

Konfigurieren von ACS 5.2 für die portbasierte Authentifizierung mit einer LAP

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konventionen](#)
[Hintergrundinformationen](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Annahmen](#)
[Konfigurationsschritte](#)
[Konfigurieren von LAP](#)
[Switch konfigurieren](#)
[Konfigurieren des RADIUS-Servers](#)
[Netzwerkressourcen konfigurieren](#)
[Benutzer konfigurieren](#)
[Definieren von Richtlinienelementen](#)
[Zugriffsrichtlinien anwenden](#)
[Überprüfung](#)
[Fehlerbehebung](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie ein Lightweight Access Point (LAP) als 802.1x-Komponente konfiguriert wird, um sich gegenüber einem RADIUS-Server wie einem Zugriffssteuerungsserver (ACS) 5.2 zu authentifizieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen, bevor Sie diese Konfiguration vornehmen:

- Grundkenntnisse der Wireless LAN Controller (WLC) und LAPs
- Besitzen funktionale Kenntnisse des AAA-Servers.
- Besitzen fundierte Kenntnisse über Wireless-Netzwerke und Wireless-Sicherheitsprobleme

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco 5508 WLC mit Firmware-Version 7.0.220.0
- Cisco Serie 3502 - LAP
- Cisco Secure ACS mit Version 5.2
- Cisco Switch der Serie 3560

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

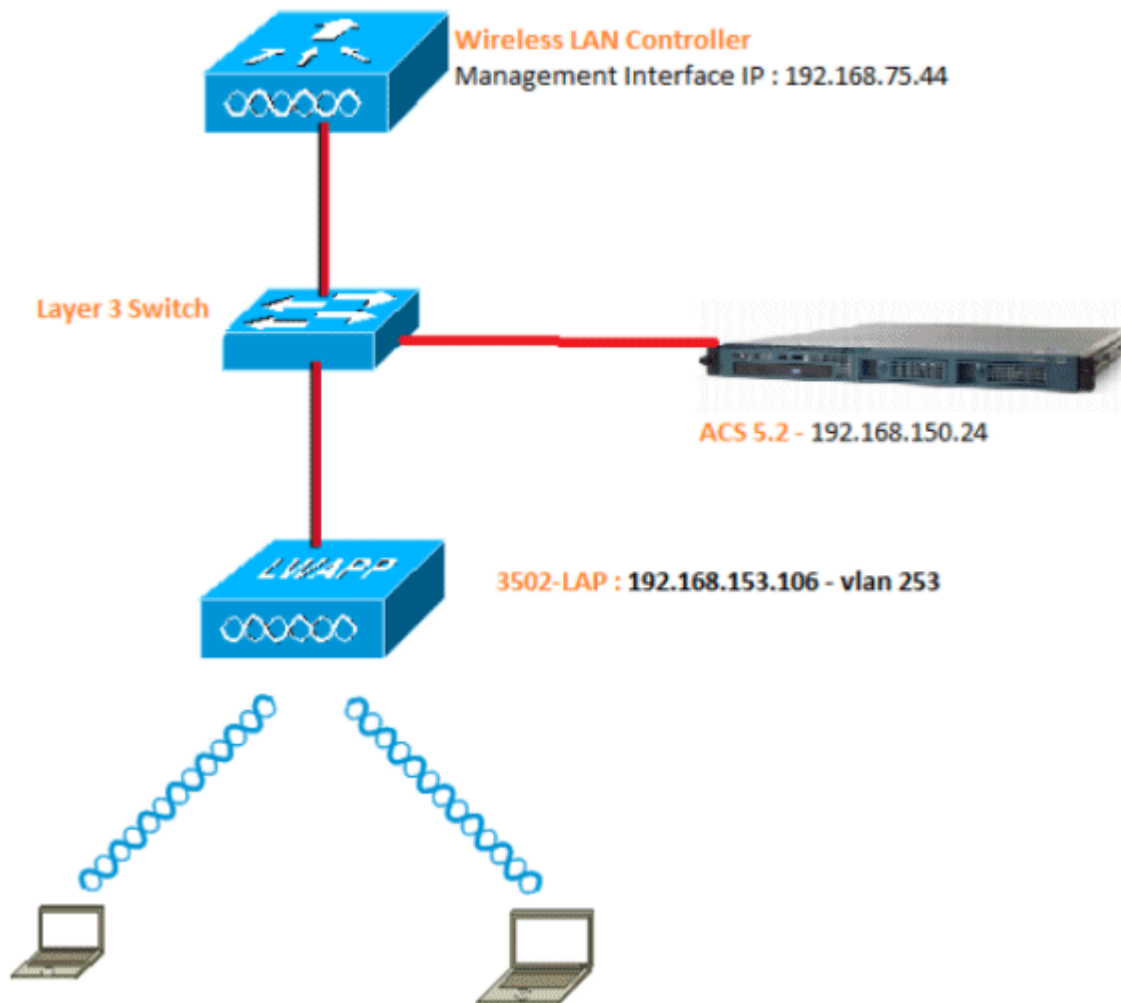
LAPs verfügen über werkseitig installierte X.509-Zertifikate, die von einem privaten Schlüssel signiert und zum Zeitpunkt der Herstellung in das Gerät eingebrannt werden. LAPs verwenden dieses Zertifikat, um sich beim Join-Prozess beim WLC zu authentifizieren. Diese Methode beschreibt eine andere Methode zur Authentifizierung von LAPs. Mit der WLC-Software können Sie die 802.1x-Authentifizierung zwischen einem Cisco Aironet Access Point (AP) und einem Cisco Switch konfigurieren. In diesem Fall fungiert der Access Point als 802.1x-Komponente und wird vom Switch über einen RADIUS-Server (ACS) authentifiziert, der EAP-FAST mit anonymer PAC-Bereitstellung verwendet. Nach der Konfiguration für die 802.1x-Authentifizierung lässt der Switch den Datenverkehr, der nicht 802.1x-Datenverkehr ist, erst über den Port zu, wenn sich das mit dem Port verbundene Gerät erfolgreich authentifiziert hat. Ein AP kann authentifiziert werden, bevor er einem WLC beitrifft, oder nachdem er einem WLC beigetreten ist. In diesem Fall konfigurieren Sie 802.1x auf dem Switch, nachdem der LAP dem WLC beigetreten ist.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Nachfolgend sind die Konfigurationsdetails der in diesem Diagramm verwendeten Komponenten aufgeführt:

- Die IP-Adresse des ACS (RADIUS)-Servers lautet 192.168.150.24.
- Die Management- und AP-Manager-Schnittstellenadresse des WLC lautet 192.168.75.44.
- Die DHCP-Server-Adresse lautet 192.168.150.25.
- Die LAP wird in VLAN 253 platziert.
- VLAN 253: 192.168.153.x/24 Gateway: +192 168 153 10
- VLAN 75: 192.168.75.x/24 Gateway: 192.168.75.1

Annahmen

- Switches werden für alle Layer-3-VLANs konfiguriert.
- Dem DHCP-Server wird ein DHCP-Bereich zugewiesen.
- Zwischen allen Geräten im Netzwerk bestehen Layer-3-Verbindungen.
- Die LAP ist bereits mit dem WLC verbunden.
- Jedes VLAN hat eine /24-Maske.

- In ACS 5.2 ist ein selbstsigniertes Zertifikat installiert.

Konfigurationsschritte

Diese Konfiguration ist in drei Kategorien unterteilt:

1. [Konfigurieren der LAP](#)
2. [Konfigurieren Sie den Switch.](#)
3. [Konfigurieren Sie den RADIUS-Server.](#)

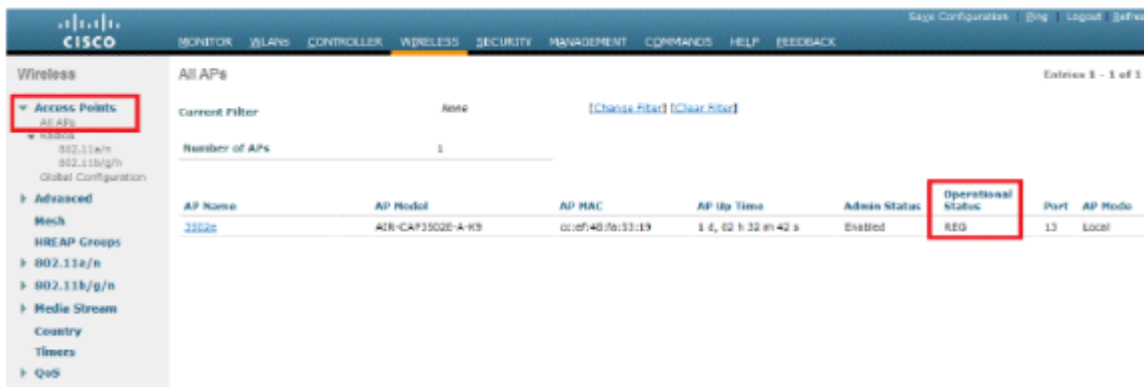
Konfigurieren von LAP

Annahmen:

LAP ist bereits mithilfe von Option 43, DNS, oder der statisch konfigurierten WLC-Verwaltungsschnittstellen-IP beim WLC registriert.

Führen Sie diese Schritte aus:

1. Gehen Sie zu **Wireless > Access Points > All APs**, um die LAP-Registrierung auf dem WLC zu überprüfen.

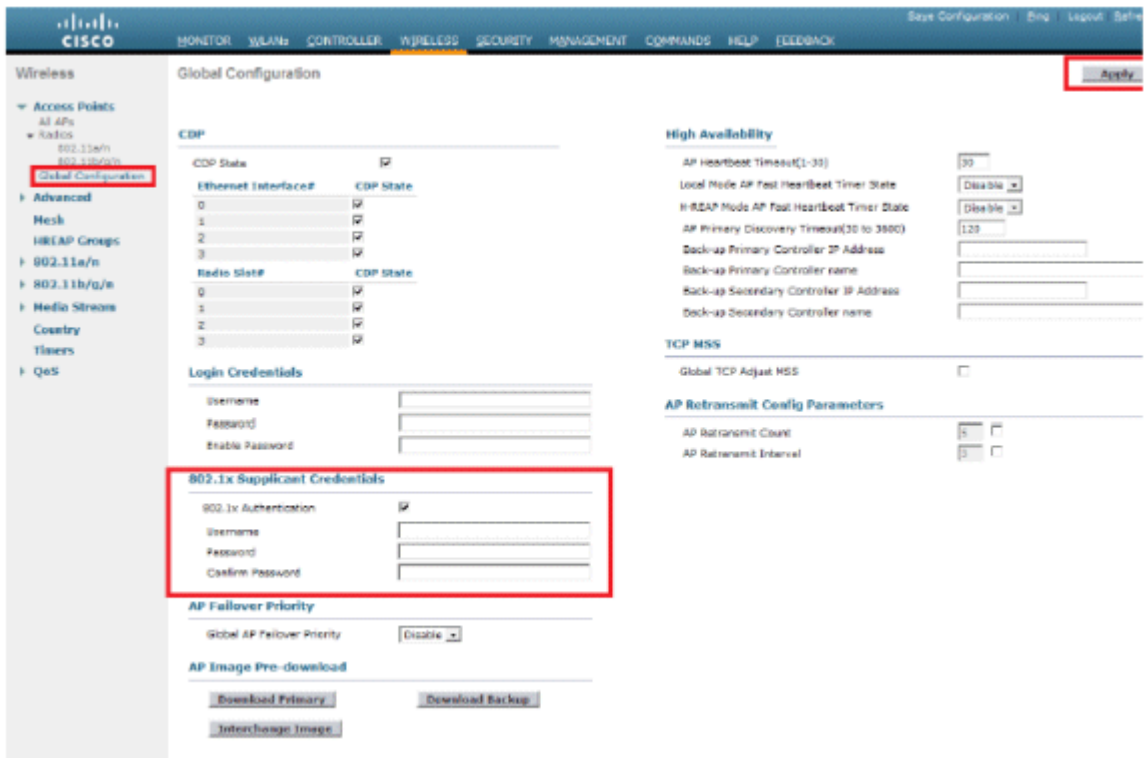


AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
3302e	AIR-CT5502E-A-K9	cc:ef:48:7a:51:19	1 d, 02 h 32 m 42 s	Enabled	REG	13	Local

2. Sie haben zwei Möglichkeiten, die 802.1x-Anmeldedaten (d. h. Benutzername/Kennwort) für alle LAPs zu konfigurieren:

- **Global**

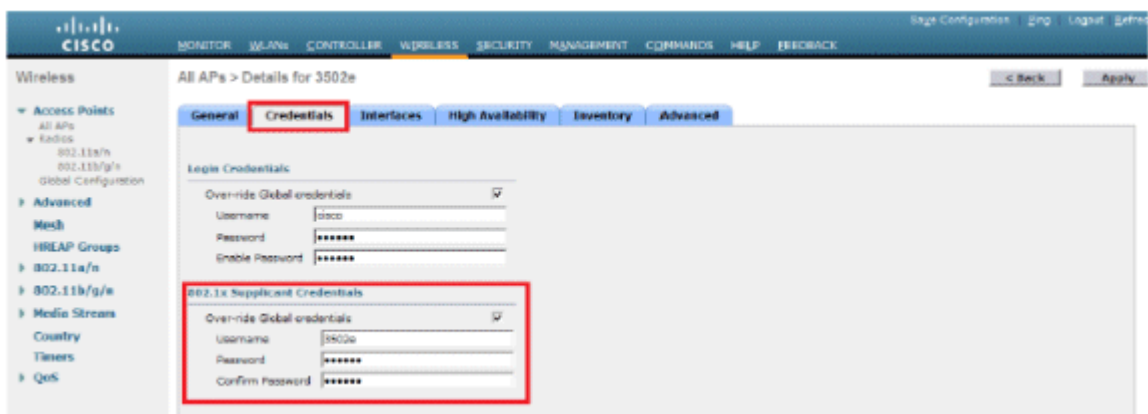
Bei einem bereits verbundenen LAP können Sie die Anmeldeinformationen global festlegen, sodass jeder dem WLC beitretende LAP diese Anmeldeinformationen übernimmt.



- **Individuell**

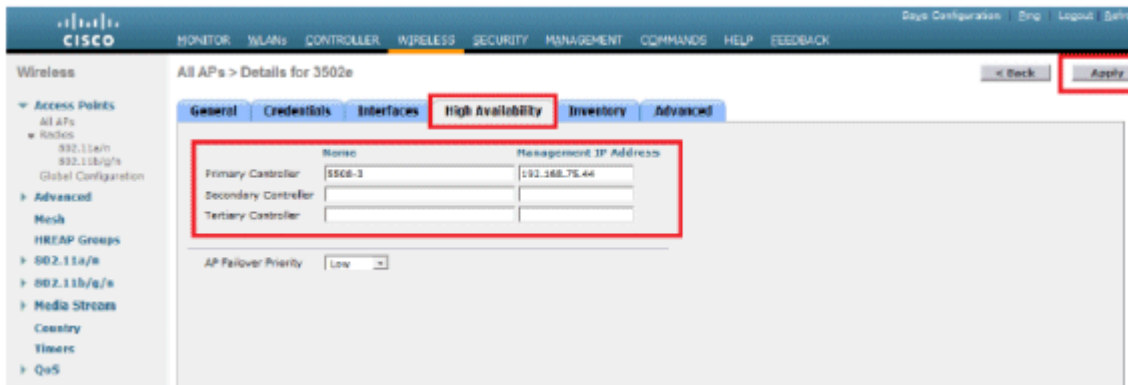
Konfigurieren von 802.1 x-Profilen pro AP In unserem Beispiel werden Anmeldeinformationen pro Access Point konfiguriert.

- Gehen Sie zu **Wireless > All APs**, und wählen Sie den betreffenden Access Point aus.
- Fügen Sie den Benutzernamen und das Kennwort in den Feldern **für die 802.1x-Anmeldeinformationen für die Komponente hinzu**.



Hinweis: Anmeldeinformationen werden für Telnet, SSH oder die Konsole beim AP verwendet.

- Konfigurieren Sie den Abschnitt "Hohe Verfügbarkeit", und klicken Sie auf **Anwenden**.



Hinweis: Nach dem Speichern werden diese Anmeldeinformationen im gesamten WLC beibehalten, und der Access Point wird neu gestartet. Die Anmeldeinformationen ändern sich nur, wenn der LAP einem neuen WLC beitrifft. Die LAP übernimmt den Benutzernamen und das Kennwort, die auf dem neuen WLC konfiguriert wurden.

Wenn der Access Point noch keinem WLC beigetreten ist, müssen Sie in der LAP eine Konsole einrichten, um die Anmeldeinformationen festzulegen. Geben Sie diesen CLI-Befehl im privilegierten Modus ein:

LAP#lwapp ap dot1x Benutzername <Benutzername> Kennwort <Kennwort>

Oder

LAP#capwap ap dot1x Benutzername <Benutzername> Kennwort <Kennwort>

Hinweis: Dieser Befehl steht nur für APs zur Verfügung, die das Wiederherstellungs-Image ausführen.

Der Standardbenutzername und das Standardkennwort für die LAP sind `cisco` und `Cisco`.

Switch konfigurieren

Der Switch fungiert als Authentifizierer für die LAP und authentifiziert die LAP über einen RADIUS-Server. Wenn der Switch nicht über die entsprechende Software verfügt, führen Sie ein Upgrade des Switches durch. Geben Sie in der Switch-CLI die folgenden Befehle ein, um die 802.1x-Authentifizierung an einem Switch-Port zu aktivieren:

```
<#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.

Hinweis: Wenn sich auf demselben Switch andere APs befinden, die 802.1x nicht verwenden sollen, können Sie den Port für 802.1x entweder unkonfiguriert lassen oder den folgenden Befehl ausführen:

```
<#root>
```

```
switch(config-if)authentication port-control force-authorized
```

Konfigurieren des RADIUS-Servers

LAP wird mit EAP-FAST authentifiziert. Stellen Sie sicher, dass der verwendete RADIUS-Server diese EAP-Methode unterstützt, wenn Sie Cisco ACS 5.2 nicht verwenden.

Die Konfiguration des RADIUS-Servers ist in vier Schritte unterteilt:

1. [Netzwerkressourcen konfigurieren](#)
2. [Konfigurieren Sie Benutzer.](#)
3. [Definieren Sie Richtlinienelemente.](#)
4. [Wenden Sie Zugriffsrichtlinien an.](#)

ACS 5.x ist ein richtlinienbasierter ACS. Anders ausgedrückt: ACS 5.x verwendet ein regelbasiertes Richtlinienmodell anstelle des in Version 4.x verwendeten gruppenbasierten Modells.

Das regelbasierte ACS 5.x-Richtlinienmodell bietet im Vergleich zum älteren gruppenbasierten Ansatz eine leistungstärkere und flexiblere Zugriffskontrolle.

Im älteren gruppenbasierten Modell definiert eine Gruppe eine Richtlinie, da sie drei Informationstypen enthält und miteinander verknüpft:

- **Identitätsinformationen** - Diese Informationen können auf der Mitgliedschaft in AD- oder LDAP-Gruppen oder einer statischen Zuweisung für interne ACS-Benutzer basieren.
- **Andere Einschränkungen oder Bedingungen** - Zeitbeschränkungen, Gerätebeschränkungen usw.
- **Berechtigungen** - VLANs oder Cisco IOS[®]-Berechtigungsebenen

Das ACS 5.x-Richtlinienmodell basiert auf folgenden Regeln:

Wenn Bedingung dann Ergebnis

Wir verwenden z. B. die für das gruppenbasierte Modell beschriebenen Informationen:

Wenn Identität-Bedingung, Restriktionsbedingung dann Autorisierungsprofil.

Dies gibt uns die Flexibilität, die Bedingungen, unter denen der Benutzer auf das Netz zugreifen darf, und auch die Berechtigungsstufe, die erlaubt ist, wenn bestimmte Bedingungen erfüllt sind, zu begrenzen.

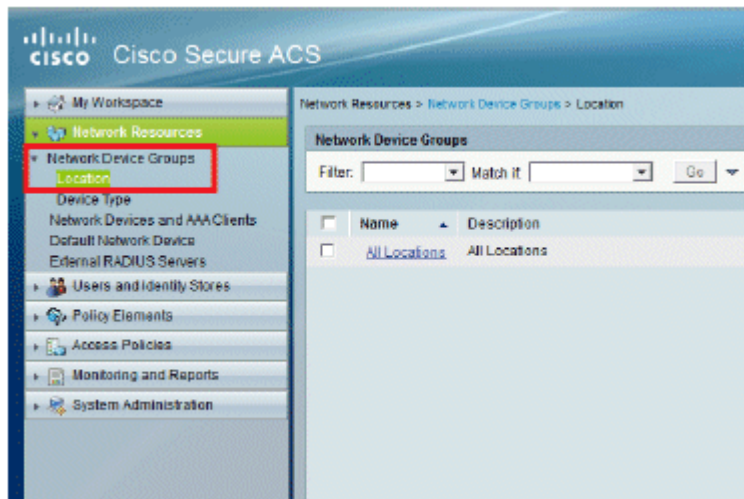
Netzwerkressourcen konfigurieren

In diesem Abschnitt wird der AAA-Client für den Switch auf dem RADIUS-Server konfiguriert.

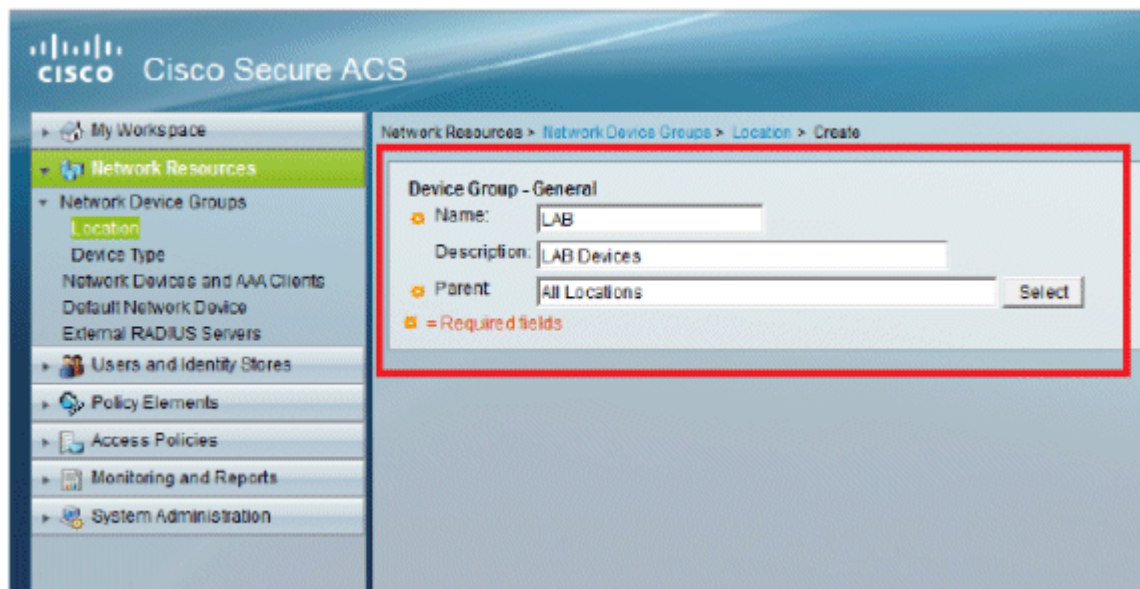
In diesem Verfahren wird erläutert, wie der Switch als AAA-Client auf dem RADIUS-Server hinzugefügt wird, damit der Switch die Benutzeranmeldeinformationen der LAP an den RADIUS-Server weitergeben kann.

Führen Sie diese Schritte aus:

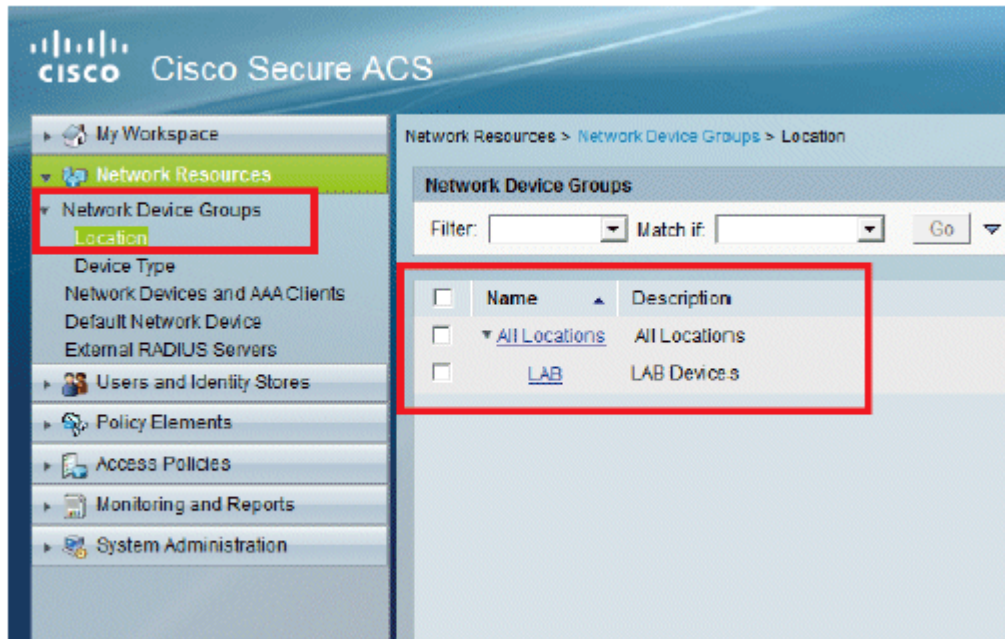
1. Klicken Sie in der ACS-GUI auf **Netzwerkressourcen**.
2. Klicken Sie auf **Netzwerkgerätegruppen**.
3. Gehen Sie zu **Location > Create** (unten).



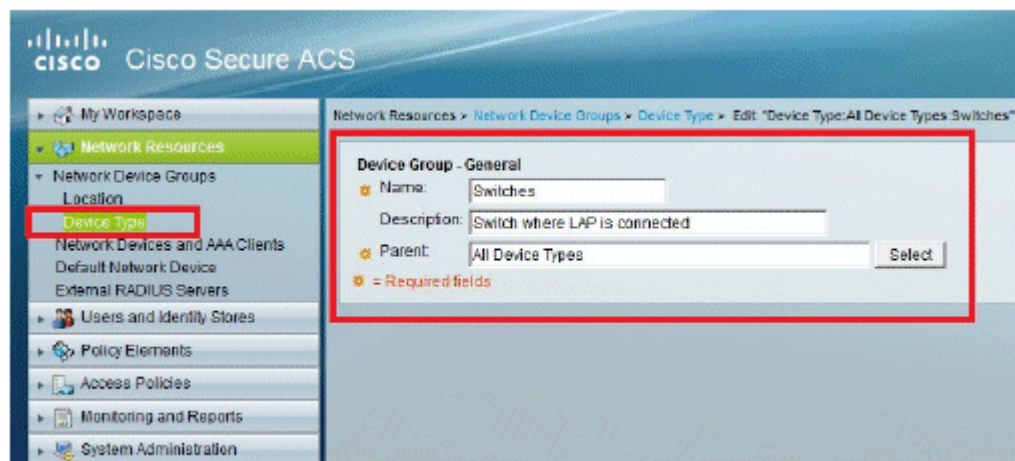
4. Fügen Sie die erforderlichen Felder hinzu, und klicken Sie auf **Senden**.



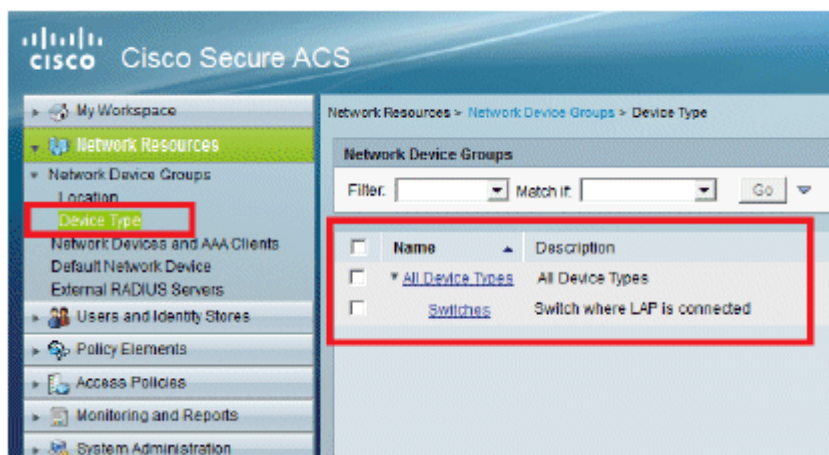
5. Das Fenster wird aktualisiert:



6. Klicken Sie auf **Gerätetyp** > **Erstellen**.

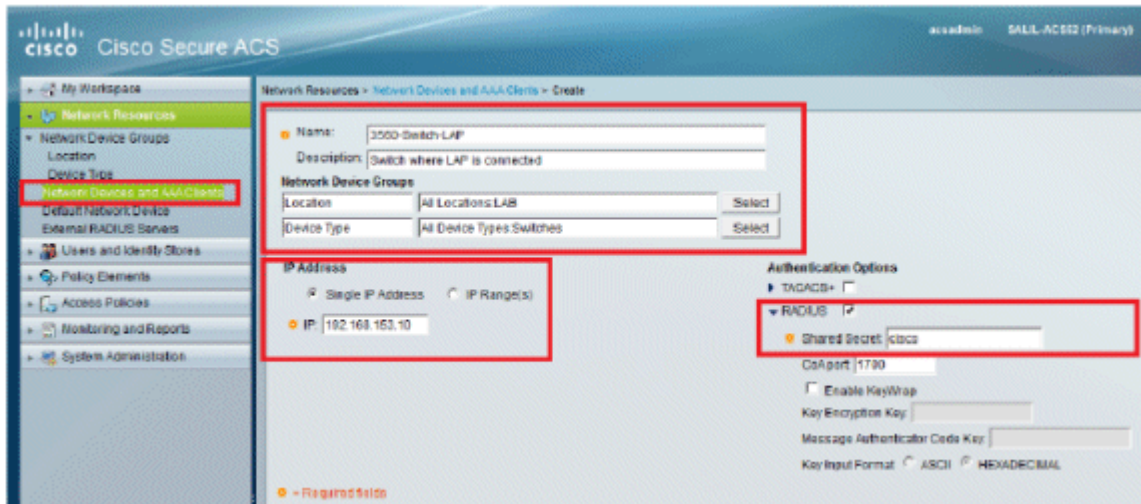


7. Klicken Sie auf **Senden**. Nach Abschluss des Vorgangs wird das Fenster aktualisiert:

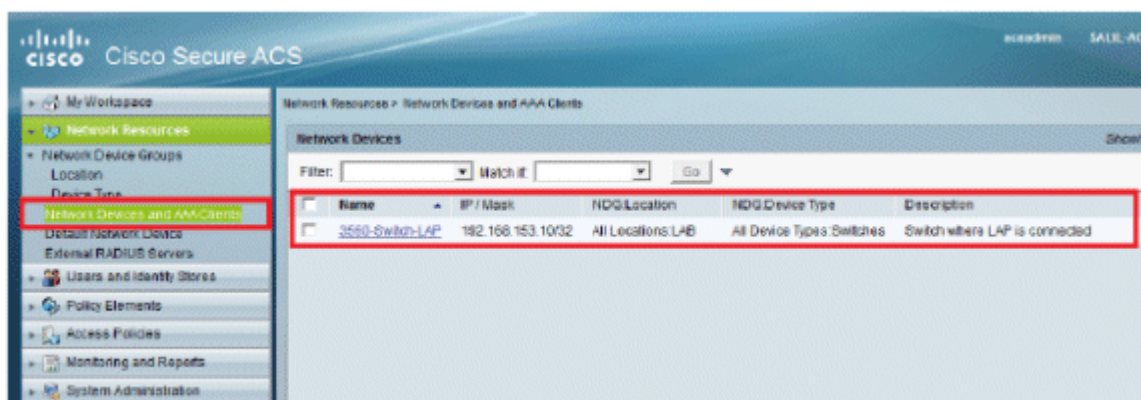


8. Gehen Sie zu **Network Resources** > **Network Devices and AAA Clients**.

9. Klicken Sie auf **Erstellen**, und geben Sie die hier abgebildeten Details ein:



10. Klicken Sie auf **Senden**. Das Fenster wird aktualisiert:

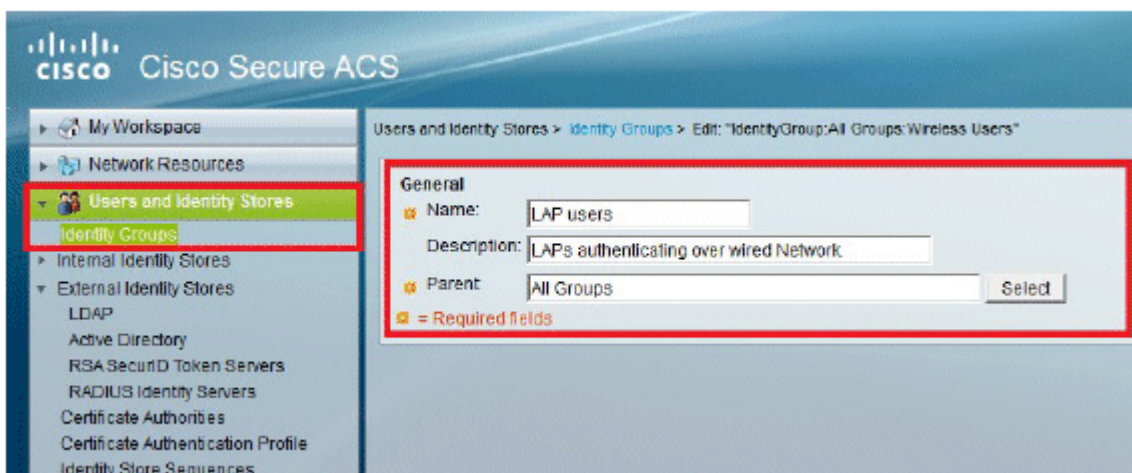


Benutzer konfigurieren

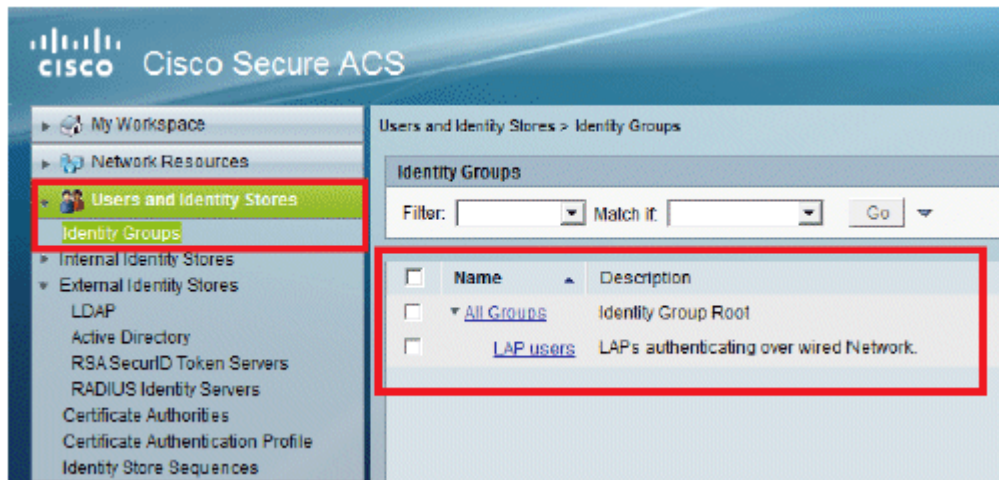
In diesem Abschnitt erfahren Sie, wie Sie einen Benutzer auf dem zuvor konfigurierten ACS erstellen. Sie weisen den Benutzer einer Gruppe mit der Bezeichnung "LAP-Benutzer" zu.

Führen Sie diese Schritte aus:

1. Gehen Sie zu **Benutzer und Identitätsdaten > Identitätsgruppen > Erstellen**.

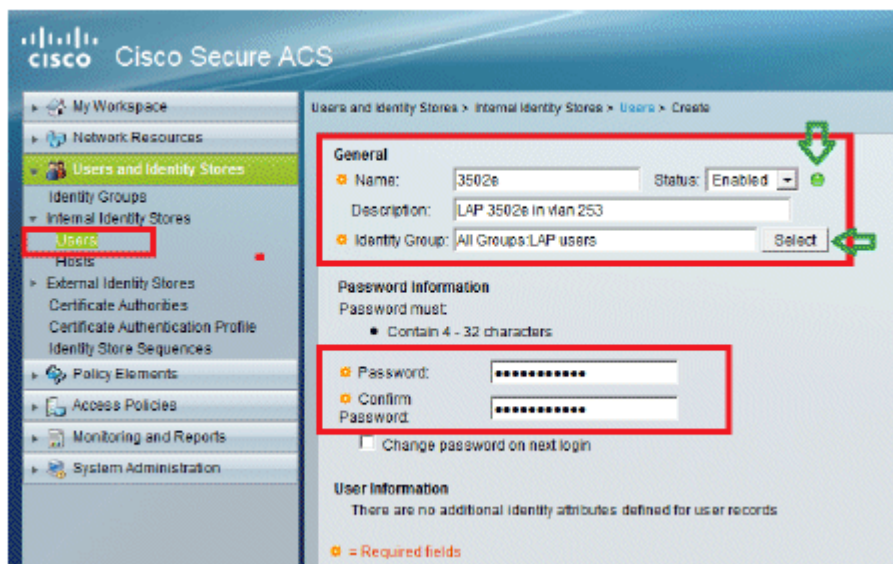


2. Klicken Sie auf **Senden**.

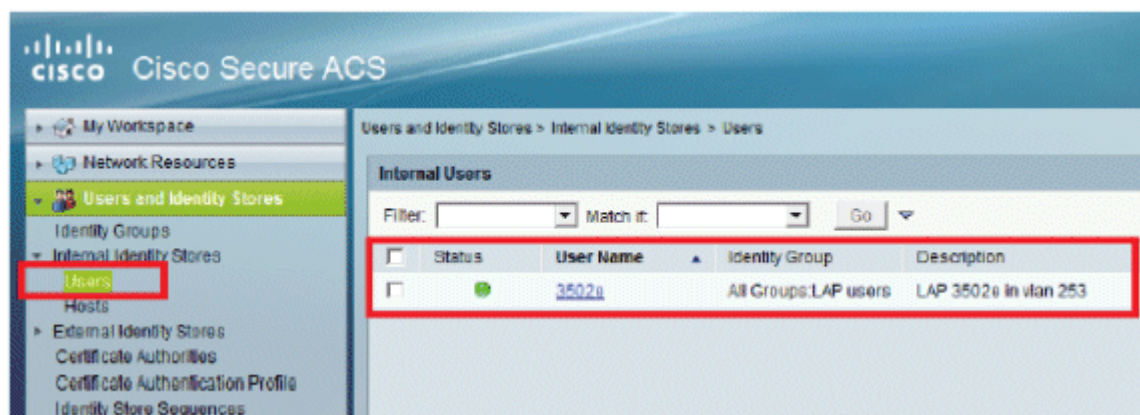


3. Erstellen Sie **3502e**, und weisen Sie es der Gruppe "LAP-Benutzer" zu.

4. Gehen Sie zu **Benutzer und Identitätsdaten** > **Identitätsgruppen** > **Benutzer** > **Erstellen**.

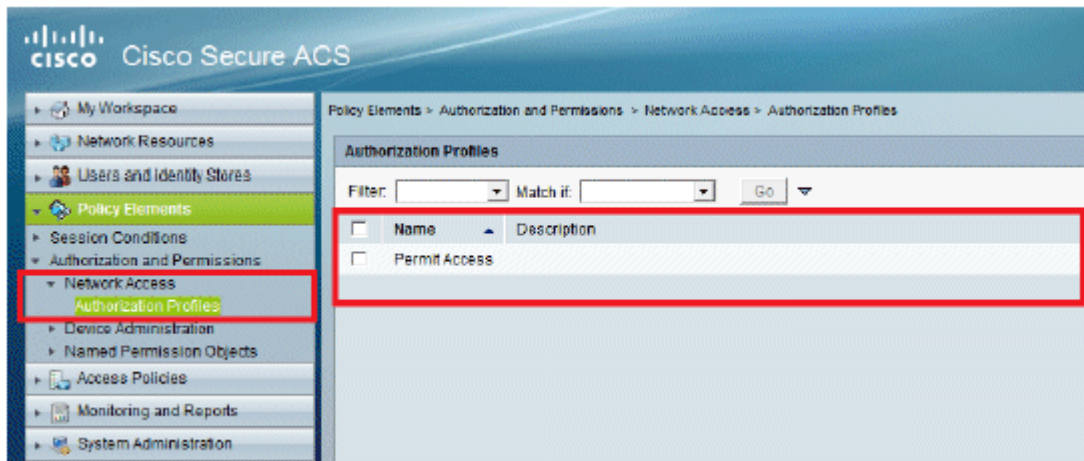


5. Die aktualisierten Informationen werden angezeigt:



Definieren von Richtlinienelementen

Überprüfen Sie, ob **Zugriffsberechtigung** festgelegt ist.

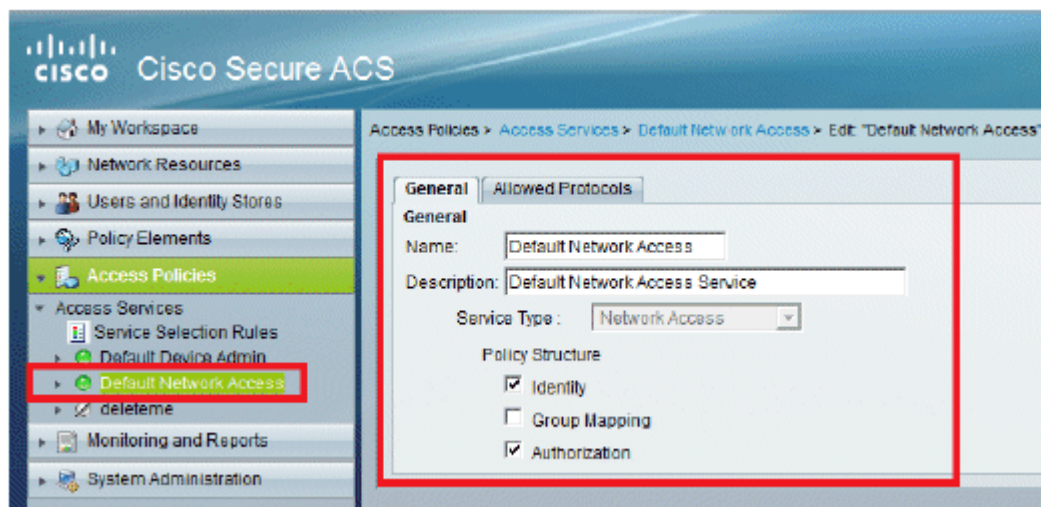


Zugriffsrichtlinien anwenden

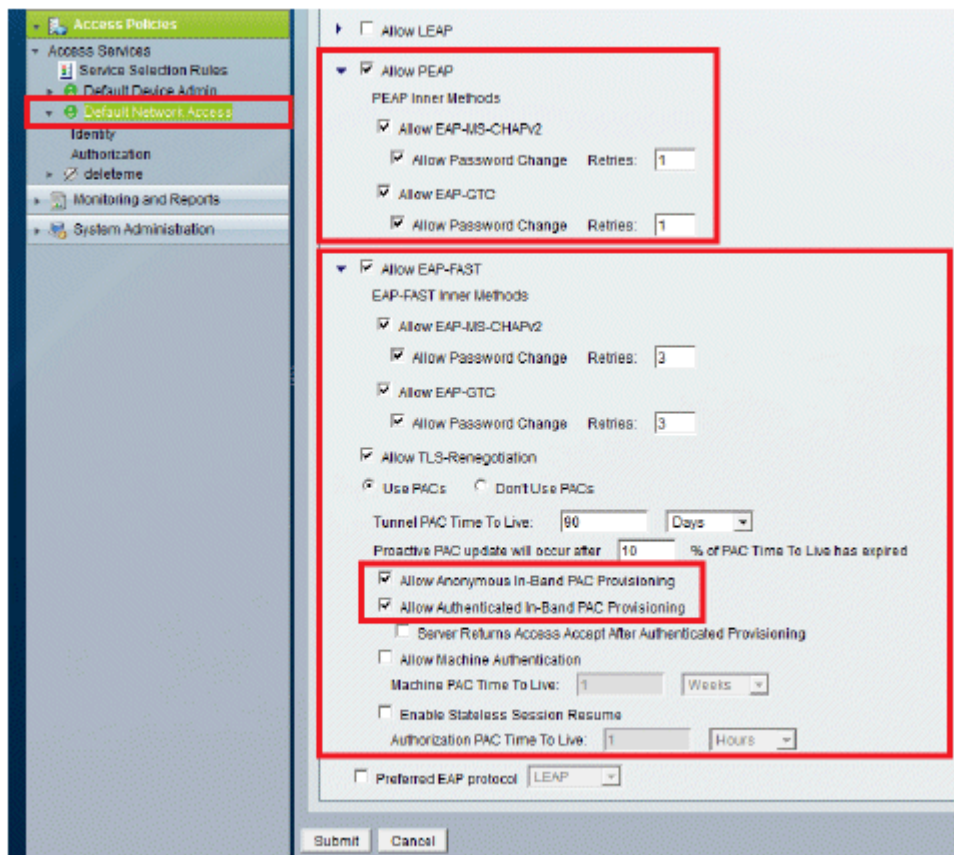
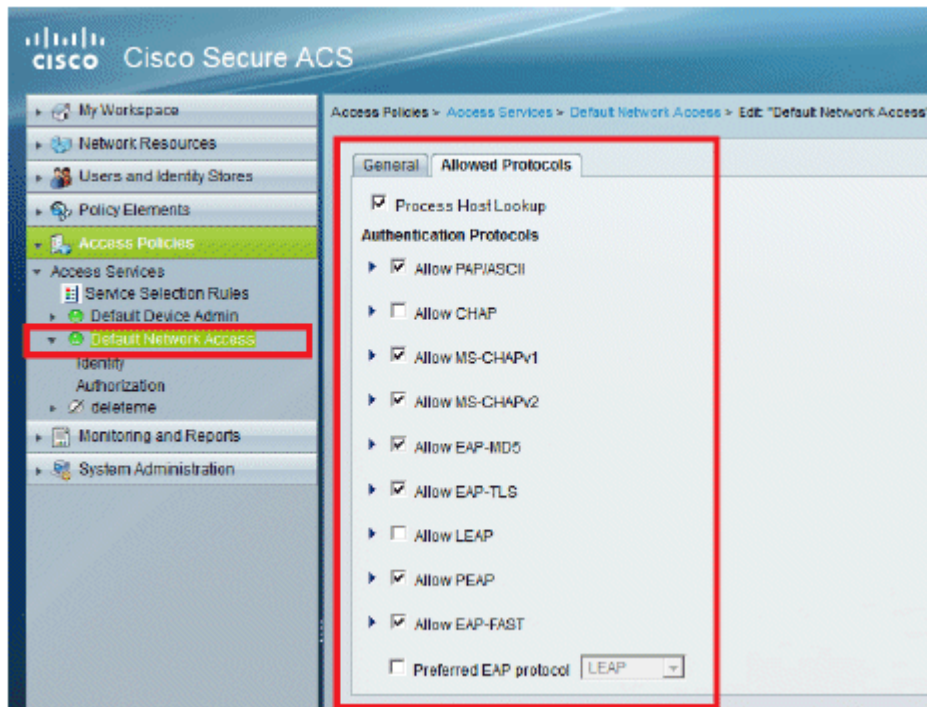
In diesem Abschnitt wählen Sie EAP-FAST als Authentifizierungsmethode für LAPs für die Authentifizierung aus. Anschließend erstellen Sie Regeln, die auf den vorherigen Schritten basieren.

Führen Sie diese Schritte aus:

1. Gehen Sie zu **Zugriffsrichtlinien > Zugriffsdienste > Standard-Netzwerkzugriff > Bearbeiten: "Standard-Netzwerkzugriff"**.

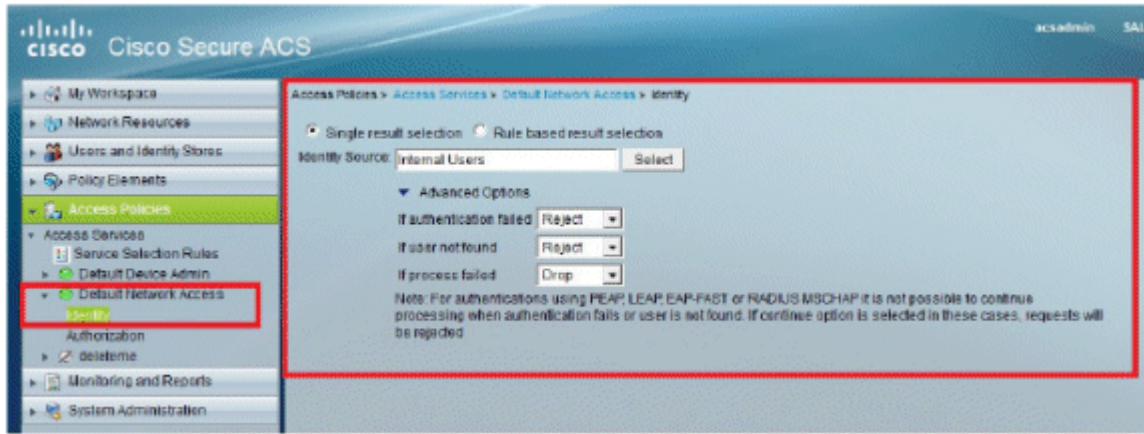


2. Stellen Sie sicher, dass Sie die **EAP-FAST-** und die **anonyme In-Band-PAC-Bereitstellung** aktiviert haben.



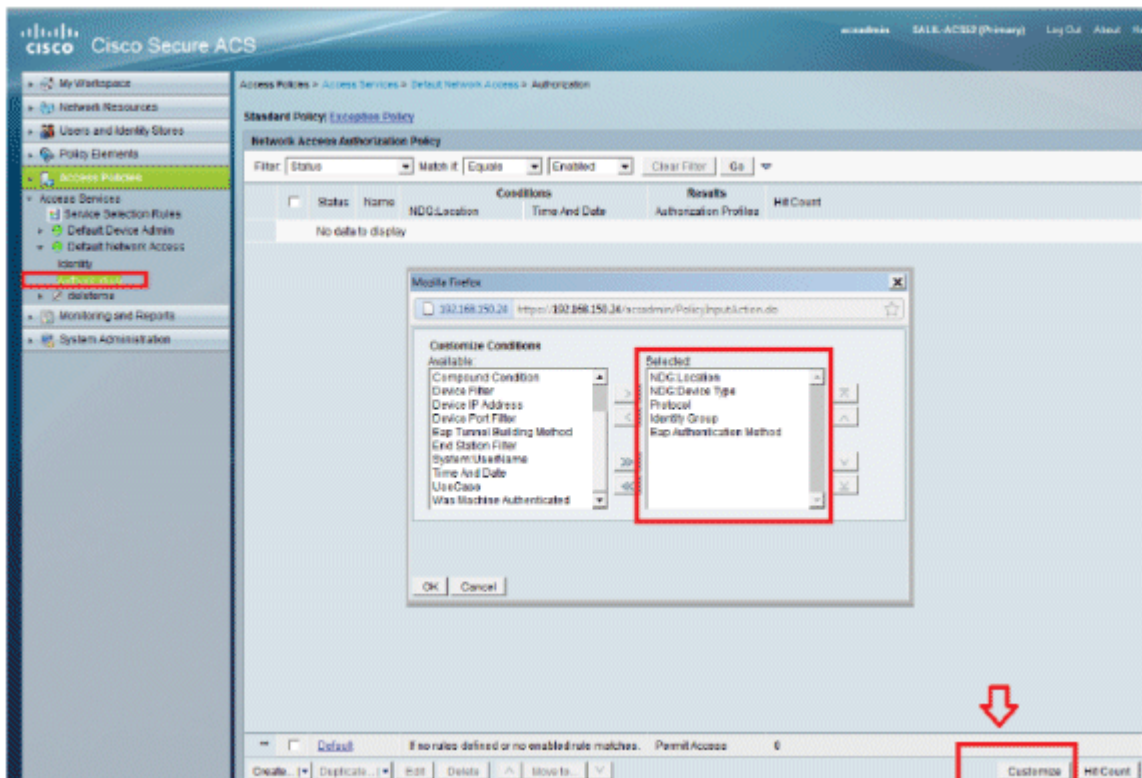
3. Klicken Sie auf **Senden**.

4. Überprüfen Sie die ausgewählte Identitätsgruppe. Verwenden Sie in diesem Beispiel **Internal Users** (die auf dem ACS erstellt wurde), und speichern Sie die Änderungen.

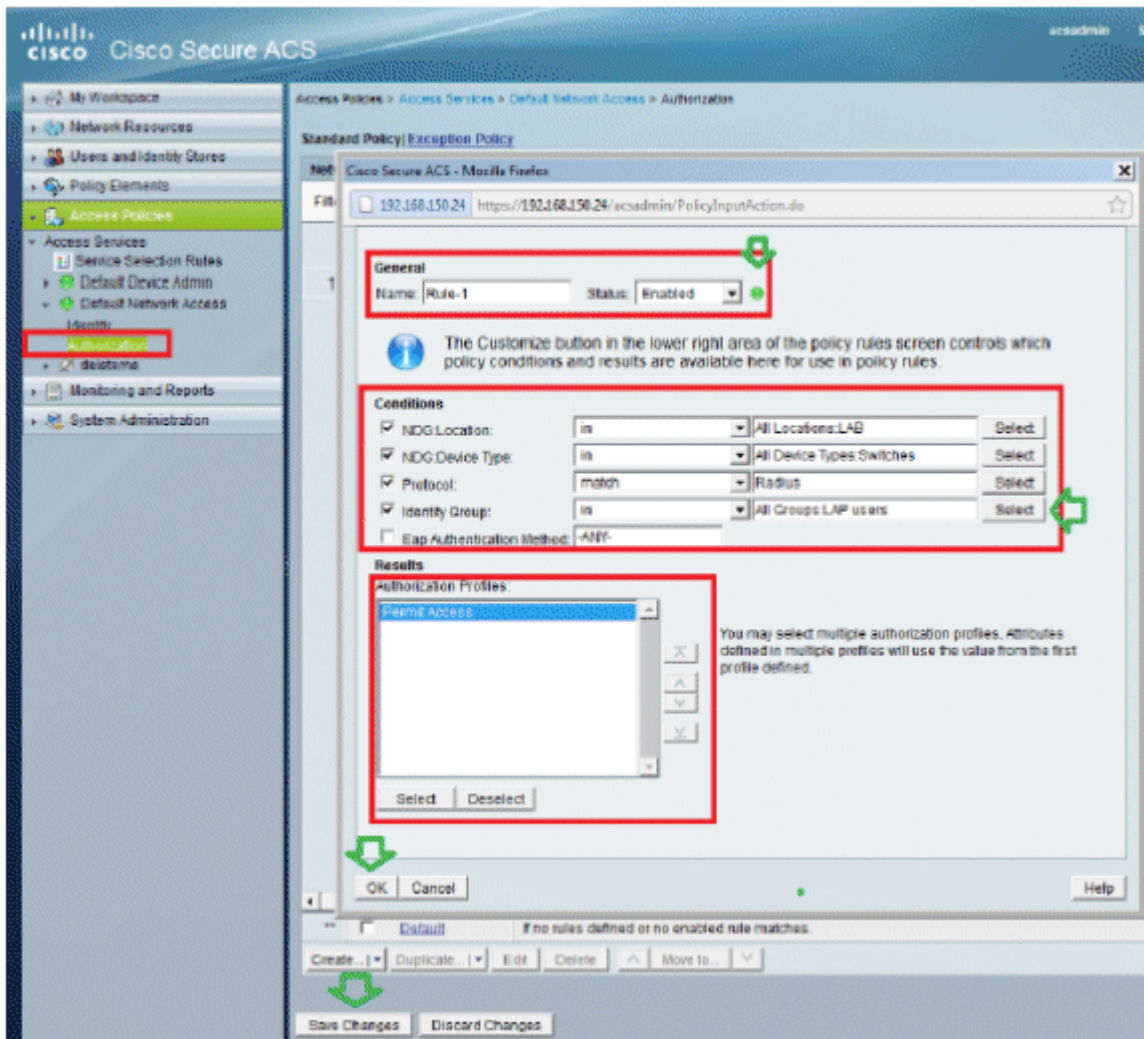


5. Gehen Sie zu **Access Policies > Access Services > Default Network Access > Authorization**, um das Autorisierungsprofil zu überprüfen.

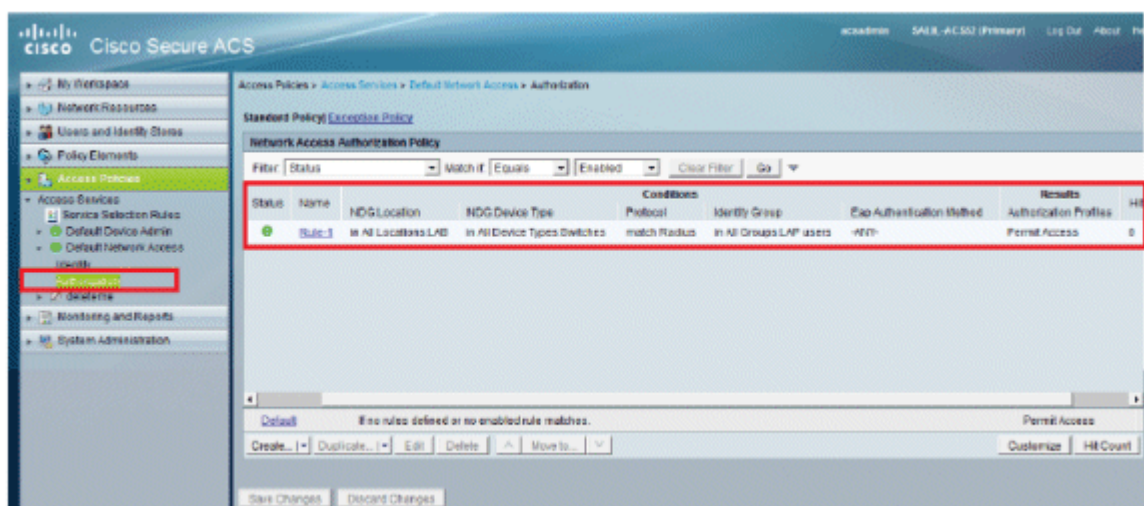
Sie können festlegen, unter welchen Bedingungen Sie einem Benutzer Zugriff auf das Netzwerk gewähren und welches Autorisierungsprofil (Attribute) Sie nach der Authentifizierung weitergeben. Diese Granularität ist nur in ACS 5.x verfügbar. In diesem Beispiel werden **Location, Device Type, Protocol, Identity Group** und **EAP Authentication Method** ausgewählt.



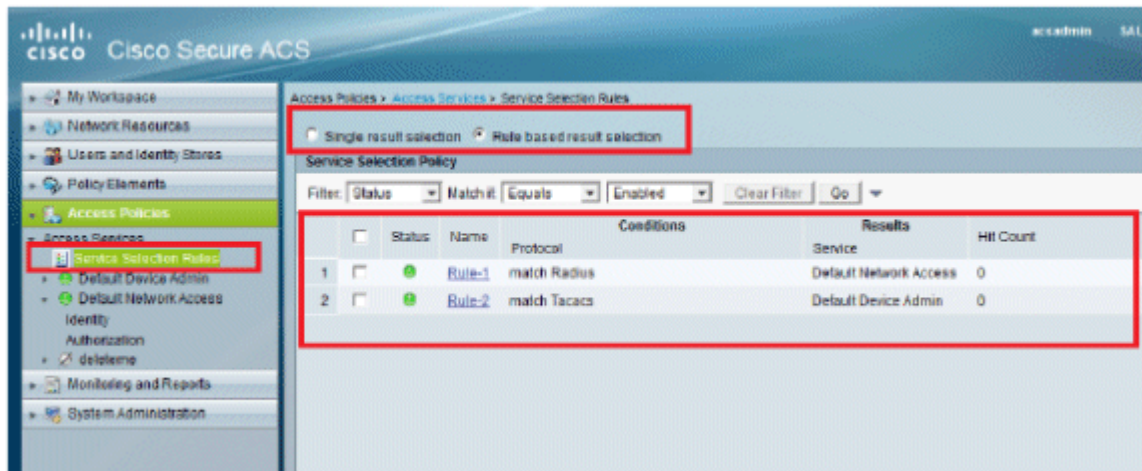
6. Klicken Sie auf **OK**, und **speichern Sie die Änderungen**.
7. Der nächste Schritt ist das Erstellen einer Regel. Wenn keine Regeln definiert sind, wird LAP der Zugriff ohne Bedingungen gewährt.
8. Klicken Sie auf **Erstellen > Regel-1**. Diese Regel ist für Benutzer in der Gruppe "LAP-Benutzer".



9. Klicken Sie auf **Änderungen speichern**. Wenn Benutzer, die nicht den Bedingungen entsprechen, abgelehnt werden sollen, ändern Sie die Standardregel so, dass "Zugriff verweigern" angezeigt wird.



10. Der letzte Schritt besteht in der Definition von Serviceauswahlregeln. Auf dieser Seite können Sie eine einfache oder regelbasierte Richtlinie konfigurieren, um zu bestimmen, welcher Service auf eingehende Anfragen angewendet werden soll. Beispiele:



Überprüfung

Sobald 802.1x auf dem Switch-Port aktiviert ist, wird der gesamte Datenverkehr über diesen Port blockiert, mit Ausnahme des 802.1x-Datenverkehrs. Die LAP, die bereits beim WLC registriert ist, wird getrennt. Erst nach einer erfolgreichen 802.1x-Authentifizierung wird der andere Datenverkehr zugelassen. Wenn die LAP erfolgreich beim WLC registriert wurde, nachdem 802.1x auf dem Switch aktiviert wurde, ist die LAP-Authentifizierung erfolgreich.

AP-Konsole:

```
<#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

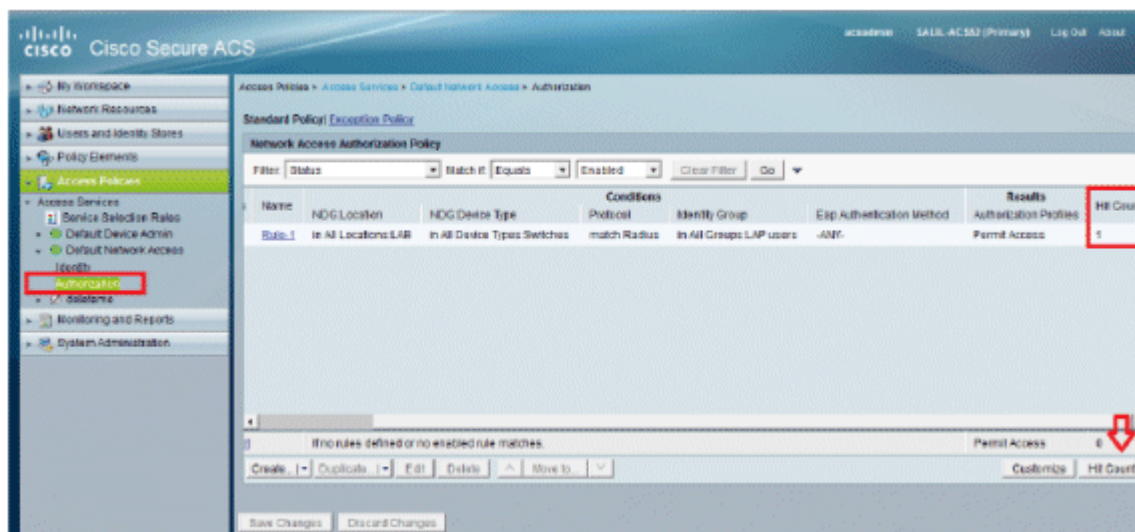
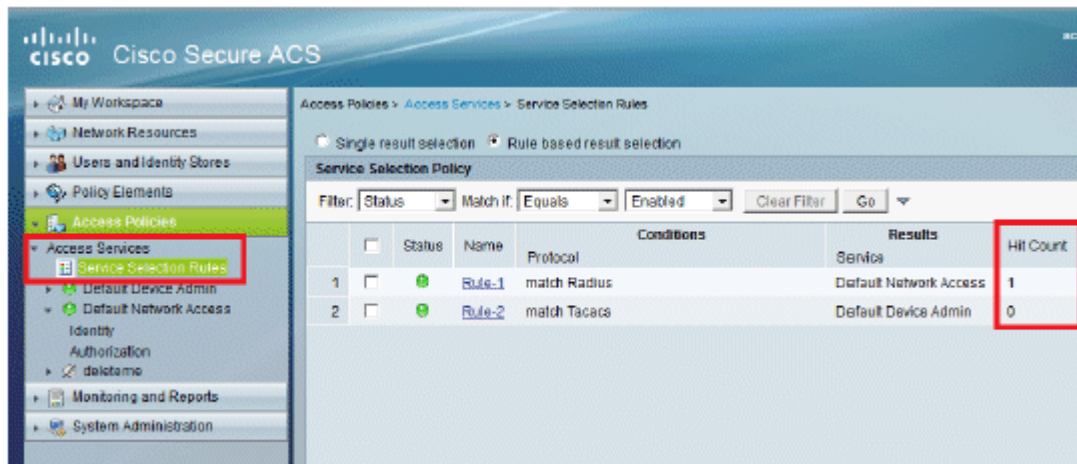
*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
  down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
  reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: 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.

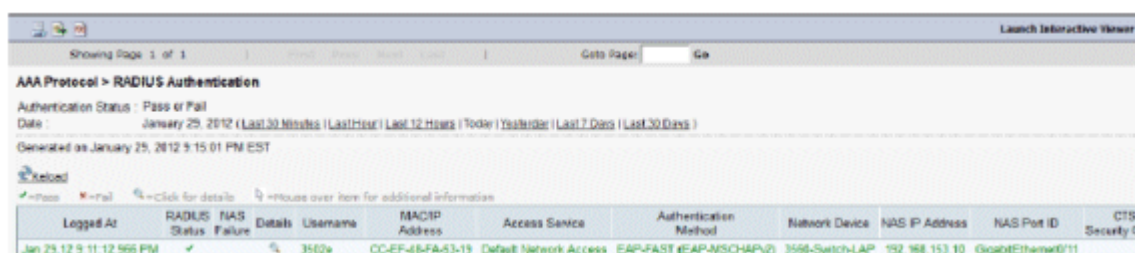
ACS-Protokolle:

1. Anzeige der Trefferanzahl:

Wenn Sie Protokolle innerhalb von 15 Minuten nach der Authentifizierung überprüfen, stellen Sie sicher, dass Sie die Trefferanzahl aktualisieren. Auf derselben Seite befindet sich unten die Registerkarte **Hit Count (Trefferanzahl)**.



2. Klicken Sie auf **Überwachung und Berichte**, um ein neues Popup-Fenster zu öffnen. Klicken Sie auf **Authentifizierungen -RADIUS -Heute**. Sie können auch auf **Details** klicken, um zu überprüfen, welche Serviceauswahlregel angewendet wurde.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- [Cisco Secure Access Control System](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.