# Configurar o fluxo do convidado com ISE 2.0 e Aruba WLC

## Índice



## Introdução

Os descrbies deste documento pisam para configurar portais do convidado com o controlador do Wireless LAN de Aruba (WLC). Do apoio da versão 2.0 do Identity Services Engine (ISE) para o acesso de rede da terceira parte os dispositivos (NAD) são introduzidos. O ISE apoia atualmente a integração com o Sem fio de Aruba para o convidado, postura e Bring Your Own Device (BYOD) flui.

> Nota: Cisco não é responsável para a configuração ou o apoio para dispositivos dos outros fornecedores.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

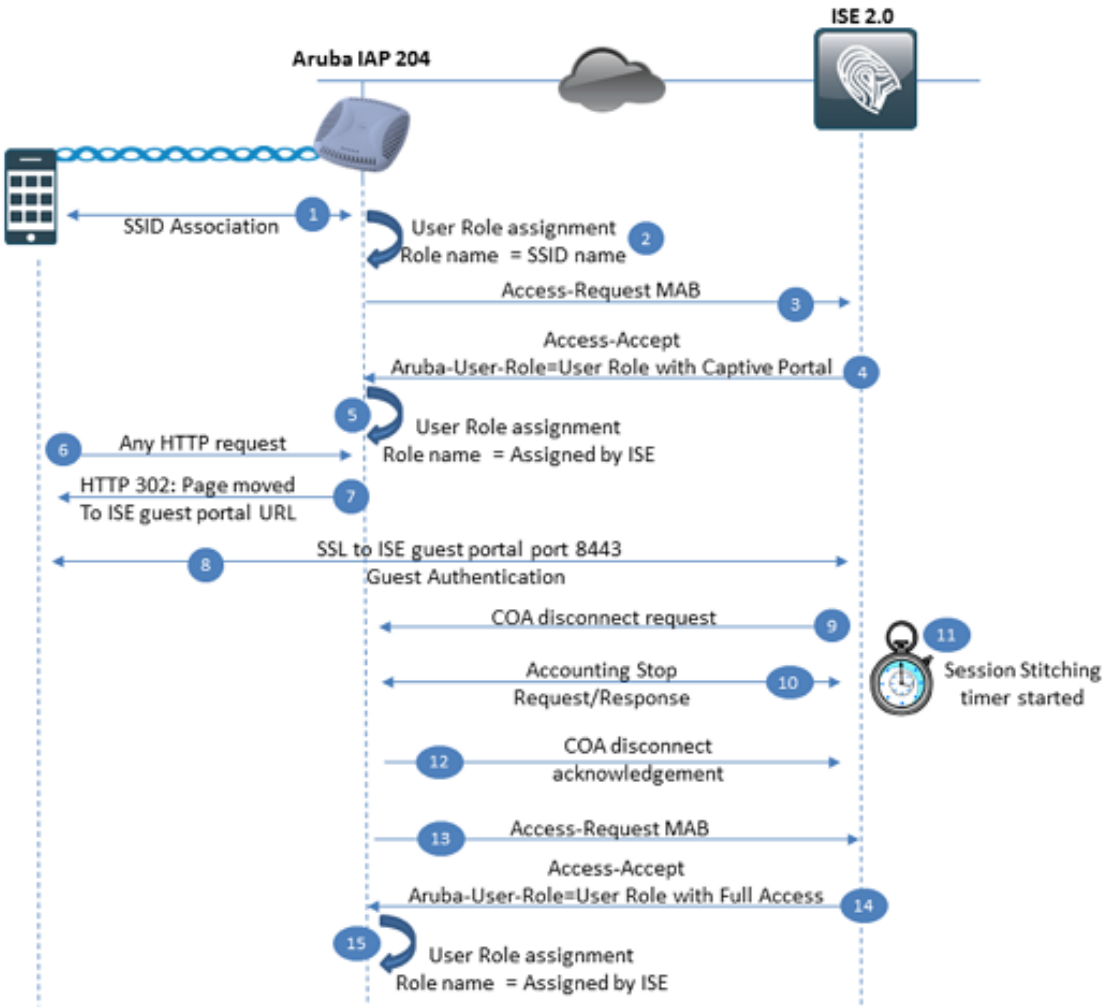
- Configuração de Aruba IAP
- Fluxo do convidado no ISE

## Componentes Utilizados

- Software 6.4.2.3 de Aruba IAP 204
- Cisco Identity Services Engine 2.0

# Informações de Apoio

### Fluxo do convidado




**Etapa 1.** O usuário é associado ao conjunto de serviço Identifer (SSID). O SSID pode ser configurado como aberto ou com autenticação da chave pré-compartilhada.

**Etapa 2.** Aruba aplica o papel de usuário a esta conexão. O primeiro papel de usuário é sempre SSID próprio. O papel de usuário contém ajustes diferentes como o VLAN, a limitação do controle de acesso, o ajuste do Cativo-portal e o mais. No papel de usuário do padrão do exemplo atual atribuído ao SSID tem somente Licença-toda indicação.

**Etapa 3.** O SSID é configurado para fornecer o MAC que filtra sobre o servidor de raio externo. A solicitação de acesso MAB do raio (desvio da autenticação de MAC) é enviada ao ISE.

Etapa 4. No tempo da avaliação da política o ISE seleciona o perfil da autorização para o convidado. Este perfil da autorização contém o tipo de acesso igual a ACCESS_ACCEPT e o Aruba-USER-papel igual ao papel de usuário do nome configurado localmente em Aruba WLC (controlador do Wireless LAN). Este papel de usuário é configurado para o Cativo-portal e o tráfego é reorientado para o ISE.

### Papéis de usuário de Aruba

O componente principal que é usado por Aruba WLC é papel de usuário. O papel de usuário define a restrição de acesso aplicável ao usuário na altura da conexão. A restrição de acesso pode incluir: Reorientação portal prisioneira, Access Control List, VLAN (rede de área local virtual), limitação de largura de banda e outro. Cada SSID que existe em Aruba WLC tem o papel de usuário do padrão onde o papel de usuário é igual ao nome SSID, todos os usuários conectados ao SSID específico obtém inicialmente limitações do papel do padrão. O papel de usuário pode ser overwritten pelo servidor Radius, neste caso aceitação de acesso deve conter o Aruba-USER-papel específico do atributo do vendedor de Aruba. O valor deste atributo é usado pelo WLC para encontrar o papel de usuário local.

Etapa 5. Com verificações do Aruba-USER-papel WLC do atributo localmente para papéis de usuário configurados e aplica exigido.

Etapa 6. O usuário inicia o pedido do HTTP no navegador.

Etapa 7. Pedido das intercepções de Aruba WLC devido ao papel de usuário configurado para o portal prisioneiro. Como uma resposta a este pedido WLC retorna a página do código 302 HTTP movida com o portal do convidado ISE como um lugar novo.

Etapa 8. O usuário estabelece a conexão SSL ao ISE na porta 8443, e fornece o username/senha no portal do convidado.

Etapa 9. O ISE envia a mensagem da solicitação de desconexão COA a Aruba WLC.

Etapa 10. Depois que a mensagem WLC da disconexão COA deixa cair a conexão com o usuário e informa o ISE que a conexão deve ser terminada usando a mensagem do Contabilidade-pedido do raio (parada). O ISE tem que confirmar que esta mensagem esteve recebida com contabilidade.

Etapa 11. O ISE começa o temporizador de costura da sessão. Este temporizador é usado para ligar junto a sessão antes e depois do COA. Durante este tempo o ISE recorda todos os parâmetros de sessão como o username, etc. A segunda tentativa de autenticação deve ser feita antes que este temporizador expire para selecionar a política correta da autorização para o cliente. Caso que se o temporizador expira, a solicitação de acesso nova será interpretada como uma sessão completamente nova e política da autorização com convidado Redirect será aplicada outra vez.

Etapa 12. Aruba WLC confirma a solicitação de desconexão previamente recebida COA com o reconhecimento da disconexão COA.

Etapa 13. Aruba WLC envia a solicitação de acesso nova do raio MAB.

Etapa 14. No tempo da avaliação da política o ISE seleciona o perfil da autorização para o convidado após a autenticação. Este perfil da autorização contém o tipo de acesso igual a ACCESS_ACCEPT e o Aruba-USER-papel igual ao papel de usuário do nome configurado

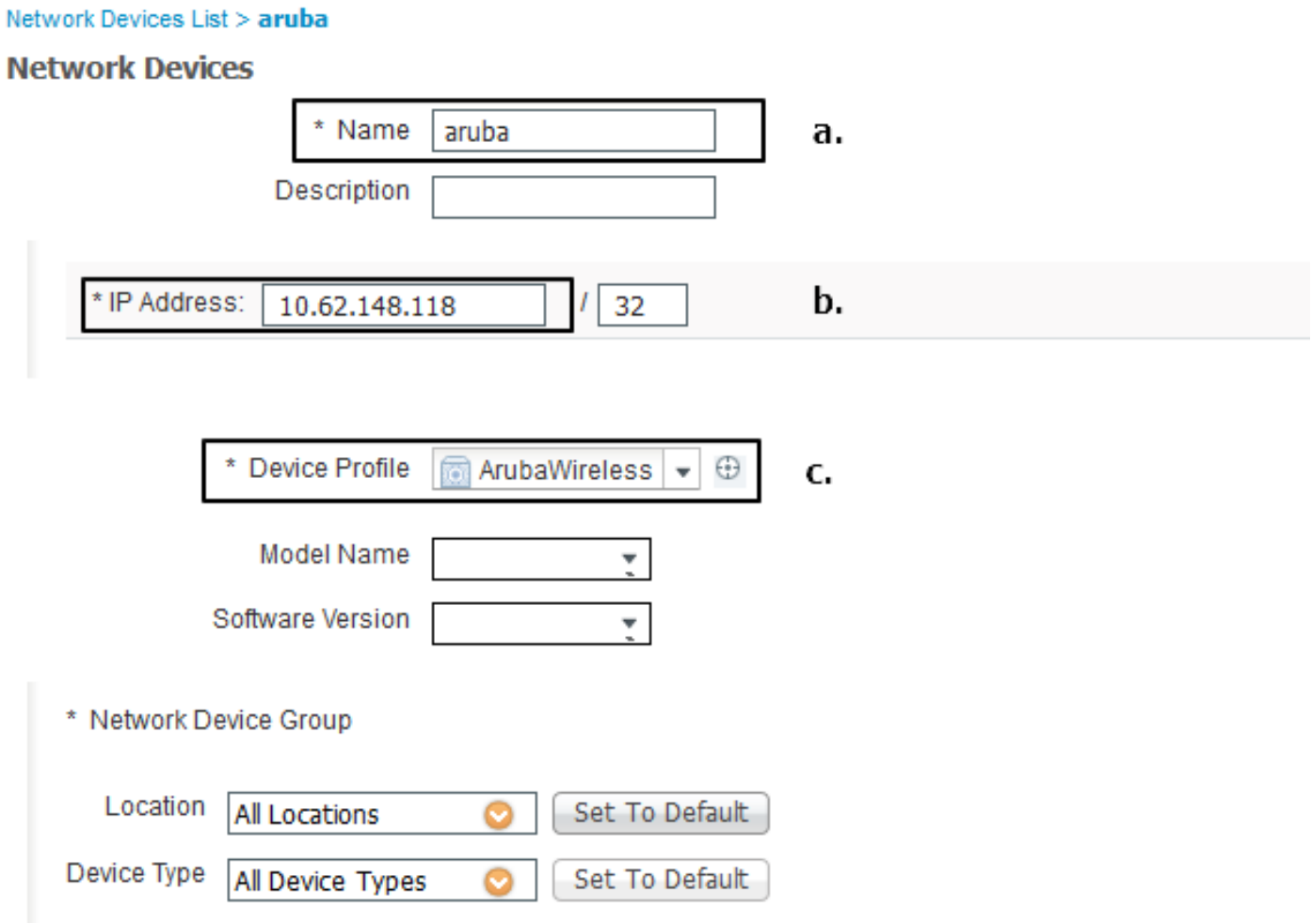
localmente em Aruba WLC. Este papel de usuário configurado para permitir todo o tráfego.

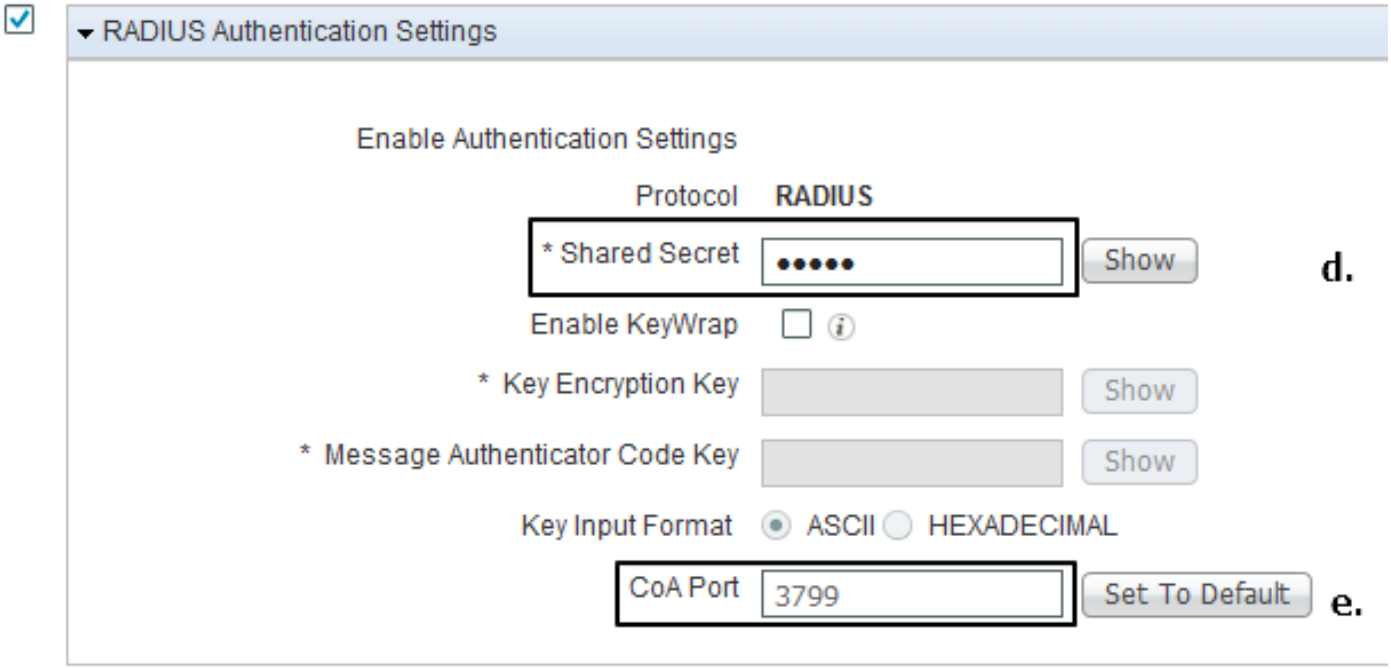
**Etapa 15.** Com Aruba-USER-papel do atributo o WLC verifica papéis de usuário localmente configurados e aplica exigido.

# Configurar

## Etapa 1. Adicionar Aruba WLC como o NAD no ISE.

Navegue à **administração > aos recursos de rede > aos dispositivos de rede** e o clique **adiciona**

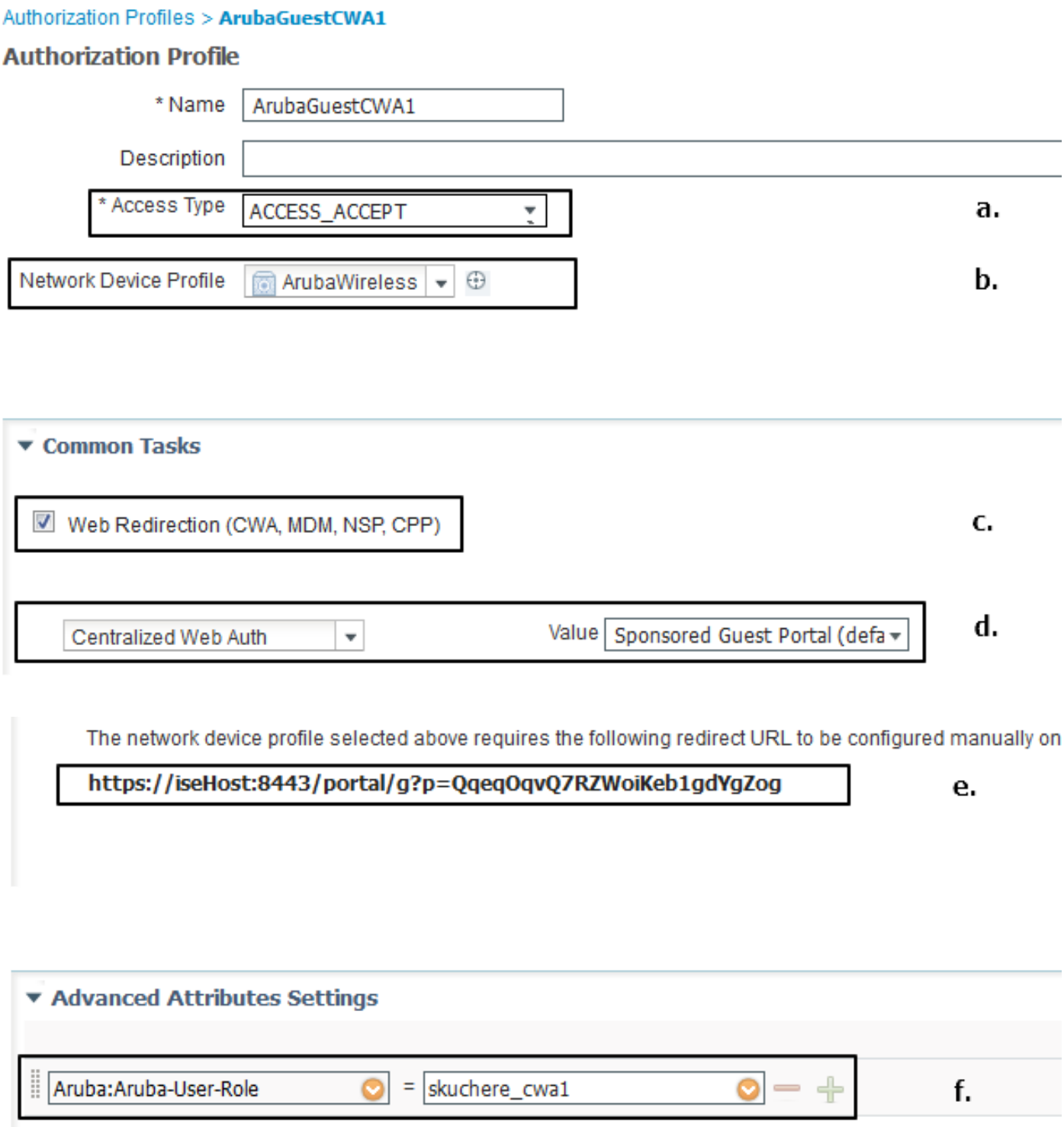





1. Forneça o nome do dispositivo do acesso de rede (NAD).
2. Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT NAD.
3. Escolha o perfil do dispositivo de rede. Para Aruba WLC você pode usar o perfil incorporado ArubaWireless.
4. Forneça a chave pré-compartilhada.
5. Defina a porta COA, a porta 3799 do uso UDP do exemplo atual do formulário do dispositivo para o COA.

## Etapa 2. Configurar perfis da autorização.

Navegue à **política > aos elementos da política > aos resultados > à autorização > ao perfil da autorização** e o clique **adiciona.** Primeiramente você tem que criar o perfil da autorização para a autenticação da Web central (CWA) reorienta, segundo as indicações da imagem.

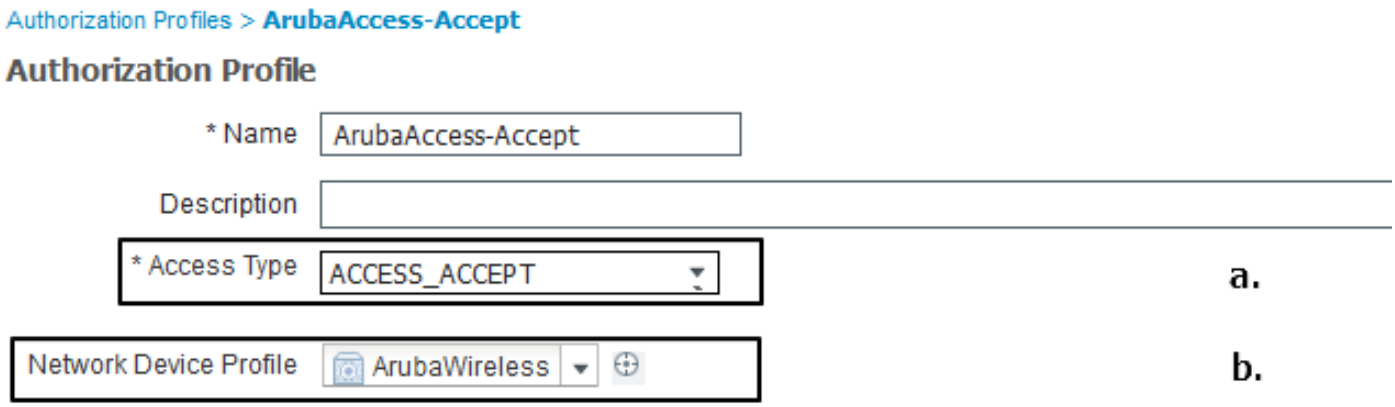


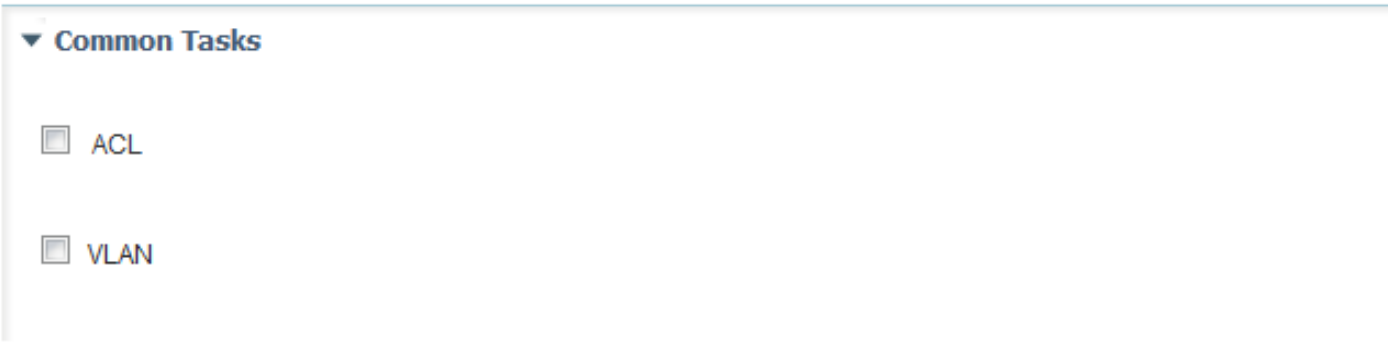

Nota: À revelia todos os perfis da autorização têm o tipo de dispositivo de rede igual a Cisco. Se o NAD próprio está configurado como ArubaWireless e perfil da autorização está criada para o tipo de outro dispositivo, este perfil está combinado nunca para este dispositivo.

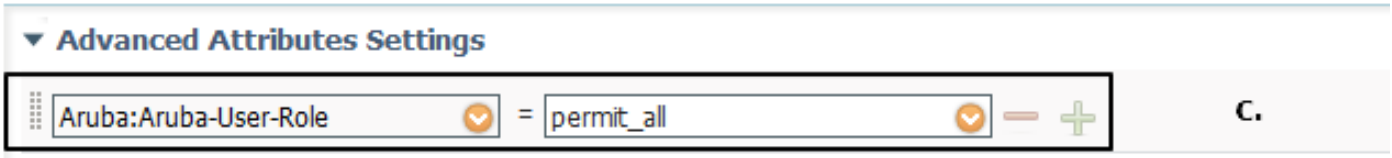
1. Defina o **tipo de acesso** como a **aceitação de acesso**.
2. **No perfil do** dispositivo de rede selecione **ArubaWireless**.
3. Na seção comum da tarefa, permita a opção da **reorientação da Web**.
4. Porque um tipo **AUTH centralizado** seleto da reorientação da **Web** e seleciona o portal do convidado que você gostaria de usar para a reorientação.
5. A URL que o ISE apresenta deve ser definida em Aruba WLC como o portal prisioneiro externo URL.

6. **Em atributo avançado os ajustes** secionam, definem o papel de usuário do valor de atributo de Aruba.

O segundo perfil da autorização deve ser criado para fornecer o acesso para usuários convidado após a autenticação portal:




1. Defina o **tipo de acesso** como a **aceitação de acesso**.
2. **No perfil do dispositivo de rede** selecione **ArubaWireless**.
3. Em seção **avançada dos ajustes do atributo** defina o papel de usuário do valor de atributo de Aruba. Mais tarde você configurará o papel de usuário local em Aruba WLC com o mesmo nome.

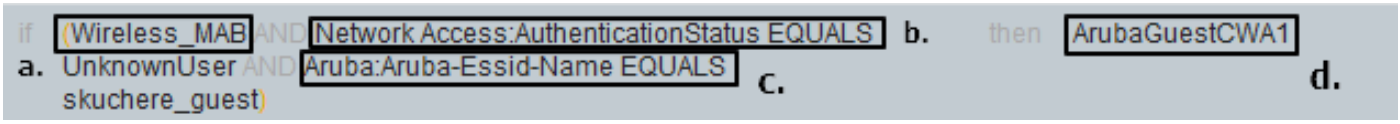
## Etapa 3. Configurar a política da autorização.

A primeira política da autorização é responsável para a reorientação do usuário ao portal do convidado. No caso o mais simples, você pode usar-se construído em condições compostas

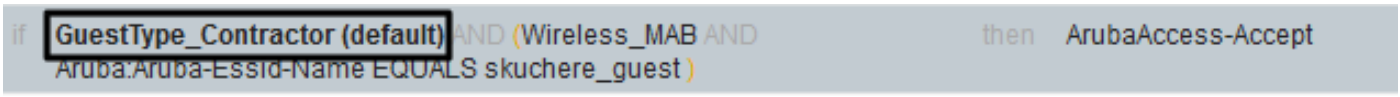
- Wireless_MAB (A.) e
- Igual de AuthenticationStatus do acesso de rede ao usuário desconhecido (B.) e
- Aruba-Essid-nome de Aruba igual a seu nome do convidado SSID (C.).

Para esta política, configurar o perfil da autorização com reorientam ao portal do convidado em

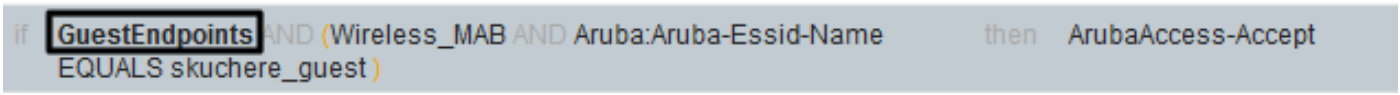
consequência (o D.)




A segunda política da autorização deve fornecer o acesso para o usuário convidado após a autenticação através do portal. Esta política pode confiar em dados de sessão (fluxo do convidado do caso do grupo da identidade do usuário/uso e assim por diante). Nesta encenação o usuário deve reconectar antes que o temporizador de costura da sessão expire:




Para proteger-se da expiração do temporizador de costura da sessão você pode confiar em dados do valor-limite em vez dos dados de sessão. À revelia, o portal patrocinado do convidado em ISE 2.0 é configurado para o registro automático do dispositivo do convidado (o dispositivo do convidado é colocado automaticamente no grupo da identidade do valor-limite de Guest_Endpoints). Este grupo pode ser usado como uma circunstância:

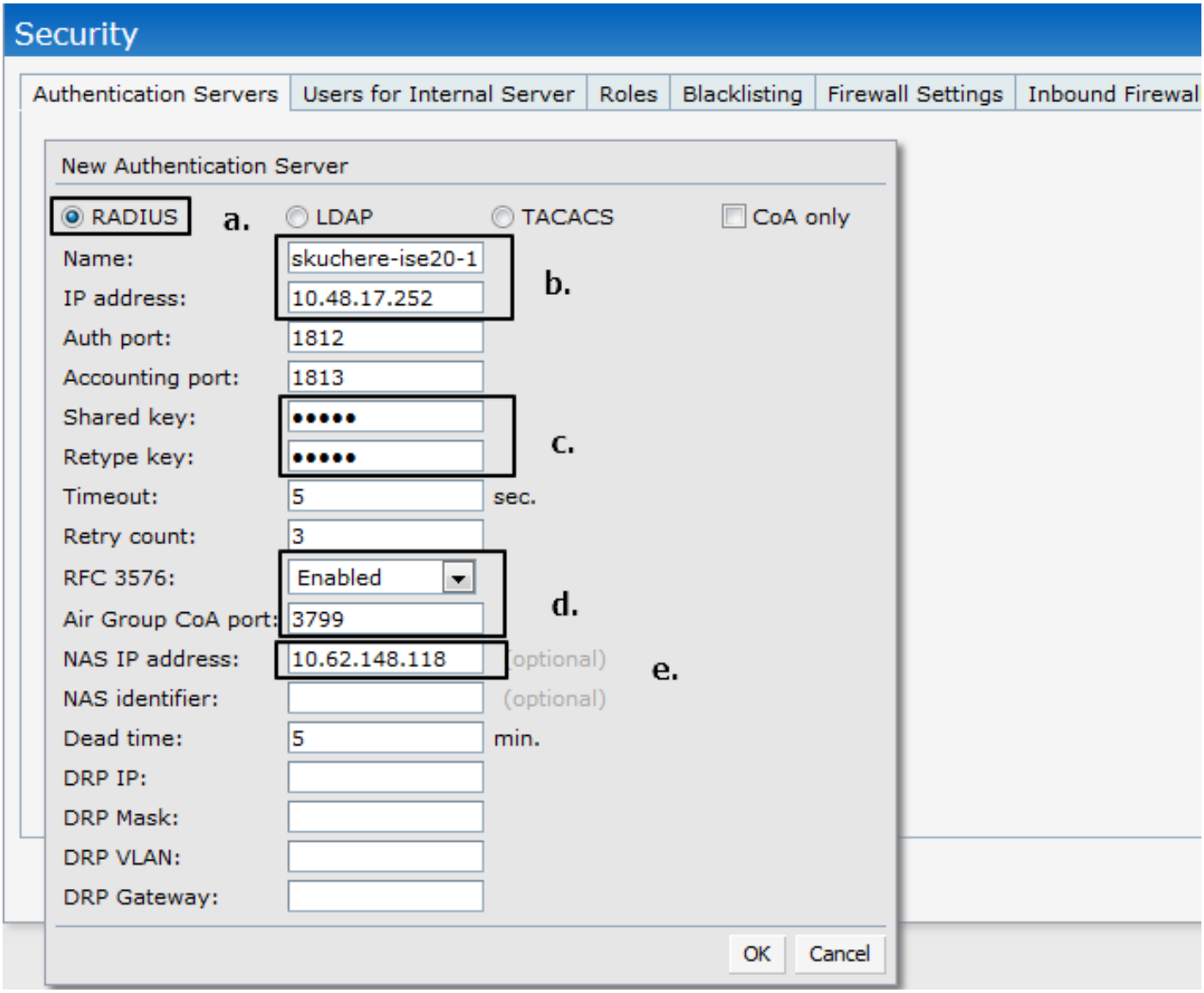



Política da autorização na ordem correta:

| | | | |
|---|---|---|---|
| if | **GuestEndpoints** AND (Wireless_MAB AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest ) | then | ArubaAccess-Accept |
| if | (Wireless_MAB AND Network Access:AuthenticationStatus EQUALS UnknownUser AND Aruba:Aruba-Essid-Name EQUALS skuchere_guest ) | then | ArubaGuestCWA1 |

## Etapa 4. Configurar o servidor Radius em Aruba.

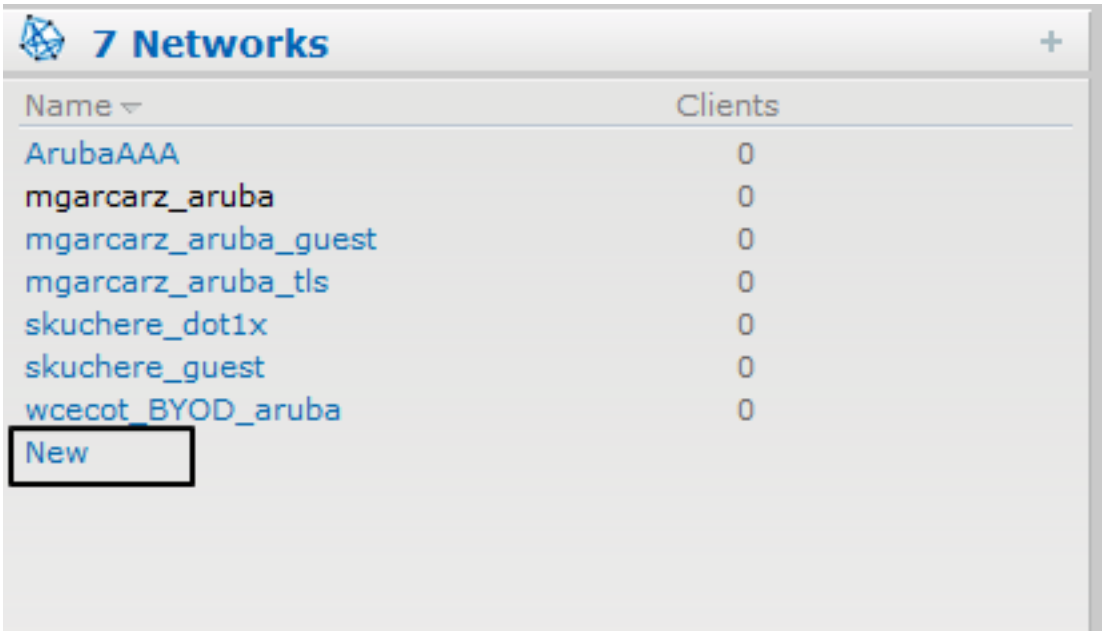
Navegue **Security > Authentication aos server** e clique **novo:**



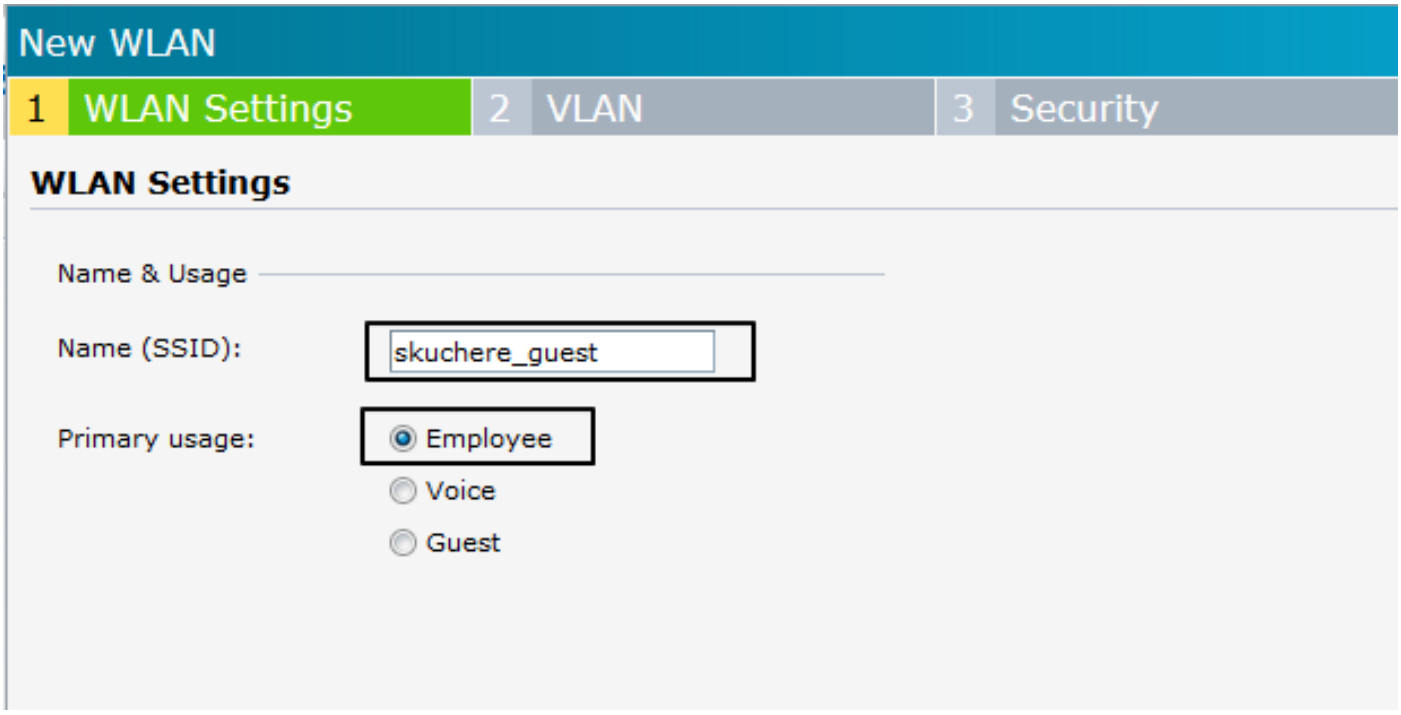

1. Escolha o RAIO como o protocolo de AAA.
2. Defina o nome e o endereço IP de Um ou Mais Servidores Cisco ICM NT de servidor AAA.
3. Especifique a chave pré-compartilhada.
4. Permita o apoio do RFC 3576 e defina a porta COA.
5. Especifique o IP da interface de gerenciamento de Aruba WLC como o endereço IP de Um ou Mais Servidores Cisco ICM NT NAS.

## Etapa 5. Crie o convidado SSID em Aruba.

Na página do painel selecione **novo na** extremidade do liste de redes. O wizard de criação SSID deve começar. Siga etapas do assistente.

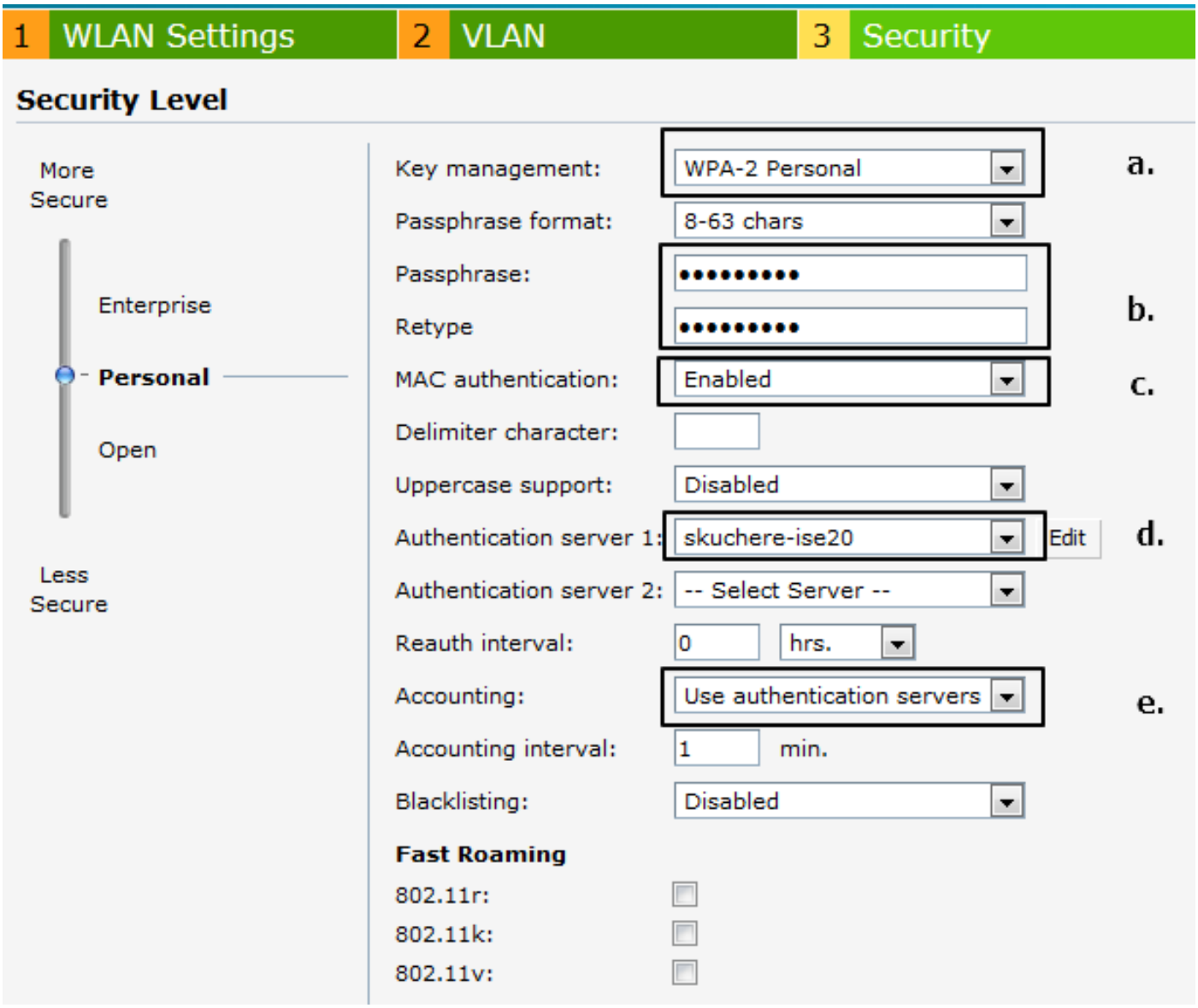



Etapa 1. Defina o nome SSID e selecione o tipo SSID. Aqui, o tipo empregado SSID é usado. Este tipo SSID não tem o papel com licença todos do padrão e nenhuma aplicação portal prisioneira. Também, você pode escolher o tipo convidado. Em tal encenação você deve definir os ajustes portais prisioneiros durante a configuração SSID.




Etapa 2. VLAN e atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT. Aqui, os ajustes são deixados como padrões, segundo as indicações da imagem.


Etapa 3. Configurações de segurança. Para o convidado SSID você pode selecionar abre ou pessoal. Pessoal exige a chave do PRE-fragmento.



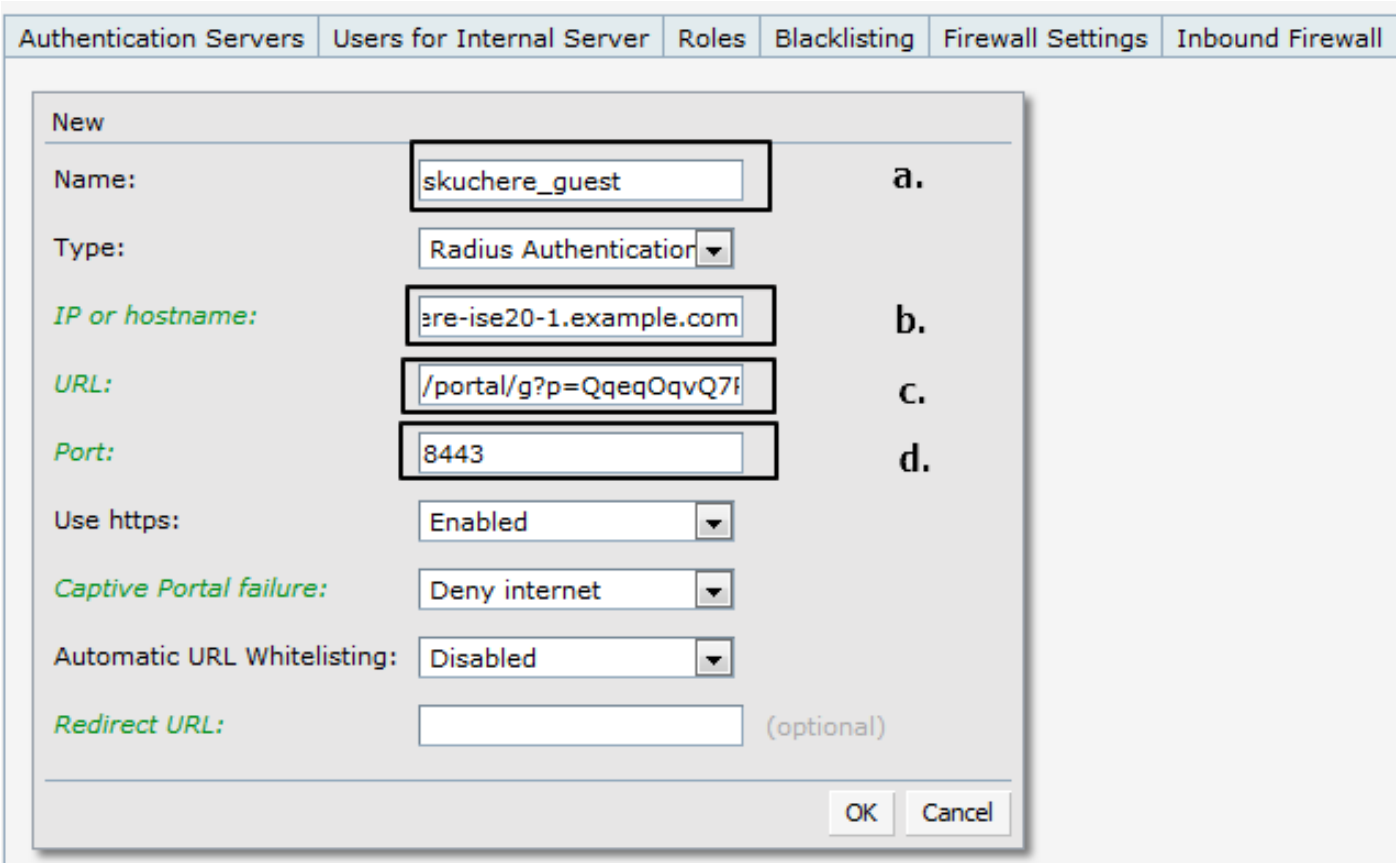

1. Escolha o mecanismo do gerenciamento chave.
2. Defina a chave pré-compartilhada.
3. Para autenticar o usuário contra o ISE usando a necessidade de filtração MAB MAC de ser permitido.
4. Na lista de servidor de autenticação escolha seu servidor AAA.

5. Para permitir a contabilidade para o servidor AAA previamente definido escolha o Authentication Server do uso na lista de drop-down.

Nota: A contabilidade é crucial com terceiro-parte NADs. Se o nó do serviço da política (PSN) não recebe a Contabilidade-parada para o usuário do NAD, a sessão pode obter colada no estado começado.

## Etapa 6. Configurar o portal prisioneiro.

Navegue à **Segurança > portais prisioneiros externos** e crie o portal novo, segundo as indicações da imagem:




Etapa 1. Especifique o nome portal prisioneiro.

Steo 2. define seu FQDN ISE ou endereço IP de Um ou Mais Servidores Cisco ICM NT. Se você usa o endereço IP de Um ou Mais Servidores Cisco ICM NT, assegure-se de que este IP definido no campo alternativo sujeito de Name(SAN) do certificado do portal do convidado.

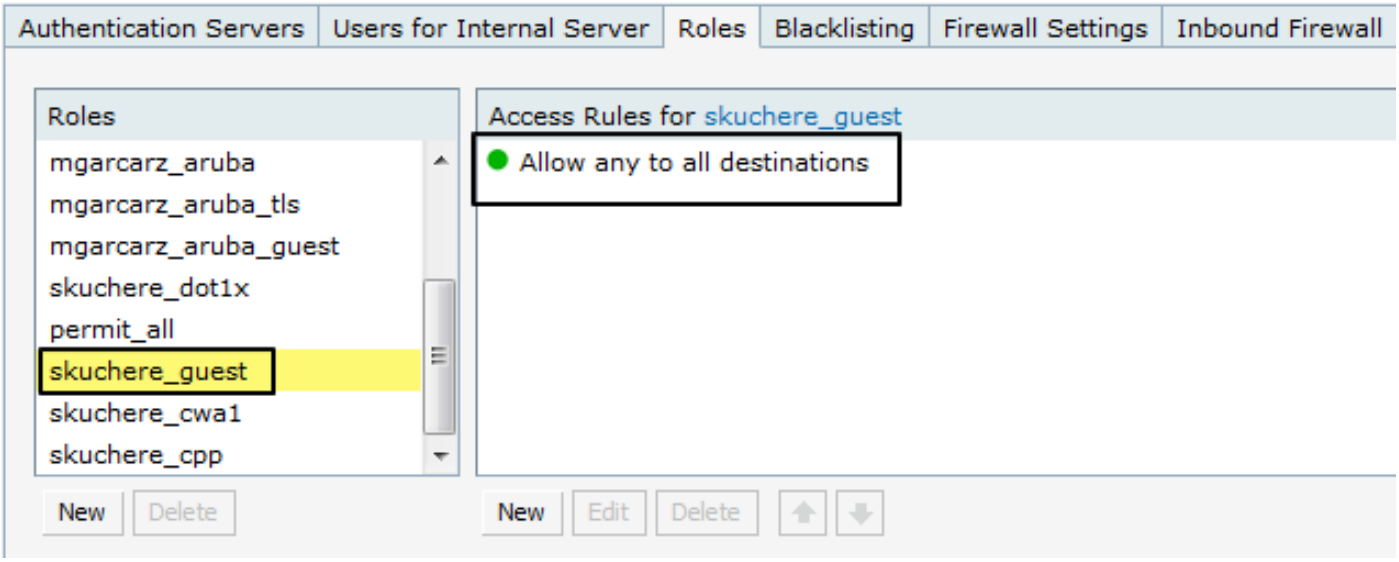
Nota: Você pode usar todo o server PSN, mas o usuário deve sempre ser reorientado ao server onde o MAB ocorreu. Geralmente você tem que definir o FQDN do servidor Radius que foi configurado no SSID.

Etapa 3. Provide reorienta do perfil da autorização ISE. Você deve pôr aqui a peça após o número de porta,

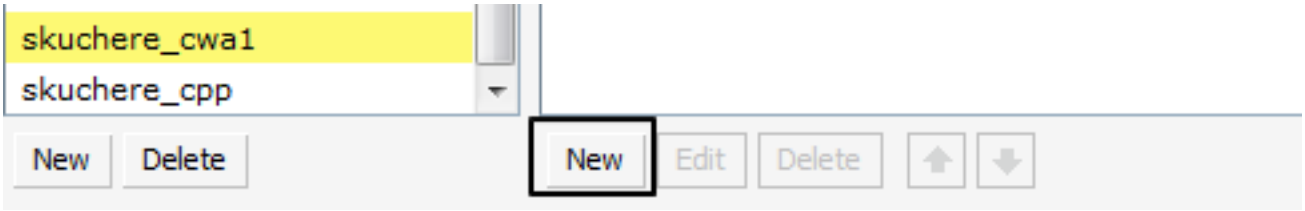
Etapa 4. Defina a porta do portal do convidado ISE.

## Etapa 7. Configurar papéis de usuário.

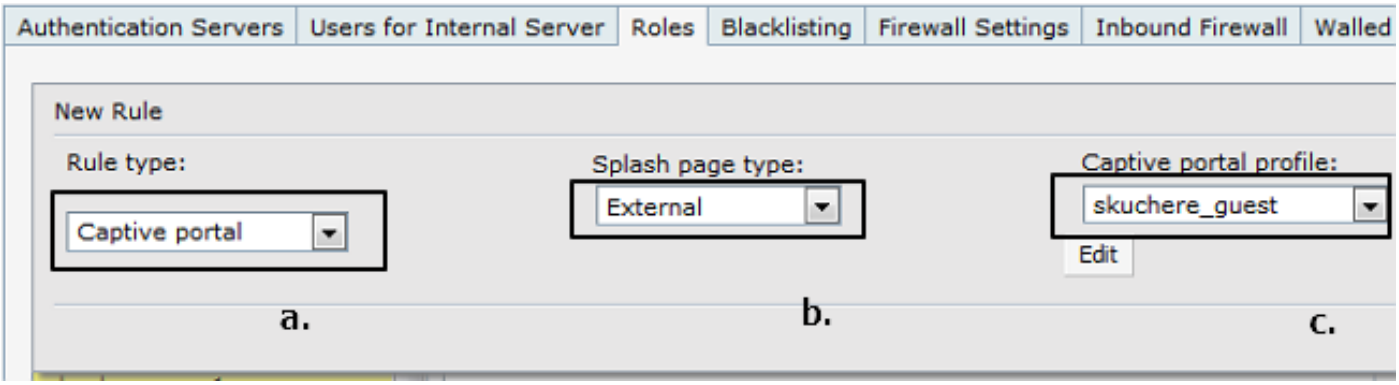
Navegue à **Segurança > aos papéis.** Assegure-se de que depois que o SSID é criado, o papel novo com o mesmo nome este presente na lista com licença da regra do acesso a todos os destinos. Adicionalmente, crie dois papéis: um para CWA reorienta e em segundo para o acesso da licença após a autenticação em portais do convidado. Os nomes destes papéis devem ser idênticos ao papel de usuário de Aruba definido em perfis da autorização ISE.



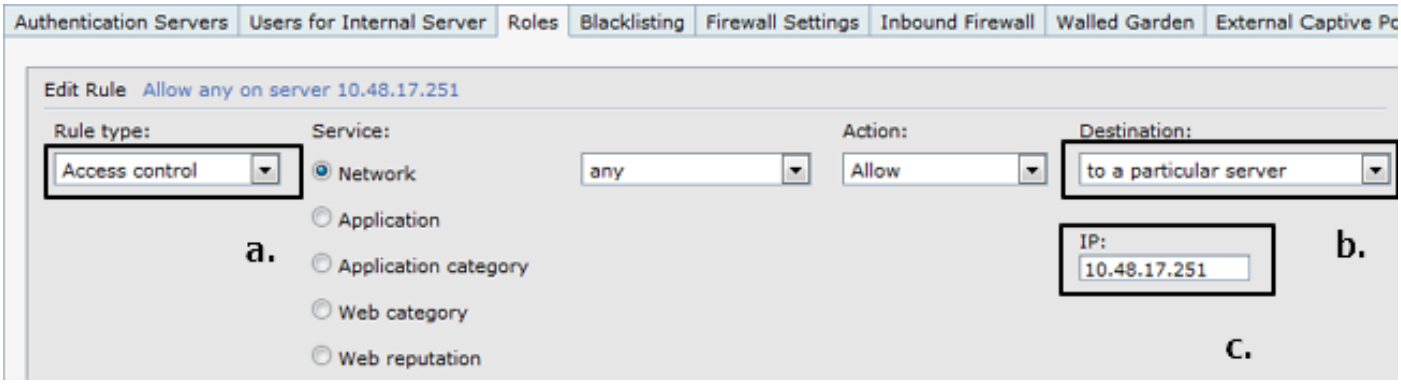

Segundo as indicações da imagem, crie o papel de novo usuário para reorientam e adicionam a restrição de segurança.



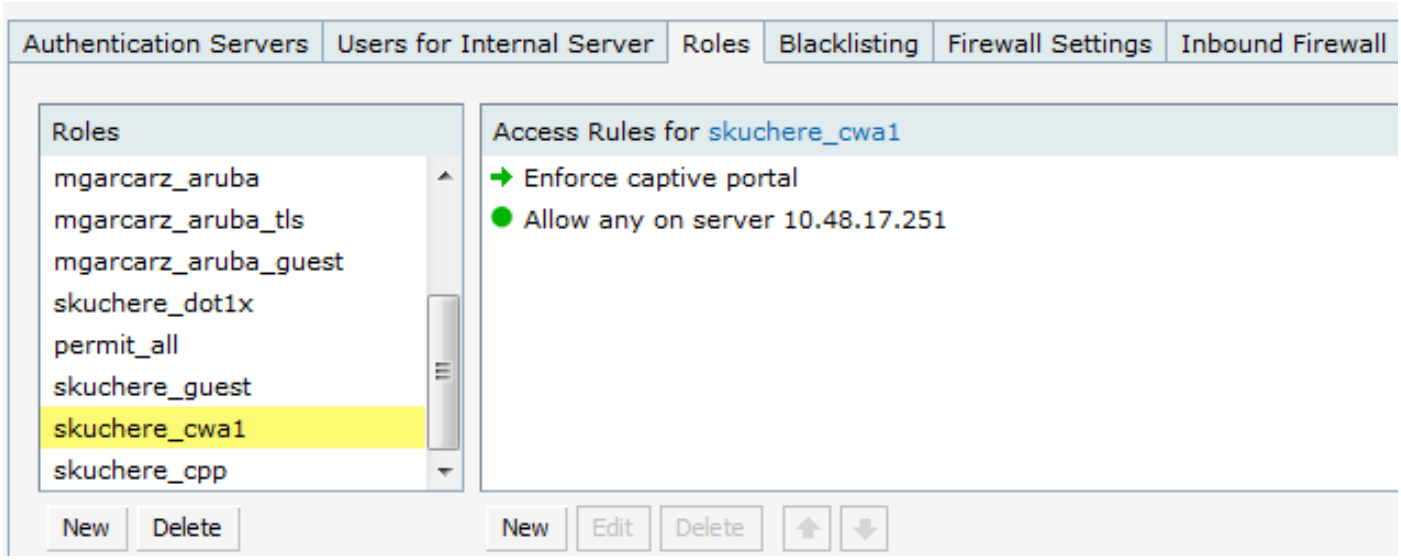

Para a primeira limitação você precisa de definir:




Para a segunda limitação você precisa de definir:

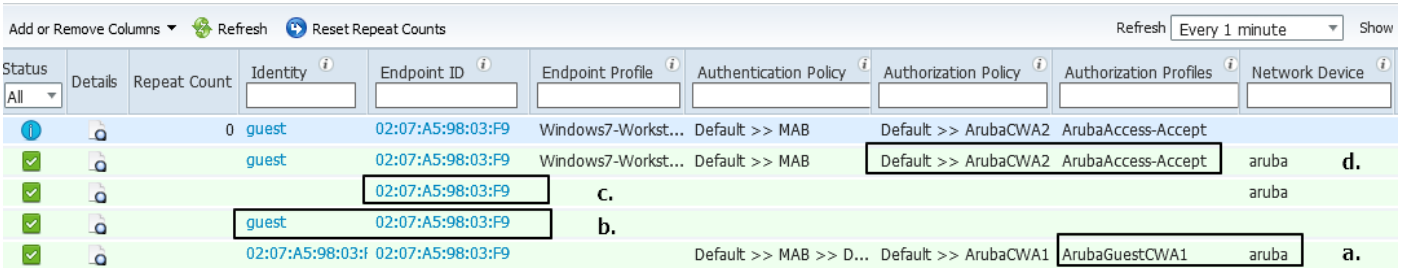



Segundo as indicações da imagem, a regra de padrão permite alguns a todos os destinos pode ser suprimida. Este é um resultado sumário da configuração do papel.




# Verificar

Exemplo do fluxo do convidado em **operações** ISE **> em raio Livelog**.




1. Os primeiros MAB e em consequência, um perfil da autorização com CWA reorientam e papel de usuário que têm o portal prisioneiro configurado no lado de Aruba.
2. Autenticação do convidado.
3. Mudança bem sucedida da autorização (CoA).
4. Segundo MAB e em consequência um perfil da autorização com acesso e papel de usuário da licença que tem a licença toda a regra no lado de Aruba.

No lado de Aruba você pode usar **clientes da mostra** comanda para assegurar-se de que o usuário esteja conectado, endereço IP de Um ou Mais Servidores Cisco ICM NT é atribuído e corrige o papel de usuário é atribuído em consequência da autenticação:

```
04:bd:88:c3:88:14# show clients

Client List
-----------
Name              IP Address    MAC Address        OS     Network        Access Point       Channel  Type  Role
----              ----------    -----------        --     -------        ------------       -------  ----  ----
02-07-A5-98-03-F9  10.62.148.77  02:07:a5:98:03:f9  Win 7  skuchere_guest  04:bd:88:c3:88:14  11       GN    skuchere_cwa1
Number of Clients   :1
Info timestamp      :92552
```

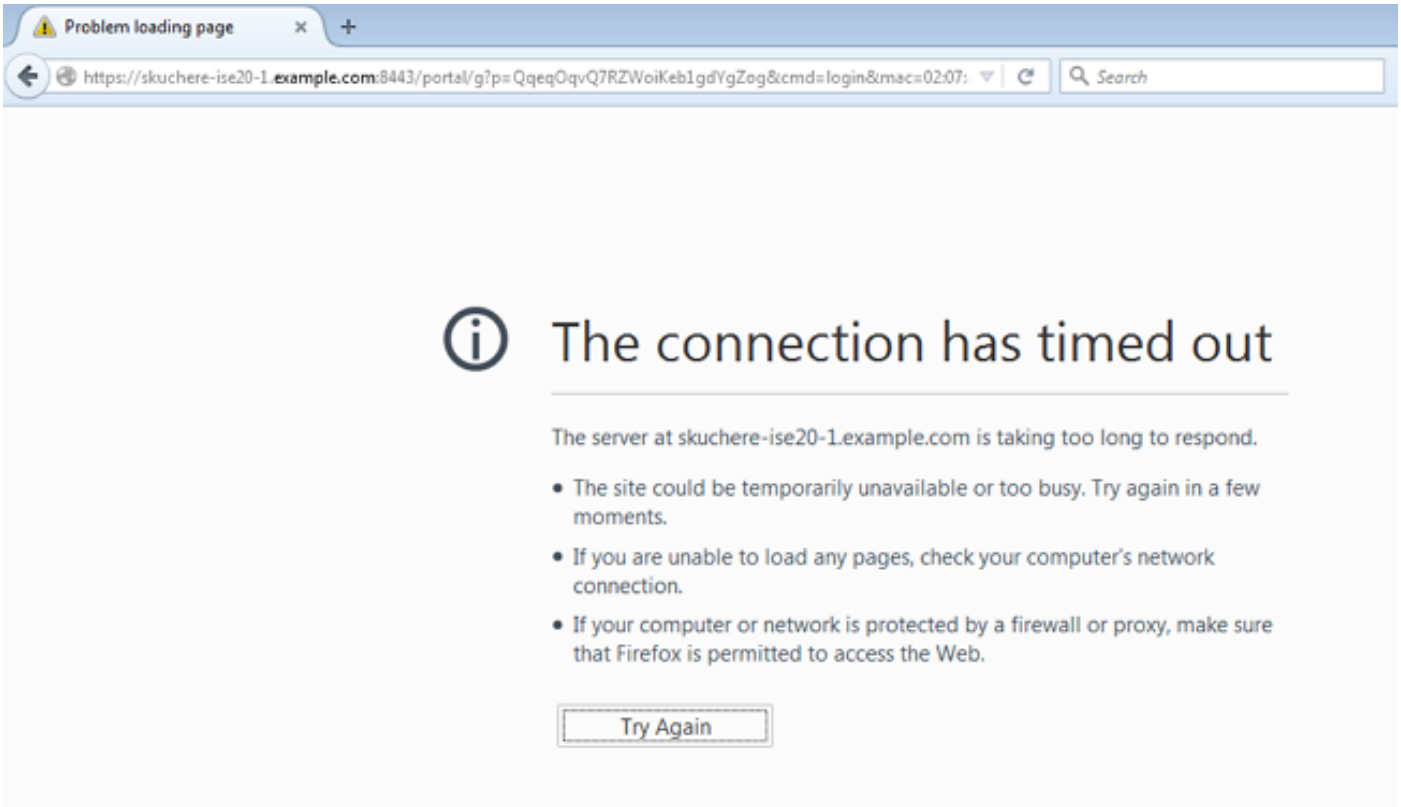
# Troubleshooting

## COA falhado

Em ajustes ISE, assegure-se de que Aruba NAD esteja configurada com tipo de dispositivo de rede correto no lado ISE e porta COA esteja definido corretamente em ajustes NAD. No lado de Aruba assegure-se de que o RFC 3576 esteja permitido em ajustes do Authentication Server e porta COA esteja definido corretamente. Da perspectiva de rede certifique-se da porta 3799 UDP esteja permitida entre ISE e Aruba WLC.

## Reoriente a edição

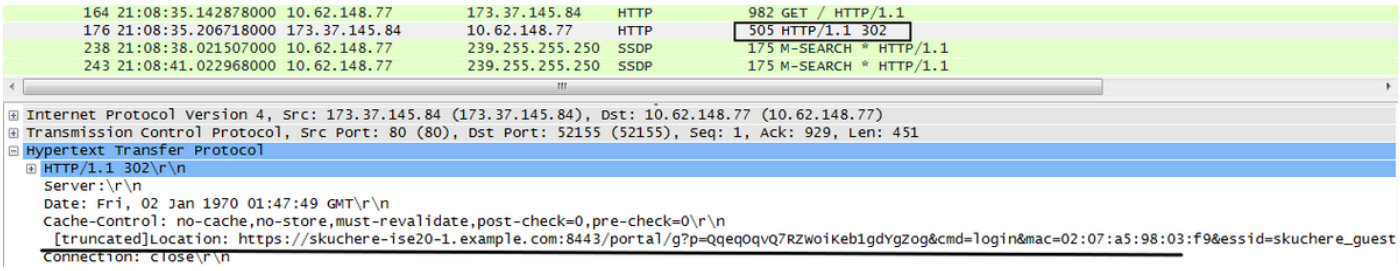
O usuário vê ISE URL no navegador mas a página ISE não é indicada, segundo as indicações da imagem:




No lado do usuário assegure-se de que o FQDN ISE possa com sucesso ser resolvido corrigir o IP. Na verificação lateral de Aruba que o ISE URL está definido corretamente nos ajustes e no tráfego portais prisioneiros para o ISE permitido no papel de usuário das restrições de acesso. Igualmente certifique-se do servidor Radius em SSID e em ISE PSN nos ajustes portais prisioneiros seja o mesmo dispositivo. Da perspectiva de rede certifique-se da porta TCP 8443 esteja permitida do segmento do usuário ao ISE.

## Nenhum presente da reorientação URL no navegador do usuário

No lado do usuário assegure-se de que como o resultado de cada pedido do HTTP Aruba WLC retorna a página do código 302 HTTP movida com ISE URL.




## O temporizador de costura da sessão expirou

O sintoma típico deste problema é que o usuário está reorientado pela segunda vez ao portal do convidado. Neste caso no raio Livelog ISE você deve ver aquele depois que o COA para o segundo perfil da autorização da autenticação com CWA foi selecionado outra vez. No lado de Aruba, verifique o papel de usuário real com a ajuda do comando dos **clientes da mostra**.

Como uma ação alternativa para esta edição você pode usar a política baseada valor-limite da autorização no ISE para conexões após a autenticação bem sucedida do convidado.