一般的なISEゲストアクセス問題のトラブルシューティング

内容

概要

このドキュメントでは、導入における一般的なゲストの問題のトラブルシューティング方法、問題の切り分けと確認方法、および試みる簡単な回避策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。

- ISEゲストの設定
- ネットワークアクセスデバイス(NAD)のCoA設定
- ワークステーション上のキャプチャツールが必要です。

使用するコンポーネント

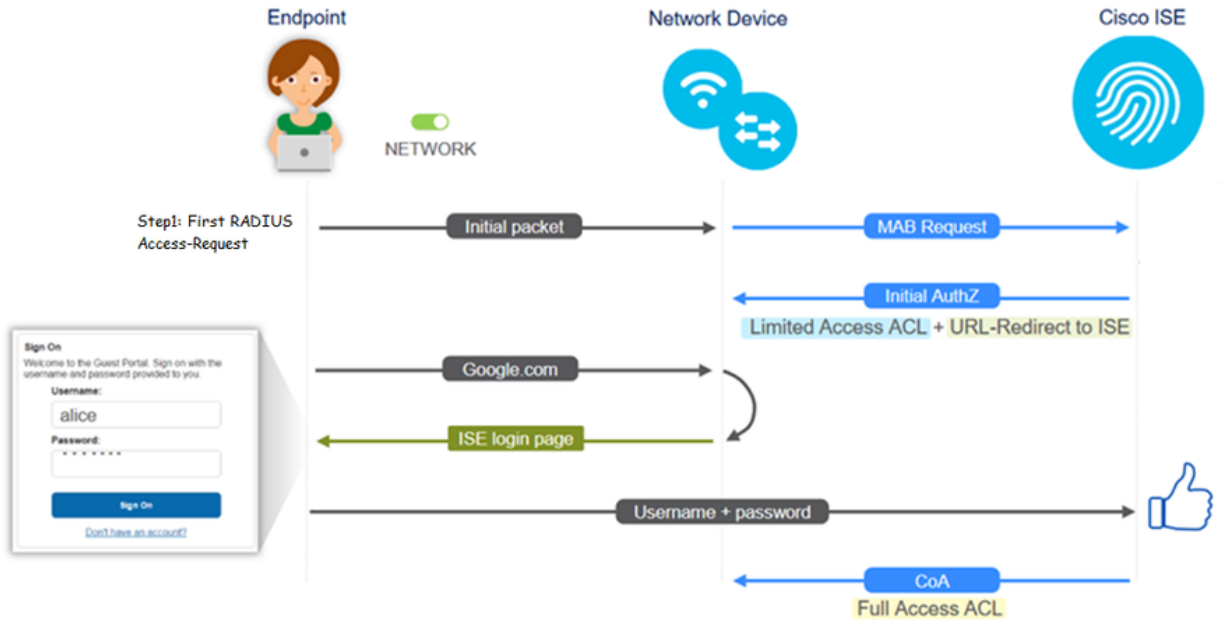
このドキュメントの情報は、次に基づくものです。 Cisco ISEリリース2.6および：

- WLC 5500
- Catalystスイッチ3850 15.xバージョン
- Windows 10ワークステーション

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、クリアな（デフォルト）設定で作業を開始しています。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。

ゲストフロー

ゲストフローの概要は、有線またはワイヤレスの設定と似ています。次の図は、ドキュメント全体を通して参照するために使用できます。ステップとエンティティを視覚化するのに役立ちます。



このフローは、エンドポイントIDをフィルタリングすることで、ISEライブログ[Operations > RADIUS Live Logs]でも追跡できます。

- MAB認証に成功：ユーザ名フィールドにMACアドレスがある：URLがNADにプッシュされる：ユーザがポータルを取得する
- Guest Authentication successful：ユーザ名フィールドにはゲストユーザ名が含まれています。これは、GuestType_Daily（またはゲストユーザ用に設定されたタイプ）として識別されています。
- CoAが開始：ユーザ名フィールドが空白、詳細レポートにDynamic Authorization successfulが表示される
- ゲストアクセスの提供

イメージ内のイベントのシーケンス（下から上）

一般的な導入ガイド

設定に関するサポートへのリンクを次に示します。特定のユースケースのトラブルシューティングを行う場合は、理想的な設定または予期される設定を把握しておくと役立ちます。

- 有線ゲストの設定
- ワイヤレスゲストの設定
- FlexAuth APを使用したワイヤレスゲストCWA

頻繁に発生する問題

このドキュメントでは、主に次の問題について説明します。

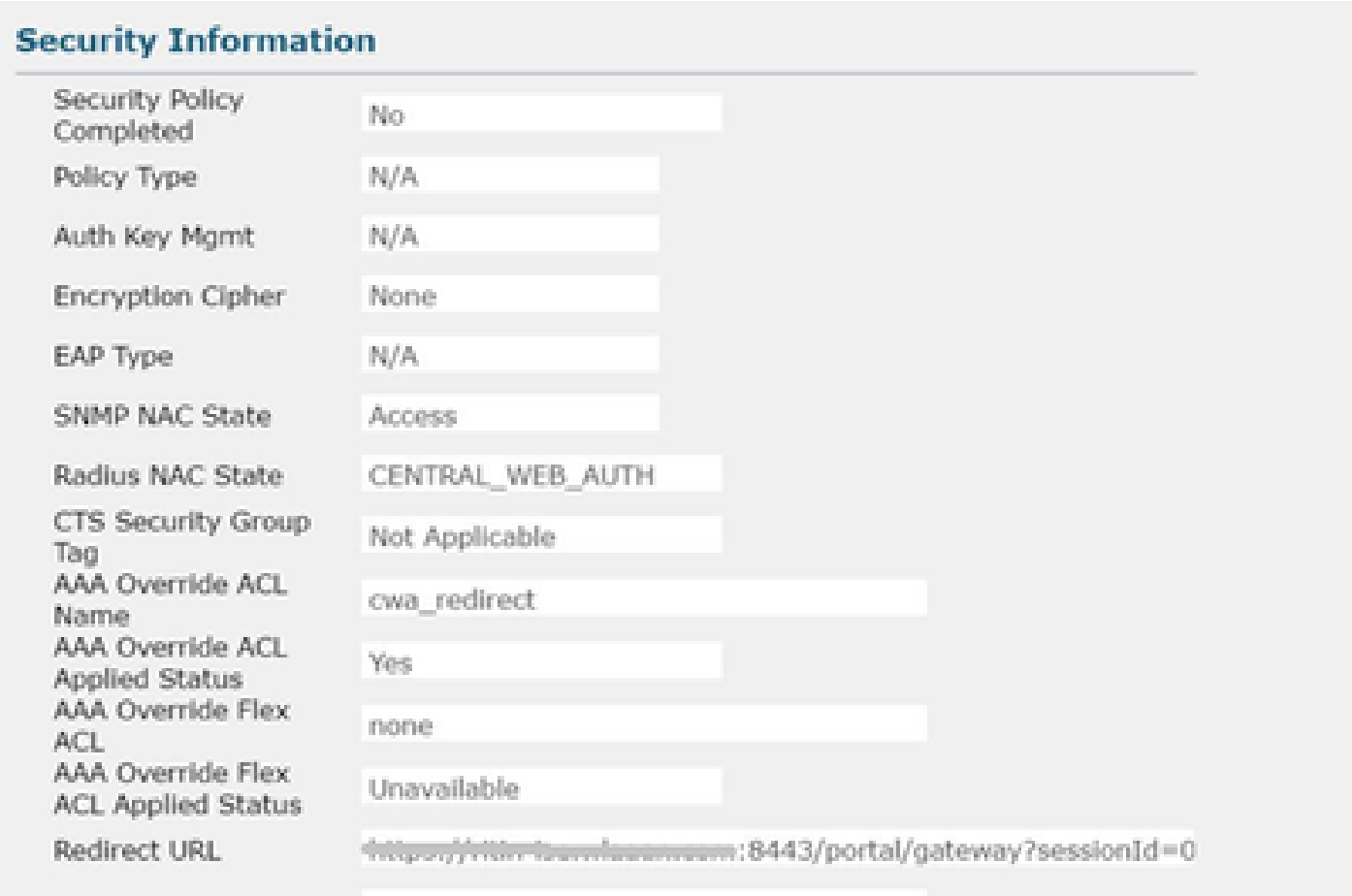
ゲストポータルへのリダイレクトが機能しない

リダイレクトURLとACLがISEからプッシュされたら、次の点を確認します。

1.コマンドshow authentication session int <interface> detailsを使用した、スイッチのクライアントステータス（有線ゲストアクセスの場合）。

```
guestlab#sh auth sess int T1/0/48 de
            Interface:  TenGigabitEthernet1/0/48
              IIF-ID:  0x1096380000001DC
         MAC Address:  b496.9126.dd6d
        IPv6 Address:  Unknown
        IPv4 Address:  10.106.37.18
           User-Name:  B4-96-91-26-DD-6D
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
   Common Session ID:  0A6A25110000012652C64B014
     Acct Session ID:  0x0000124F
              Handle:  0x5E00014D
      Current Policy:  POLICY_Te1/0/48

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:

        URL Redirect:  https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A25110000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
    URL Redirect ACL:  REDIRECT_ACL

Method status list:
      Method           State
      mab              Authc Success
```

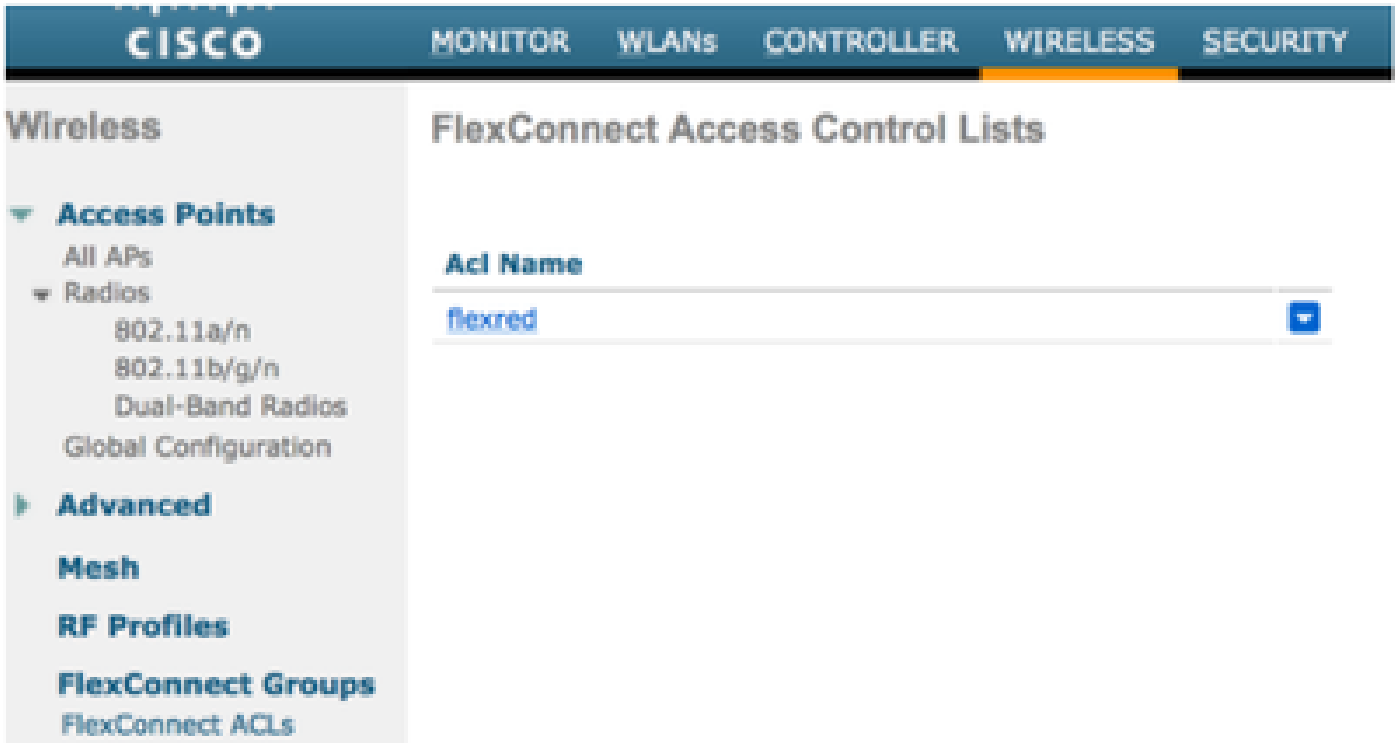
2.ワイヤレスLANコントローラ(WLC)のクライアントステータス（ワイヤレスゲストアクセスの場合）:Monitor > Client > MAC address



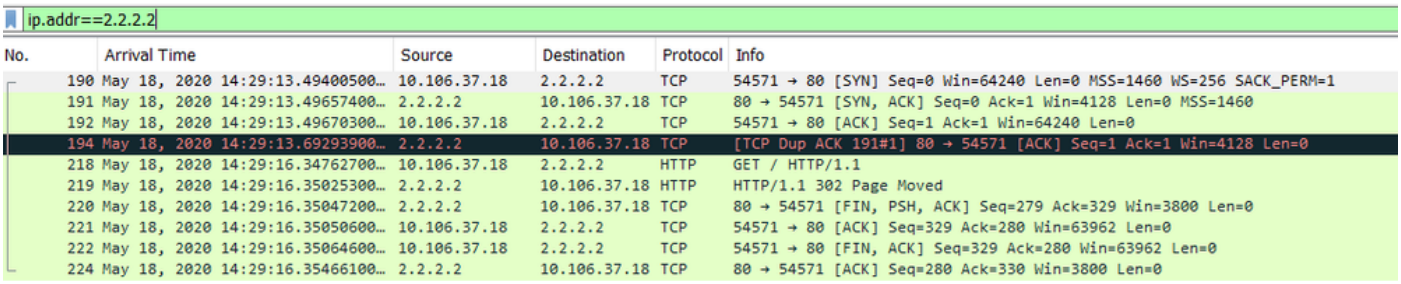
3.コマンドプロンプトを使用した、エンドポイントからTCPポート8443のISEへの到達可能性 ： C:\Users\user>telnet <ISE-IP> 8443

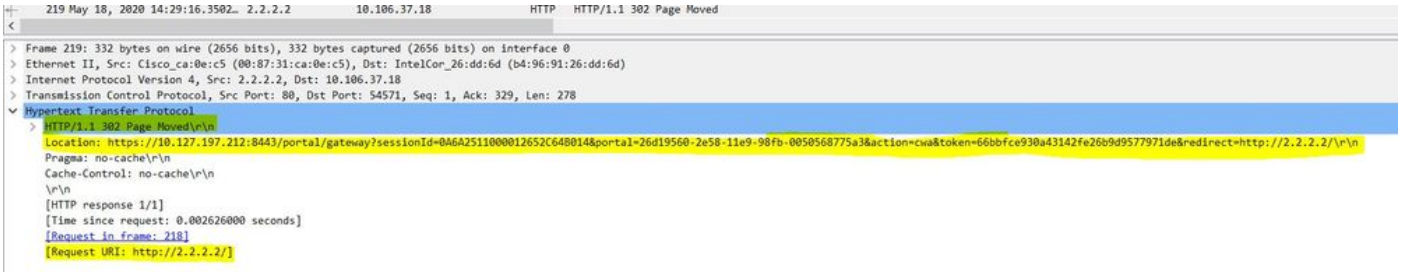
4.ポータルのリダイレクトURLにFQDNがある場合は、クライアントがコマンドプロンプトから解決できるかどうかを確認します。 C:\Users\user>nslookup guest.ise.com

5.フレックス接続の設定で、ACLとフレックスACLに同じACL名が設定されていることを確認します。また、ACLがAPにマッピングされているかどうかも確認します。詳細については、前のセクション「ステップ7 bおよびc」の設定ガイドを参照してください。



6.クライアントからパケットキャプチャを取得し、リダイレクションを確認します。パケット「HTTP/1.1 302 Page Moved」は、アクセスされたサイトをISEゲストポータル（リダイレクトされたURL）にリダイレクトしたWLC/スイッチを示します。





7.ネットワークアクセスデバイスでHTTP(s)エンジンが有効になっている。

スイッチ側：

```
guestlab#sh run | in ip http
ip http server
ip http secure-server
```

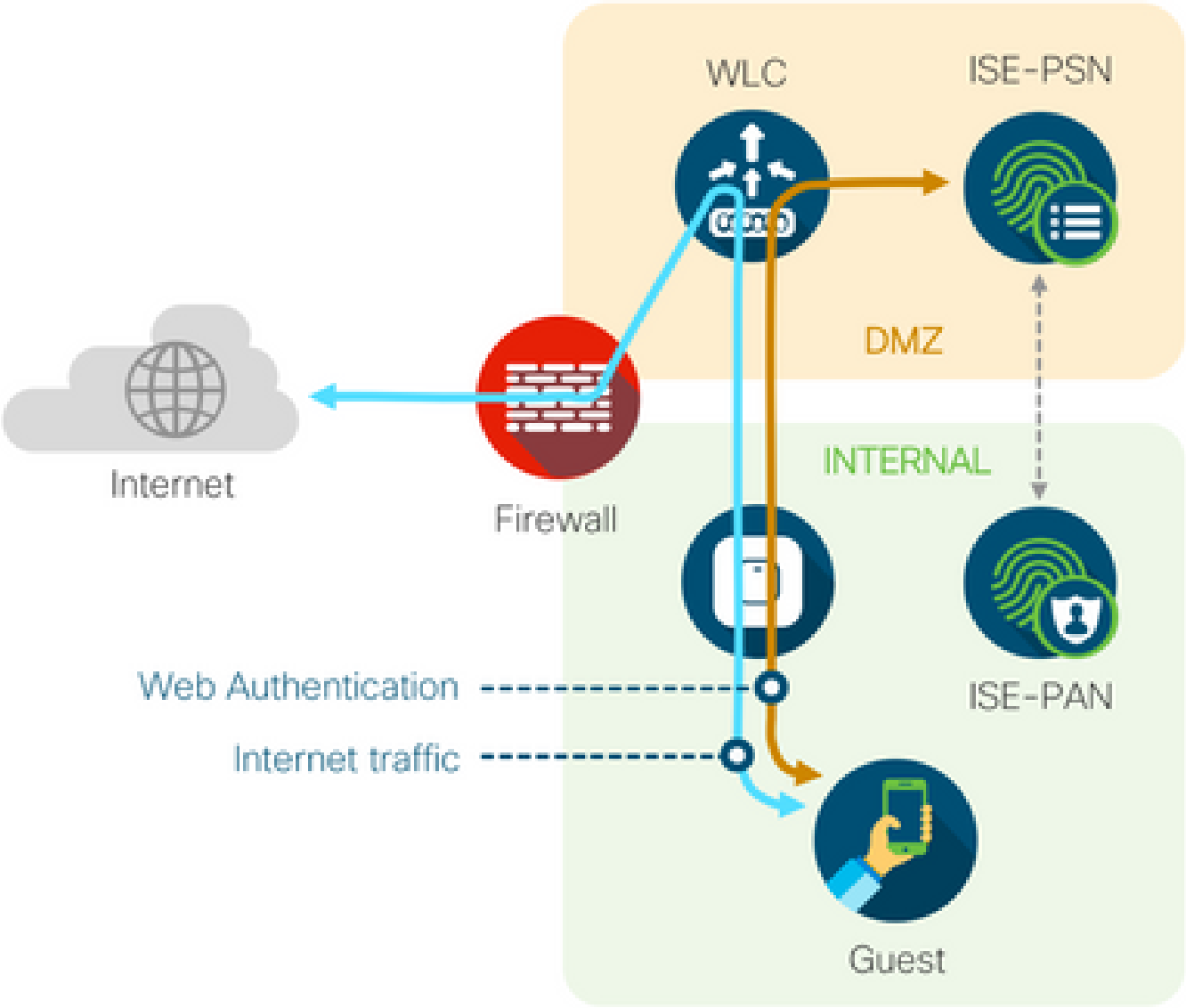
WLC 上：

8. WLCが外部アンカー設定の場合は、次のことを確認します。

ステップ 1：クライアントステータスは、両方のWLCで同じである必要があります。

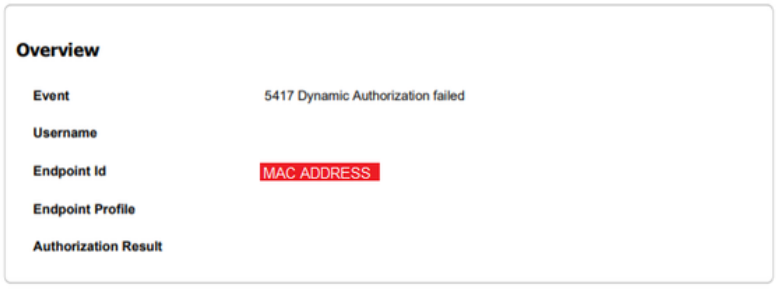
ステップ 2：リダイレクトURLが両方のWLCで表示される必要があります。

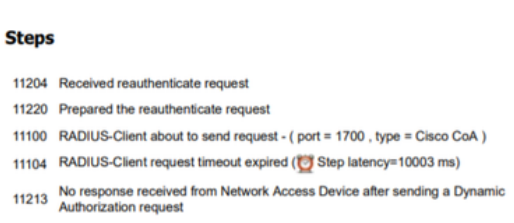
ステップ 3：アンカーWLCでRADIUSアカウンティングを無効にする必要があります。



動的認可の失敗

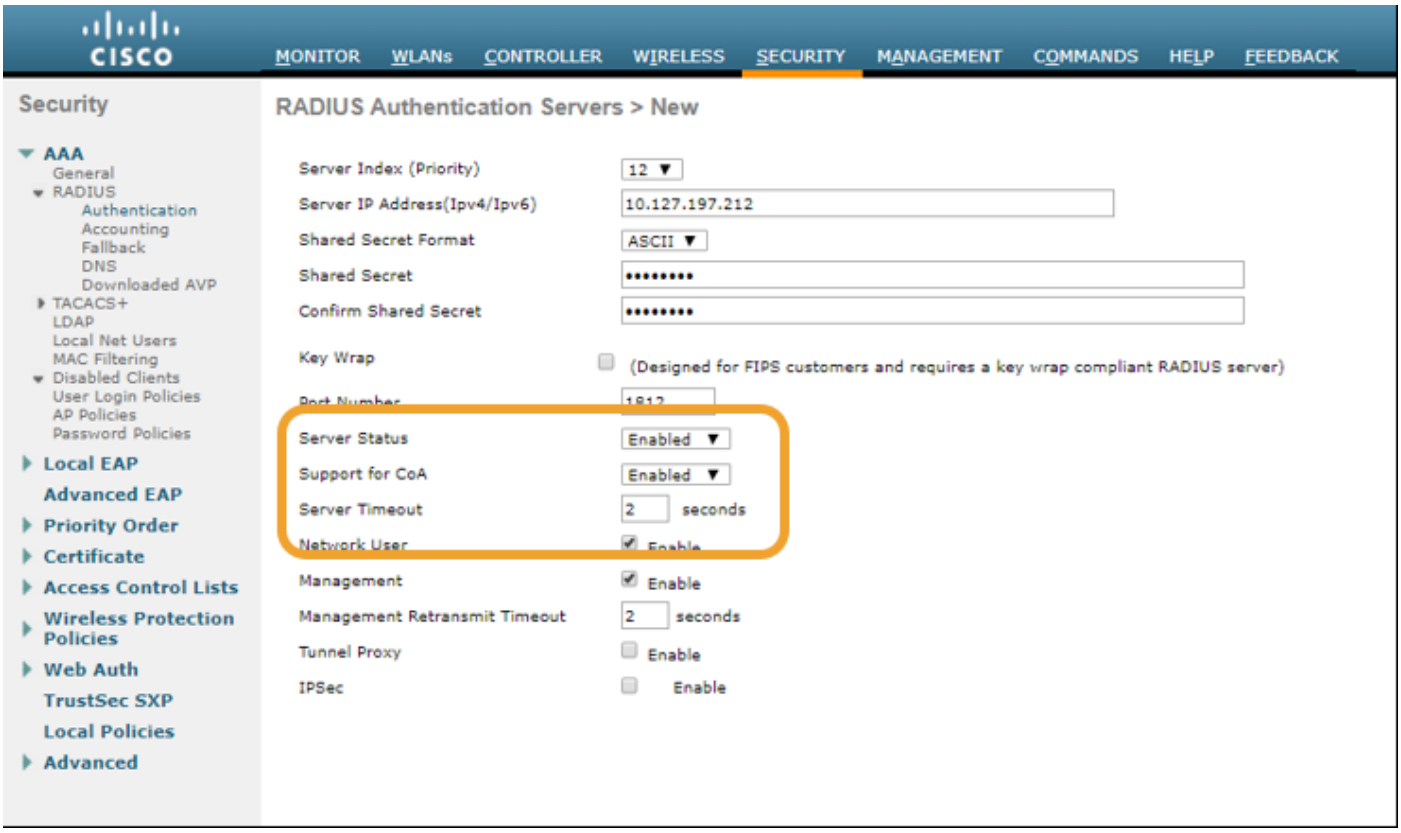
エンドユーザがゲストポータルにアクセスして正常にログインできる場合、次のステップはユーザに完全なゲストアクセスを提供するための許可の変更です。これが機能しない場合は、ISE Radiusライブログにダイナミック認証の失敗が表示されます。この問題を修正するには、次の点を確認します。





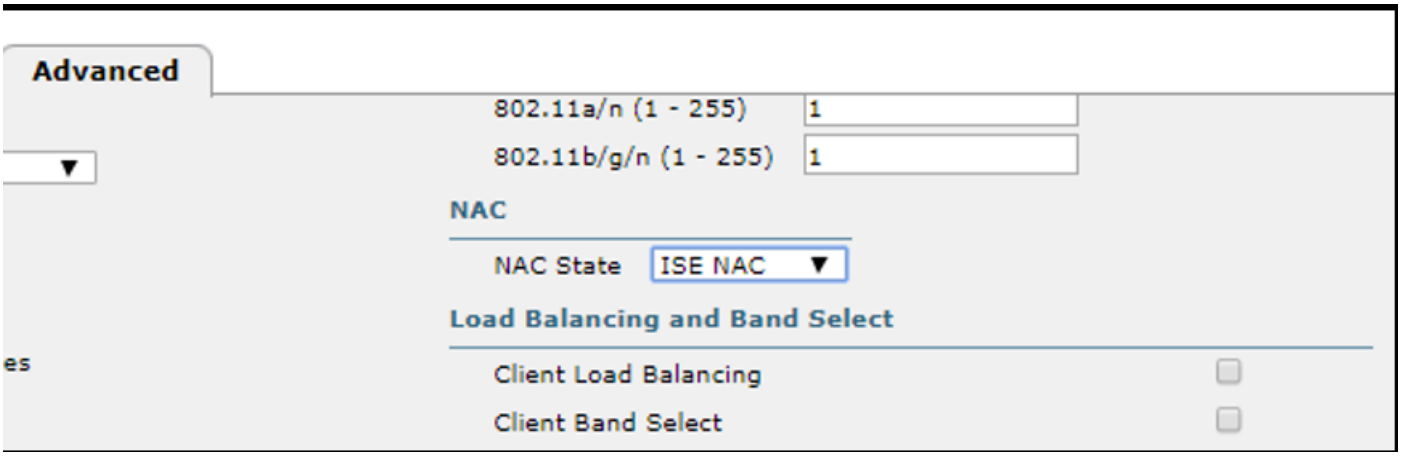
1.認可変更(CoA)がNADで有効/設定されている必要があります。

```
!
aaa server radius dynamic-author
 client 10.127.197.209 server-key cisco123
 client 10.127.197.212 server-key cisco123
!
.
```



2. UDPポート1700がファイアウォールで許可されていること。

3. WLCのNAC状態が正しくない。WLC GUI > WLANのAdvanced settingsで、NACの状態をISE NACに変更します。

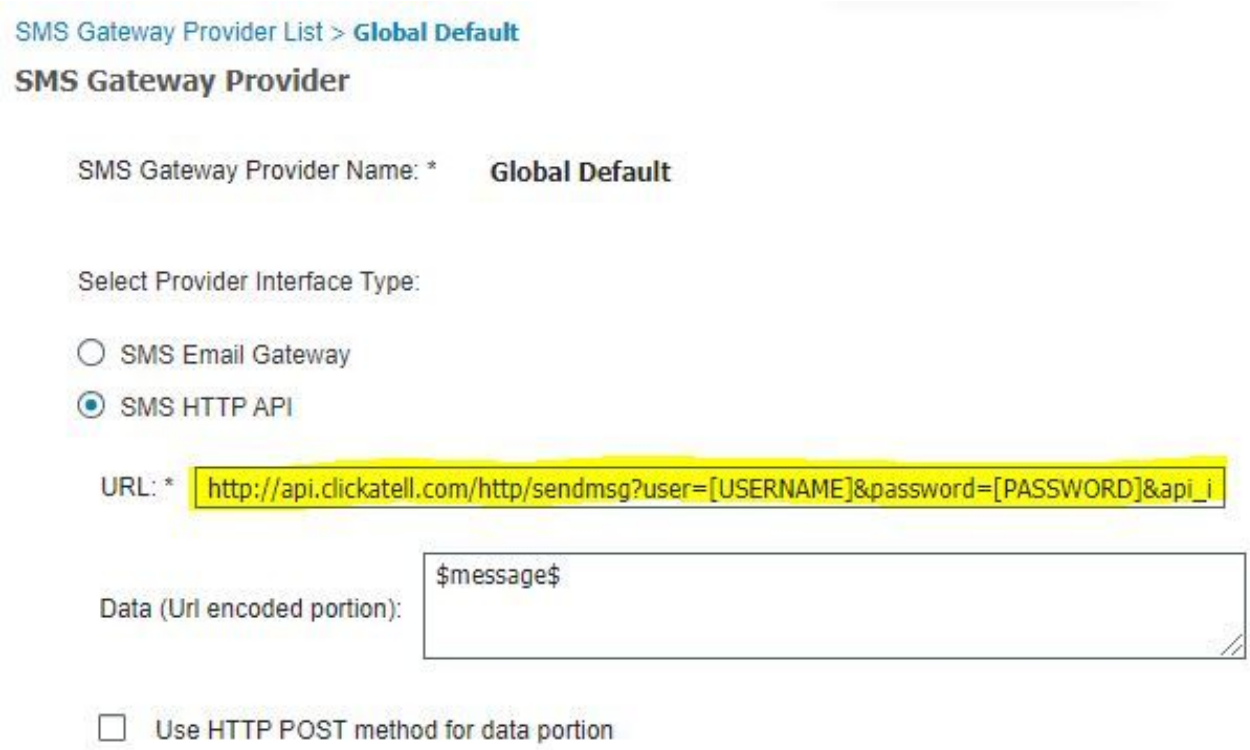


SMS/電子メール通知が送信されない

1. Administration > System > Settings > SMTPでSMTP設定を確認します。

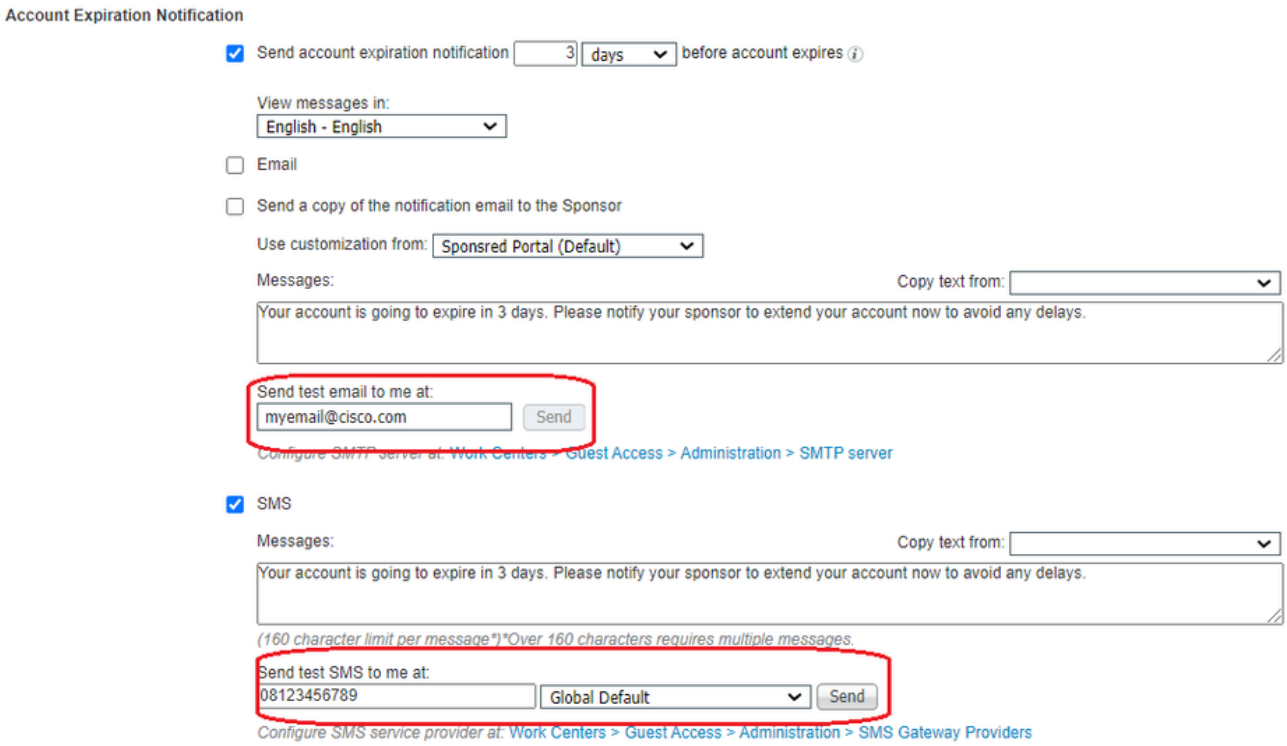
2. ISE外のSMS/EメールゲートウェイのAPIを確認します。

ベンダーから提供されたURLをAPIクライアントまたはブラウザでテストし、ユーザ名、パスワード、携帯電話番号などの変数を置き換えて、到達可能性をテストします。[管理>システム>設定 > SMSゲートウェイ]



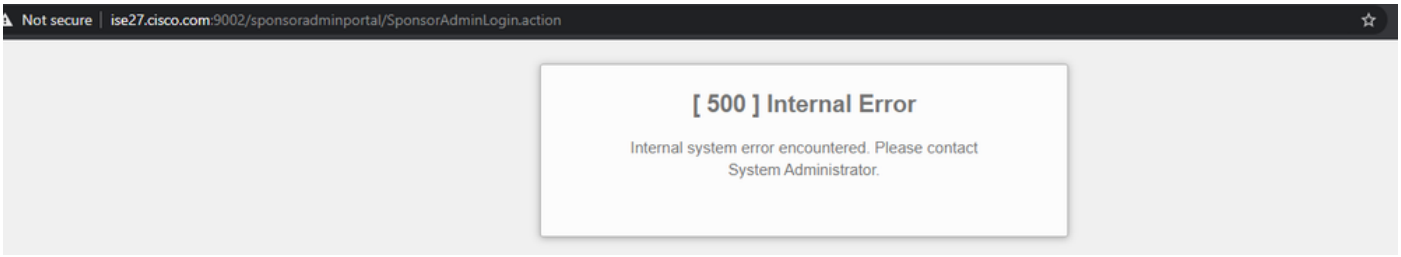
または、ISEスポンサーグループ[Workcentres > Guest Access > Portals and Components > Guest Types]からテストする場合は、ISEとSMS/SMTPゲートウェイでパケットキャプチャを実行して、次のことを確認します

1. 要求パケットは改ざんされずにサーバに到達します。
2. ISEサーバには、ゲートウェイがこの要求を処理するためのベンダー推奨の権限または特権があります。



[アカウントの管理]ページにアクセスできません

1. [Workcentres] > [Guest Access] > [Manage accounts] ボタンで、ISE管理者がスポンサーポータルにアクセスできるように、ポート9002のISE FQDNにリダイレクトします。



2.コマンドnslookup <FQDN of ISE PAN>を使用して、スポンサーポータルへのアクセス元のワークステーションでFQDNが解決されているかどうかを確認します。

3.コマンドshow portsを使用して、ISEのCLIからISE TCPポート9002が開いているかどうかを確認します | include 9002コマンドを使用します。

ポータル証明書のベストプラクティス

- シームレスなユーザエクスペリエンスを実現するには、ポータルと管理者ロールに使用する証明書が、一般的にブラウザで信頼されている有名な公開認証局（GoDaddy、DigiCert、VeriSignなど）によって署名されている必要があります（Google Chrome、Firefoxなど）。

- ゲストのリダイレクトにスタティックIPを使用することは、ISEのプライベートIPがすべてのユーザに認識されるようにするため、推奨されません。ほとんどのベンダーは、プライベートIP用のサードパーティ署名証明書を提供していません。

- ISE 2.4 p6からp8またはp9に移行する際には、既知のバグがあります。Cisco Bug ID CSCvp75207では、パッチアップグレードの後で、「ISE内の認証の信頼」ボックスと「クライアント認証の信頼」ボックスと「Syslog」ボックスを手動でチェックする必要があります。これにより、ISEはゲストポータルにアクセスするときにTLSフローの完全な証明書チェーンを送信します。

これらの操作を行ってもゲストアクセスの問題が解決しない場合は、TACに連絡して、『ISEで有効にするデバッグ』の手順で収集したサポートバンドルを入手してください。

関連情報

- シスコテクニカルサポートおよびダウンロード

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。