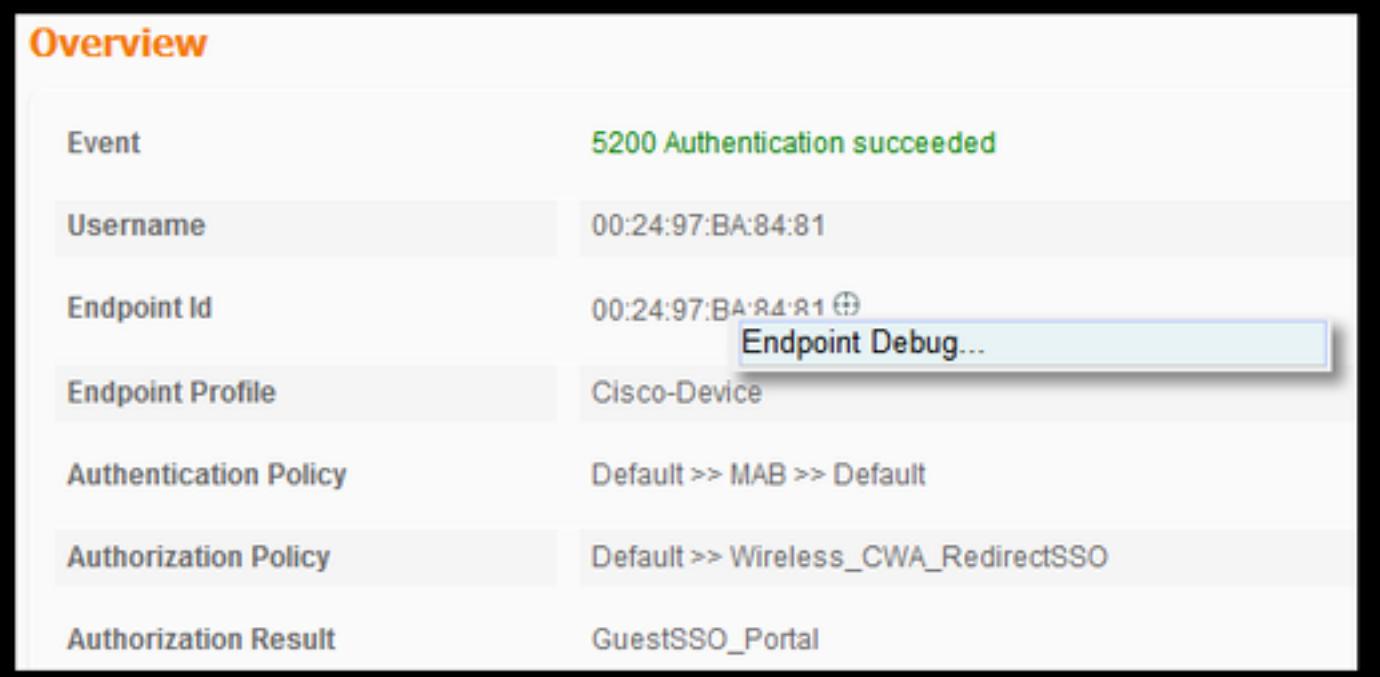
redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a050000aa05565e1c9&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622

AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)

エンドポイント デバッグ

ポリシーの決定、ポータルを選択、ゲスト認証を含むISEプロセスについて詳しく調べる必要がある場合、CoAによる最も簡単な対処方法は、完全なコンポーネントをデバッグレベルに設定する代わりに、**エンドポイントデバッグ**を有効にすることです。

これを有効にするには、[Operations] > [Troubleshooting] > [DiagnosticTools] > [General Tools] > [EndPoint Debug] の順に選択します。

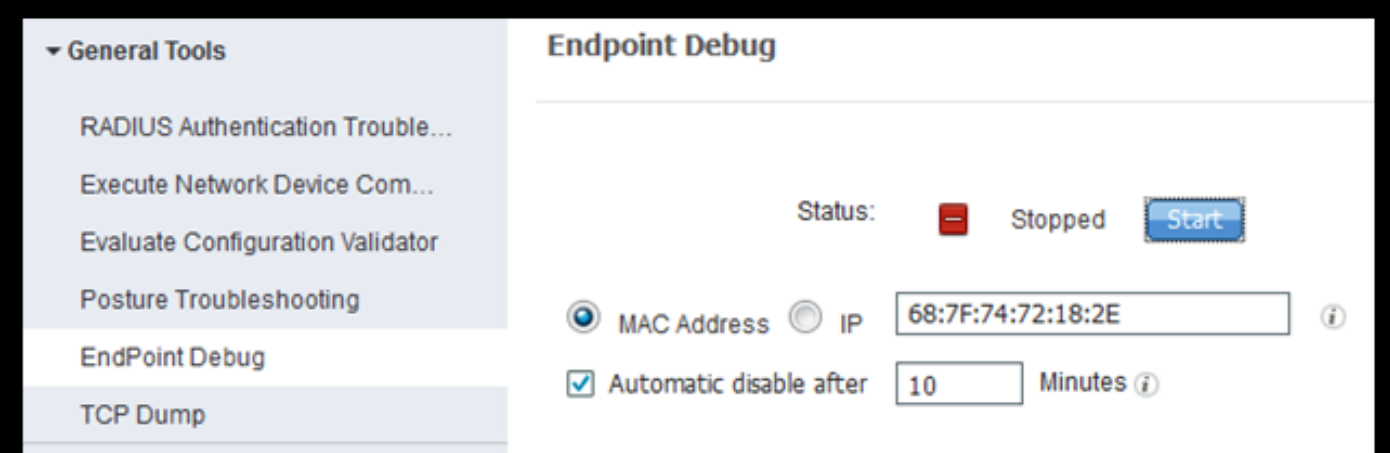


The screenshot shows the 'Overview' page of the ISE GUI. It displays the following information:

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 ⓘ
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

A tooltip labeled 'Endpoint Debug...' is visible over the Endpoint Id field.

[Endpoint Debug] ページで、エンドポイントの MAC アドレスを入力し、問題を再作成する準備が整ったら [Start] をクリックします。





The screenshot shows the 'Endpoint Debug' configuration page. The left sidebar lists 'General Tools' with 'EndPoint Debug' selected. The main area shows the following configuration:


- Status: ■ Stopped Start
- MAC Address IP ⓘ
- Automatic disable after Minutes ⓘ

デバッグが停止したら、エンドポイント ID を識別するリンクをクリックしてデバッグ出力をダウンロードします。

Endpoint Debug

Status:  Processing ...

MAC Address IP 

Automatic disable after Minutes 

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

関連情報

[TAC が推薦する AireOS のビルド](#)

[Cisco Wireless Controller コンフィギュレーションガイド リリース 8.0](#)

[Cisco Identity Services Engine 管理者ガイド リリース 2.1](#)

[Universal NGWC Wireless Configuration with Identity services Engine](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。