LAPを使用したポートベース認証のためのACS 5.2の設定

内容

はじめに

このドキュメントでは、Access Control Server（ACS）5.2 などの RADIUS サーバに対して認証するために、802.1x サプリカントとして Lightweight アクセス ポイント（LAP）を設定する方法について説明します。

前提条件

要件

この設定を行う前に、以下の要件を満たしていることを確認してください。

- ワイヤレス LAN コントローラ（WLC）と LAP の基礎知識があること。
- AAA サーバに関する機能的知識があること。

- ワイヤレス ネットワークとワイヤレスのセキュリティ問題に関する全般的な知識があること。

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。

- ファームウェア リリース 7.0.220.0 が稼働している Cisco 5508 WLC
- Cisco 3502 シリーズ LAP
- バージョン 5.2 が稼働している Cisco Secure ACS
- Cisco 3560 シリーズ スイッチ

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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

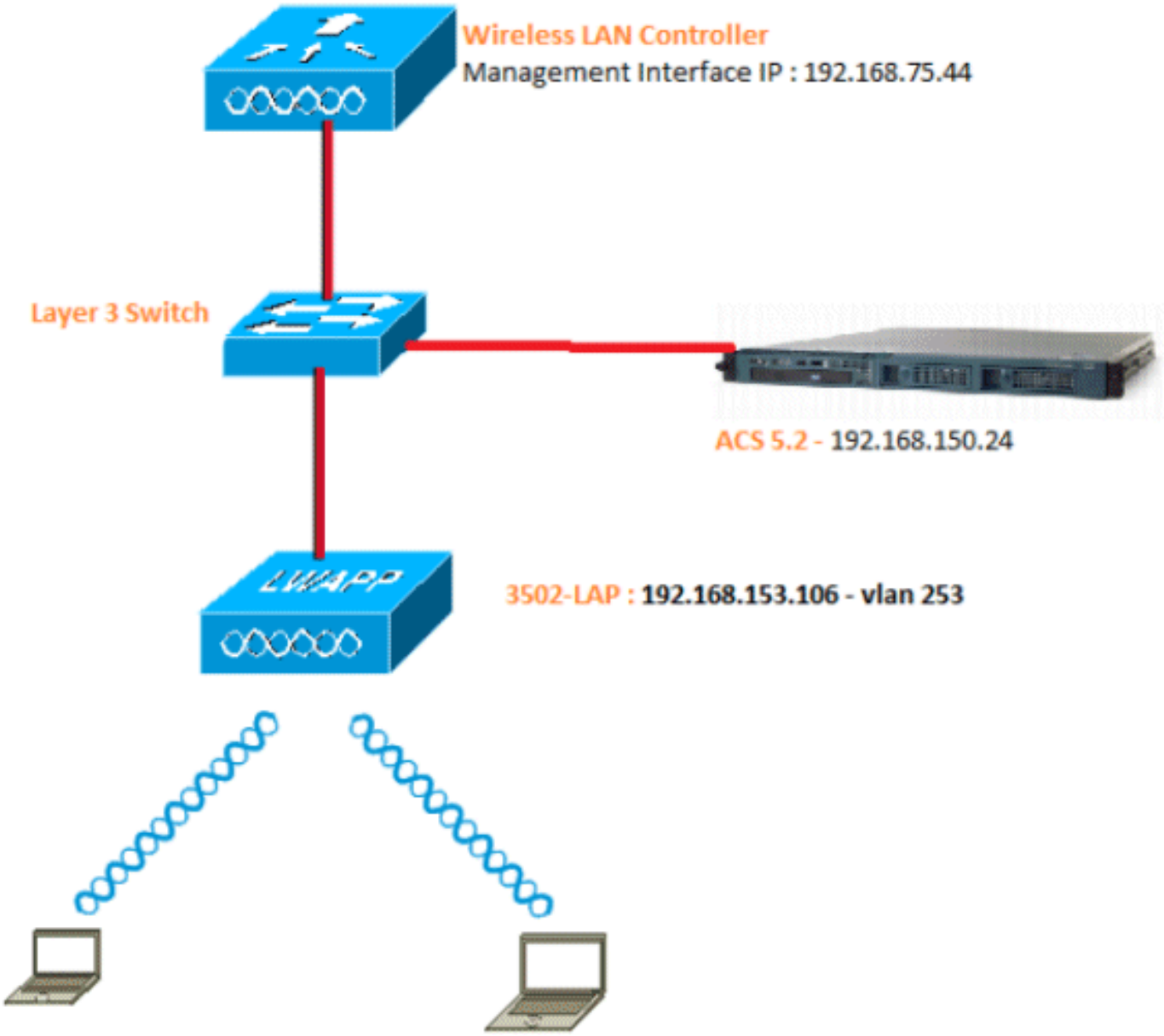
LAP には、秘密キーで署名された X.509 証明書が出荷時に組み込まれ、これは製造時にデバイスに書き込まれます。LAP はこの証明書を使用して、加入プロセス時に WLC との認証を行います。ここでは LAP を認証する別の方法について説明します。WLC ソフトウェアでは、Cisco Aironet アクセス ポイントと Cisco スイッチの間に 802.1x 認証を設定できます。この例では、AP は 802.1x サプリカントとして機能し、匿名 PAC プロビジョニングによる EAP-FAST を使用する RADIUS サーバ（ACS）に対して、スイッチによって認証されます。802.1x 認証が設定されると、スイッチは、ポートに接続されたデバイスが正しく認証されるまでは、802.1x トラフィック以外のトラフィックがポートを通過することを許可しません。AP の認証は、WLC に参加する前か、WLC に参加した後に実行できます。後者の場合、LAP が WLC に参加した後で 802.1x をスイッチに設定します。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



この図で使用されているコンポーネントの設定の詳細は、次のとおりです。

- ACS（RADIUS）サーバの IP アドレスは 192.168.150.24 です。
- WLC の管理インターフェイスおよび AP マネージャ インターフェイスのアドレスは 192.168.75.44 です。
- DHCP サーバのアドレスは 192.168.150.25 です。
- LAP は VLAN 253 に配置されます。
- VLAN 253:192.168.153.x/24。ゲートウェイ：192.168.153.10
- VLAN 75:192.168.75.x/24ゲートウェイ：192.168.75.1

前提

- スイッチには、レイヤ 3 VLAN がすべて設定されています。

- DHCP サーバには DHCP スコーが割り当てられています。
- ネットワーク内すべてのデバイス間ではレイヤ 3 接続が確立しています。
- LAP はでに WLC に登録されています。
- 各 VLAN は /24 マスクを使用しています。
- ACS 5.2 には自己署名証明書がインストールされています。

設定手順

この設定は、次の 4 つのカテゴリに分類されます。

1. LAP を設定します。
2. スイッチを設定します。
3. RADIUS サーバの設定

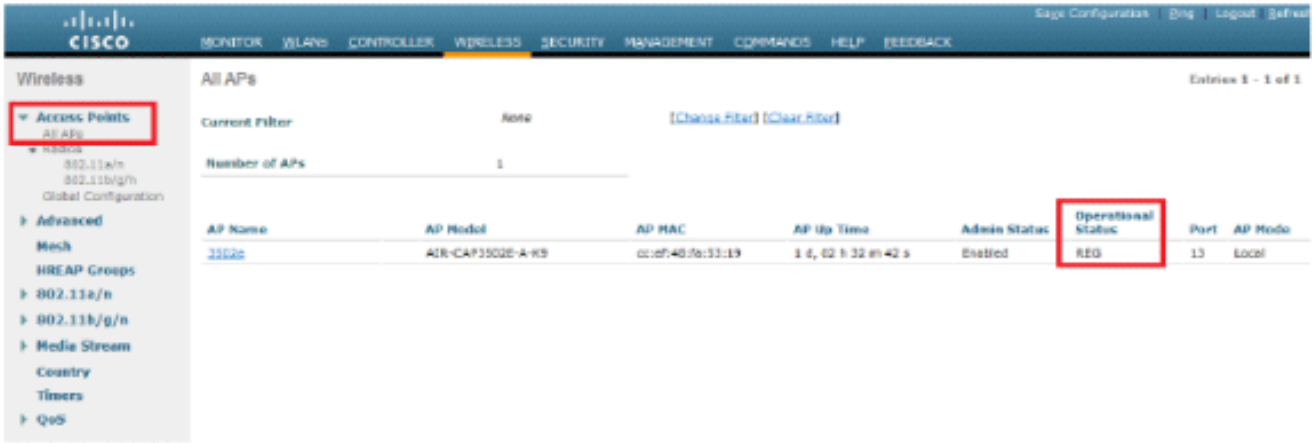
LAP の設定

前提条件：

LAP は、オプション 43、DNS、または静的に設定された WLC 管理インターフェイス IP を使用して WLC にすでに登録されている必要があります。

次のステップを実行します。

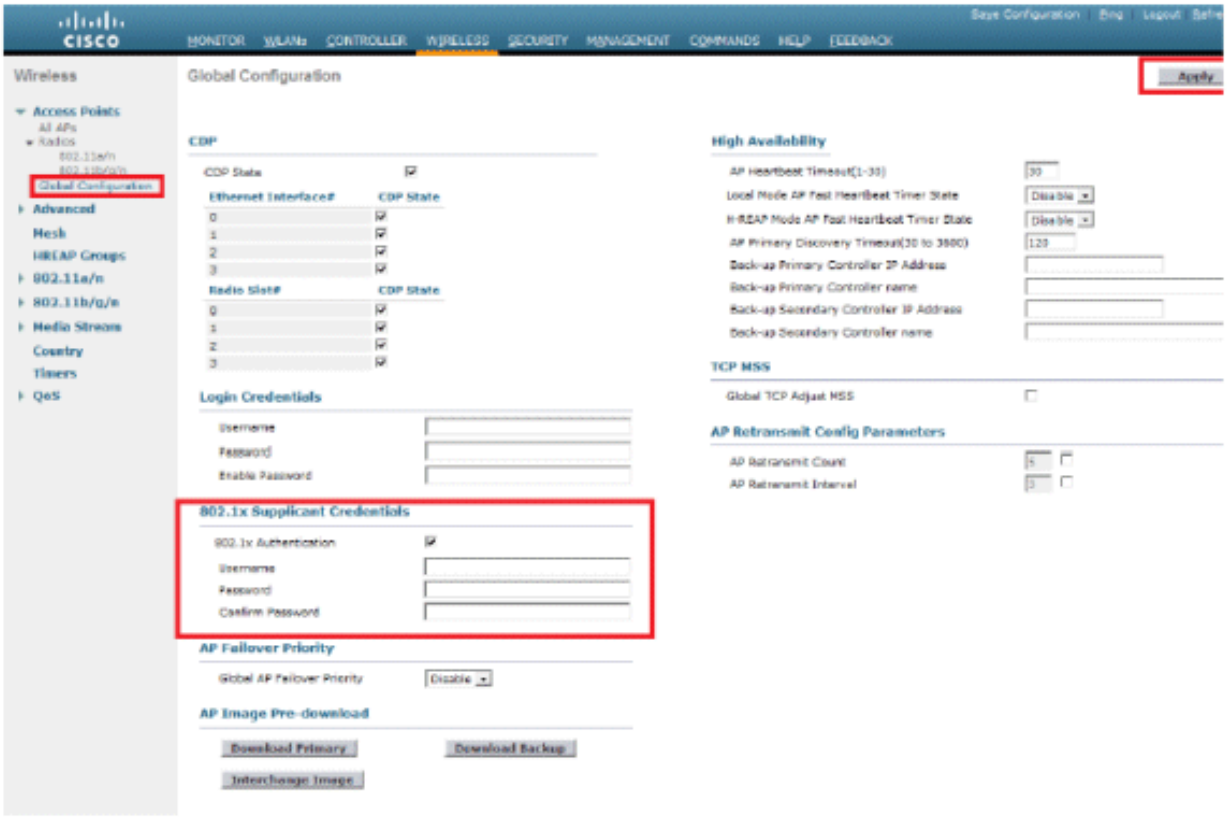
1. [Wireless] > [Access Points] > [All APs] の順に移動し、WLC に LAP が登録されていることを確認します。



2. 次の 2 つの方法で、すべての LAP に対して 802.1x クレデンシャル (ユーザ名/パスワード) を設定できます。
   - グローバル

     すでに LAP が参加している場合、クレデンシャルをグローバルに設定して、WLC に

参加するすべての LAP がそれらのクレデンシャルを継承するようにできます。

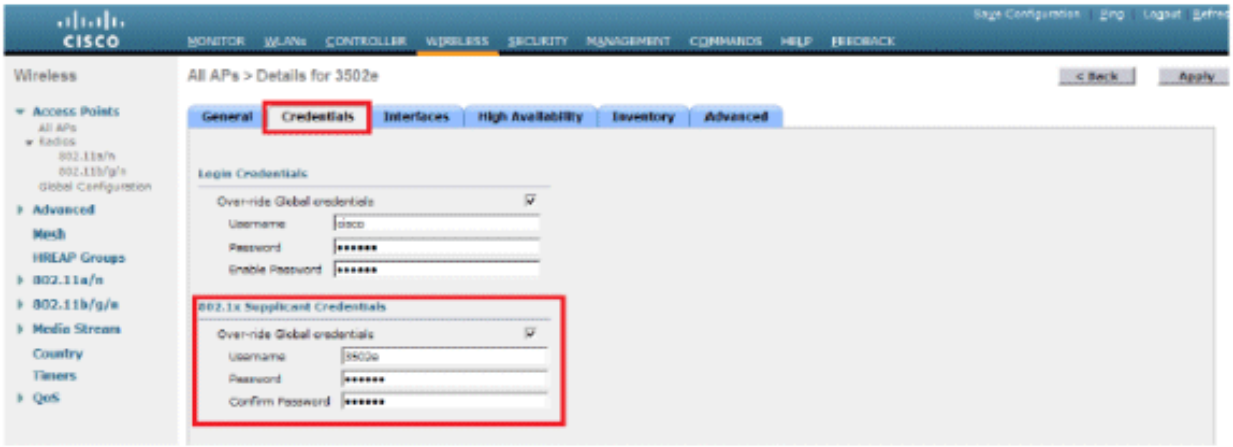


- 個別

  AP ごとに 802.1 x プロファイルを設定します。この例では、AP ごとにクレデンシャルを設定します。

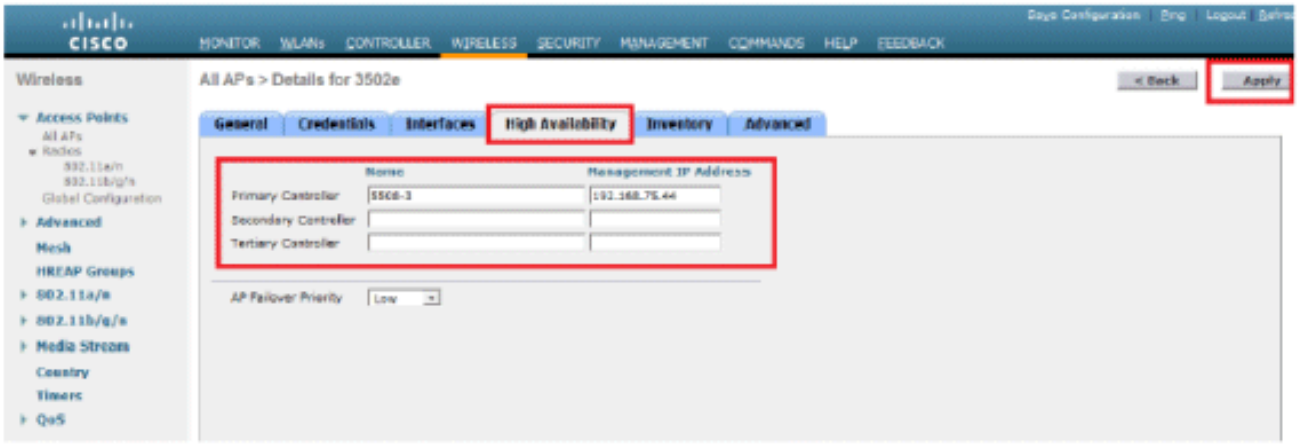
  a. [Wireless] > [All APs] に移動して、接続された AP を選択します。

  b. [802.1x Supplicant Credentials] フィールドにユーザ名とパスワードを追加します。



注：ログインクレデンシャルは、APへのTelnet、SSH、またはコンソールインに使用されます。

3. [High Availability] セクションを設定し、[Apply] をクリックします。



注：保存したクレデンシャルは、WLCとAPのリブート後も保持されます。クレデンシャルは LAP が新しい WLC に加入した場合に限り変更されます。LAP は、新しい WLC に設定されているユーザ名およびパスワードを受け入れます。

AP が WLC にまだ参加していない場合、クレデンシャルを設定するには、LAP にコンソールを使用してアクセスする必要があります。イネーブル モードで次の CLI コマンドを実行します。

LAP#lwapp ap dot1x username <username> password <password>

または

LAP#capwap ap dot1x username <username> password <password>

注：このコマンドは、リカバリイメージを実行するAPでのみ使用できます。

LAP のデフォルトのユーザ名とパスワードはそれぞれ「cisco」と「Cisco」です。

スイッチの設定

スイッチは LAP のオーセンティケータとして機能し、RADIUS サーバに対して LAP を認証します。準拠したソフトウェアがスイッチにない場合、スイッチをアップグレードします。スイッチ CLI で次のコマンドを発行して、スイッチ ポート上で 802.1X 認証を有効にします。

<#root>

```
switch#
configure terminal
switch(config)#
dot1x system-auth-control
switch(config)#
aaa new-model

!--- Enables 802.1x on the Switch.
```

```
switch(config)#
aaa authentication dot1x default group radius
switch(config)#
radius server host 192.168.150.24 key cisco

!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x information

switch(config)#
ip radius source-interface vlan 253

!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.

switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp
switch(config-if)spanning-tree portfast

!--- gig0/11 is the port number on which the AP is connected.

switch(config-if)dot1x pae authenticator

!--- Configures dot1x authentication.

switch(config-if)dot1x port-control auto

!--- With this command, the switch initiates the 802.1x authentication.
```

注：同じスイッチ上に他のAPがあり、それらのAPに802.1xを使用させたくない場合は、ポートを802.1x用に未設定のままにするか、次のコマンドを発行できます。

```
<#root>
switch(config-if)authentication port-control force-authorized
```

RADIUS サーバの設定

LAP は EAP-FAST で認証されます。Cisco ACS 5.2 を使用していない場合、使用する RADIUS サーバがこの EAP 方式をサポートすることを確認してください。

RADIUS サーバの設定は次の 4 つのステップで構成されます。

1. ネットワーク リソースの設定
2. ユーザの設定
3. ポリシー要素の定義

4. アクセス ポリシーの適用

ACS 5.x は、ポリシーベースの ACS です。つまり、ACS 5.x では、4.x バージョンで使用されていたグループベースのモデルの代わりに、ルールベース ポリシー モデルが使用されています。

ACS 5.x のルールベース ポリシー モデルを使用すると、以前のグループベースの手法よりも強力で柔軟なアクセス コントロールを実現できます。

以前のグループベース モデルでは、グループを使用してポリシーを定義していました。これは、グループに次の 3 つのタイプの情報が結合されていたためです。

- 識別情報：この情報は、AD グループまたは LDAP グループでのメンバーシップ、または ACS 内部ユーザの静的割り当てに基づいています。
- その他の制限または条件：時間制限、デバイス制限など。
- 許可：VLAN または Cisco IOS® の特権レベル。

ACS 5.x ポリシー モデルは、次の形式のルールに基づいています。

If condition then result

たとえば、グループベース モデルに関して記述されている次の情報を使用します。

If identity-condition, restriction-condition then authorization-profile

これにより、ユーザがネットワークにアクセスするための条件や、特定の条件を満たす場合に許可する承認レベルを、柔軟に制御できるようになります。

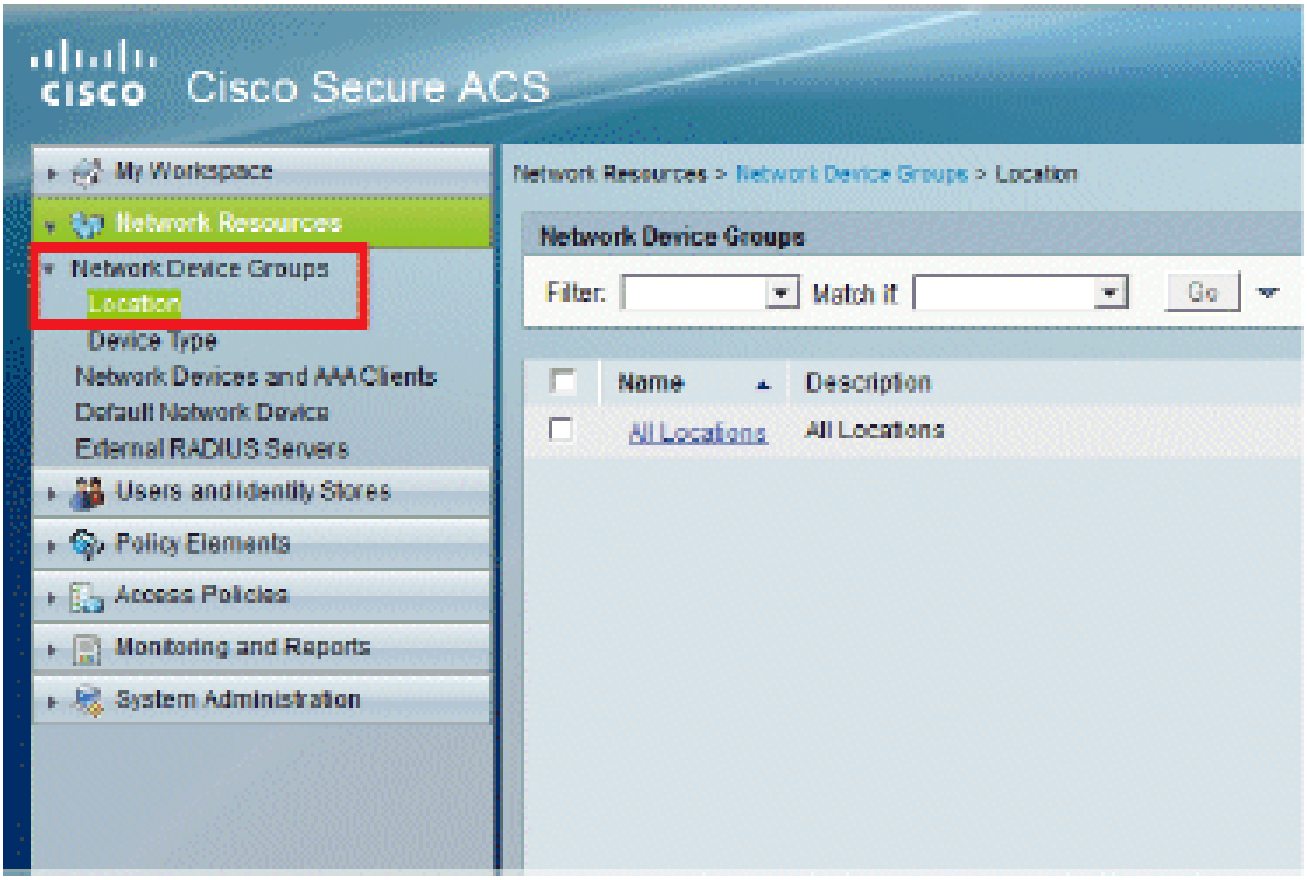
ネットワーク リソースの設定

ここでは、RADIUS サーバ上のスイッチに AAA クライアントを設定します。

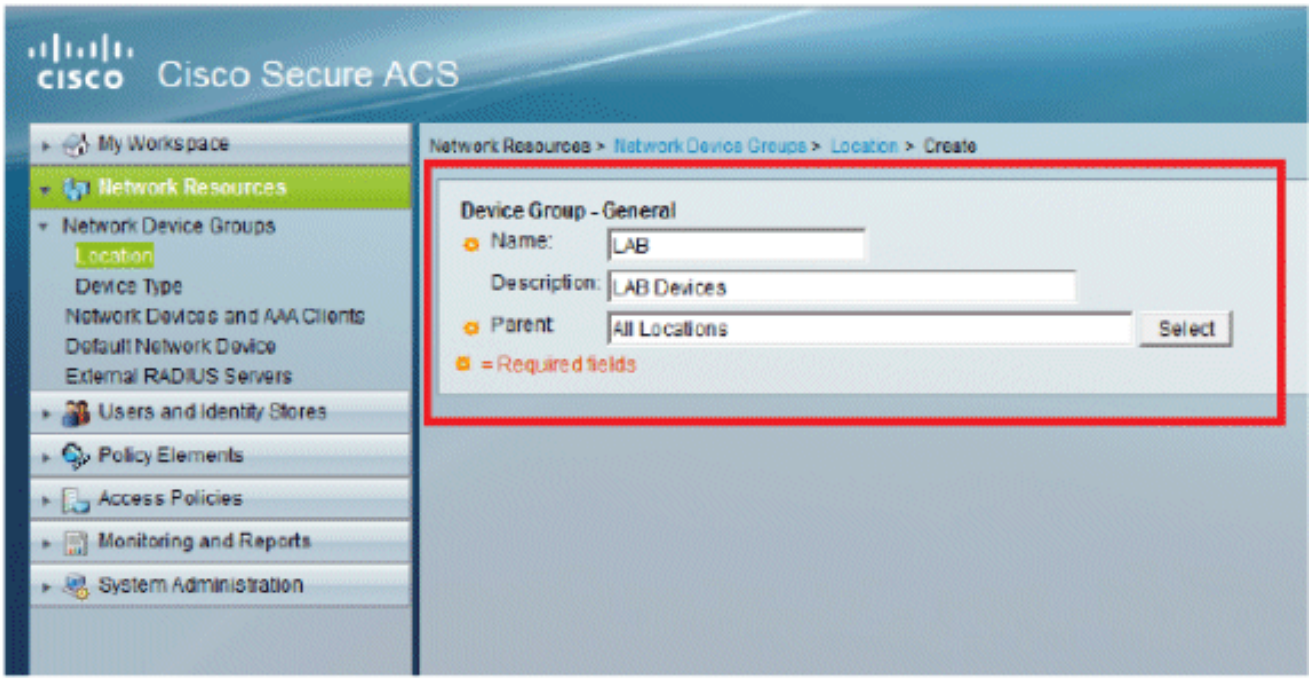
この手順では、スイッチから RADIUS サーバにユーザ クレデンシャルを渡せるように、RADIUS サーバで AAA クライアントとしてスイッチを追加する方法について説明します。

次のステップを実行します。

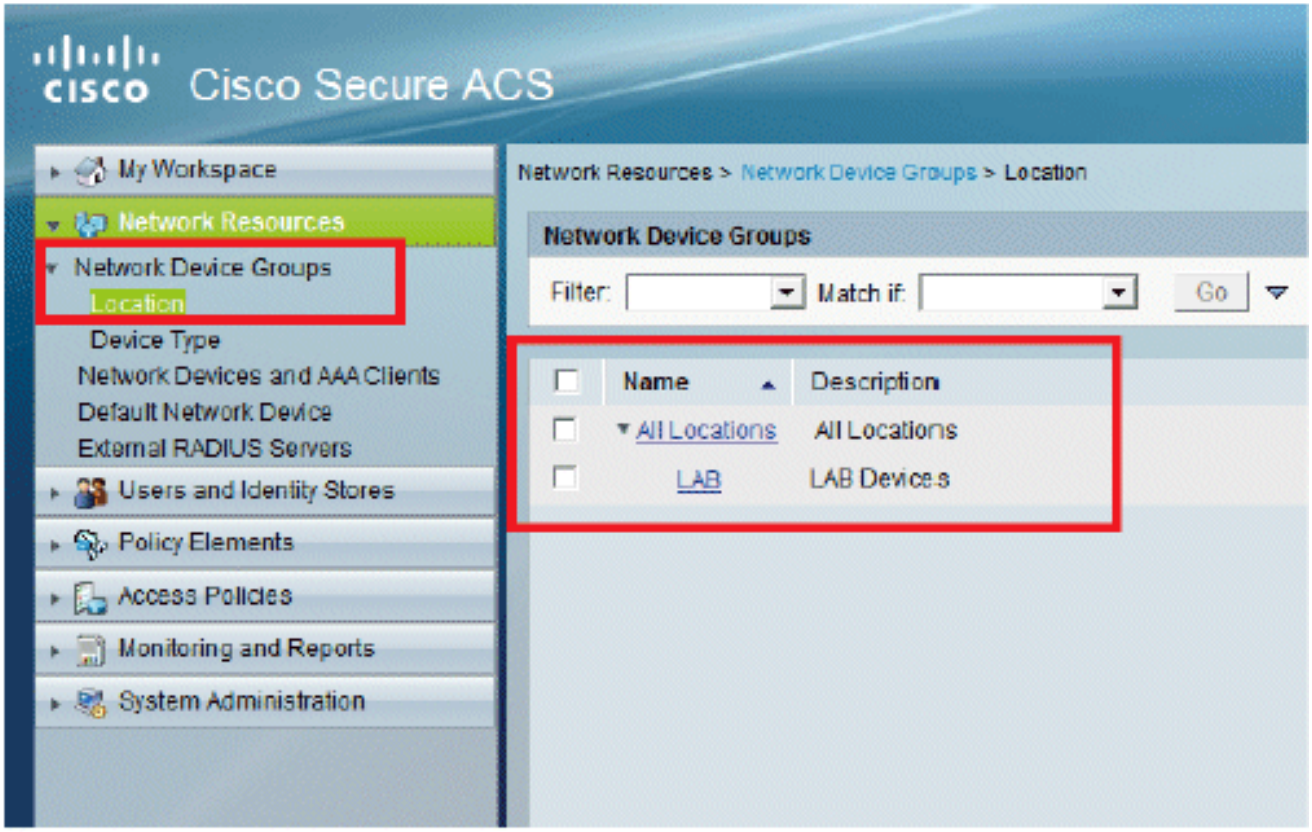
1. ACS の GUI で、[Network Resources] をクリックします。
2. [Network Device Groups] をクリックします。
3. [Location] > [Create] に移動します（ 下の方にあります。



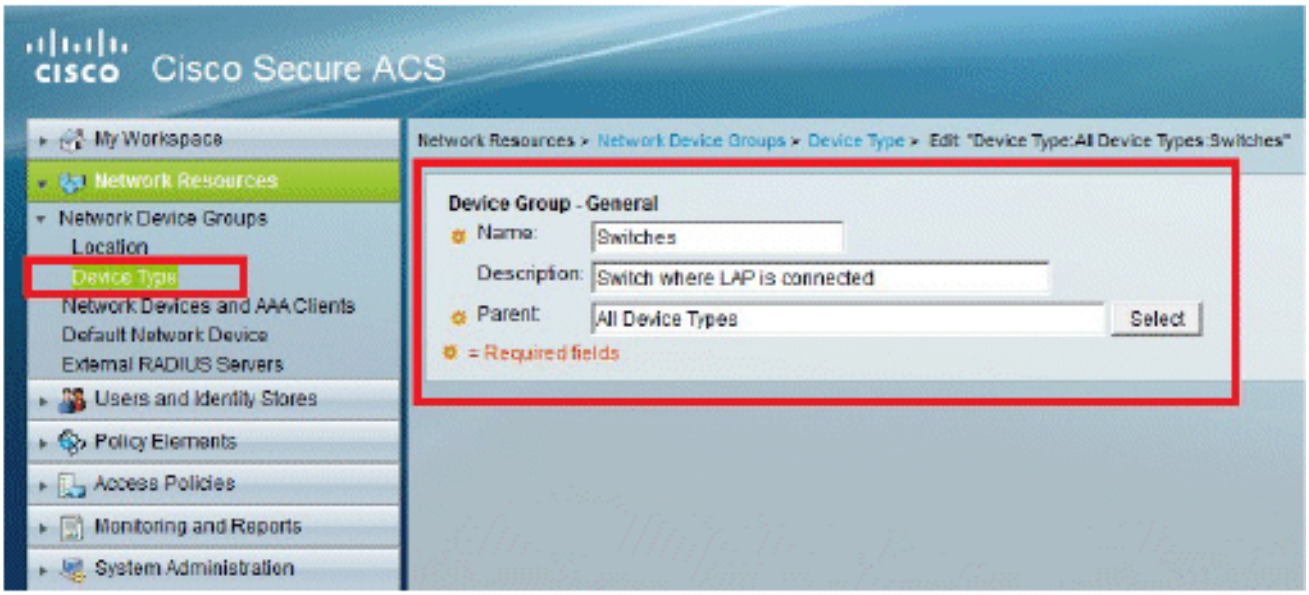
4. 必要なフィールドを追加して [Submit] をクリックします。



5. ウィンドウが更新されます。

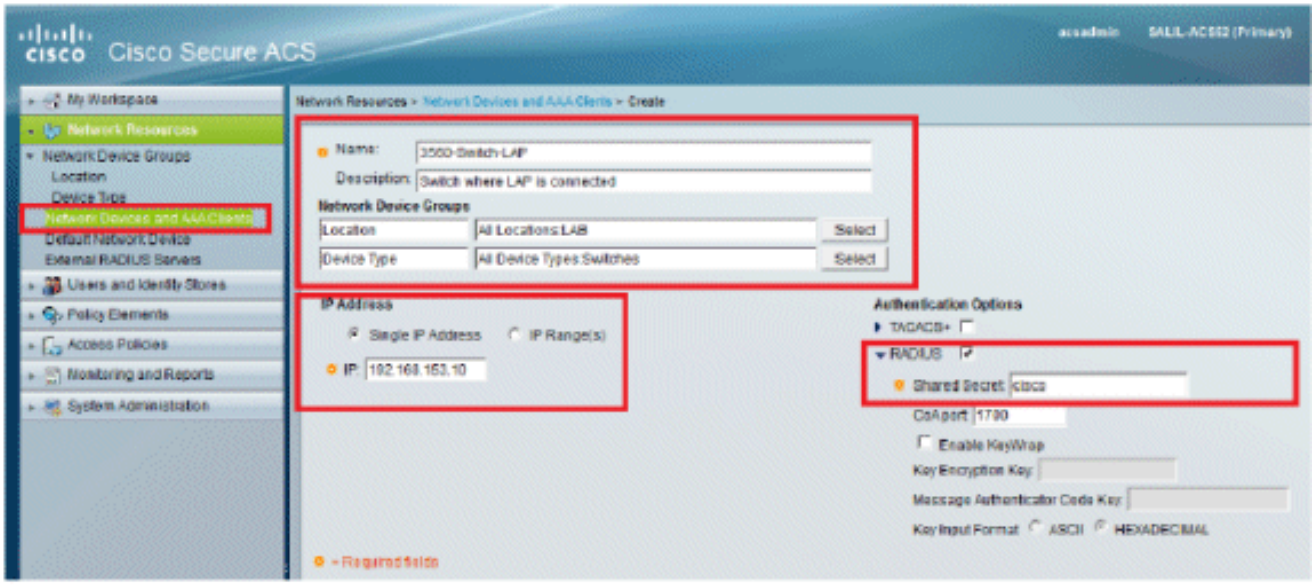


6. [Device Type] > [Create] をクリックします。

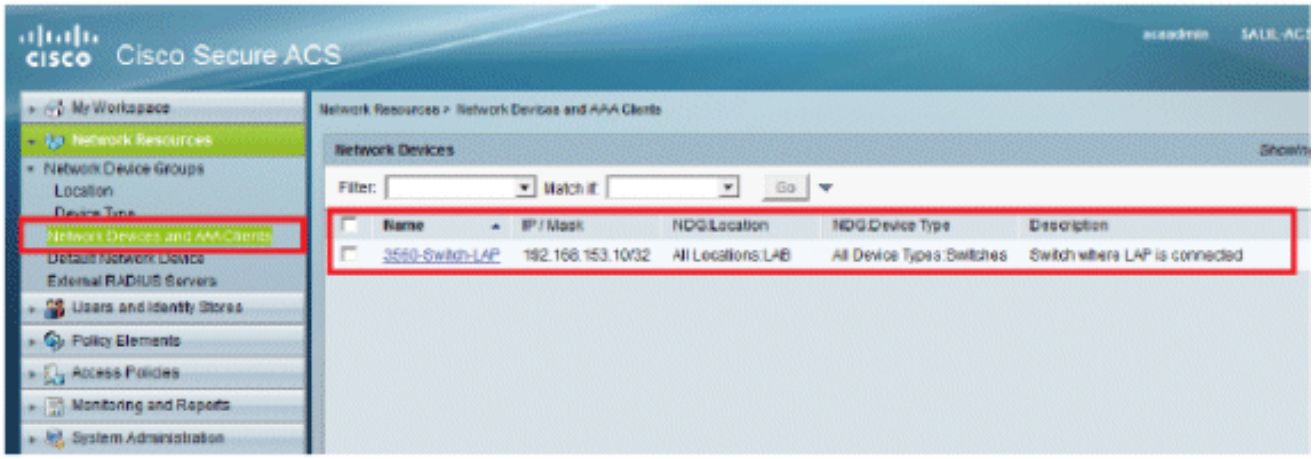


7. [Submit] をクリックします。完了すると、ウィンドウが更新されます。

8. [Network Resources] > [Network Devices and AAA Clients] に移動します。
9. [Create] をクリックして、次のように詳細を入力します。



10. [Submit] をクリックします。ウィンドウが更新されます。

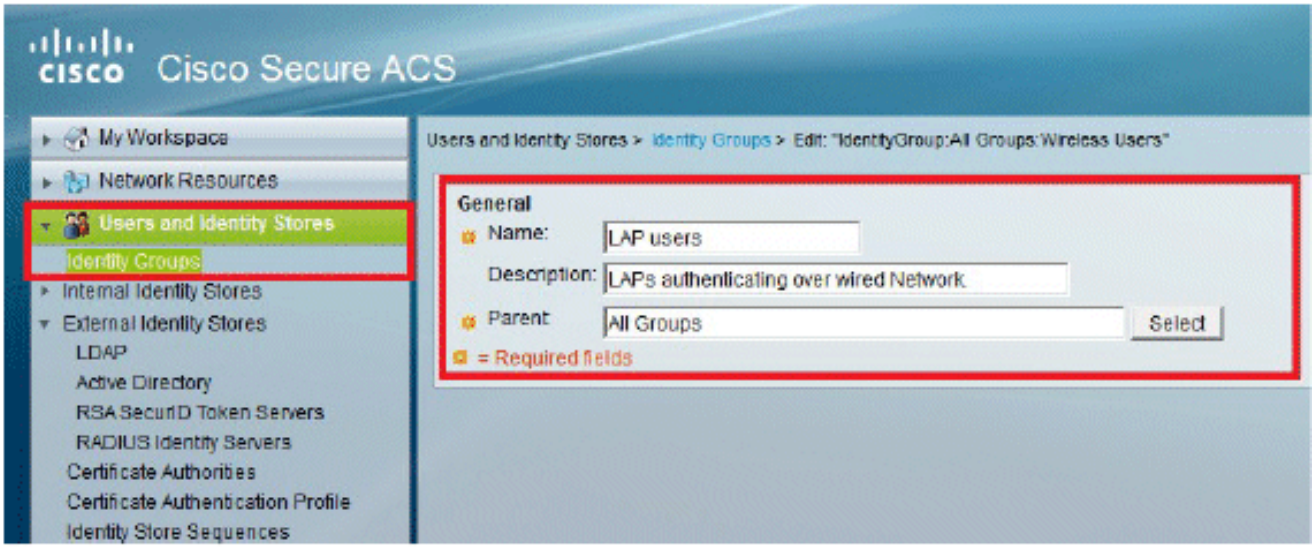


ユーザの設定

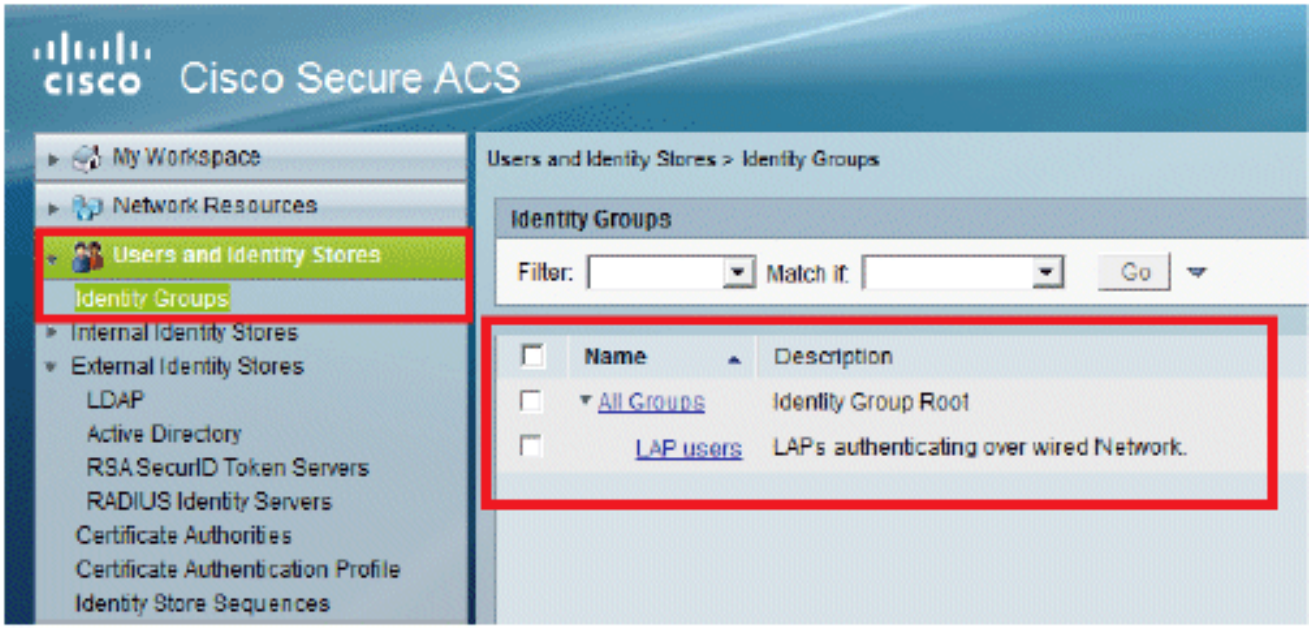
このセクションでは、前に設定した ACS でユーザを作成する方法を説明します。「LAP users」というグループにユーザを割り当てます。

次のステップを実行します。

1. [Users and Identity Stores] > [Identity Groups] > [Create] に移動します。

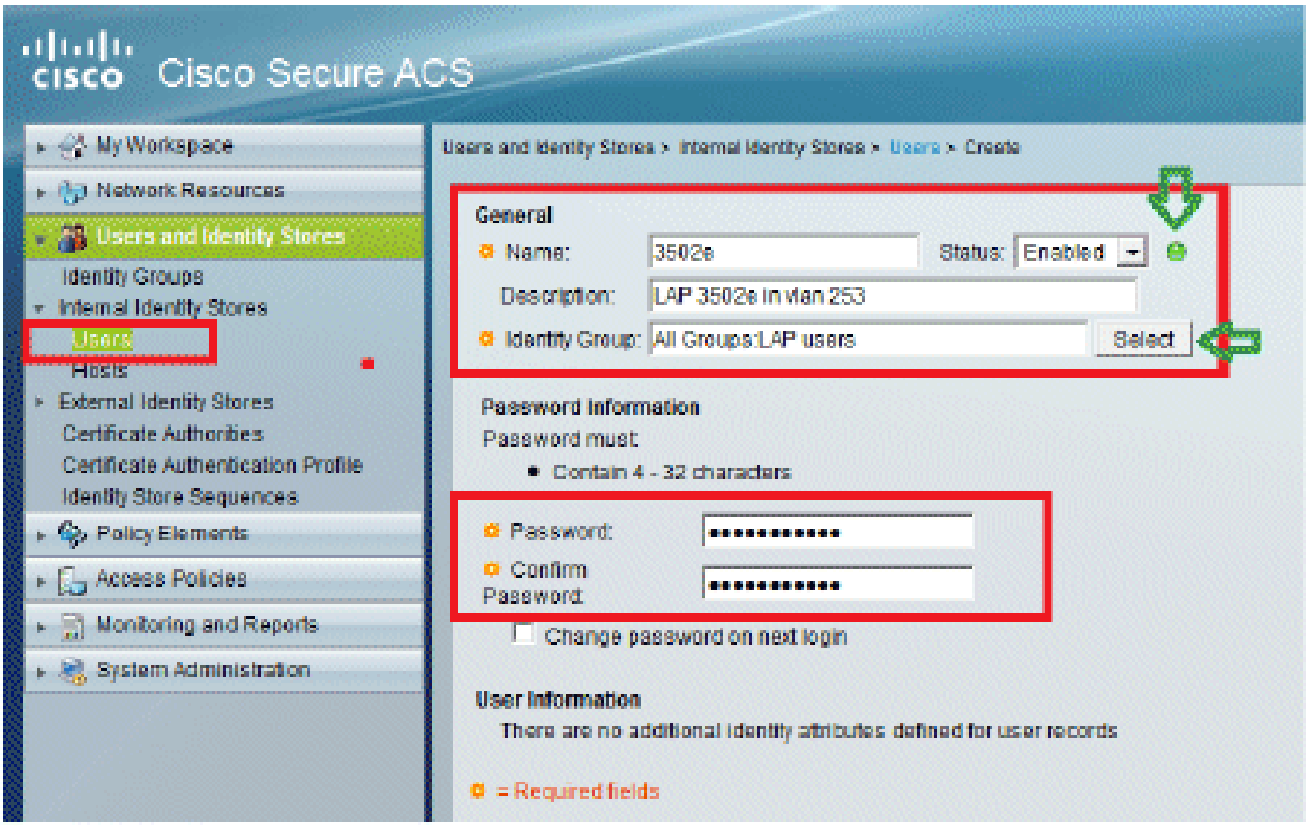


2. [Submit] をクリックします。

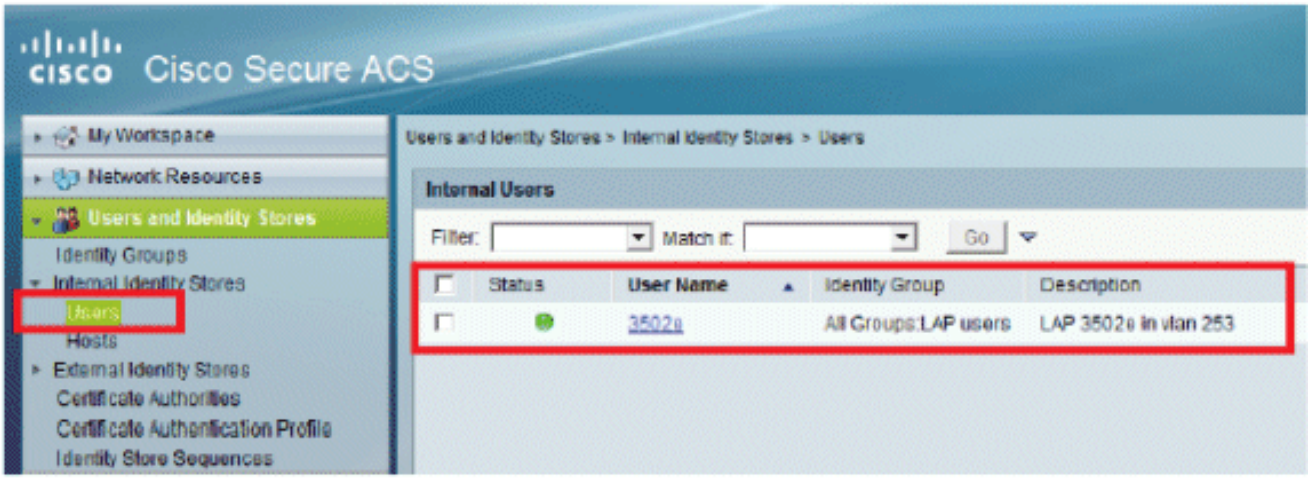


3. 3502e を作成し、グループ「LAP users」に割り当てます。

4. [Users and Identity Stores] > [Identity Groups] > [Users] > [Create] に移動します。

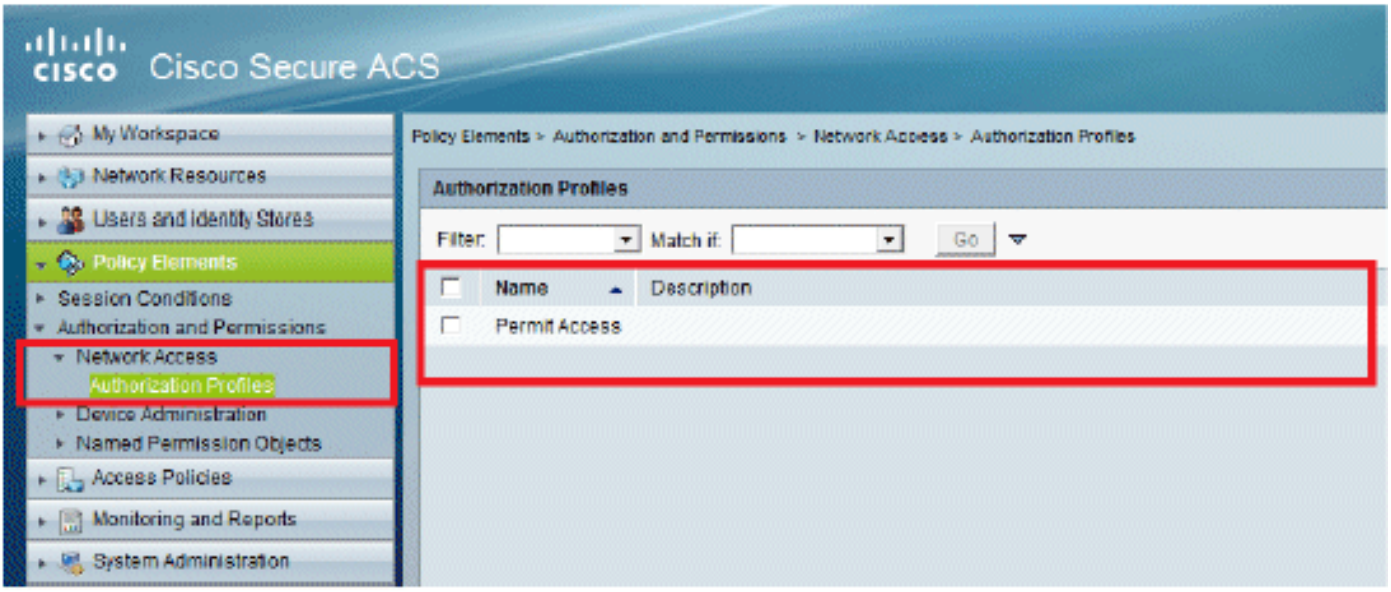


5. 更新された情報が表示されます。



ポリシー要素の定義

[Permit Access] が設定されていることを確認します。

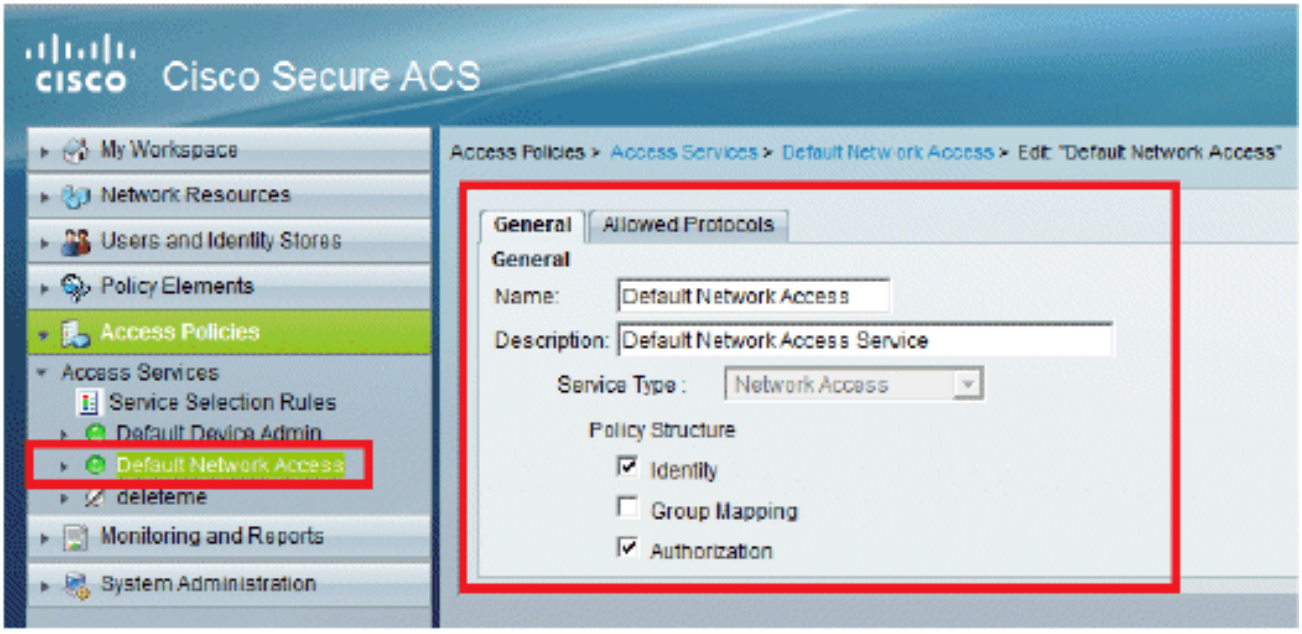


アクセス ポリシーの適用

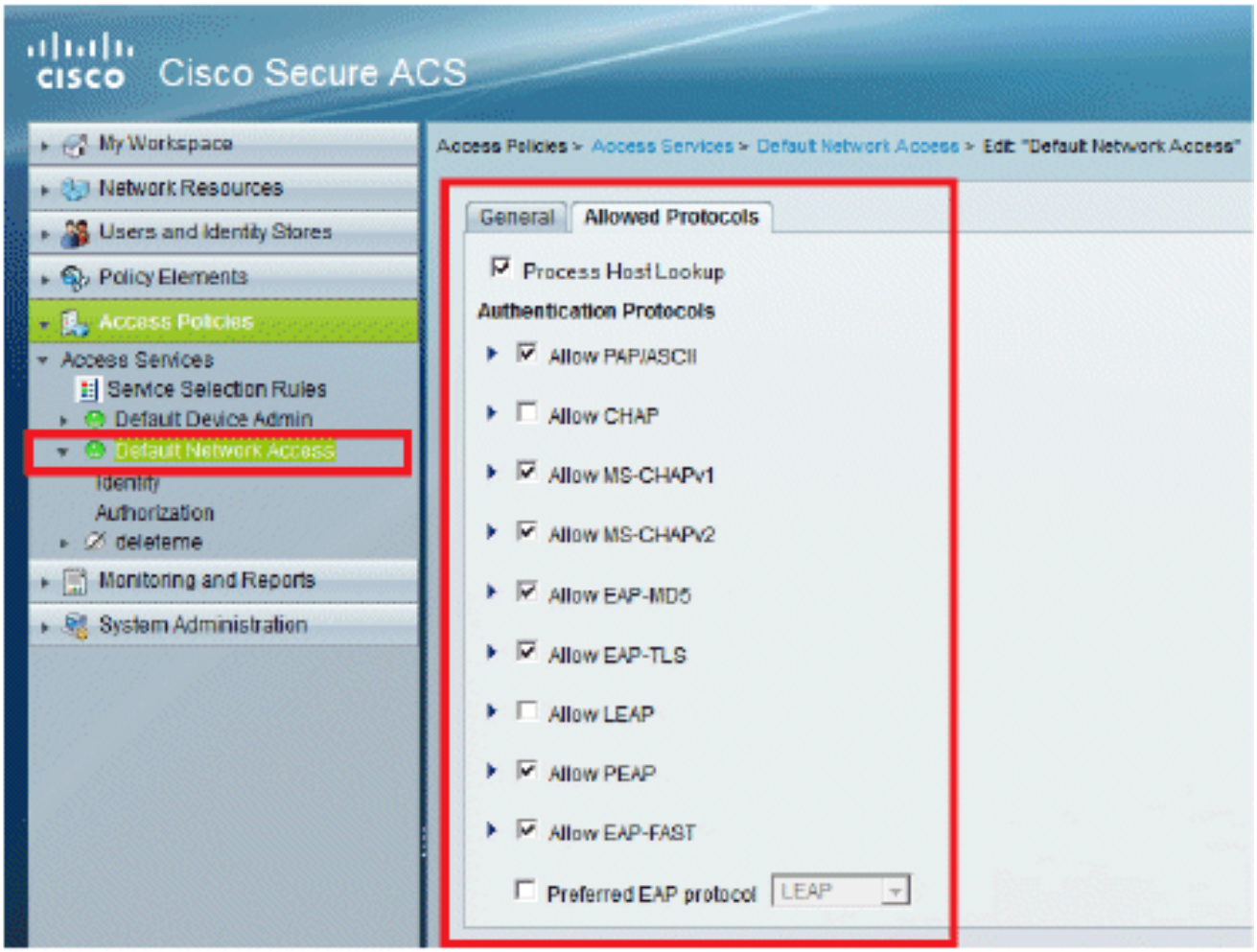
このセクションでは、認証するために LAP で使用する認証方式として EAP-FAST を選択します。これまでのステップに基づいてルールを作成します。

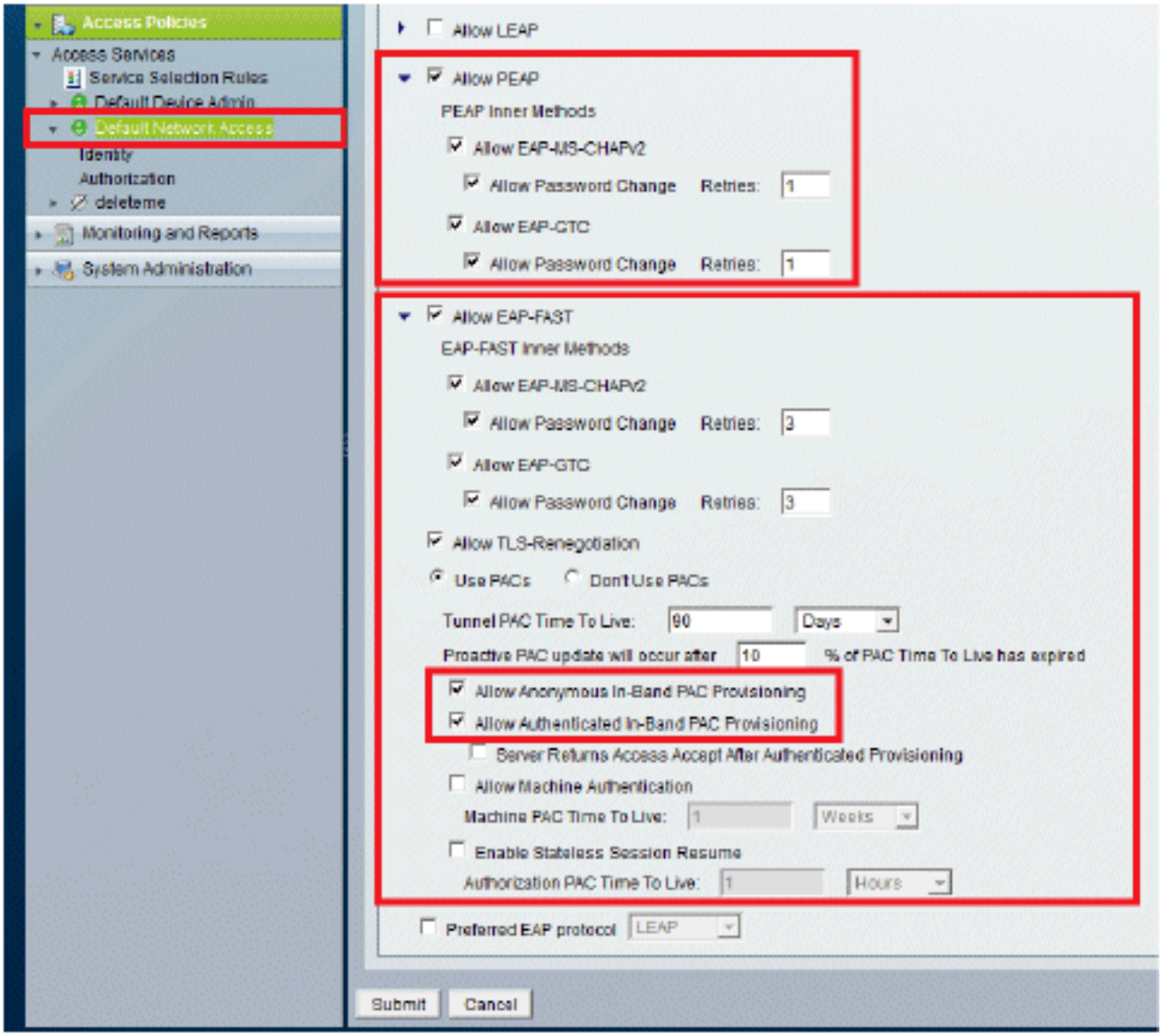
次のステップを実行します。

1. Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"の順に選択します。



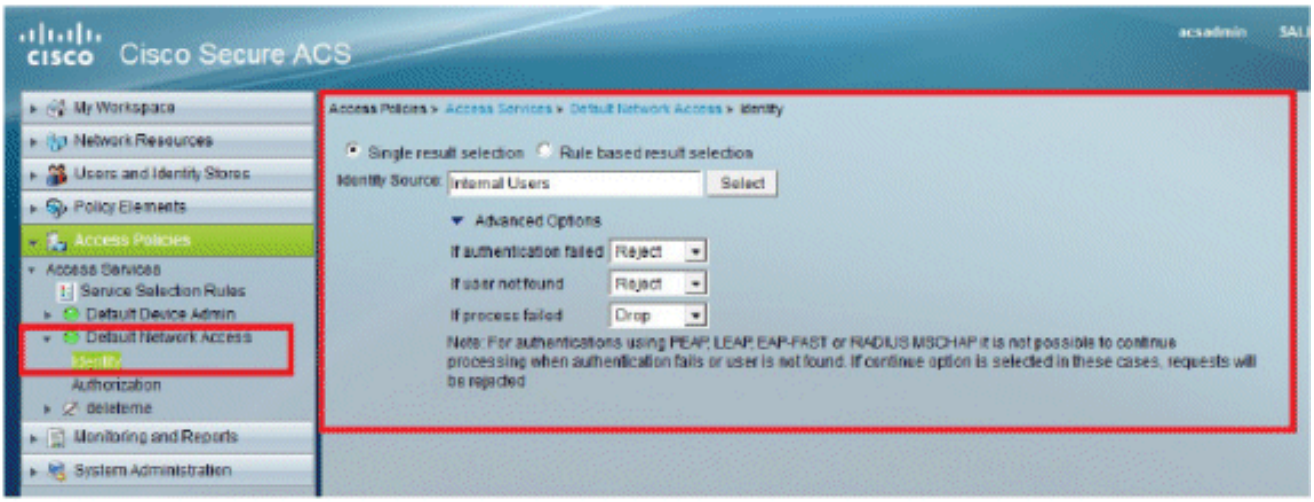
2. [EAP-FAST] と [Anonymous In-Band PAC Provisioning] が有効であることを確認します。





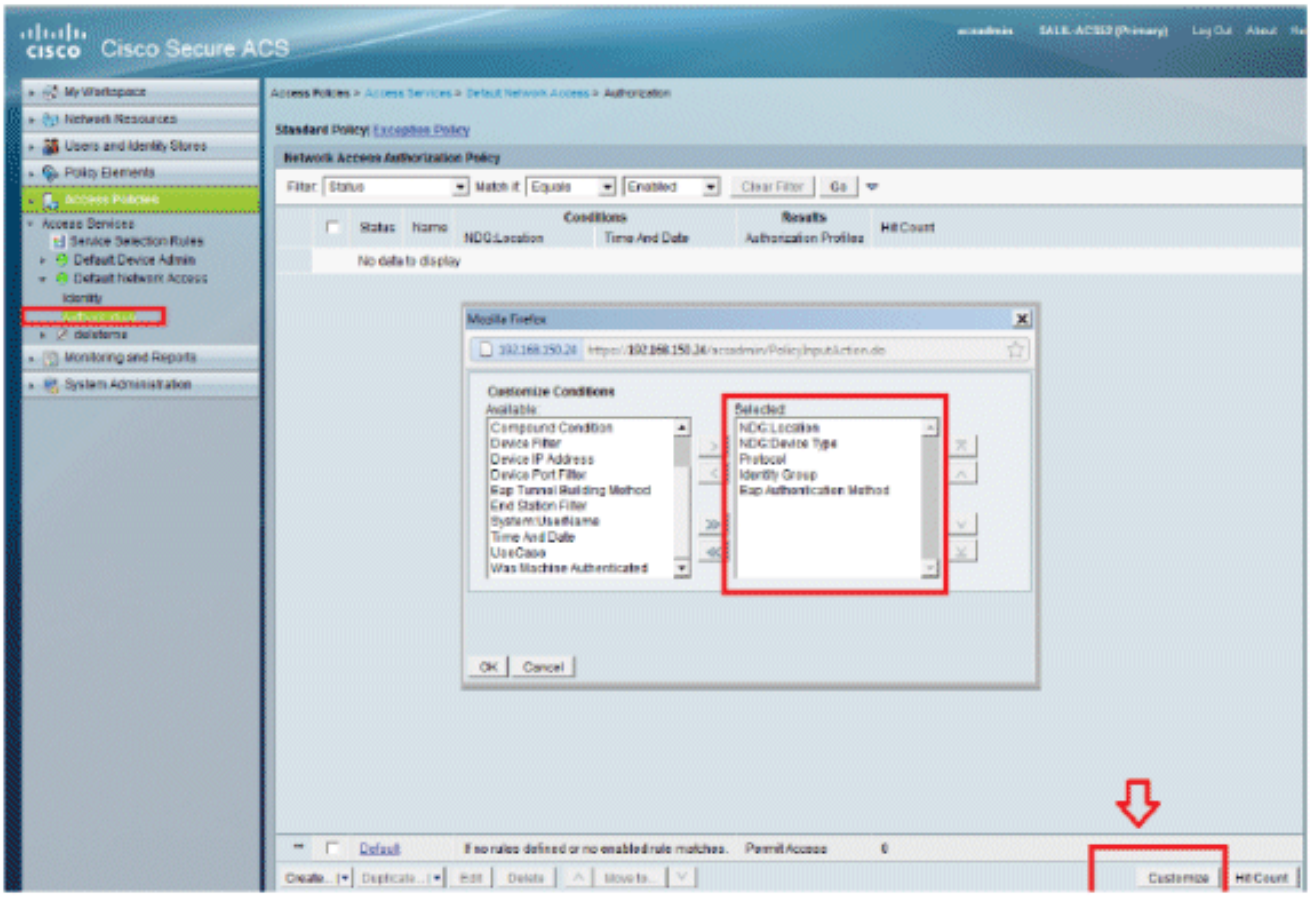
3. [Submit] をクリックします。

4. 選択した Identity グループを確認します。この例では、[Internal Users]（ACS で作成済み）を使用し、変更を保存します。



5. [Access Policies] > [Access Services] > [Default Network Access] > [Authorization] に移動し、許可プロファイルを確認します。

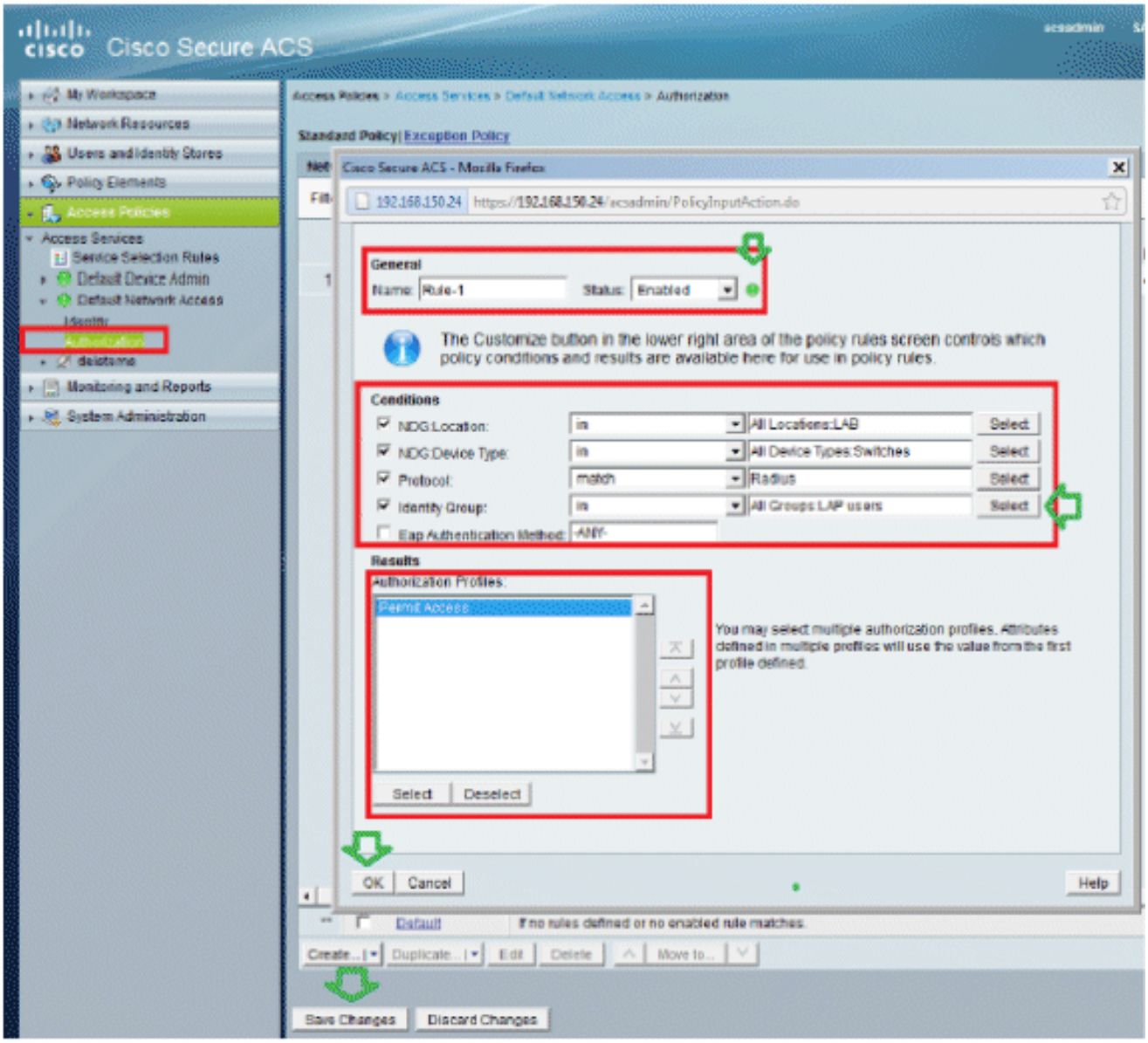
   ユーザのネットワークに対するアクセス条件や、認証後に許可する許可プロファイル（属性）をカスタマイズできます。この精度は ACS 5.x でしか利用できません。この例では、[Location]、[Device Type]、[Protocol]、[Identity Group]、および [EAP Authentication Method] が選択されています。



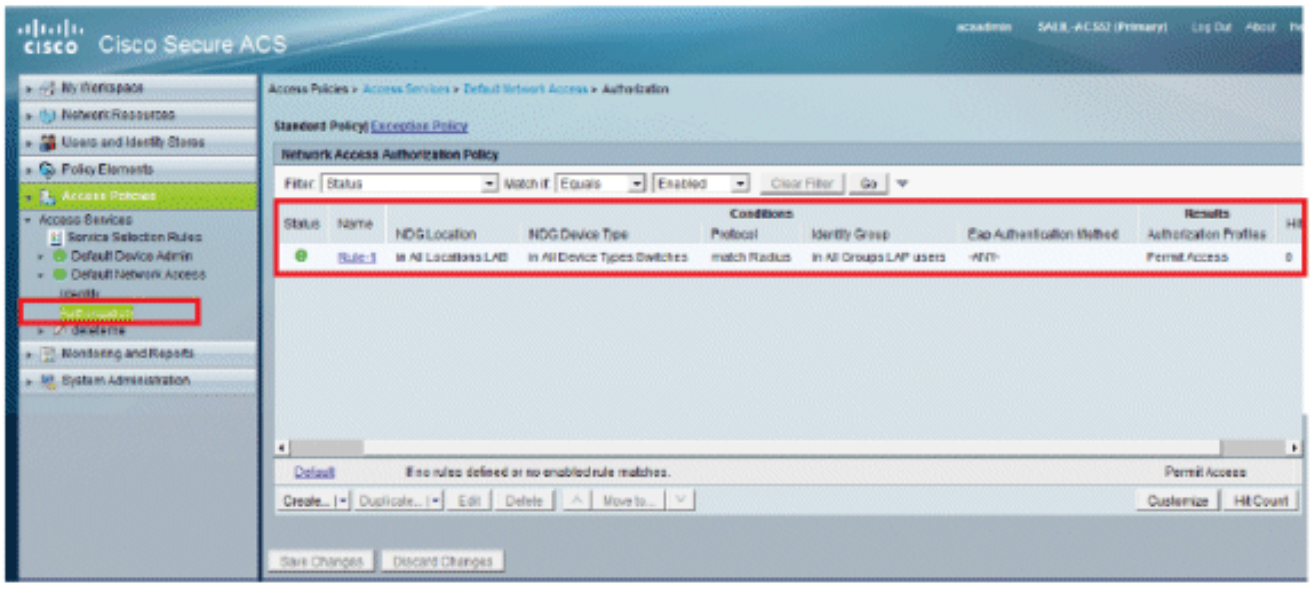
6. [OK] をクリックして変更を保存します。

7. 次に、ルールを作成します。ルールが定義されていない場合、LAP は条件なしでアクセスが許可されます。

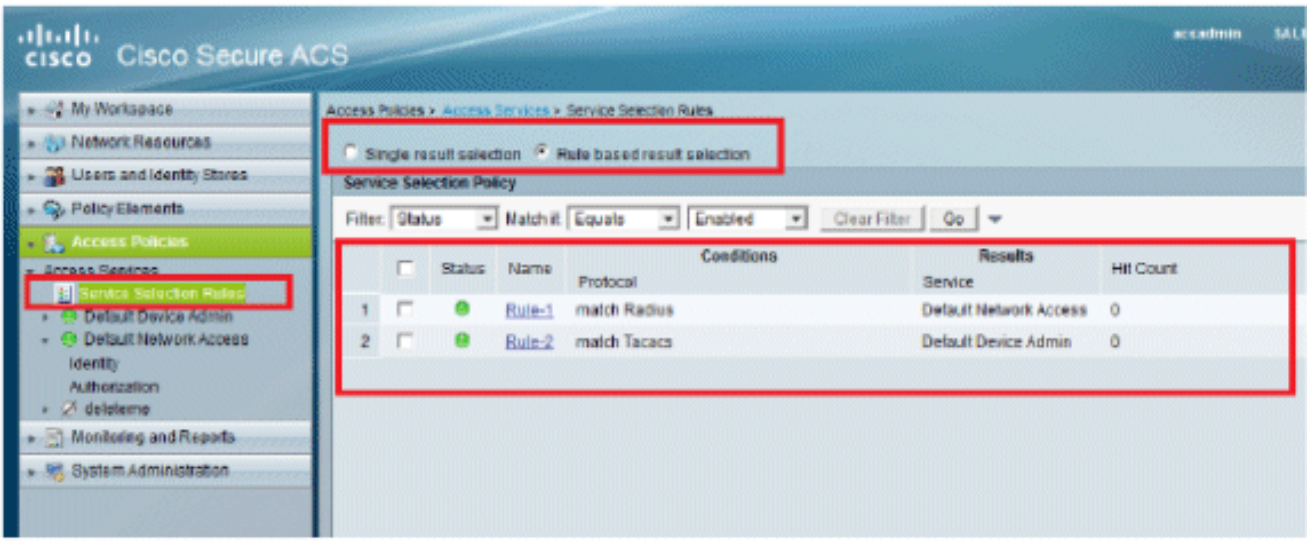
8. [Create] > [Rule-1] をクリックします。このルールは、グループ "LAP users" 内のユーザ向けです。



9. [Save Changes] をクリックします。条件と一致しないユーザを拒否する場合は、デフォルト ルールを「Deny Access」に編集します。



10. 最後の手順では、サービス選択ルールを定義します。このページは、着信要求に適用するサービスを決定する単純なポリシーまたはルール ベースのポリシーを設定する場合に使用します。例：



確認

802.1x がスイッチ ポートで有効になると、802.1x トラフィック以外のすべてのトラフィックがポートでブロックされます。WLC に登録されている LAP は、アソシエーションが解除されます。他のトラフィックは、802.1x 認証に成功した場合に限り、通過が許可されます。802.1x がスイッチ上で有効になった後、WLC に対して LAP の登録が成功したということは、LAP 認証が成功したことを示します。

AP コンソール：

<#root>

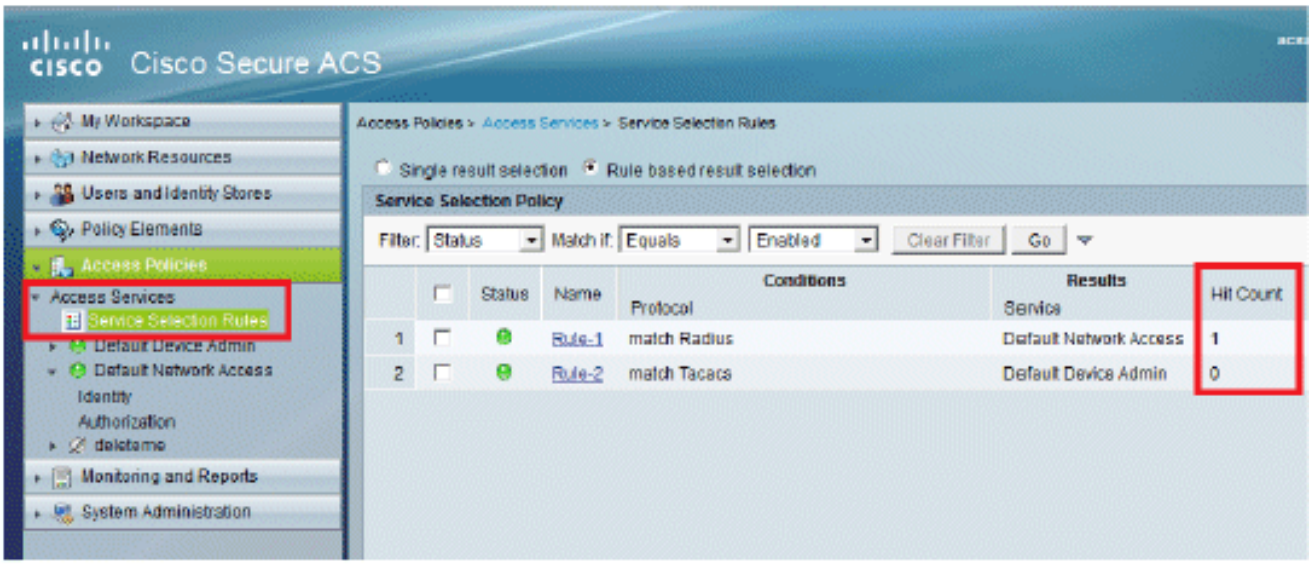
```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247

!--- AP disconnects upon adding dot1x information in the gig0/11.

*Jan 29 09:10:30.104: %WIDS-5-DISABLED: IDS Signature is removed and disabled.
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to DISCOVERY
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   administratively down
*Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   administratively down
*Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
Translating "CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25)
*Jan 29 09:10:36.203: status of voice_diag_test from WLC is false
```

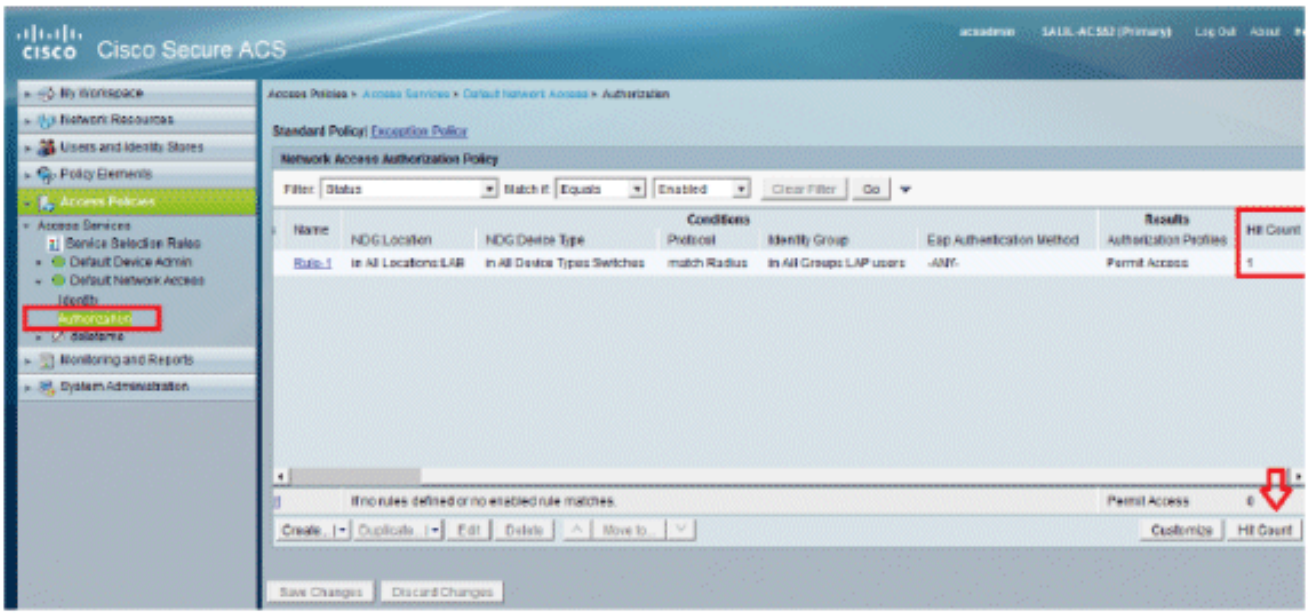
```
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST] *Jan 29

!--- Authentication is successful and the AP gets an IP.

Translating "CISCO-CAPWAP-CONTROLLER.Wlab"...domain server (192.168.150.25)
*Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent
   peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.000: %CAPWAP-5-CHANGED: CAPWAP changed state to
*Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS connection created
   successfully peer_ip: 192.168.75.44 peer_port: 5246
*Jan 29 09:11:37.578: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44

*Jan 29 09:11:37.578: %CAPWAP-5-CHANGED: CAPWAP changed state to JOIN


*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
   Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
   down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
   keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
   established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled

!--- AP joins the 5508-3 WLC.
```

ACS ログ：

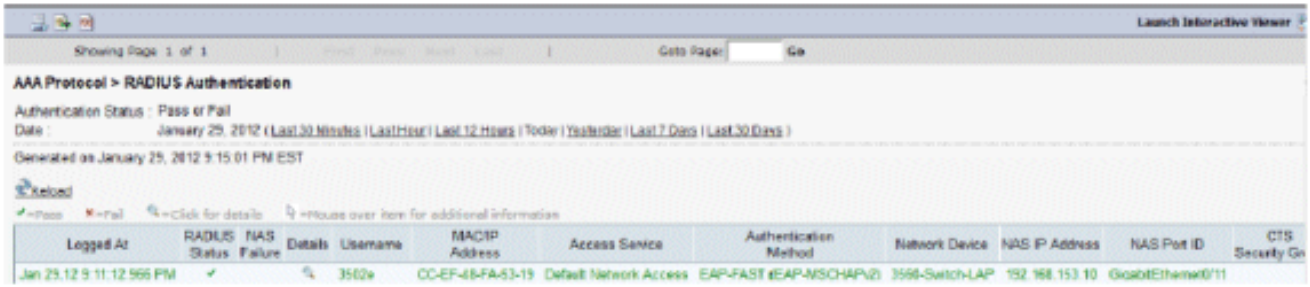
1. ヒット カウントを確認します。

   認証から 15 分以内にログを確認するときは、必ずヒット カウントを更新してください。同じページの下の方に、[Hit Count] タブがあります。





2. [Monitoring and Reports] をクリックすると、新たにポップアップ ウィンドウが表示されます。Authentications -RADIUS -Todayの順にクリックします。このほか、どのサービス選択ルールが適用されたかについては、[Details] をクリックすると確認できます。



トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Secure Access Control System
- テクニカル サポートとドキュメント - Cisco Systems

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。