

Configurar o ACS 5.2 para autenticação baseada em porta com um LAP

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Hipóteses](#)

[Configuration Steps](#)

[Configurar LAP](#)

[Configurar o switch](#)

[Configurar servidor RADIUS](#)

[Configurar recursos de rede](#)

[Configurar usuários](#)

[Definir Elementos da Política](#)

[Aplicar políticas de acesso](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como configurar um Lightweight Access Point (LAP) como um solicitante 802.1x para autenticar em um servidor RADIUS, como um Access Control Server (ACS) 5.2.

[Prerequisites](#)

[Requirements](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Ter conhecimento básico da controladora Wireless LAN (WLC) e dos LAPs.
- Ter conhecimento funcional do servidor AAA.
- Ter conhecimento completo das redes wireless e das questões de segurança wireless.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- WLC Cisco 5508 com firmware versão 7.0.220.0
- LAP Cisco 3502 Series
- Cisco Secure ACS que executa a versão 5.2
- Switch Cisco Série 3560

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

Informações de Apoio

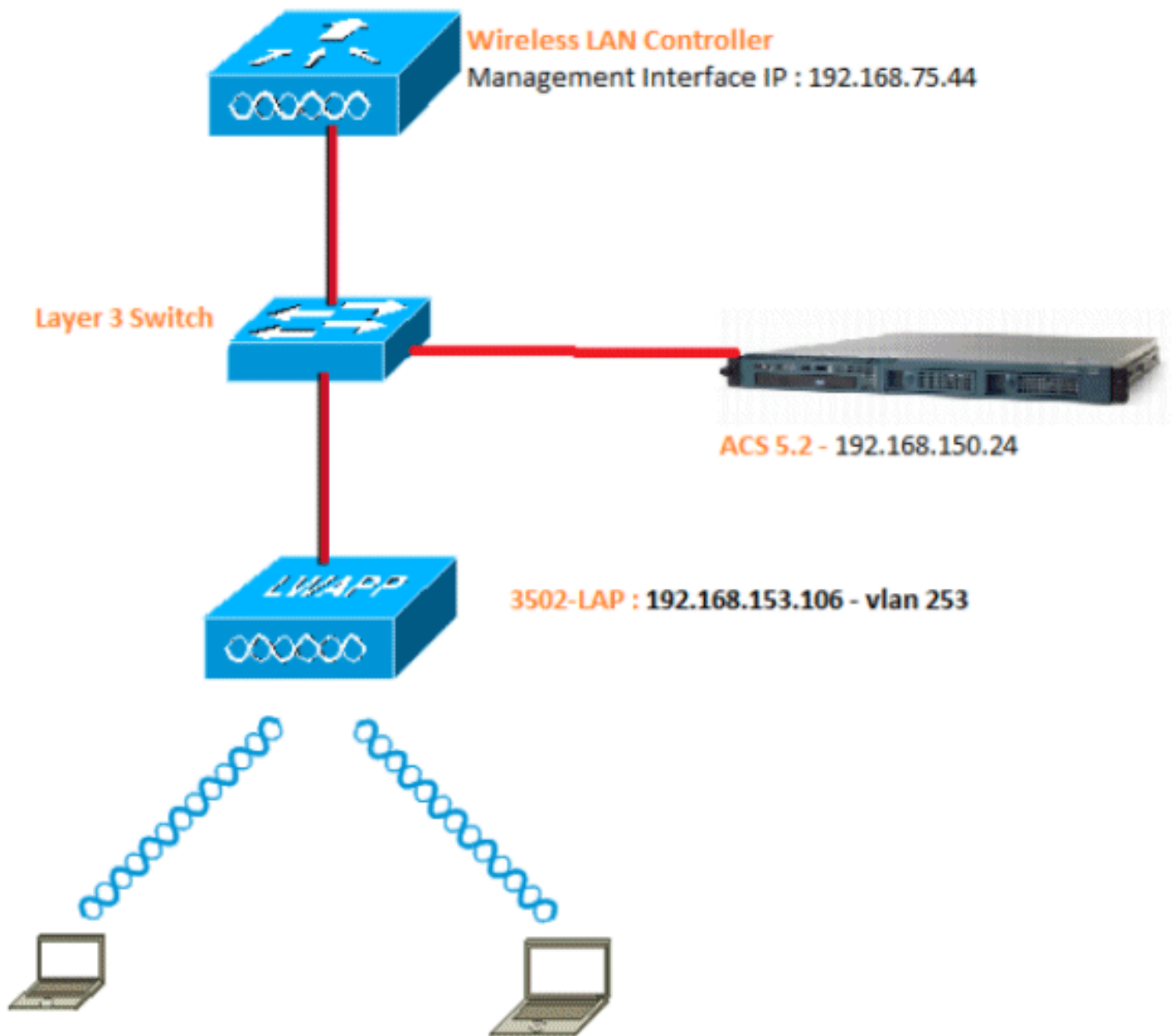
Os LAPs têm certificados X.509 instalados de fábrica - assinados por uma chave privada - que são gravados no dispositivo no momento da fabricação. Os LAPs usam esse certificado para autenticar com a WLC no processo de junção. Esse método descreve outra maneira de autenticar LAPs. Com o software WLC, você pode configurar a autenticação 802.1x entre um ponto de acesso (AP) Cisco Aironet e um switch Cisco. Nesse caso, o AP atua como o solicitante 802.1x e é autenticado pelo switch em um servidor RADIUS (ACS) que usa EAP-FAST com fornecimento de PAC anônimo. Depois de configurado para autenticação 802.1x, o switch não permite que nenhum tráfego diferente de 802.1x passe pela porta até que o dispositivo conectado à porta seja autenticado com êxito. Um AP pode ser autenticado antes de ingressar em uma WLC ou depois de ingressar em uma WLC; nesse caso, você configura 802.1x no switch depois que o LAP ingressar na WLC.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Estes são os detalhes de configuração dos componentes usados neste diagrama:

- O endereço IP do servidor ACS (RADIUS) é 192.168.150.24.
- O endereço da interface do gerenciador de AP e gerenciamento do WLC é 192.168.75.44.
- O endereço dos servidores DHCP é 192.168.150.25.
- O LAP é colocado na VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Hipóteses

- Os switches são configurados para todas as VLANs de Camada 3.
- O servidor DHCP recebe um escopo DHCP.
- Existe conectividade de Camada 3 entre todos os dispositivos na rede.
- O LAP já está unido à WLC.
- Cada VLAN tem uma máscara /24.
- O ACS 5.2 tem um certificado autoassinado instalado.

Configuration Steps

Esta configuração é dividida em três categorias:

1. [Configure o LAP.](#)
2. [Configure o switch.](#)
3. [Configure o servidor RADIUS.](#)

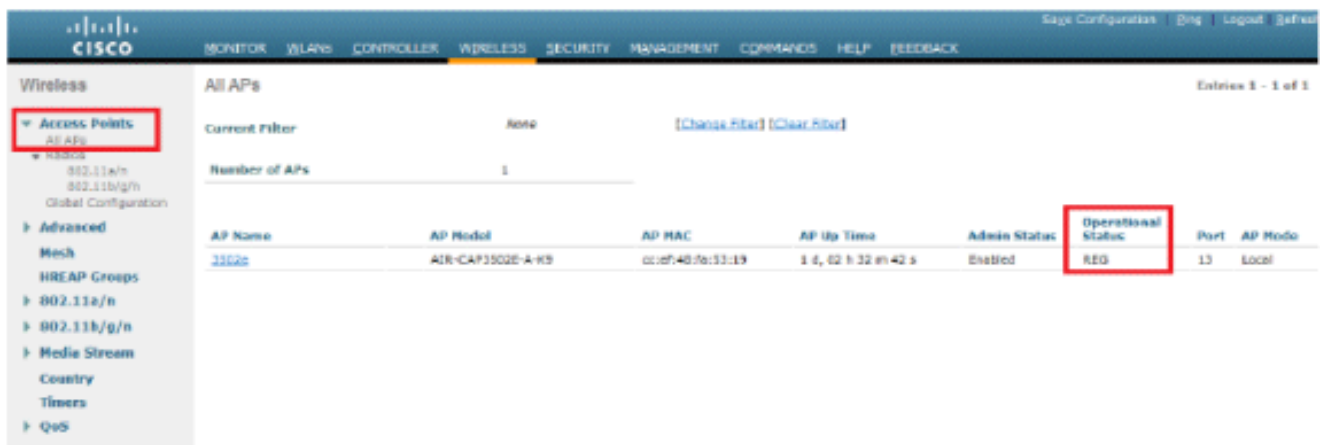
Configurar LAP

Suposições:

O LAP já está registrado na WLC usando a opção 43, DNS ou o IP da interface de gerenciamento da WLC configurado estaticamente.

Conclua estes passos:

1. Vá para **Wireless > Access Points > All APs** para verificar o registro do LAP na WLC.



The screenshot shows the Cisco WLC WebUI interface. The 'Wireless' menu is expanded, and 'Access Points' is selected. The 'All APs' page is displayed, showing a table of APs. The 'Operational Status' column for the AP '2302c' is highlighted with a red box and shows 'REG'.

AP Name	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status	Port	AP Mode
2302c	AIR-CT5502E-A-K9	cc:ef:40:7e:33:19	1 d, 02 h 32 m 42 s	Enabled	REG	13	Local

2. Você pode configurar as credenciais 802.1x (ou seja, nome de usuário/senha) para todos os LAPs de duas maneiras:**Globalmente**Para um LAP já associado, você pode definir as credenciais globalmente de modo que cada LAP que se une à WLC herde essas credenciais.

The screenshot shows the Cisco Wireless Configuration interface. The left sidebar lists various configuration options, with 'Global Configuration' highlighted. The main content area is titled 'Global Configuration' and includes several sections:

- CDP:** A table for configuring CDP on Ethernet interfaces and radio slots. All checkboxes are checked.
- High Availability:** Fields for AP heartbeat timeout, timer states, and backup controller information.
- Login Credentials:** Fields for username, password, and enable password.
- 802.1x Supplicant Credentials (highlighted):** Fields for authentication, username, password, and confirm password.
- AP Failover Priority:** A dropdown menu for global AP failover priority.
- AP Image Pre-download:** Buttons for downloading primary and backup images, and an interchange image button.

Individualmente Configurar perfis 802.1 x por AP. Em nosso exemplo, configuraremos credenciais por AP.Vá para **Wireless > All APs** e selecione o AP em questão.Adicione o nome de usuário e a senha nos campos **Credenciais do solicitante 802.1x**.

The screenshot shows the Cisco Wireless Configuration interface for 'All APs > Details for 3502e'. The 'Credentials' tab is selected, and the '802.1x Supplicant Credentials' section is highlighted with a red box. The 'Login Credentials' section is also visible.

Login Credentials:

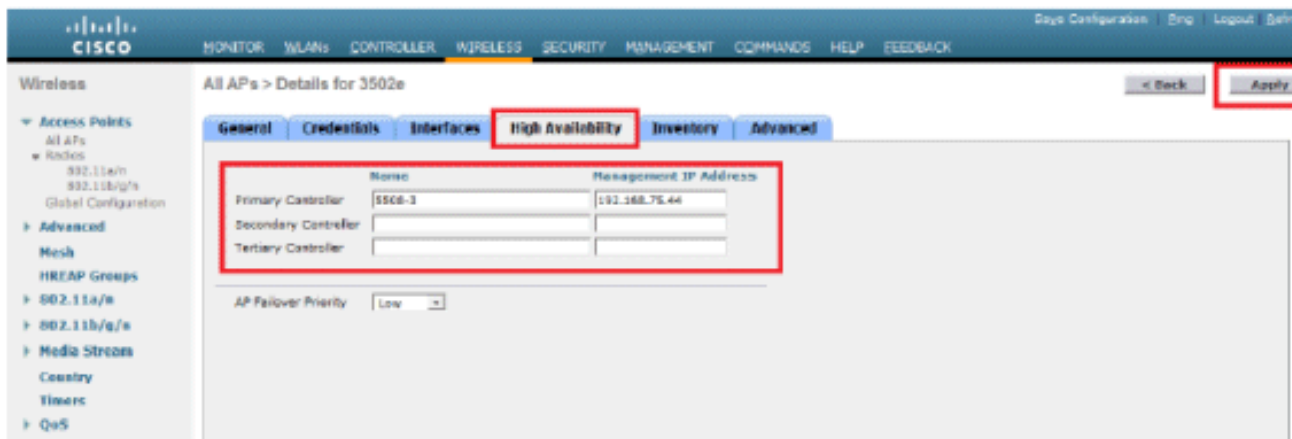
- Override Global credentials:
- Username: [text]
- Password: [password]
- Enable Password: [password]

802.1x Supplicant Credentials (highlighted):

- Override Global credentials:
- Username: [text]
- Password: [password]
- Confirm Password: [password]

Observação: as credenciais de login são usadas para Telnet, SSH ou console no AP.

3. Configure a seção Alta disponibilidade e clique em **Aplicar**.



Observação: depois de salvas, essas credenciais são retidas na WLC e o AP é reinicializado. As credenciais são alteradas somente quando o LAP ingressa em uma nova WLC. O LAP assume o nome de usuário e a senha que foram configurados na nova WLC. Se o AP ainda não ingressou em uma WLC, você deve usar o console do LAP para definir as credenciais. Emita este comando CLI no modo de ativação: **LAP#wapp ap dot1x username <username> password <password>** or **LAP#capwap ap dot1x username <username> password <password>** **Observação:** esse comando está disponível apenas para APs que executam a imagem de recuperação. O nome de usuário e a senha padrão do LAP são `cisco` e `Cisco`, respectivamente.

[Configurar o switch](#)

O switch atua como um autenticador para o LAP e autentica o LAP em um servidor RADIUS. Se o switch não tiver o software compatível, atualize o switch. Na CLI do switch, execute estes comandos para habilitar a autenticação 802.1x em uma porta do switch:

```
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 to the RADIUS server for authentication. 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.
```

Observação: se você tiver outros APs no mesmo switch e não quiser que eles usem 802.1x, poderá deixar a porta não configurada para 802.1x ou emitir este comando:

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

[Configurar servidor RADIUS](#)

O LAP é autenticado com EAP-FAST. Certifique-se de que o servidor RADIUS que você usa suporta este método EAP se você não estiver usando o Cisco ACS 5.2.

A configuração do servidor RADIUS é dividida em quatro etapas:

1. [Configurar recursos de rede.](#)
2. [Configurar usuários.](#)
3. [Definir elementos de política.](#)
4. [Aplicar políticas de acesso.](#)

O ACS 5.x é um ACS baseado em políticas. Em outras palavras, o ACS 5.x usa um modelo de política baseado em regras em vez do modelo baseado em grupos usado nas versões 4.x.

O modelo de política baseado em regras do ACS 5.x oferece um controle de acesso mais poderoso e flexível em comparação com a abordagem mais antiga baseada em grupos.

No modelo mais antigo baseado em grupos, um grupo define a política porque ela contém e une três tipos de informações:

- **Informações de identidade** - Essas informações podem ser baseadas na associação em grupos AD ou LDAP ou em uma atribuição estática para usuários internos do ACS.
- **Outras restrições ou condições** - restrições de tempo, restrições de dispositivo e assim por diante.
- **Permissões** - VLANs ou níveis de privilégio Cisco IOS®.

O modelo de política do ACS 5.x é baseado em regras do seguinte formato:

Condição If então resultado

Por exemplo, usamos as informações descritas para o modelo baseado em grupo:

Se identidade-condição, restrição-condição então autorização-perfil.

Como resultado, isso nos dá flexibilidade para limitar as condições sob as quais o usuário tem permissão para acessar a rede e também o nível de autorização permitido quando condições específicas são atendidas.

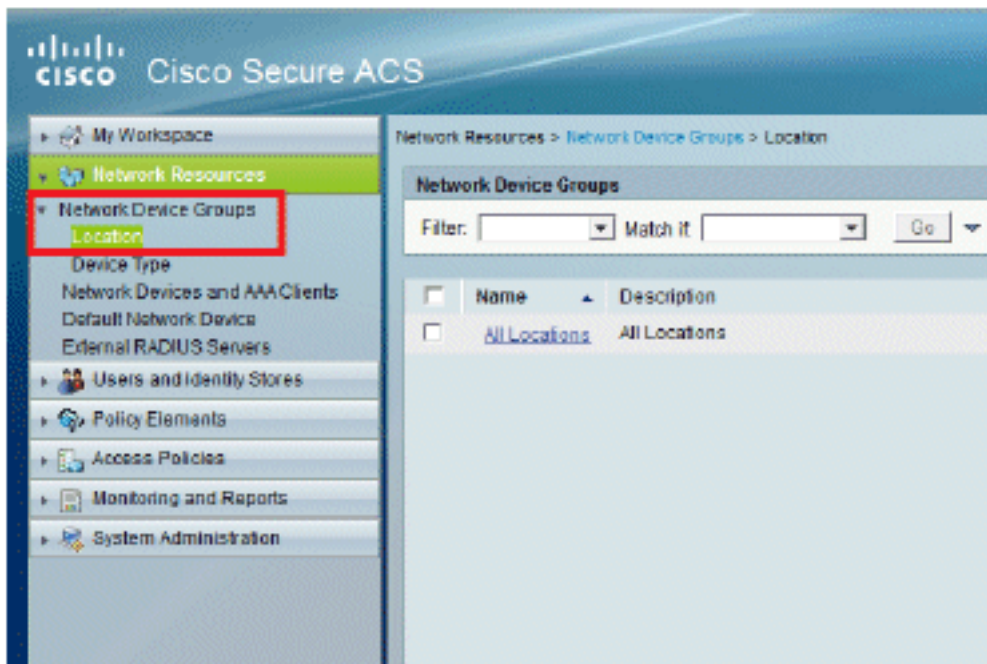
[Configurar recursos de rede](#)

Nesta seção, configuramos o cliente AAA para o switch no servidor RADIUS.

Este procedimento explica como adicionar o switch como um cliente AAA no servidor RADIUS para que o switch possa passar as credenciais do usuário do LAP para o servidor RADIUS.

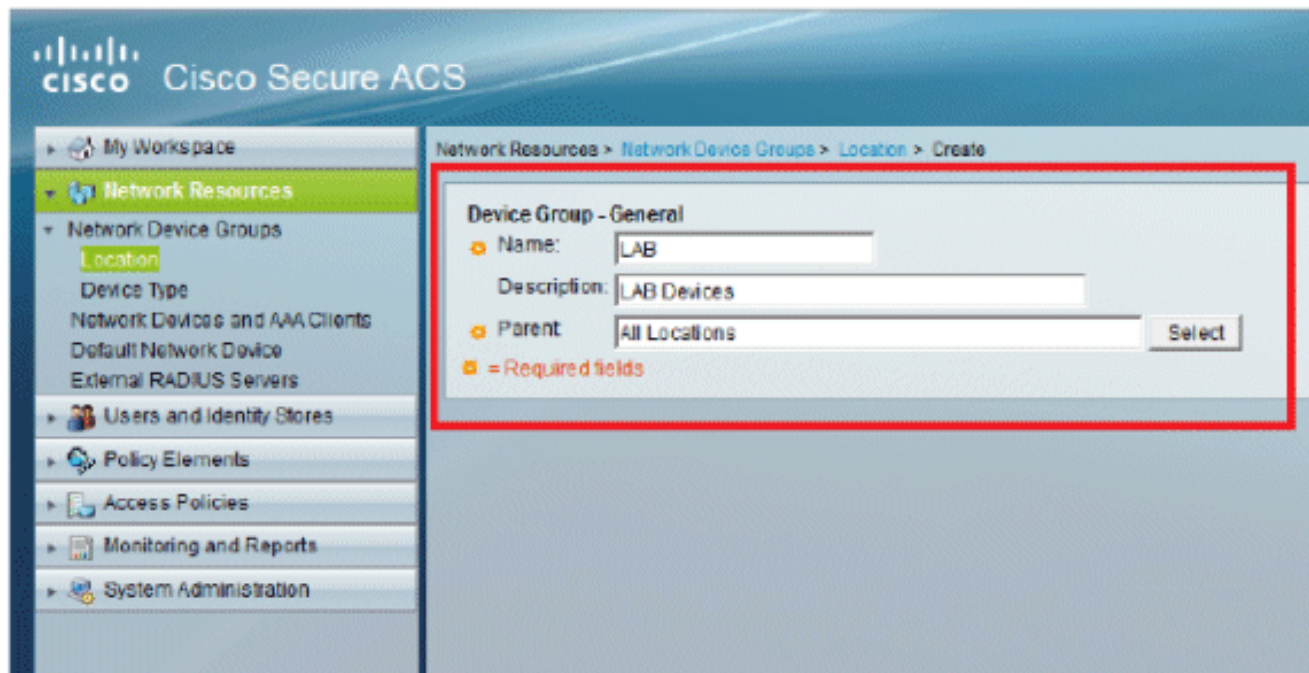
Conclua estes passos:

1. Na GUI do ACS, clique em **Network Resources**.
2. Clique em **Network Device Groups**.
3. Vá para **Location > Create (Local > Criar)** na parte

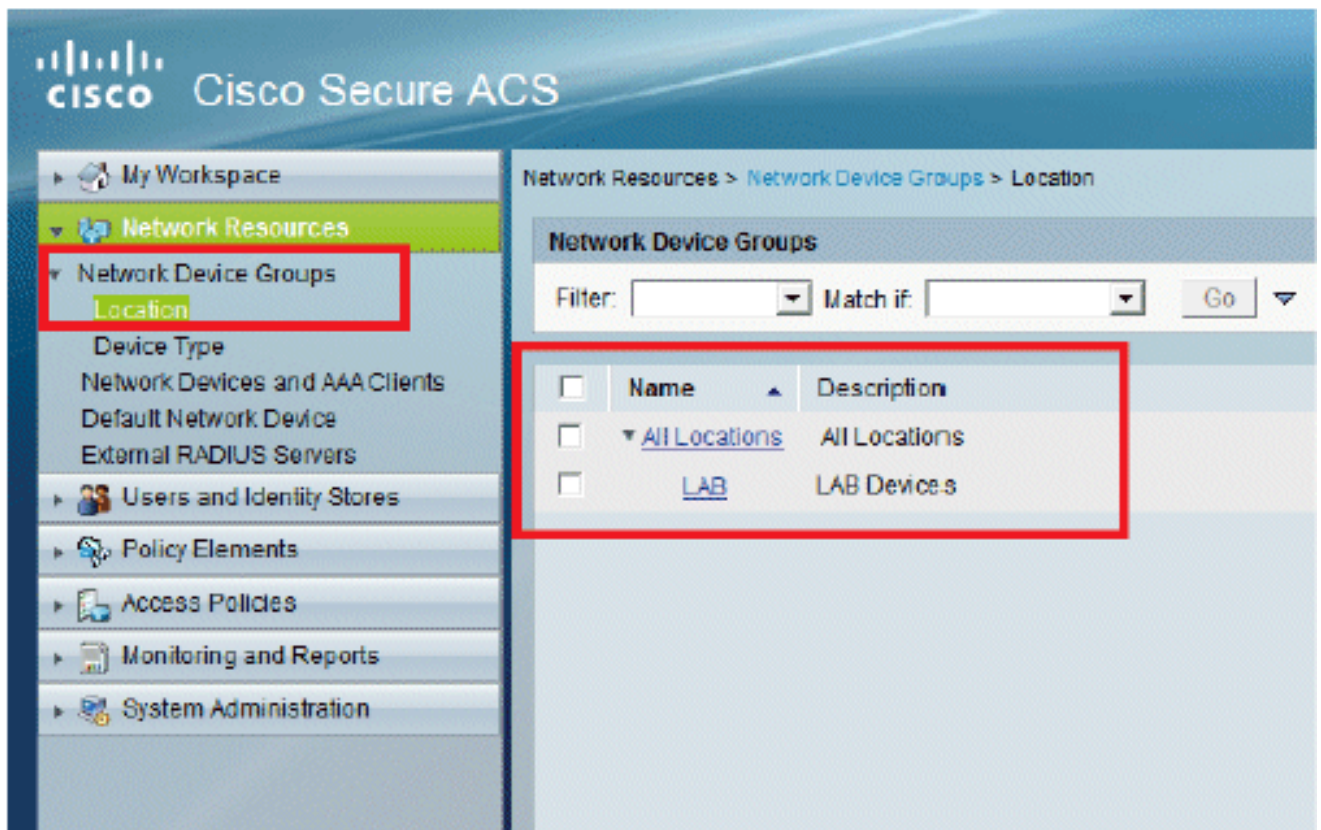


inferior.

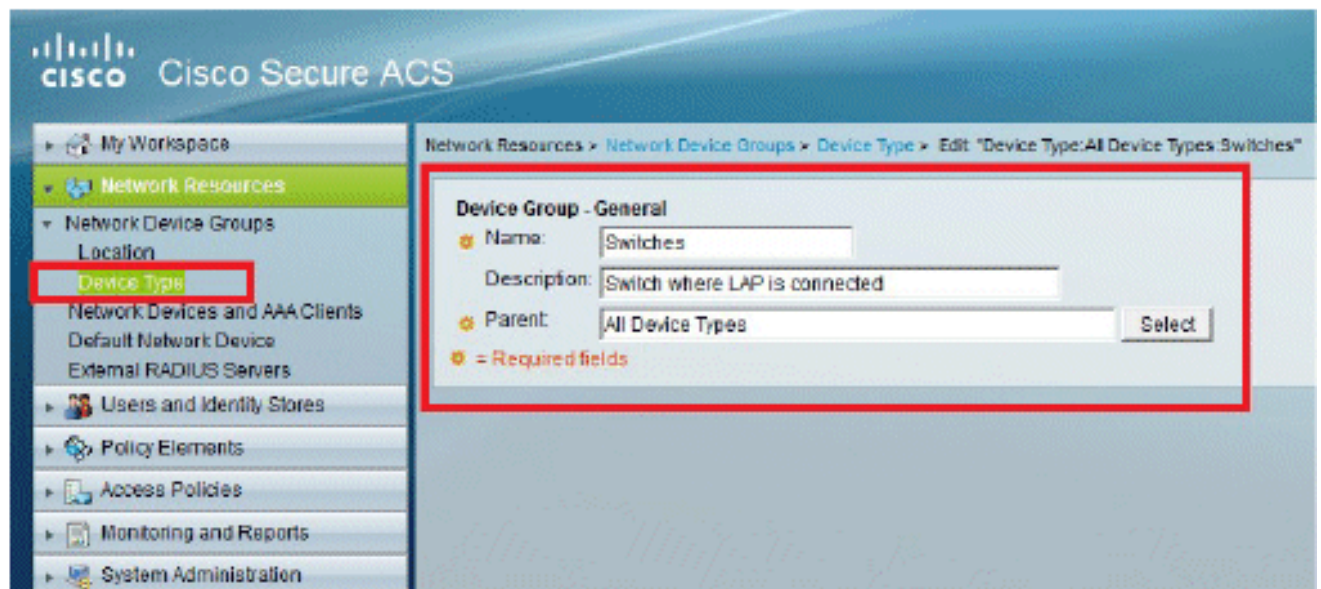
4. Adicione os campos necessários e clique em **Enviar**.



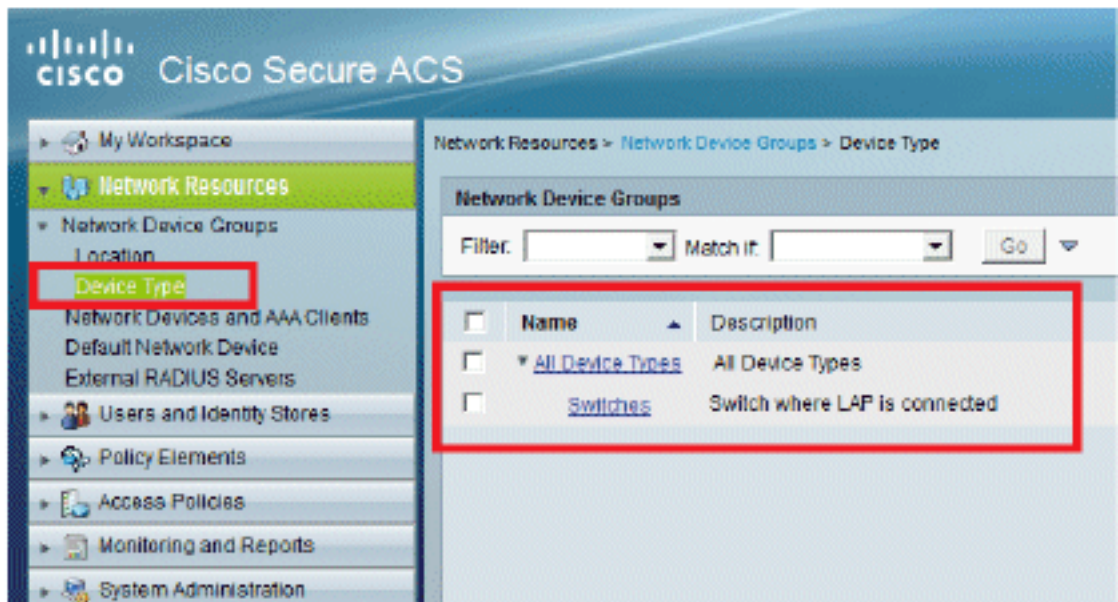
5. A janela é atualizada:



6. Clique em **Tipo de dispositivo > Criar**.



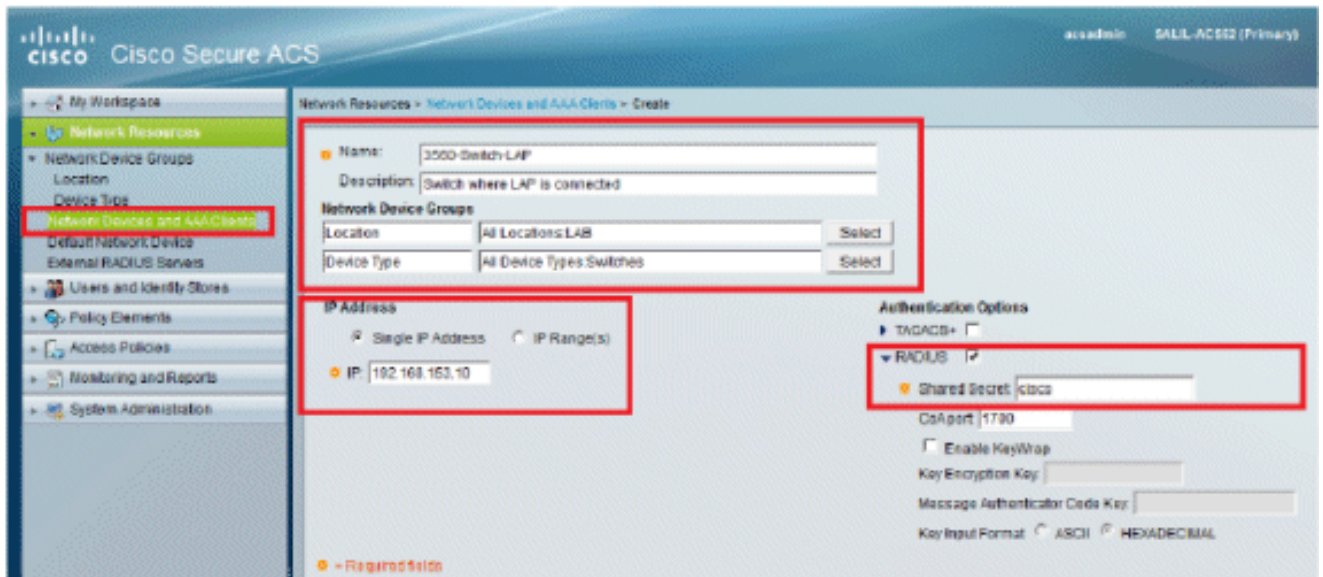
7. Clique em Submit. Depois de concluída, a janela é



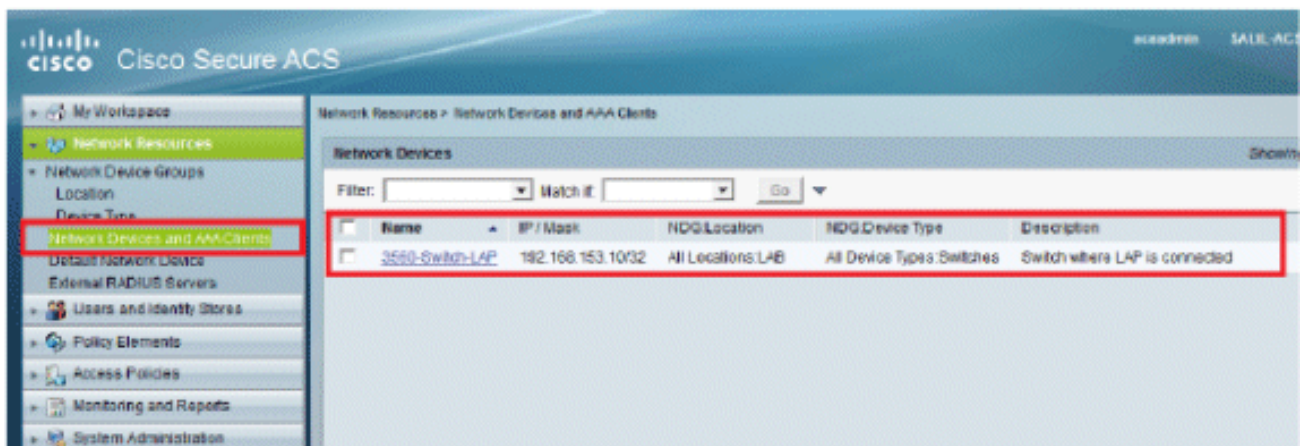
atualizada:

8. Vá para **Network Resources > Network Devices and AAA Clients**.

9. Clique em **Criar** e preencha os detalhes como descrito aqui:



10. Clique em **Submit**. A janela é atualizada:

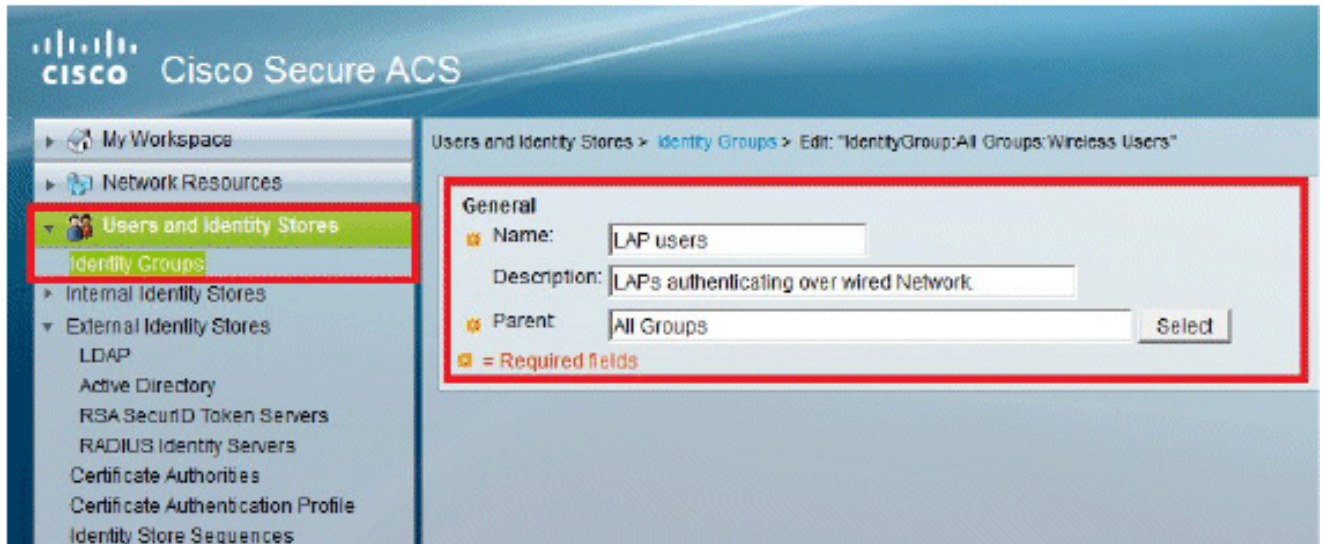


Configurar usuários

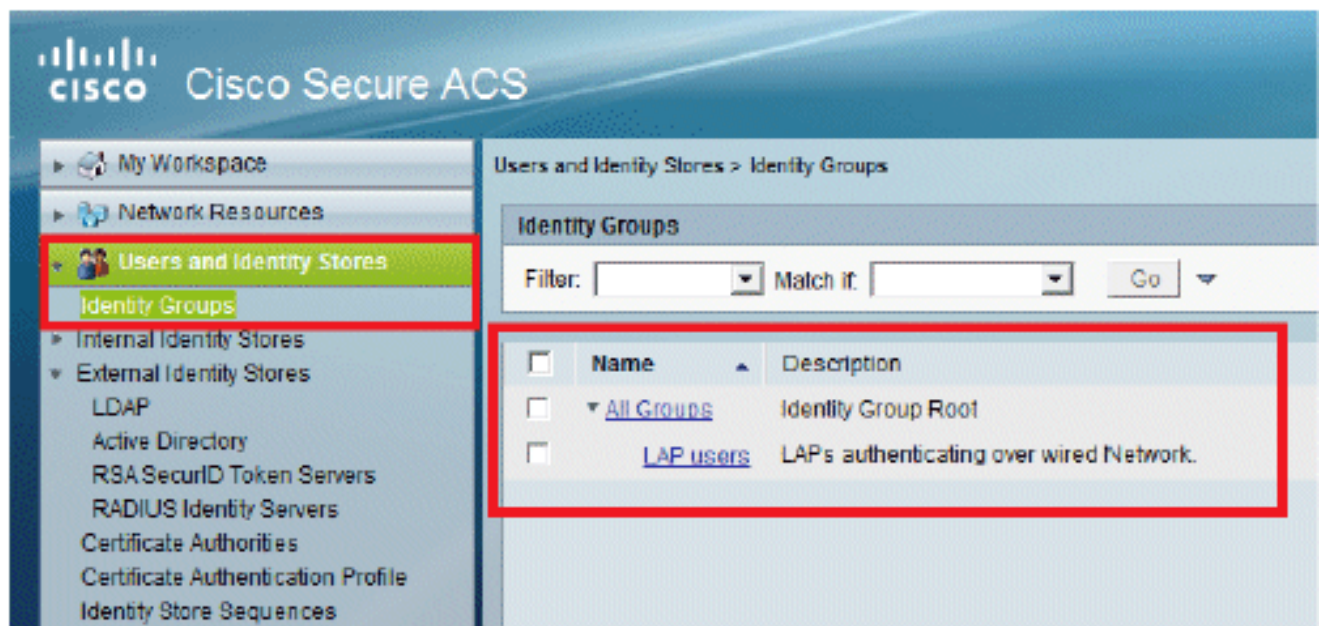
Nesta seção, você verá como criar um usuário no ACS configurado anteriormente. Você atribuirá o usuário a um grupo chamado "usuários do LAP".

Conclua estes passos:

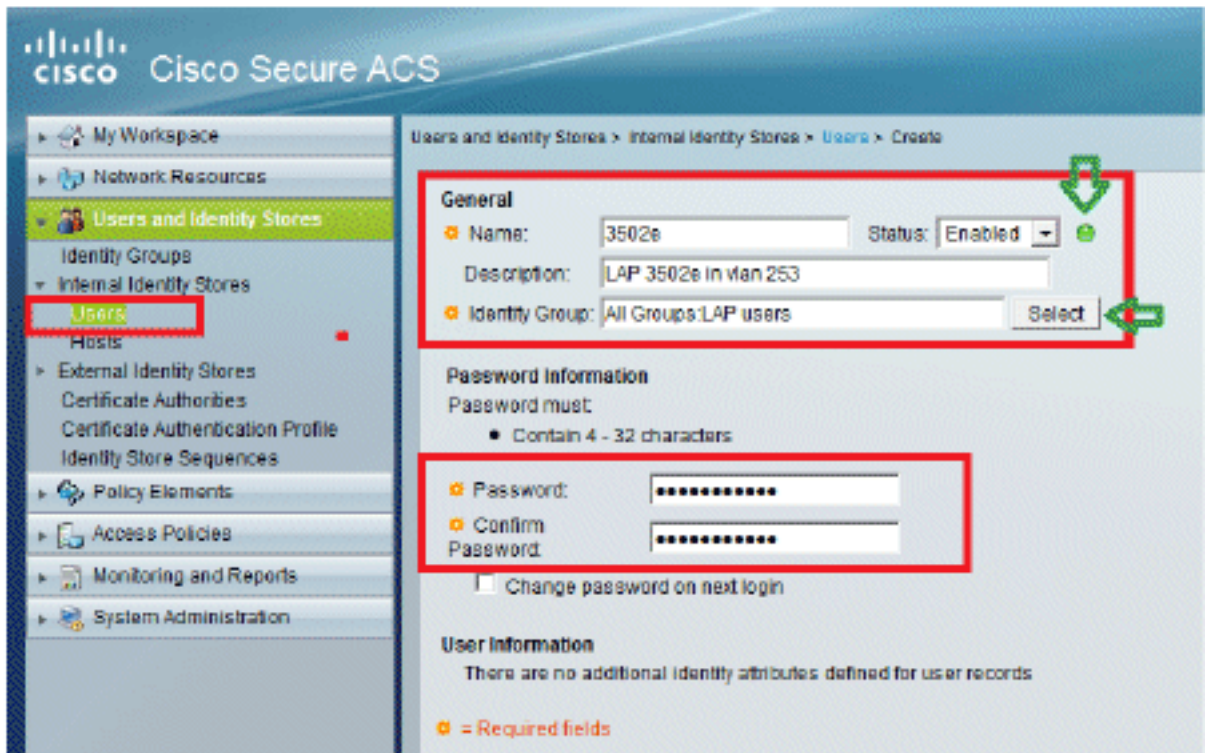
1. Vá para **Users and Identity Stores > Identity Groups > Create**.



2. Clique em **Submit**.

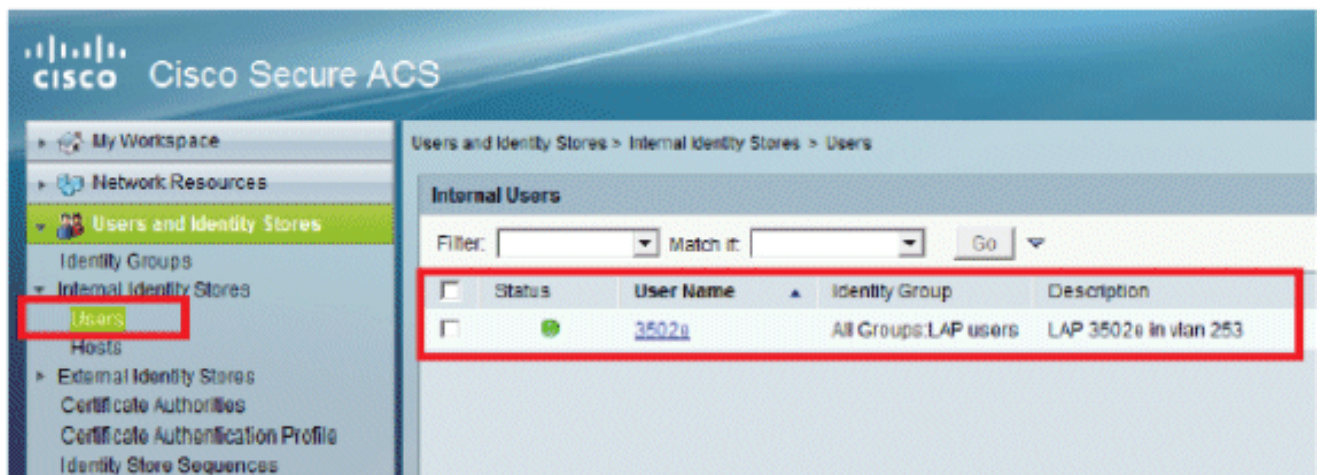


3. Crie o **3502e** e atribua-o ao grupo "usuários do LAP".
4. Vá para **Users and Identity Stores > Identity Groups > Users >**



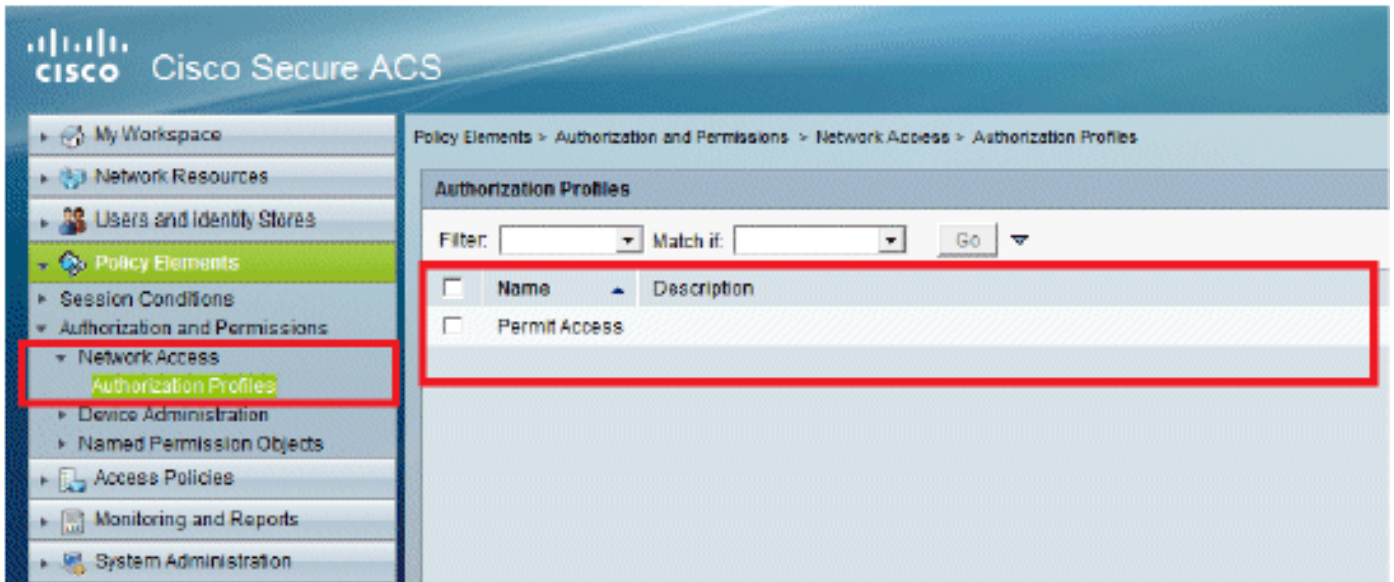
Create.

5. Você verá as informações atualizadas:



Definir Elementos da Política

Verifique se **Permit Access** está definido.

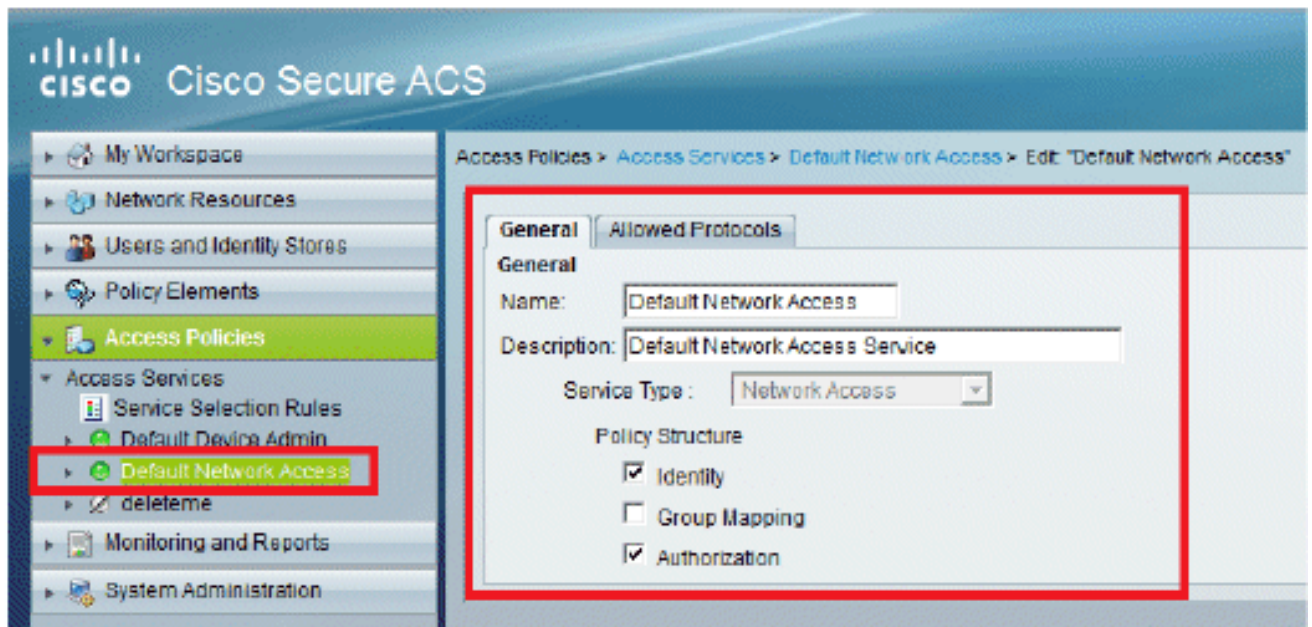


Aplicar políticas de acesso

Nesta seção, você selecionará EAP-FAST como o método de autenticação usado para LAPs para fazer a autenticação. Em seguida, você criará regras com base nas etapas anteriores.

Conclua estes passos:

1. Vá para **Access Policies > Access Services > Default Network Access > Edit: "Default Network Access"**.



2. Verifique se você habilitou o EAP-FAST e o provisionamento de PAC anônimo em banda.

- ▶ My Workspace
- ▶ Network Resources
- ▶ Users and Identity Stores
- ▶ Policy Elements
- ▶ Access Policies
- ▶ Access Services
 - ▶ Service Selection Rules
 - ▶ Default Device Admin
 - ▶ **Default Network Access**
 - ▶ Identity
 - ▶ Authorization
 - ▶ delete me
- ▶ Monitoring and Reports
- ▶ System Administration

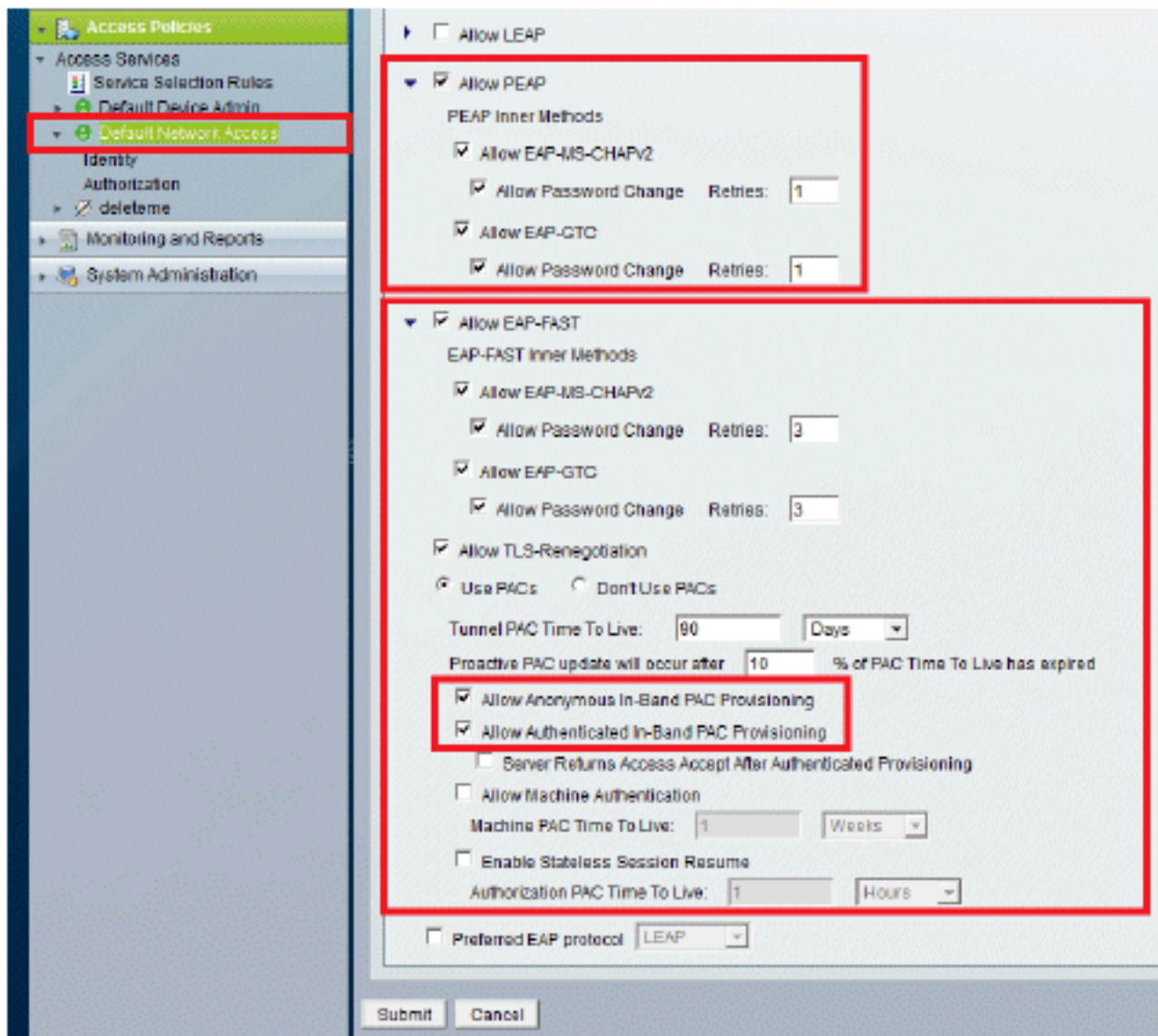
Allowed Protocols

Process Host Lookup

Authentication Protocols

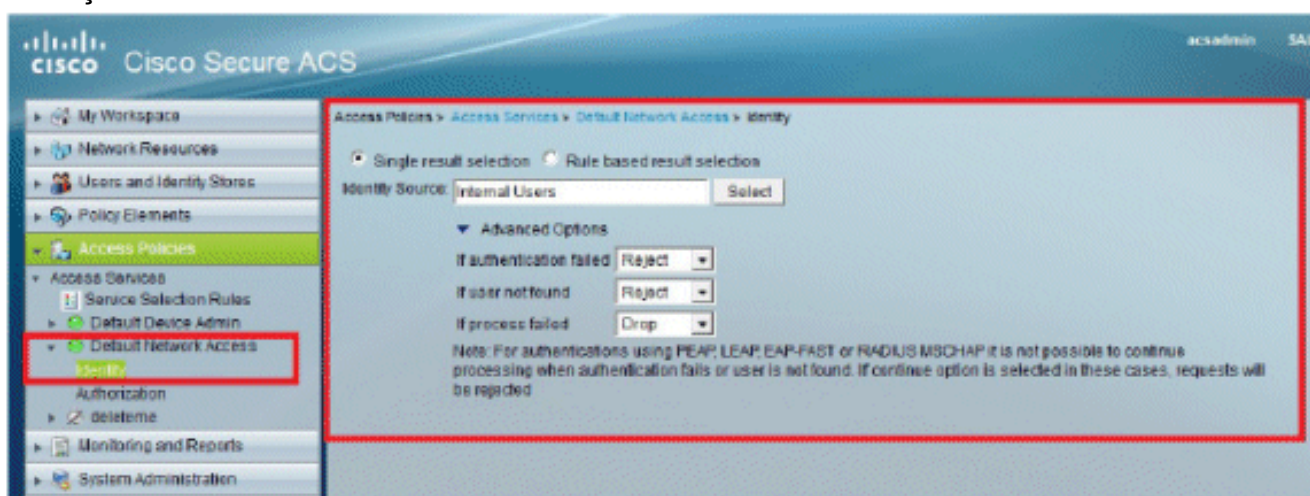
- ▶ Allow PAP/ASCII
- ▶ Allow CHAP
- ▶ Allow MS-CHAPv1
- ▶ Allow MS-CHAPv2
- ▶ Allow EAP-MD5
- ▶ Allow EAP-TLS
- ▶ Allow LEAP
- ▶ Allow PEAP
- ▶ Allow EAP-FAST

Preferred EAP protocol



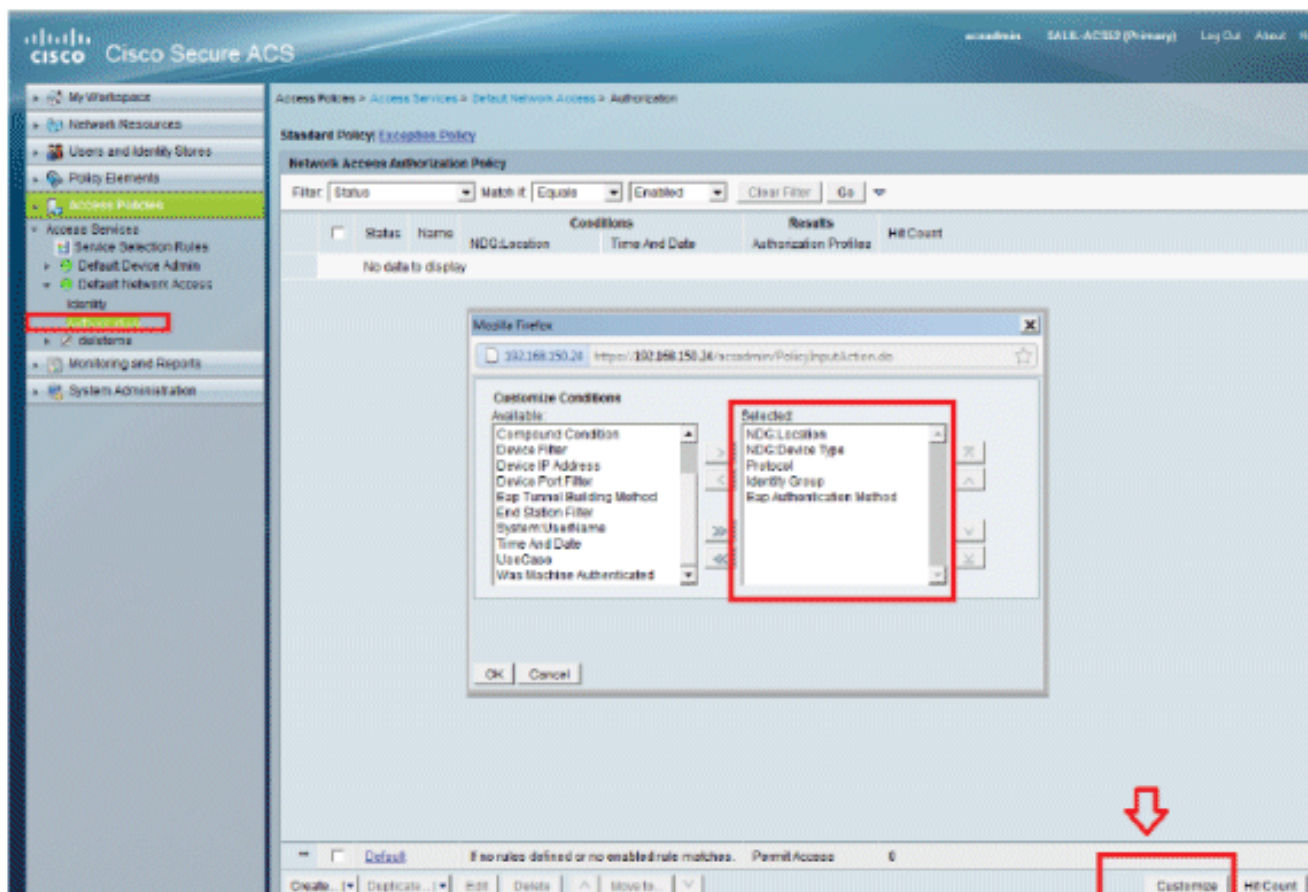
3. Clique em Submit.

4. Verifique o grupo Identidade que você selecionou. Neste exemplo, use **Internal Users** (que foi criado no ACS) e salve as alterações.



5. Vá para **Access Policies > Access Services > Default Network Access > Authorization** para verificar o perfil de autorização. Você pode personalizar sob quais condições permitirá que um usuário acesse a rede e que perfil (atributos) de autorização você passará depois de autenticado. Essa granularidade está disponível apenas no ACS 5.x. Neste exemplo,

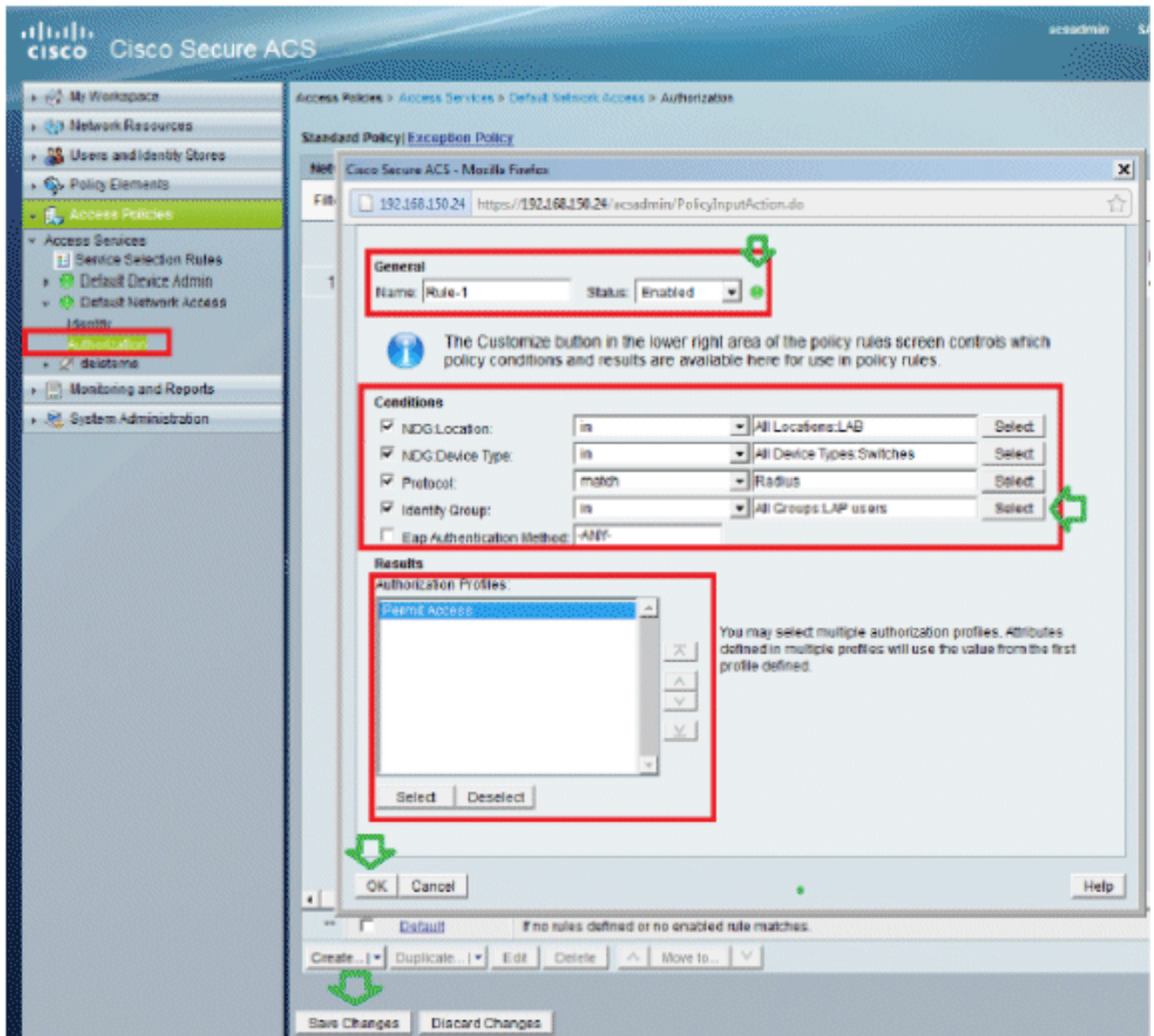
Location, Device Type, Protocol, Identity Group e EAP Authentication Method estão selecionados.



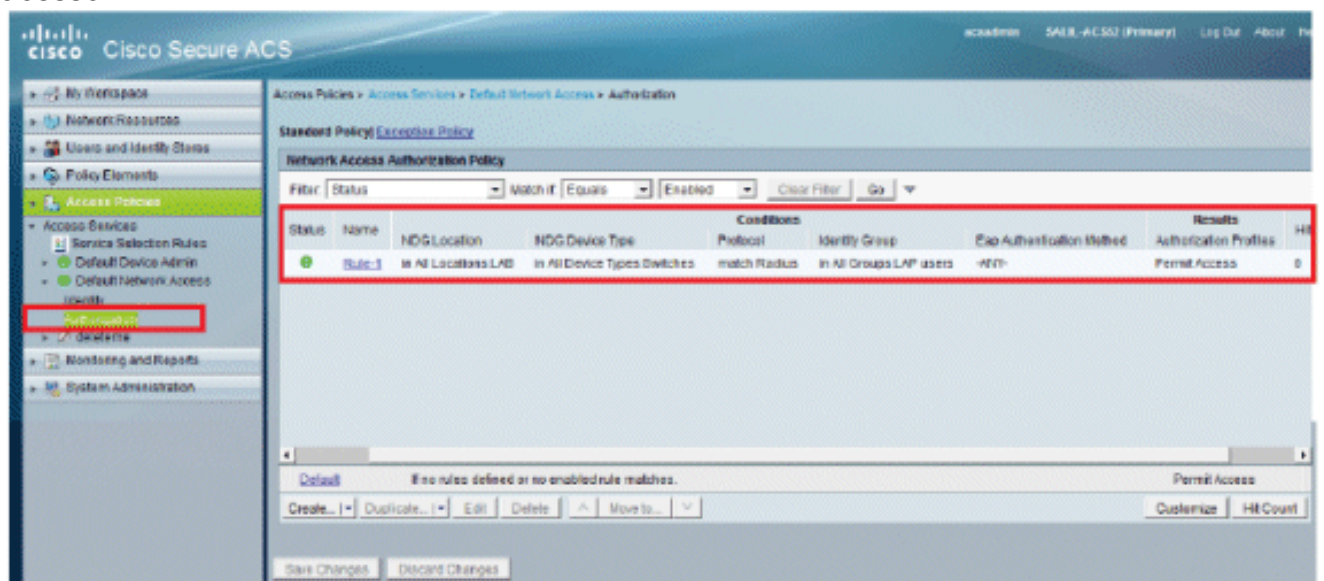
6. Clique em **OK** e em **Save Changes**.

7. A próxima etapa é criar uma regra. Se nenhuma regra for definida, o LAP terá acesso sem nenhuma condição.

8. Clique em **Criar > Regra-1**. Esta regra é para usuários no grupo "usuários LAP".

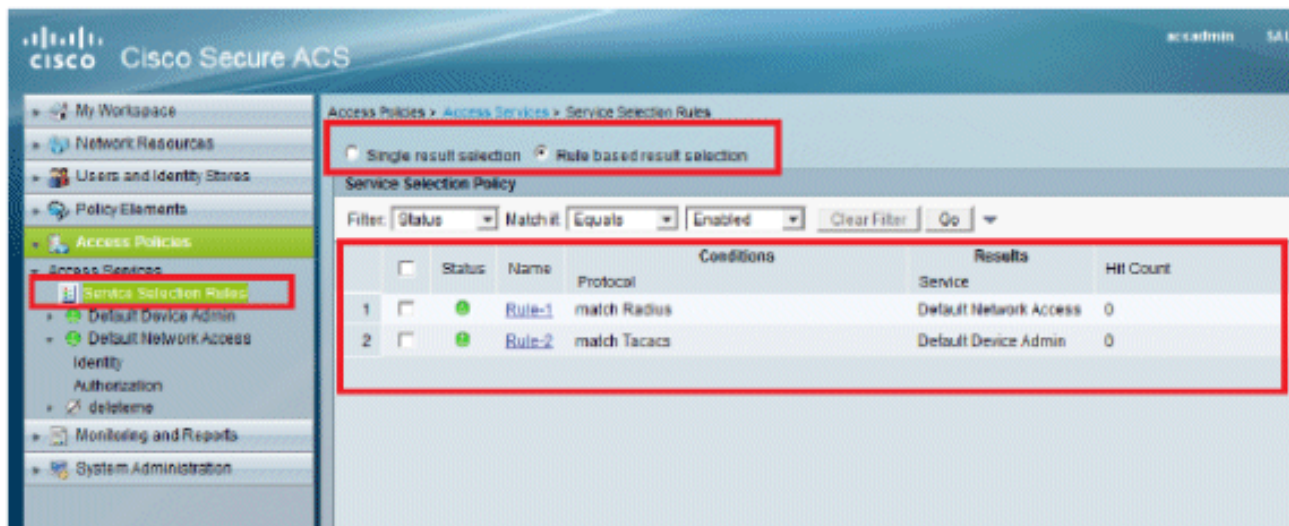


9. Clique em **Save Changes**. Se desejar que os usuários que não corresponderem às condições sejam negados, edite a regra padrão para dizer "Negar acesso".



10. A última etapa é definir as Regras de Seleção de Serviço. Utilize esta página para configurar uma política simples ou baseada em regras para determinar qual serviço será

aplicado às solicitações recebidas. Por exemplo:



Verificar

Quando 802.1x estiver habilitado na porta do switch, todo o tráfego, exceto o 802.1x, será bloqueado pela porta. O LAP, que já está registrado no WLC, é desassociado. Somente após uma autenticação 802.1x bem-sucedida é que outro tráfego pode passar. O registro bem-sucedido do LAP para o WLC depois que o 802.1x é habilitado no switch indica que a autenticação do LAP é bem-sucedida.

Console do AP:

```
*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 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- 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
```

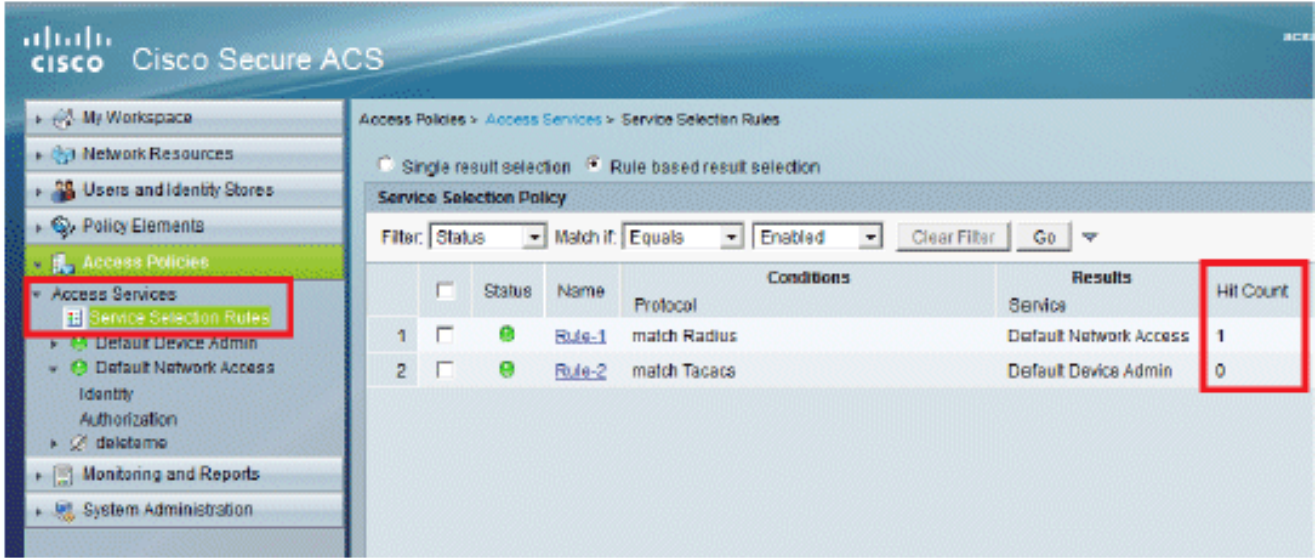
```

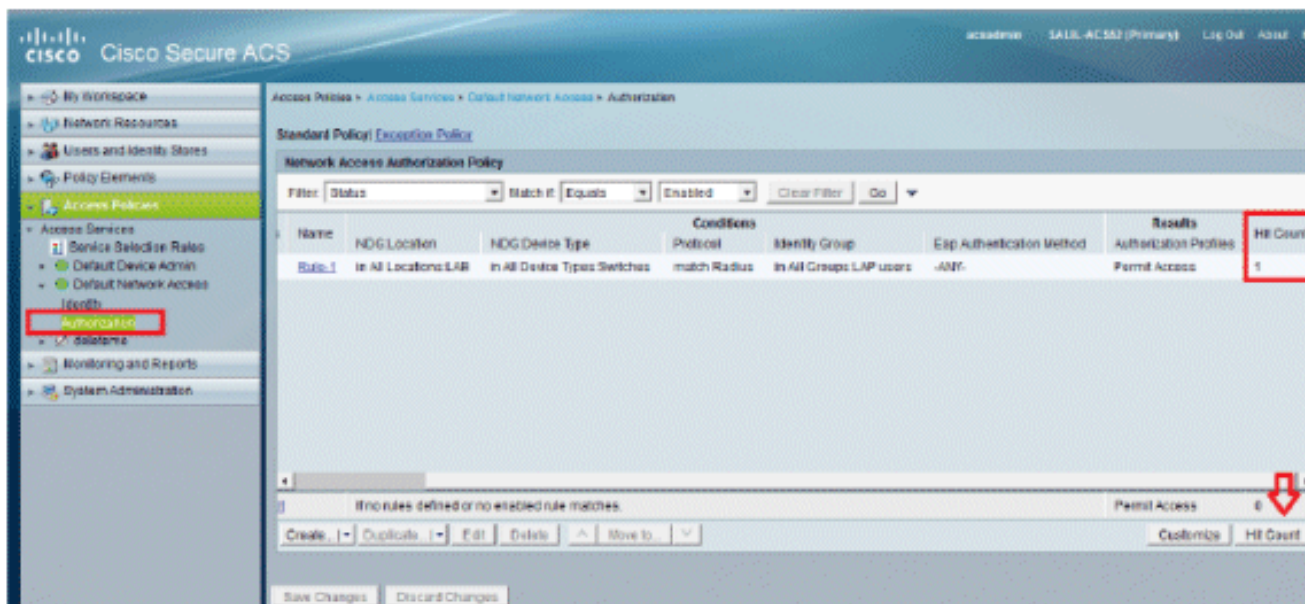
down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data 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.

```

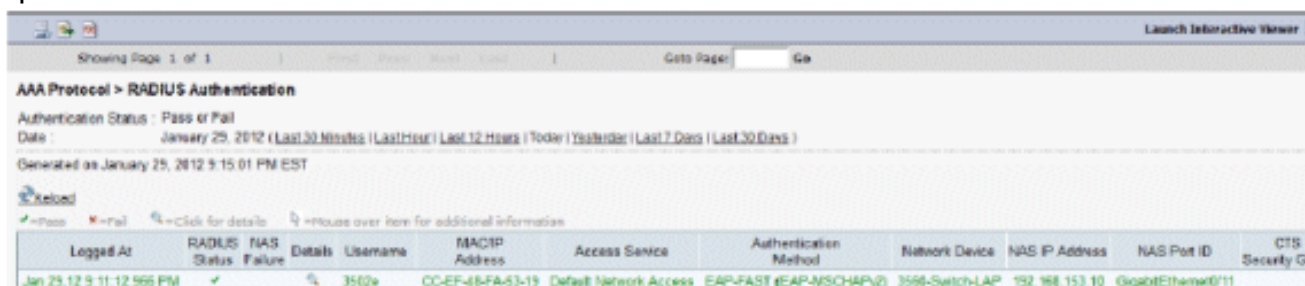
Logs ACS:

1. Veja as contagens de ocorrências: Se você estiver verificando os logs dentro de 15 minutos da autenticação, certifique-se de atualizar a contagem de ocorrências. Na mesma página, na parte inferior, você tem uma guia **Contagem de ocorrências**.





2. Clique em **Monitoring and Reports** e uma nova janela pop-up será exibida. Clique em **Authentications -RADIUS -Today**. Você também pode clicar em **Detalhes** para verificar qual regra de seleção de serviço foi aplicada.



Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Cisco Secure Access Control System](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.