

TACACS+ em um ponto de acesso Aironet para a autenticação de login com uso do exemplo de configuração GUI

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o server TACACS+ para a autenticação de login - Usando ACS 4.1](#)

[Configurar o server TACACS+ para a autenticação de login - Usando ACS 5.2](#)

[Configurar Aironet AP para a autenticação TACACS+](#)

[Verificar](#)

[Verificação para ACS 5.2](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este original explica como permitir o TACACS mais os serviços (TACACS+) em um Access Point (AP) do Cisco Aironet a fim executar a autenticação de login com o uso de um server TACACS+.

[Pré-requisitos](#)

[Requisitos](#)

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

- Conhecimento de como configurar parâmetros básicos em Aironet APs
- Conhecimento de como configurar um server TACACS+ como o Serviço de controle de acesso Cisco Secure (ACS)
- Conhecimento de conceitos TACACS+

Para obter informações sobre de como os trabalhos TACACS+, referem [compreender a seção TACACS+ de configurar server do RAI0 e TACACS+](#).

[Componentes Utilizados](#)

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

- Cisco Aironet 1240 de Aironet/1140 Series dos Access point
- ACS que executa a versão de software 4.1
- ACS que executa a versão de software 5.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

[Convenções](#)

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

[Configurar](#)

Esta seção explica como configurar Aironet AP e o server TACACS+ (ACS) para a autenticação de login TACACS+-based.

Este exemplo de configuração usa estes parâmetros:

- IP address do ACS — 172.16.1.1/255.255.0.0
- IP address do AP — 172.16.1.30/255.255.0.0
- Chave secreta compartilhada que é usada no AP e no server TACACS+ — **exemplo**

Estas são as credenciais do usuário que este exemplo configura no ACS:

- Username — **User1**
- Senha do Cisco
- Grupo — **Usuários com direitos de administrador**

Você precisa de configurar características TACACS+ para validar os usuários que tentam conectar ao AP através da interface da WEB ou através do comando line interface(cli). A fim realizar esta configuração, você deve executar estas tarefas:

1. [Configurar o server TACACS+ para a autenticação de login.](#)
2. [Configurar Aironet AP para a autenticação TACACS+.](#)

Nota: Use a ferramenta [Command Lookup Tool](#) ([apenas para clientes registrados](#)) para obter mais informações sobre os comandos usados neste documento.

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:



[Configurar o server TACACS+ para a autenticação de login - Usando ACS 4.1](#)

A primeira etapa é estabelecer um demônio TACACS+ para validar os usuários que tentam alcançar o AP. Você deve estabelecer o ACS para a autenticação TACACS+ e criar uma base de dados de usuário. Você pode usar todo o server TACACS+. Este exemplo usa o ACS como o server TACACS+. Conclua estes passos:

1. Termine estas etapas a fim adicionar o AP como um cliente do Authentication, Authorization, and Accounting (AAA): Do ACS GUI, clique a aba da **configuração de rede**. Em AAA Clients, clique em Add Entry. No indicador do cliente de AAA adicionar, incorpore o nome de host AP, o IP address do AP, e uma chave secreta compartilhada. Esta chave secreta compartilhada deve ser a mesma que a chave secreta compartilhada que você configura no AP. Da autenticação usando o menu suspenso, selecione **TACACS+ (Cisco IOS)**. Clique **Submit + Restart** a fim salvar a configuração. Aqui está um exemplo:

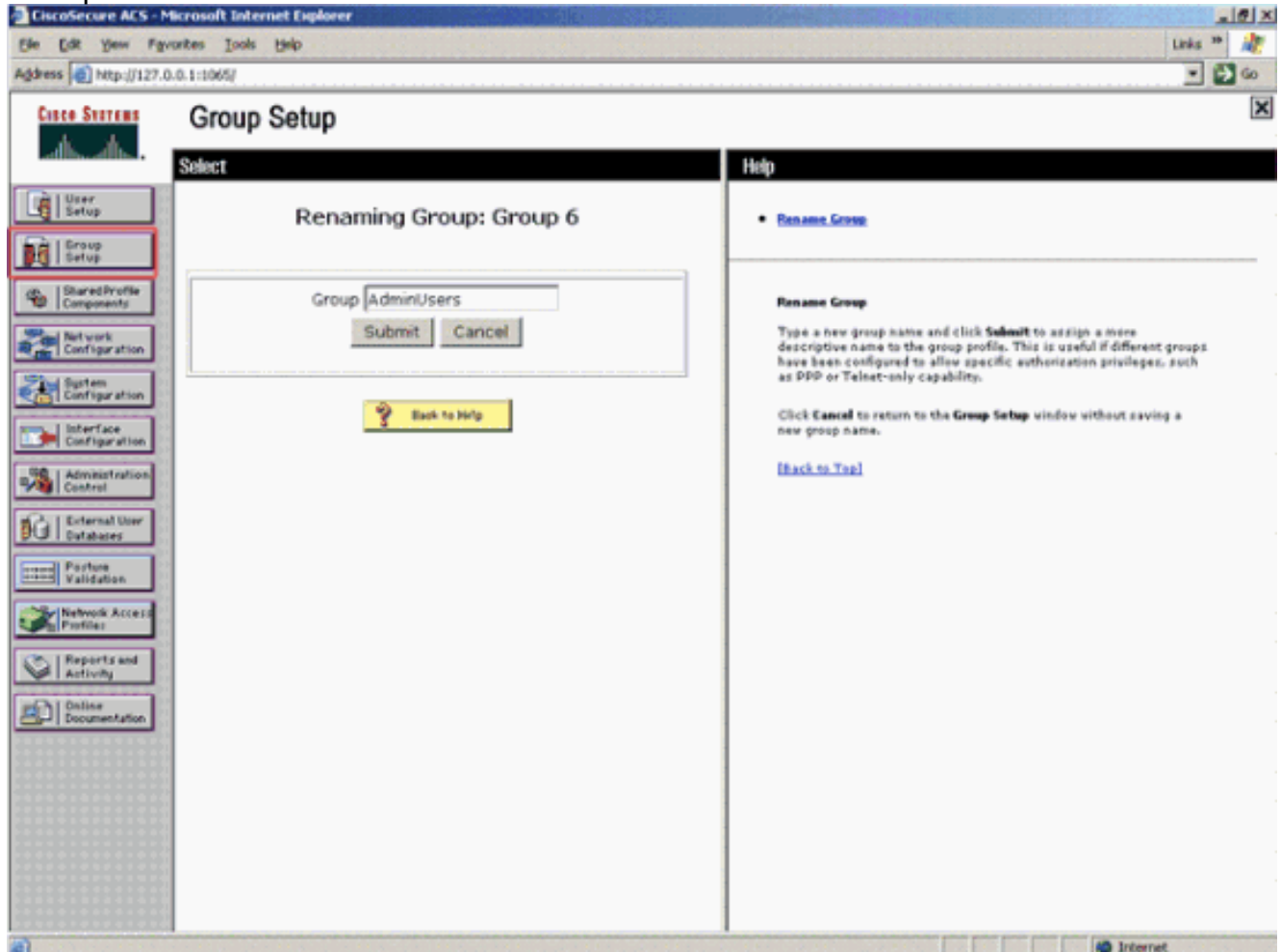
The screenshot shows the 'Add AAA Client' configuration page in the CiscoSecure ACS GUI. The page is titled 'Network Configuration' and 'Add AAA Client'. The following fields are visible:

- AAA Client Hostname:** AccessPoint
- AAA Client IP Address:** 172.16.1.30
- Shared Secret:** Example
- RADIUS Key Wrap:** Key Encryption Key, Message Authenticator Code, Key, Key Input Format (ASCII/Hexadecimal)
- Authenticate Using:** TACACS+ (Cisco IOS) (highlighted with a red oval)
- Options:**
 - Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
 - Log Update/Watchdog Packets from this AAA Client
 - Log RADIUS Tunneling Packets from this AAA Client
 - Replace RADIUS Port info with Username from this AAA Client
 - Match Framed-IP-Address with user IP address for accounting packets from this AAA Client
- Buttons:** Submit, Submit + Apply (highlighted with a red oval), Cancel

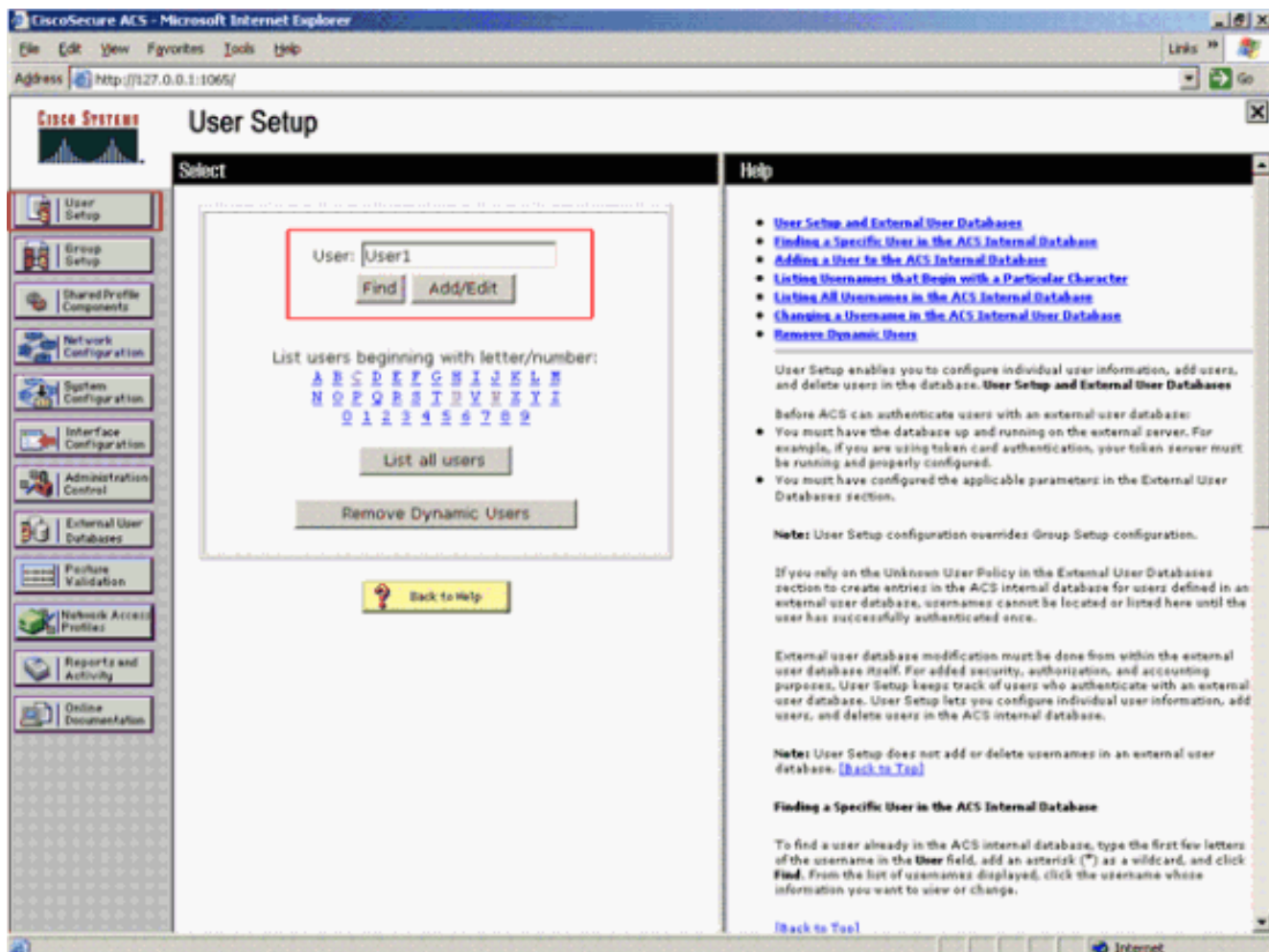
The right sidebar contains a 'Help' section with links to various AAA Client configuration topics.

Este exemplo usa-se: O hostname **AccessPoint** do cliente de AAA O endereço **172.16.1.30/16** como o IP address do cliente de AAA O exemplo compartilhado da chave secreta

2. Termine estas etapas a fim criar um grupo que contenha todos os usuários (admin) administrativos: Clique a **instalação de grupo** do menu à esquerda. Uma nova janela aparece. No indicador da instalação de grupo, selecione um grupo configurar do menu suspenso e o clique **rebatiza o grupo**. Este exemplo seleciona o grupo 6 do menu suspenso e rebatiza os usuários com direitos de administrador do grupo. Clique em Submit. Aqui está um exemplo:

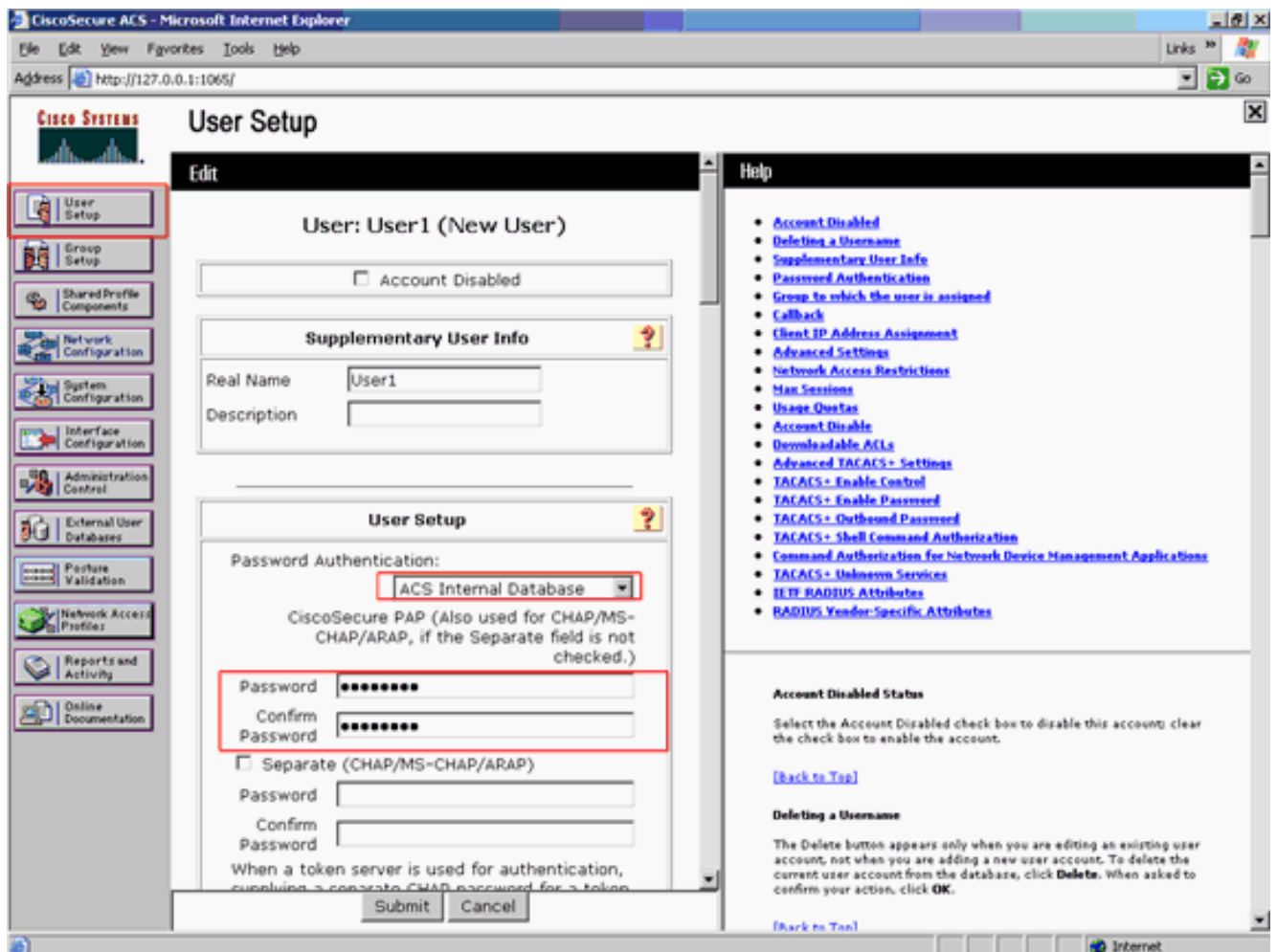


3. Termine estas etapas a fim adicionar os usuários ao base de dados TACACS+: Clique a aba da **instalação de usuário**. A fim criar um novo usuário, para incorporar o username ao campo e ao clique do usuário **adicionar/edite**. Está aqui um exemplo, que crie **User1**:

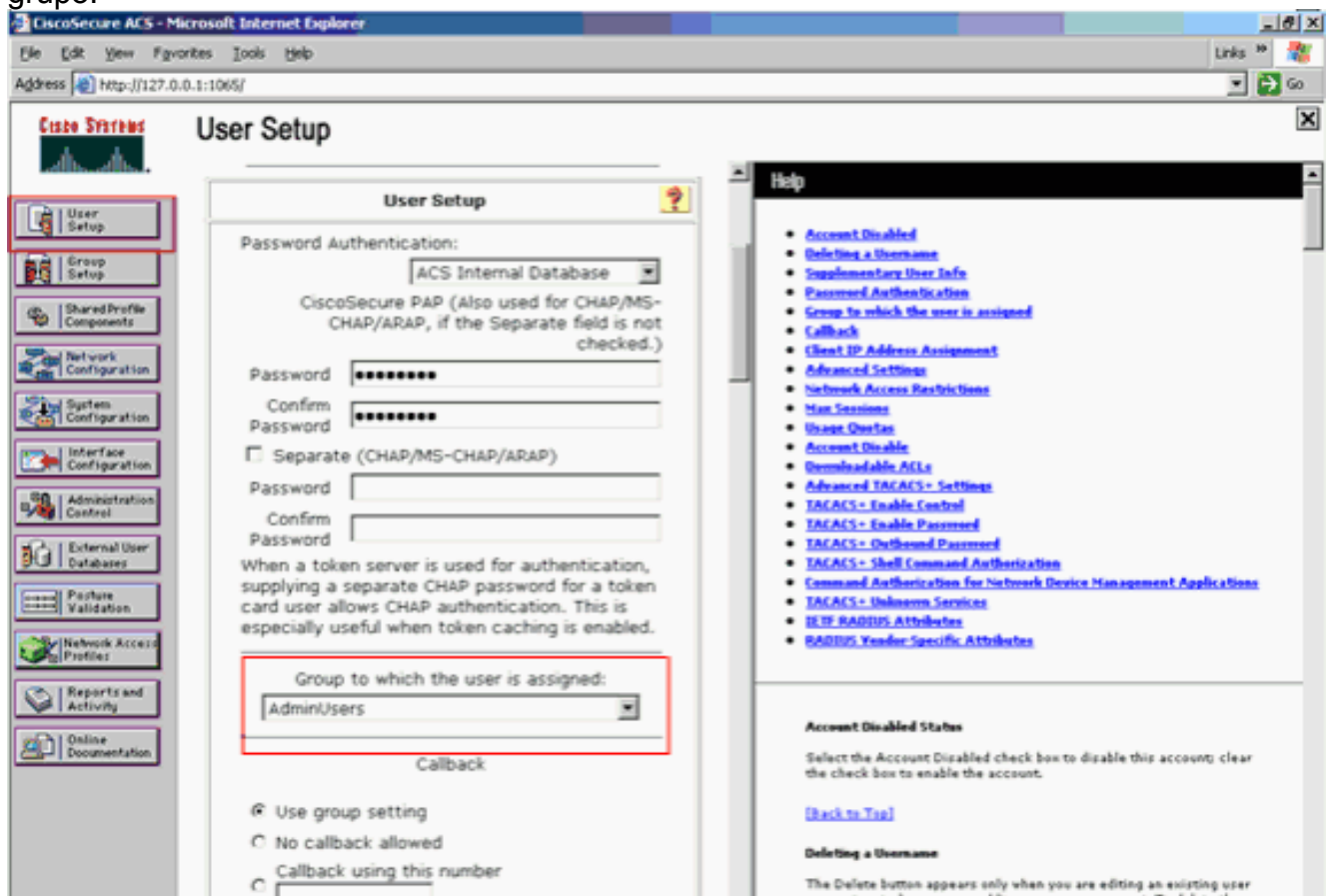


Depois que você clique adiciona/edita, adicionar/edita o indicador para este usuário aparece.

4. Incorpore as credenciais que são específicas a este usuário e o clique **se submete** a fim salvar a configuração. As credenciais que você pode incorporar incluem: Informação de usuário suplementar Instalação de usuário O grupo a que o usuário é atribuído Aqui está um exemplo:

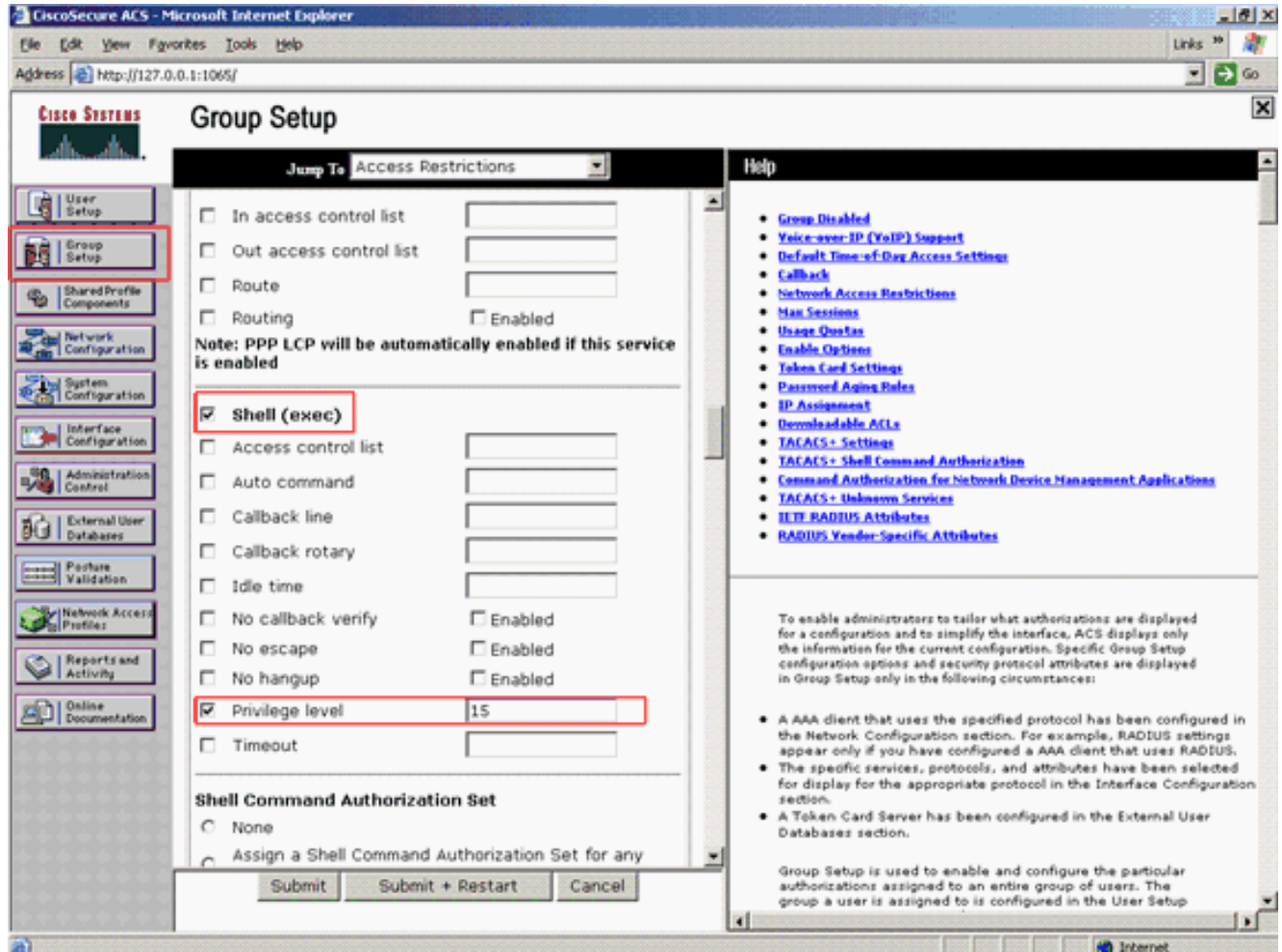


Você pode ver que este exemplo adiciona o usuário User1 aos usuários com direitos de administrador do grupo.



Nota: Se você não cria um grupo específico, os usuários estão atribuídos ao grupo padrão.

5. Termine estas etapas a fim definir o nível de privilégio: Clique a aba da **instalação de grupo**. Selecione o grupo que você atribuiu previamente a este usuário e o clique **edita ajustes**. Este exemplo usa os usuários com direitos de administrador do grupo. Sob ajustes TACACS+, verifique a caixa de verificação do **shell (exec)** e verifique a caixa de verificação do nível de privilégio que tem um valor de 15. Clique **Submit + Restart**.



Nota: O nível de privilégio 15 deve ser definido para o GUI e o telnet a fim ser acessível como o nível 15. Se não, à revelia, o usuário pode somente alcançar como o nível 1. Se o nível de privilégio não está definido e o usuário tenta incorporar o modo enable no CLI (com uso do telnet), o AP indica este Mensagem de Erro:

```
AccessPoint>enable
% Error in authentication
```

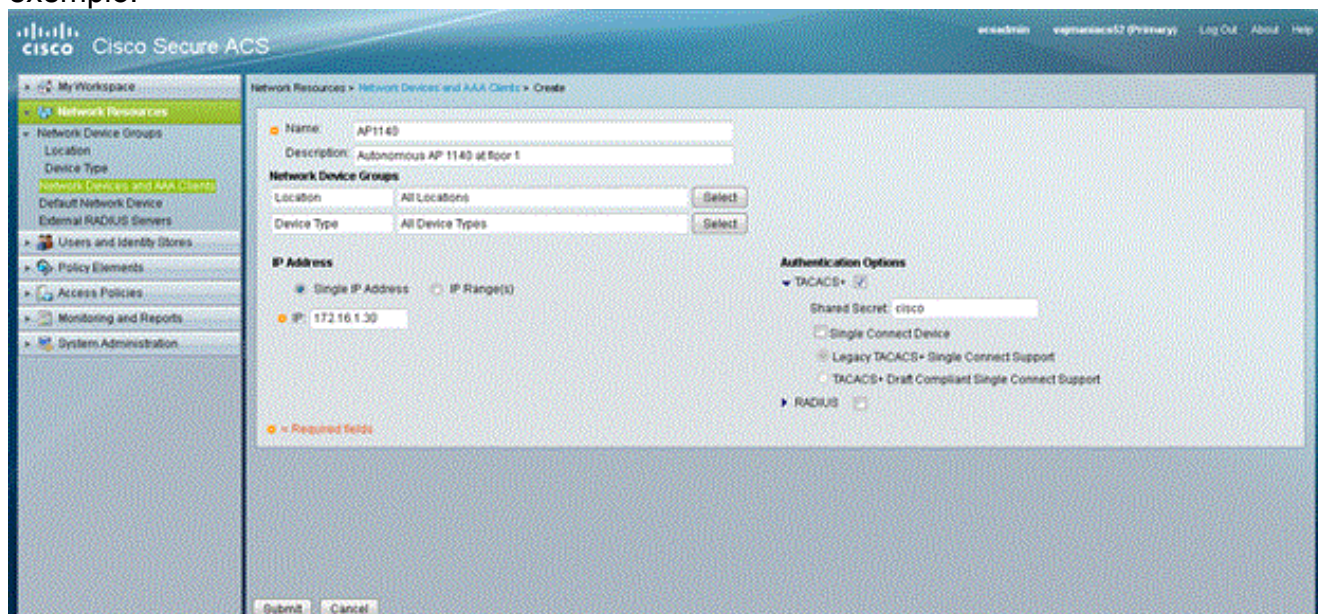
Repita etapas 2 a 4 deste procedimento se você quer adicionar mais usuários ao base de dados TACACS+. Depois que você terminou estas etapas, o server TACACS+ está pronto para validar os usuários que tentam entrar ao AP. Agora, você deve configurar o AP para a autenticação TACACS+.

[Configurar o server TACACS+ para a autenticação de login - Usando ACS 5.2](#)

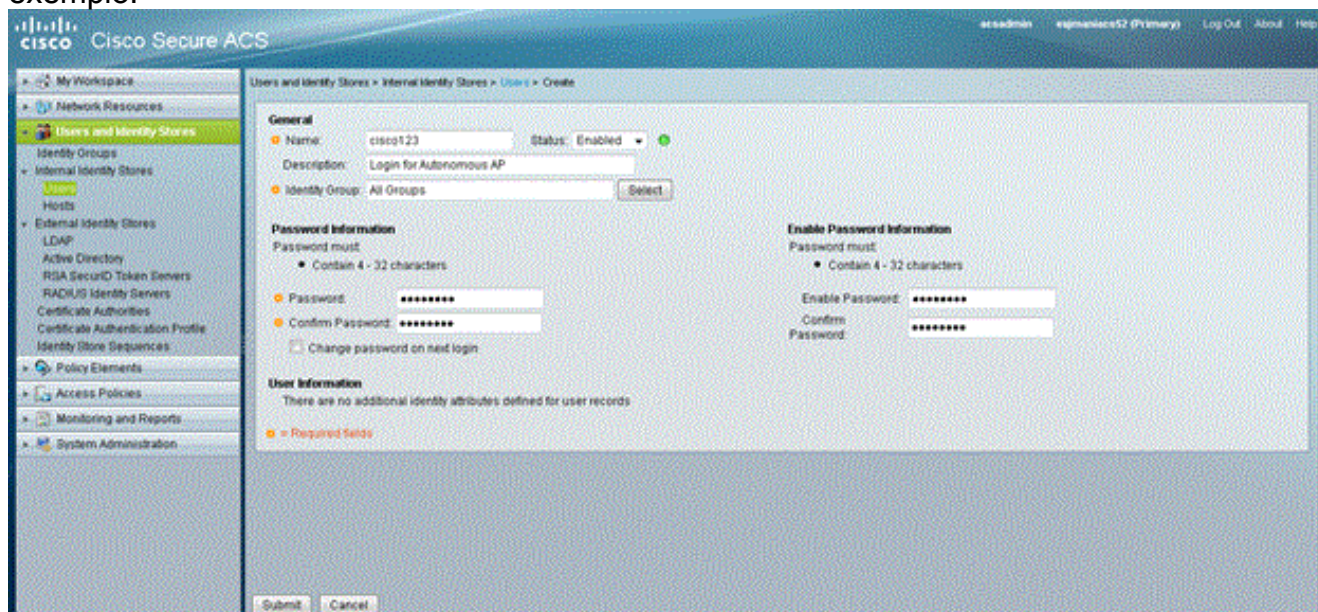
A primeira etapa é adicionar o AP como um cliente de AAA no ACS e criar uma política TACACS para o início de uma sessão.

1. Termine estas etapas a fim adicionar o AP como um cliente de AAA: Do ACS GUI, clique

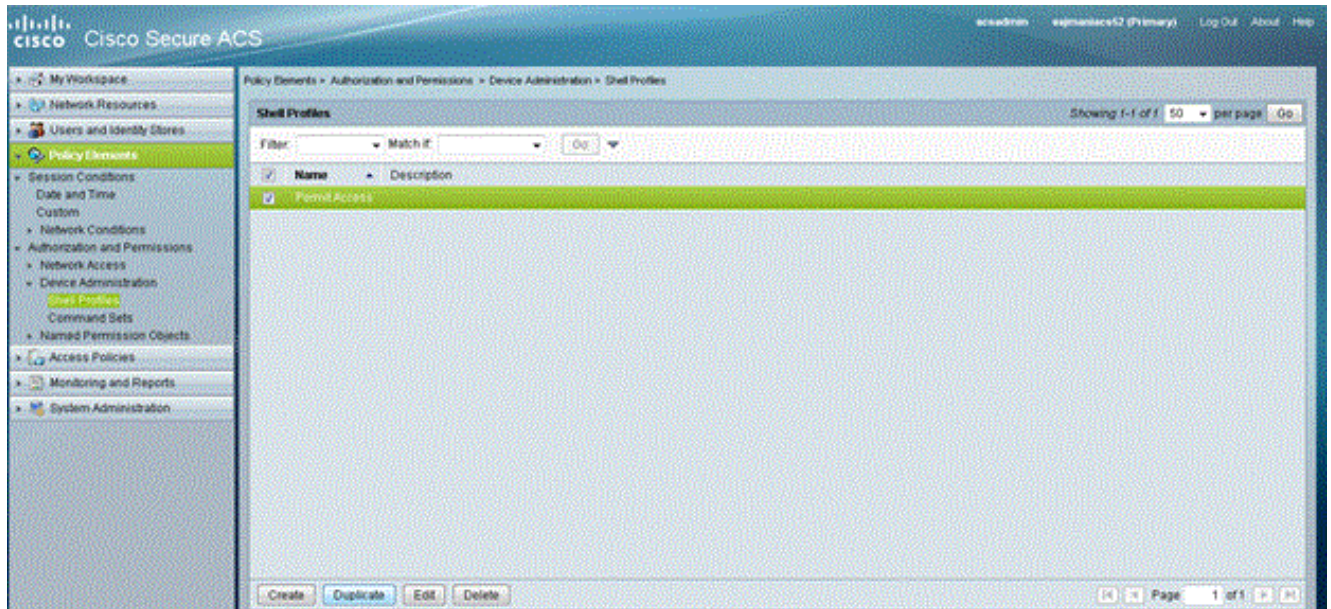
recursos de rede, a seguir clique **dispositivos de rede e clientes de AAA**. Sob dispositivos de rede, o clique **cria**. Inscreva o hostname do AP no **nome**, e forneça uma descrição sobre o AP. Selecione o **lugar** e o **tipo de dispositivo** se estas categorias são definidas. Porque somente um único AP está sendo configurado, clique o **único IP address**. Você pode adicionar a escala dos IP address para APs múltiplos clicando **escalas IP**. Então, incorpore o IP address do AP. Sob **opções de autenticação**, verifique a caixa **TACACS+** e incorpore o **segredo compartilhado**. Aqui está um exemplo:



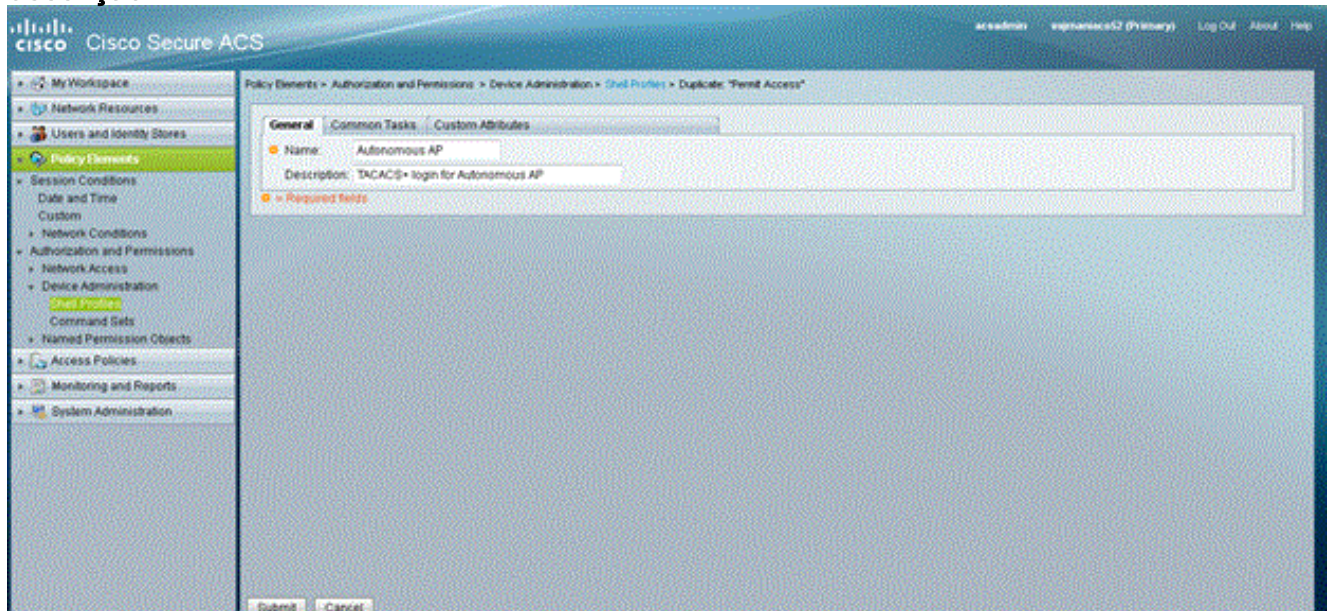
2. A próxima etapa é criar um nome de usuário e senha do início de uma sessão: Clique **usuários e lojas da identidade**, a seguir clique **usuários**. Clique em **Criar**. Dê o username sob o **nome**, e forneça uma descrição. Selecione o **grupo da identidade**, se existirem. Incorpore a senha sob a caixa de texto da **senha**, e reenter **confirmam** abaixo a **senha**. Você pode alterar a senha da possibilidade incorporando uma senha **permite** abaixo a **senha**. Reenter para confirmar. Aqui está um exemplo:



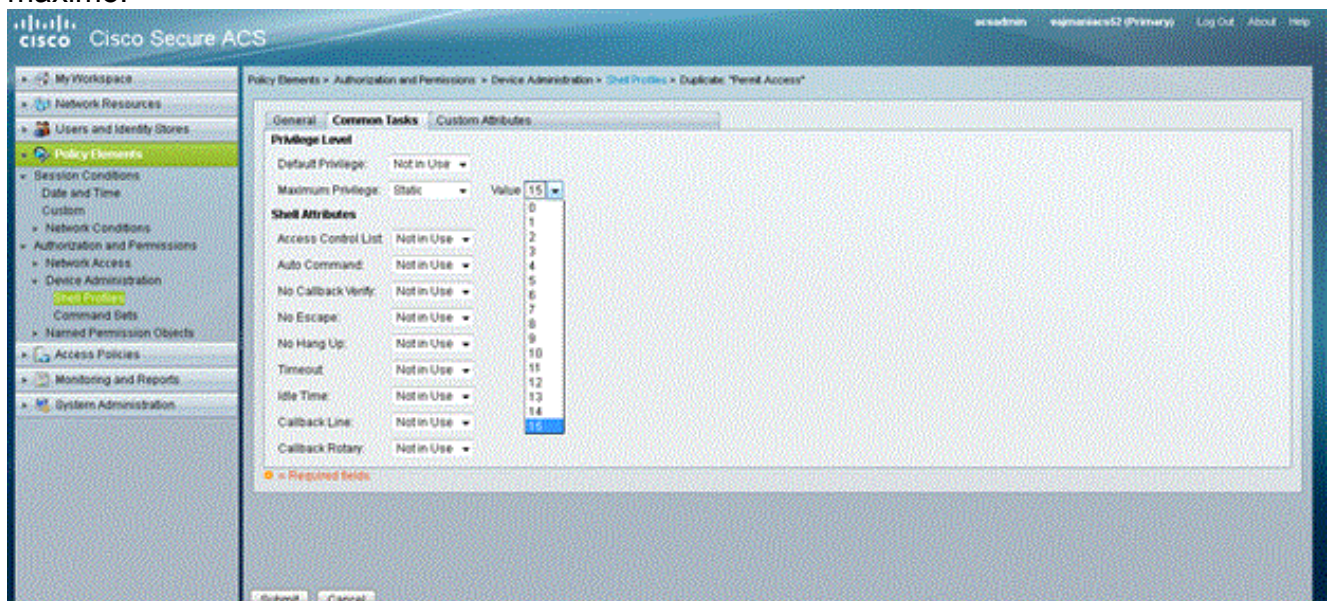
3. Termine estas etapas a fim definir o nível de privilégio: Clique **elementos da política > autorizações e permissões > de administração > de shell do dispositivo perfis**. Verifique a caixa de **verificação de acesso da licença** e clique a **duplicata**.



Incorpore o nome e a descrição.

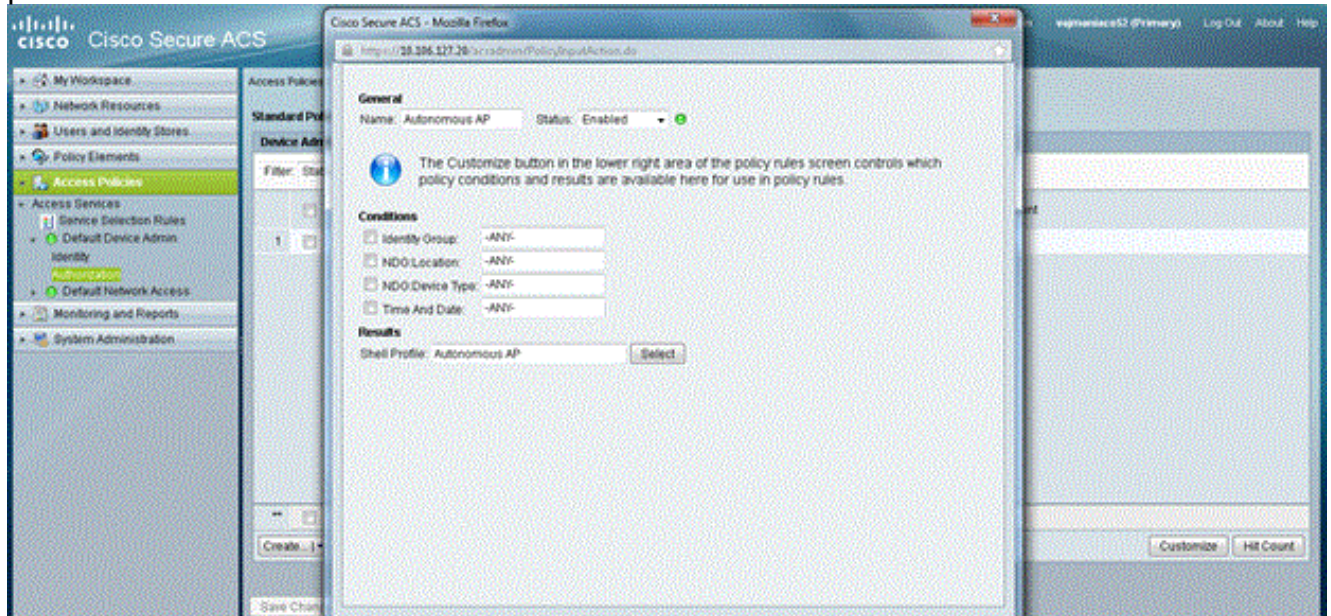


Selecione a aba comum das tarefas e escolha 15 para o privilégio máximo.

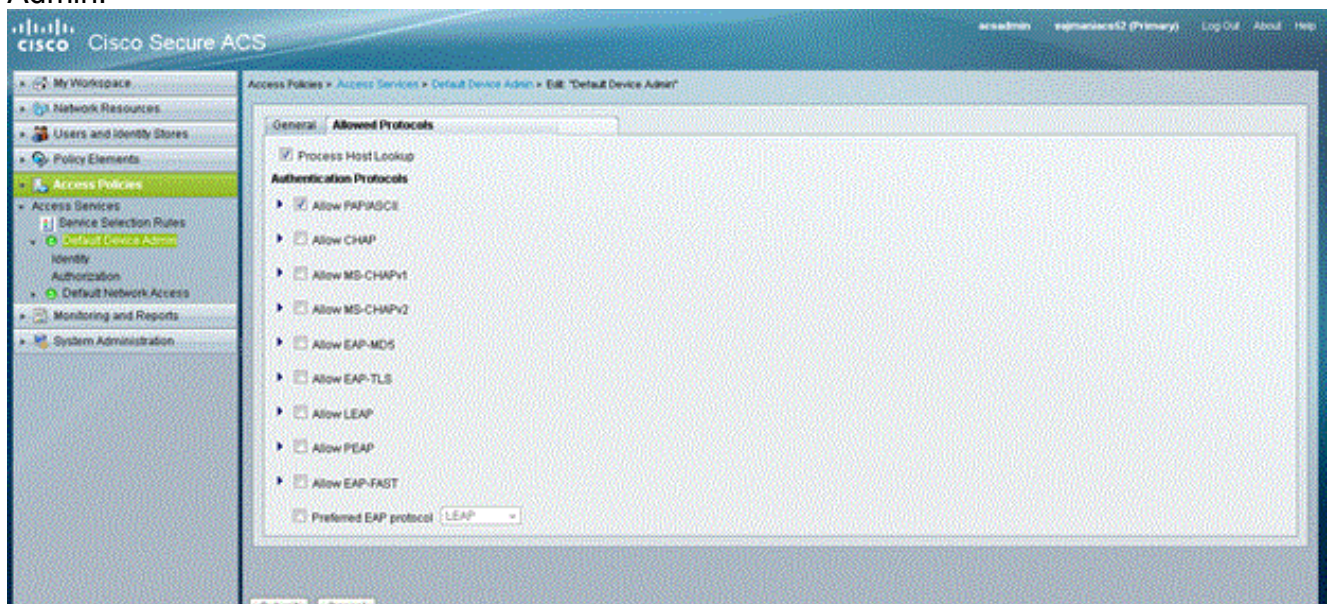


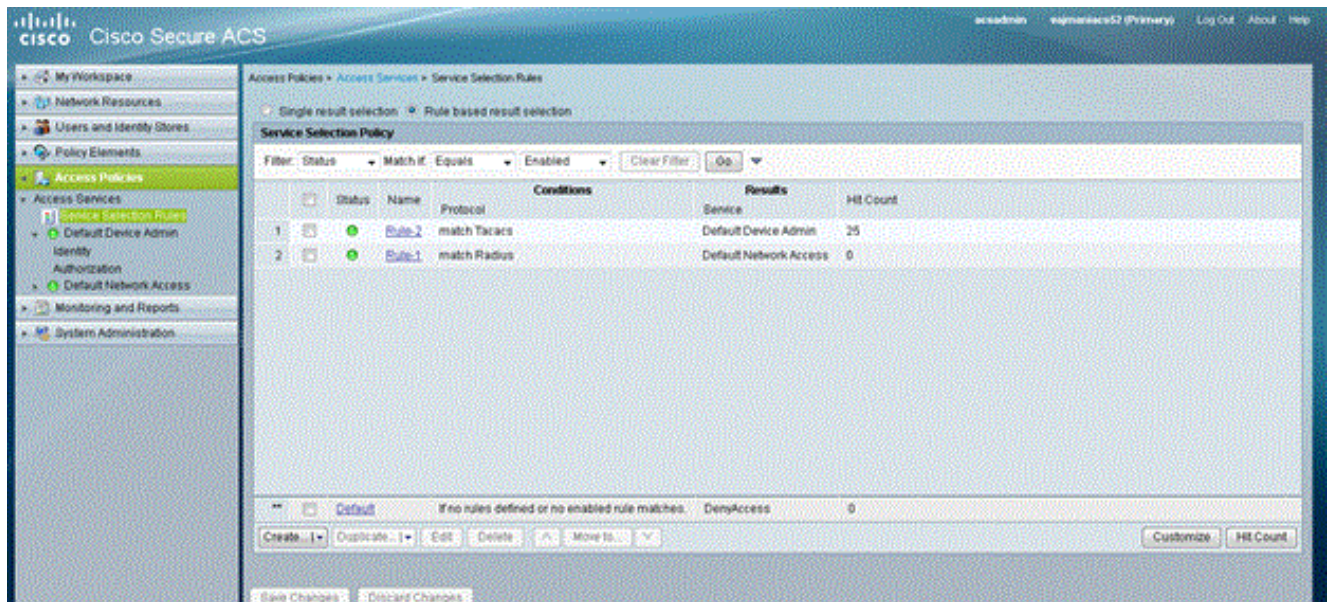
Clique em Submit.

4. Termine estas etapas a fim criar uma política da autorização: Clique **políticas de acesso > serviços do acesso > dispositivo do padrão Admin > autorização**. O clique **cria** a fim criar uma política nova da autorização. Um novo estala parece acima criar as regras para a política da autorização. Selecione o **grupo da identidade**, o **lugar** etc. para o username específico e o cliente de AAA (AP), se algum. Clique **selecionam** para que o perfil do shell escolha o AP autônomo criado perfil.



Uma vez que isto é feito, clique **mudanças da salvaguarda**. Clique o **dispositivo Admin do padrão**, a seguir clique **protocolos permitidos**. A verificação **permite PAP/ASCII**, a seguir clica-o **submete-se**. As **regras de seleção do serviço** do clique **certificar-se** lá são uma regra que combina o TACACS e que aponta para optar pelo dispositivo Admin.



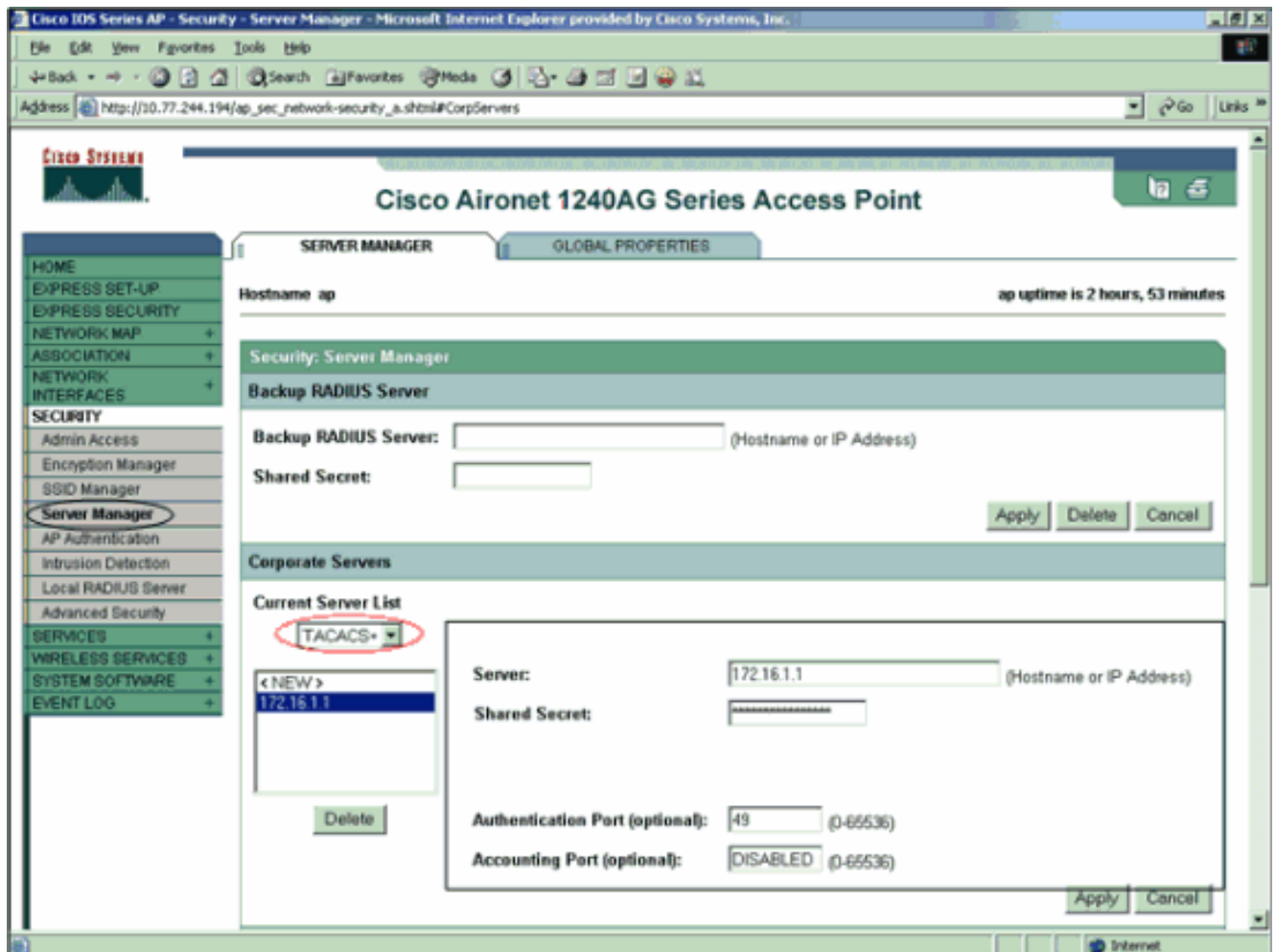


[Configurar Aironet AP para a autenticação TACACS+](#)

Você pode usar o CLI ou o GUI a fim permitir as características TACACS+ em Aironet AP. Esta seção explica como configurar o AP para a autenticação de login TACACS+ com uso do GUI.

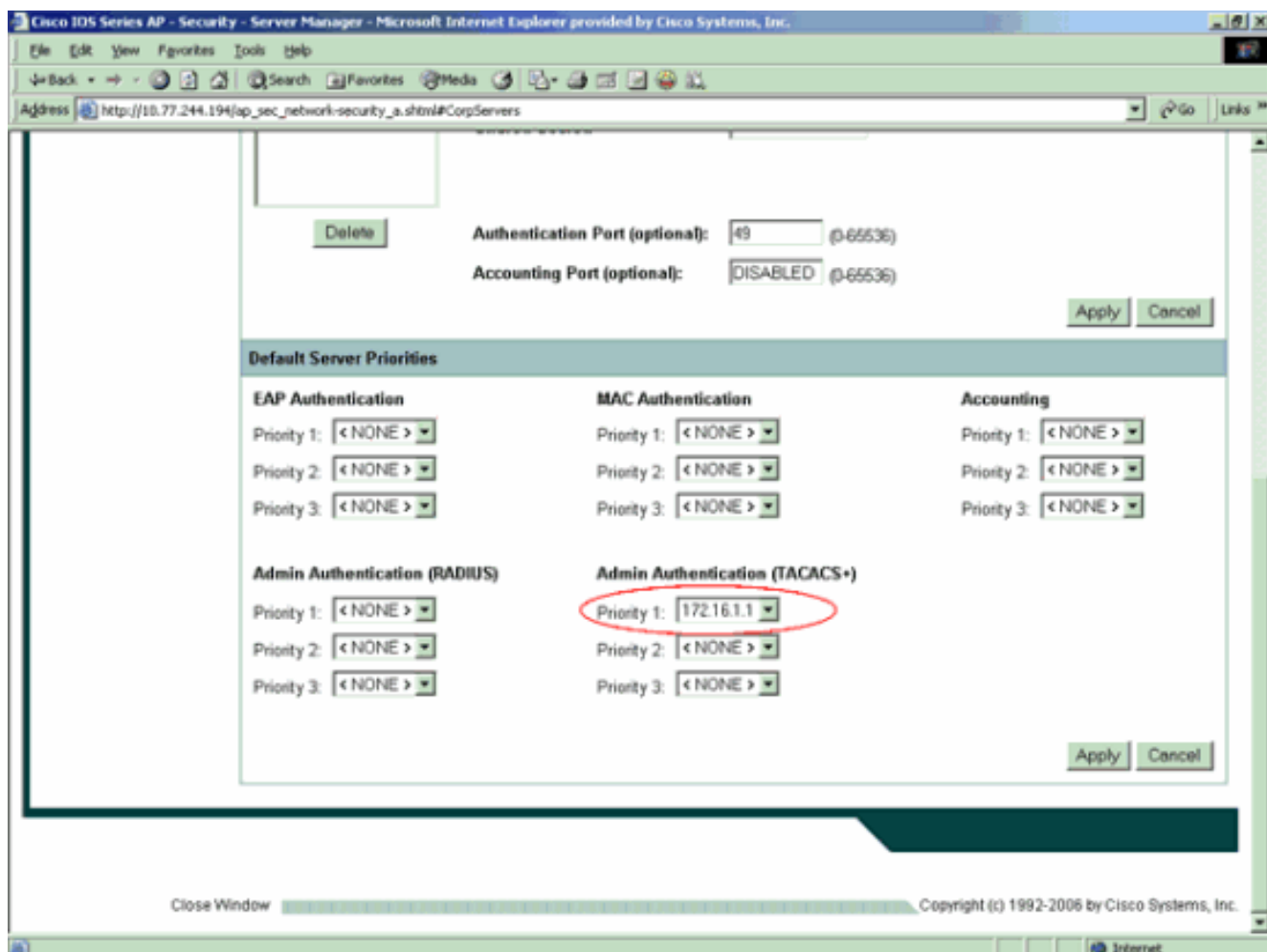
Termine estas etapas a fim configurar o TACACS+ no AP com uso do GUI:

1. Termine estas etapas a fim definir os parâmetros de servidor TACACS+:Do AP GUI, escolha a **Segurança > o gerenciador do servidor**.A Segurança: A janela do gerenciador do servidor aparece.Na área dos servidores corporativos, selecione o **TACACS+** do menu suspenso da lista do servidor atual.Nesta mesma área, incorpore o IP address, o segredo compartilhado, e o número de porta de autenticação do server TACACS+.Clique em Apply.Aqui está um exemplo:

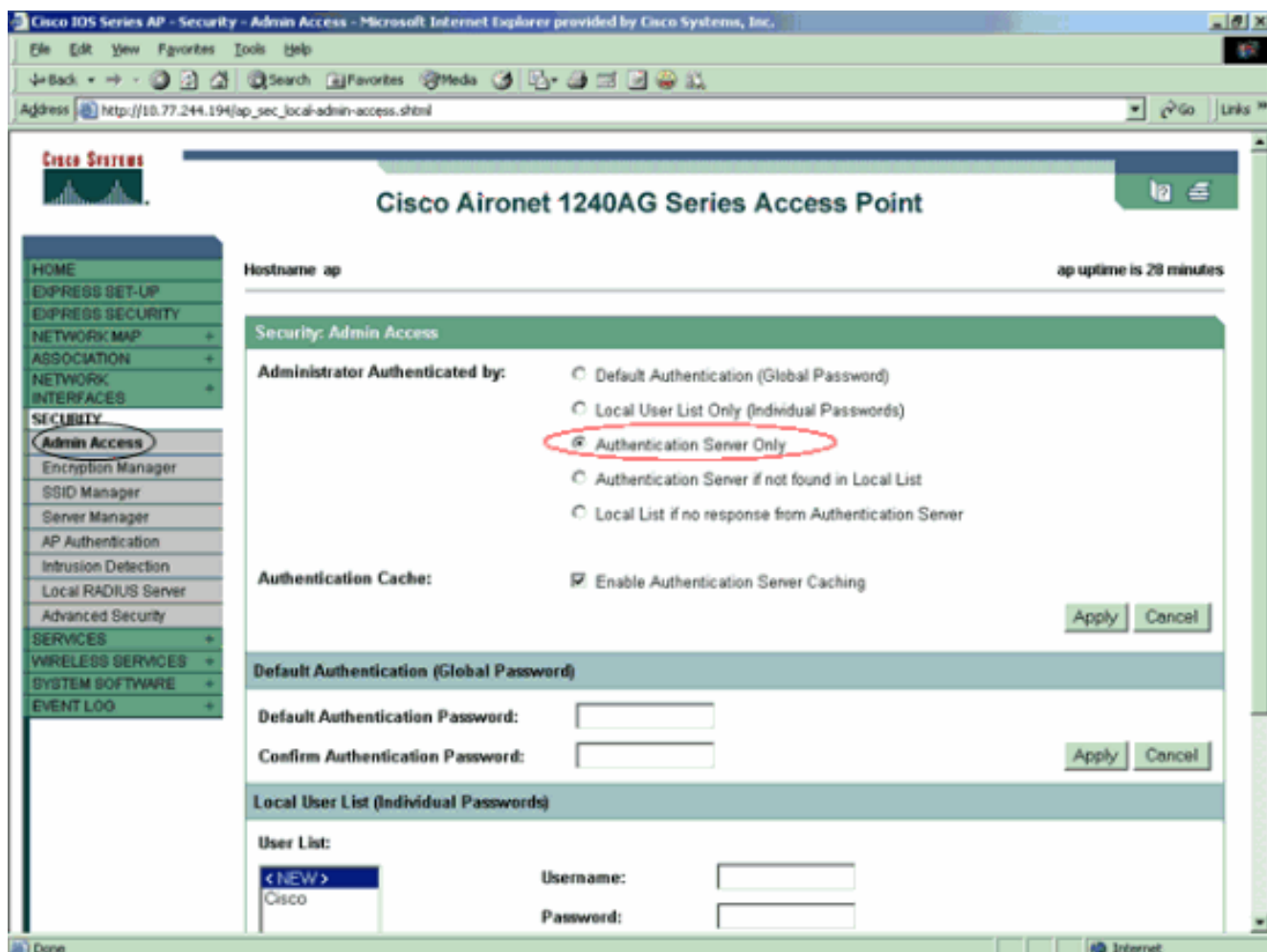


Nota: À revelia, o TACACS+ usa a porta TCP 49. **Nota:** A chave secreta compartilhada que você configura no ACS e no AP deve combinar.

- Escolha as prioridades do server do padrão > a Autenticação de admin (TACACS+), selecione do menu suspenso da prioridade 1 o endereço IP do servidor TACACS+ que você configurou, e o clique **aplica-se**. Aqui está um exemplo:



3. Escolha a **Segurança > o acesso Admin** e, porque o administrador autenticado por: , escolha o **Authentication Server somente** e o clique **aplica-se**. Esta seleção assegura-se de que os usuários que tentam entrar ao AP estejam autenticados por um Authentication Server. Aqui está um exemplo:



Esta é a configuração de CLI para o exemplo de configuração:

```

AccessPoint

AccessPoint#show running-config

Current configuration : 2535 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
!
ip subnet-zero
!
!
aaa new-model
!--- Enable AAA. !! aaa group server radius rad_eap !
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
!--- Configure the server group tac_admin. server
172.16.1.1
!--- Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1

```



```

!--- Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
  cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end

```

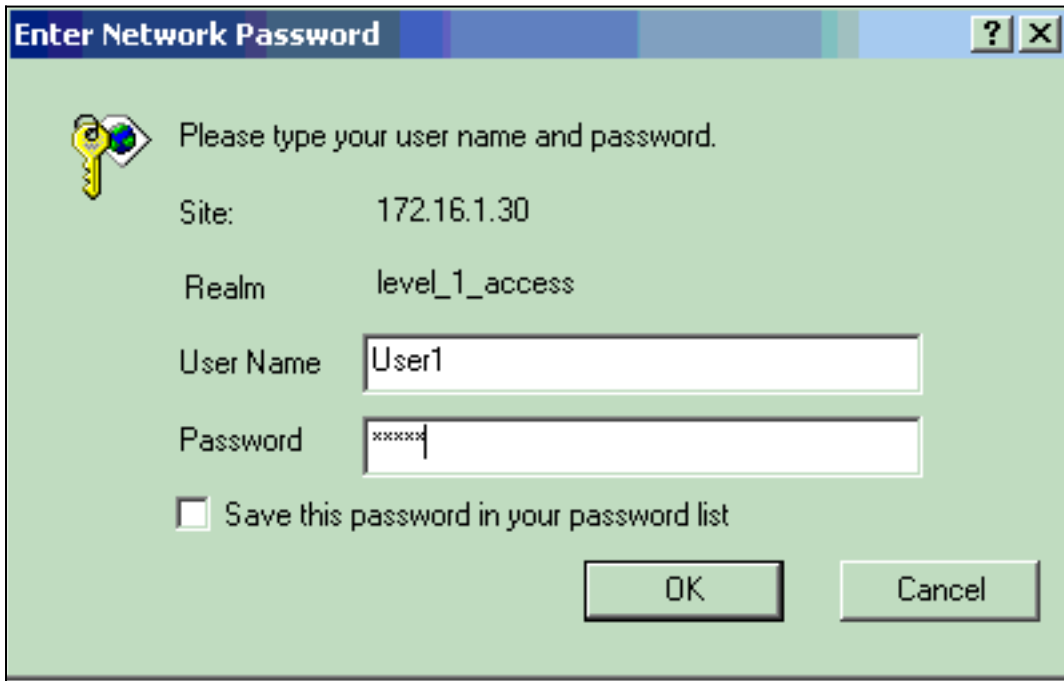
Nota: Você deve ter o Cisco IOS Software Release 12.3(7)JA ou Mais Recente para que todos os comandos nesta configuração trabalhar corretamente. Um software release mais adiantado do Cisco IOS não pôde ter todos estes comandos disponíveis.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool](#) ([apenas para clientes registrados](#)) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

A fim verificar a configuração, tente entrar ao AP com uso do GUI ou do CLI. Quando você tenta alcançar o AP, o AP alerta-o para um nome de usuário e senha.



Enter Network Password

Please type your user name and password.

Site: 172.16.1.30

Realm: level_1_access

User Name: User1

Password: *****

Save this password in your password list

OK Cancel

Quando você fornecer as credenciais do usuário, o AP para a frente as credenciais ao server TACACS+. O server TACACS+ valida as credenciais com base na informação que está disponível em seu base de dados e fornece o acesso ao AP em cima da autenticação bem sucedida. Você pode escolher **relatórios e atividade > autenticação passada no ACS** e usar o relatório passado da autenticação a fim verificar para ver se há a autenticação bem sucedida para este usuário. Aqui está um exemplo:



Select

[Refresh](#) [Download](#)

Passed Authentications active.csv

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
05/10/2006	14:57:01	Authen OK	User1	AdminUsers	172.16.1.1	tty1	172.16.1.30

Você pode igualmente usar o **comando show tacacs** a fim verificar a configuração correta do server TACACS+. Aqui está um exemplo:

```
AccessPoint#show tacacs
```

```
Tacacs+ Server      : 172.16.1.1/49
  Socket opens:      348
  Socket closes:     348
  Socket aborts:     0
  Socket errors:     0
  Socket Timeouts:   0
  Failed Connect Attempts: 0
  Total Packets Sent: 525
```

Verificação para ACS 5.2

Você pode verificar tentativas falhadas/passadas para credenciais do início de uma sessão do ACS 5.2:

1. **Monitoração do clique e relatórios > de monitoração e de relatório do lançamento visor.** Um novo estala abre acima com o painel.
2. Clique **Autenticação-TACACS-Hoje**. Isto mostra os detalhes tentativas falhadas/passadas.

Troubleshooting

Você pode usar estes comandos debug no AP a fim pesquisar defeitos sua configuração:

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- **debugar eventos dos tacacs** — Este comando indica a sequência de evento que acontece durante a autenticação TACACS. Está aqui um exemplo da saída deste comando:

```
*Mar 1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:51:21.113: TPLUS: processing authentication start request id 0
*Mar 1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
*Mar 1 00:51:21.114: TPLUS: Using server 172.16.1.1
*Mar 1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar 1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16 bytes data)
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:51:21.121: TPLUS: processing authentication continue request id 0
*Mar 1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
*Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout
*Mar 1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar 1 00:51:21.179: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar 1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

- **debug ip http authentication** — Use este comando pesquisar defeitos problemas da autenticação de HTTP. O comando indica o método de autenticação que o roteador tentou e mensagens de status autenticação-específicos.
- **debugar a autenticação aaa** — Este comando indica a informação na autenticação TACACS+ AAA.

Se o usuário incorpora um username que não exista no server TACACS+, a autenticação falha.

Está aqui o comando debug tacacs authentication output para uma autenticação falha:

```
*Mar 1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.624: TPLUS: processing authentication start request id 0
*Mar 1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3)
*Mar 1 00:07:26.624: TPLUS: Using server 172.16.1.1
*Mar 1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout
*Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar 1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading
*Mar 1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16
bytes data)
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar 1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar 1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar 1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar 1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
*Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar 1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: socket event 1
*Mar 1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar 1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar 1 00:07:26.689: TPLUS: Received authen response status FAIL (3)
```

Você pode escolher **relatórios e atividade > autenticação falha** a fim ver a tentativa da autenticação falha no ACS. Aqui está um exemplo:

Date ↓	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port
05/17/2006	19:40:14	Authen failed	User3	CS user unknown

Se você usa um software release do Cisco IOS no AP que está mais adiantado do que o Cisco IOS Software Release 12.3(7)JA, você pode bater um erro todas as vezes que você tente entrar ao AP com uso do HTTP. A identificação de bug Cisco é [CSCeb52431](#) ([clientes registrados somente](#)).

A aplicação do software HTTP/AAA do Cisco IOS exige a autenticação independente de cada um conexão de HTTP separada. Os envoltórios GUI sem fio do software do Cisco IOS a referência de muitas dúzias dos arquivos separados dentro de um único página da web (por exemplo Javascript e GIF). Assim se você carrega uma única página no software sem fio GUI do Cisco IOS, dúzias e dezenas de autenticações separadas/pedidos de autorização pode bater o servidor AAA.

Para a autenticação de HTTP, o RAI0 ou a autenticação local do uso. O servidor Radius é sujeitado ainda aos pedidos da autenticação múltipla. Mas o RAI0 é mais escalável do que o TACACS+, e assim que é provável fornecer um impacto no desempenho menos-adverso.

Se você deve usar o TACACS+ e você tem Cisco ACS, use a palavra-chave da **conexão única** com o **comando tacacs-server**. O uso desta palavra-chave com o comando poupa o ACS mais da conexão de TCP setup/carga adicional de destruição e é provável reduzir até certo ponto a carga no server.

Para os Cisco IOS Software Release 12.3(7) JA e mais tarde o AP, o software inclui um reparo. O restante desta seção descreve o reparo.

Use a característica do esconderijo da autenticação de AAA a fim pôr em esconderijo a informação que o server TACACS+ retorna. A característica do esconderijo e do perfil da autenticação permite que o AP ponha em esconderijo a autenticação/respostas de autorização para um usuário de modo que a autenticação/pedidos de autorização subsequentes não precise de ser enviada ao servidor AAA. A fim permitir esta característica com o CLI, use estes comandos:

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

Para obter mais informações sobre desta característica e dos comandos, refira [configurar a](#) seção do [esconderijo e do perfil da autenticação de administrar o Access point](#).

A fim permitir esta característica no GUI, escolher a **Segurança > o acesso Admin** e verificar o **Authentication Server da possibilidade que põe em esconderijo a caixa de verificação**. Porque este original usa o Cisco IOS Software Release 12.3(7)JA, o original usa o reparo, porque as [configurações](#) ilustram.

[Informações Relacionadas](#)

- [Configuração de servidores RADIUS e TACACS+](#)
- [Nota de campo: O Access point IO bombardeia o server TACACS+ com pedidos](#)
- [Autenticação de EAP com servidor RADIUS](#)
- [Suporte de produtos Wireless](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)