Solucionar problemas comuns de acesso de convidados do ISE

Contents

Introduction

Este documento descreve como solucionar problemas comuns de convidados na implantação, como isolar e verificar o problema e soluções alternativas simples para tentar.

Pré-requisito

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- configuração de convidado ISE
- Configuração de CoA em dispositivos de acesso à rede (NAD)
- São necessárias ferramentas de captura em estações de trabalho.

Componentes Utilizados

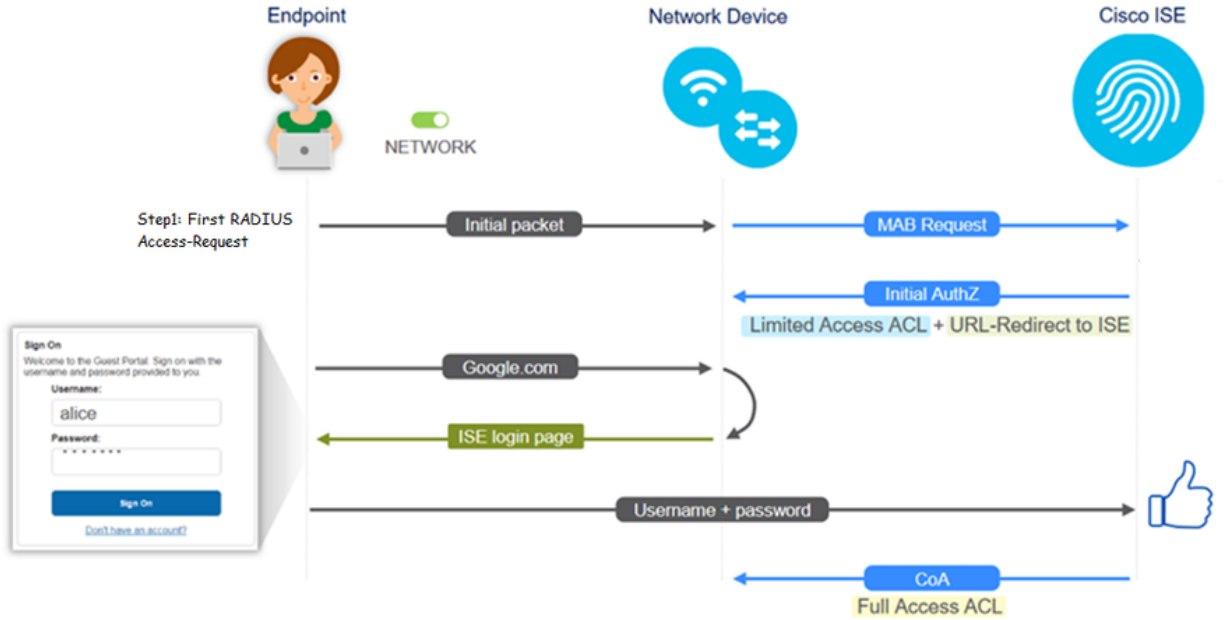
As informações neste documento são baseadas em Cisco ISE, versão 2.6 e:

- WLC 5500
- Catalyst Switch 3850 versão 15.x
- Estação de trabalho do Windows 10

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Fluxo de convidado

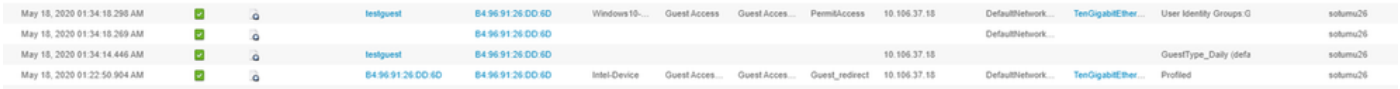
A visão geral do fluxo de convidados é semelhante às configurações com ou sem fio. Esta imagem do fluxograma pode ser usada como referência em todo o documento. Ajuda a visualizar a etapa e a entidade.



O fluxo também pode ser seguido nos logs ao vivo do ISE [**Operations > RADIUS Live Logs**] filtrando a ID do ponto final:

- Autenticação MAB bem-sucedida - o campo de nome de usuário tem o endereço MAC - o URL é enviado para o NAD - o usuário obtém o portal
- Autenticação de convidado bem-sucedida - o campo de nome de usuário tem o nome de usuário convidado e foi identificado como GuestType_Daily (ou o tipo configurado para o usuário convidado)
- CoA iniciado - o campo de nome de usuário está em branco, o relatório detalhado mostra Autorização dinâmica bem-sucedida
- Acesso de convidado fornecido

A sequência de eventos na imagem (de baixo para cima)



Guias comuns de implantação

Aqui estão alguns links para assistência na configuração. Para qualquer solução de problemas de caso de uso específico, é bom conhecer a configuração ideal ou esperada.

- Configuração de convidado com fio
- Configuração de convidado sem fio
- CWA de convidado sem fio com APs FlexAuth

Problemas encontrados com frequência

Este documento aborda principalmente estas questões:

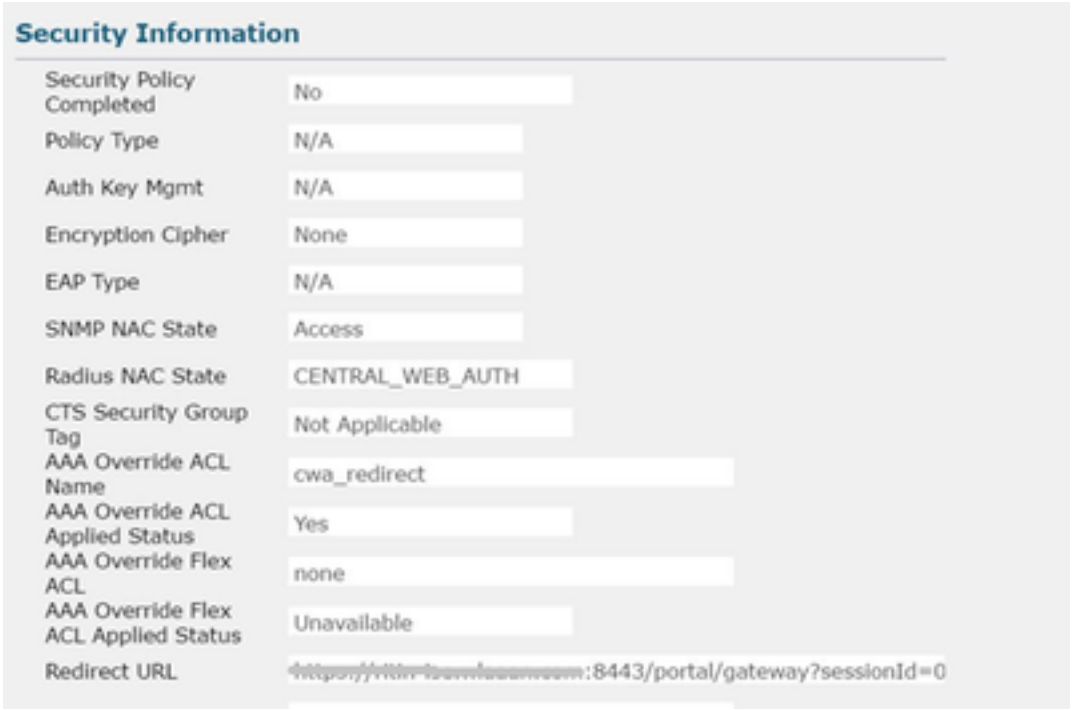
O redirecionamento para o Portal do Convidado não funciona

Depois que a URL e a ACL de redirecionamento forem enviadas do ISE, verifique:

1. O status do cliente no switch (se houver acesso de convidado com fio) com o comando **show authentication session int <interface> details**:

```
guestlab#sh auth sess int T1/0/48 de
            Interface:  TenGigabitEthernet1/0/48
              IIF-ID:  0x1096380000001DC
         MAC Address:  b496.9126.dd6d
        IPv6 Address:  Unknown
        IPv4 Address:  10.106.37.18
           User-Name:  B4-96-91-26-DD-6D
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
     Restart timeout:  N/A
   Common Session ID:  0A6A25110000012652C64B014
     Acct Session ID:  0x0000124F
              Handle:  0x5E00014D
      Current Policy:  POLICY_Te1/0/48

Local Policies:
       Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
     Security Policy:  Should Secure
     Security Status:  Link Unsecure

Server Policies:

        URL Redirect:  https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A25110000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
     URL Redirect ACL:  REDIRECT_ACL

Method status list:
      Method           State
      mab              Authc Success
```

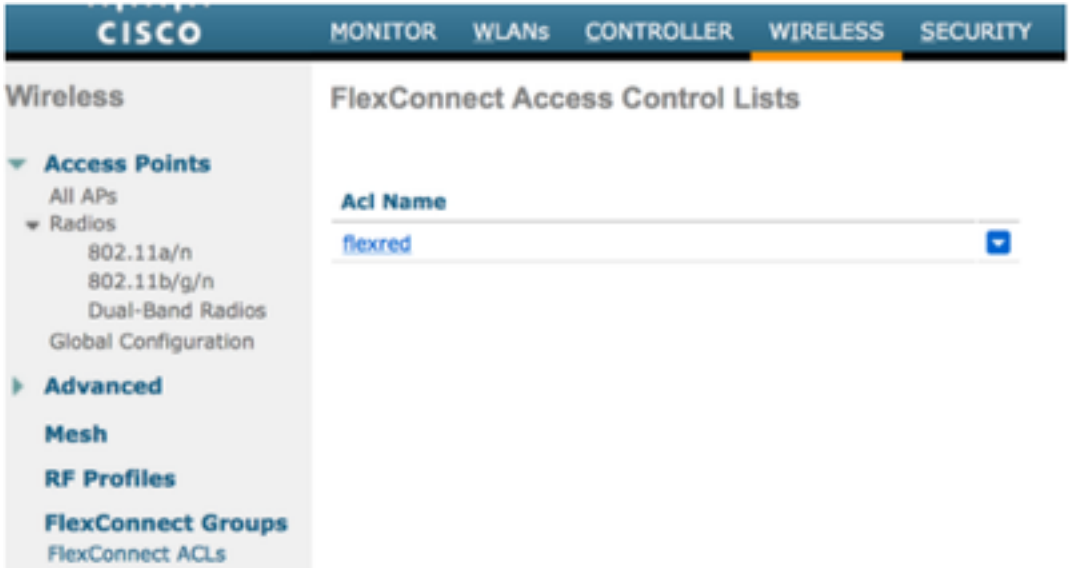
2. O status do cliente na Controladora de LAN Sem Fio (se houver acesso de convidado sem fio): **Monitor > Cliente > Endereço MAC**



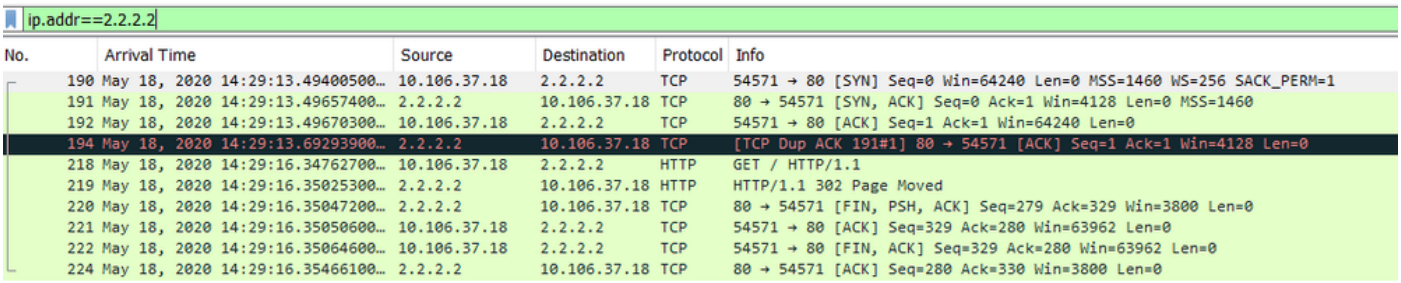
3. A acessibilidade do ponto final ao ISE na porta TCP 8443 com a ajuda do prompt de comando: **C:\Users\user>telnet <ISE-IP> 8443**

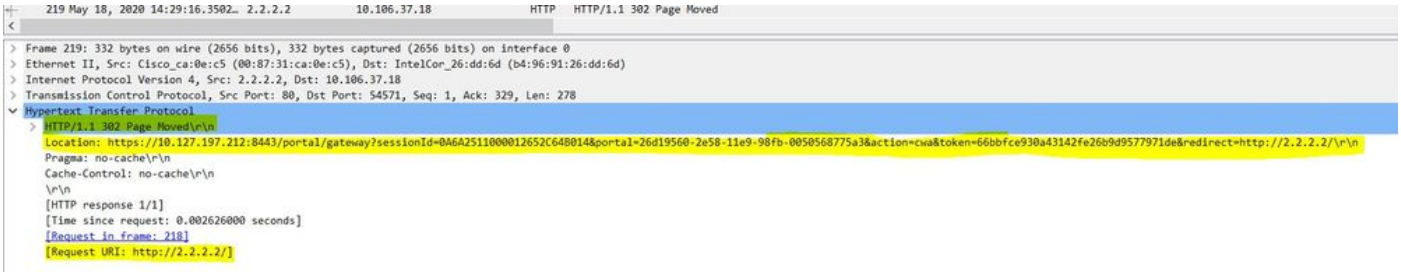
4. Se o URL de redirecionamento do portal tiver um FQDN, verifique se o cliente é capaz de resolver a partir do prompt de comando: **C:\Users\user>nslookup guest.ise.com**

5. Na configuração de conexão flexível, certifique-se de que o mesmo nome de ACL esteja configurado em ACL e ACLs flexíveis. Além disso, verifique se a ACL está mapeada para os AP. Consulte o guia de configuração da seção anterior - Etapas 7 b e c para obter mais informações.



6. Tire uma captura de pacote do cliente e verifique o redirecionamento. O pacote HTTP/1.1.302 Página Movida é para indicar que o WLC/Switch redirecionou o site acessado para o portal do convidado do ISE (URL redirecionado):





7. O mecanismo HTTP(s) está habilitado nos Dispositivos de Acesso à Rede:

No switch:

```
guestlab#sh run | in ip http
ip http server
ip http secure-server
```

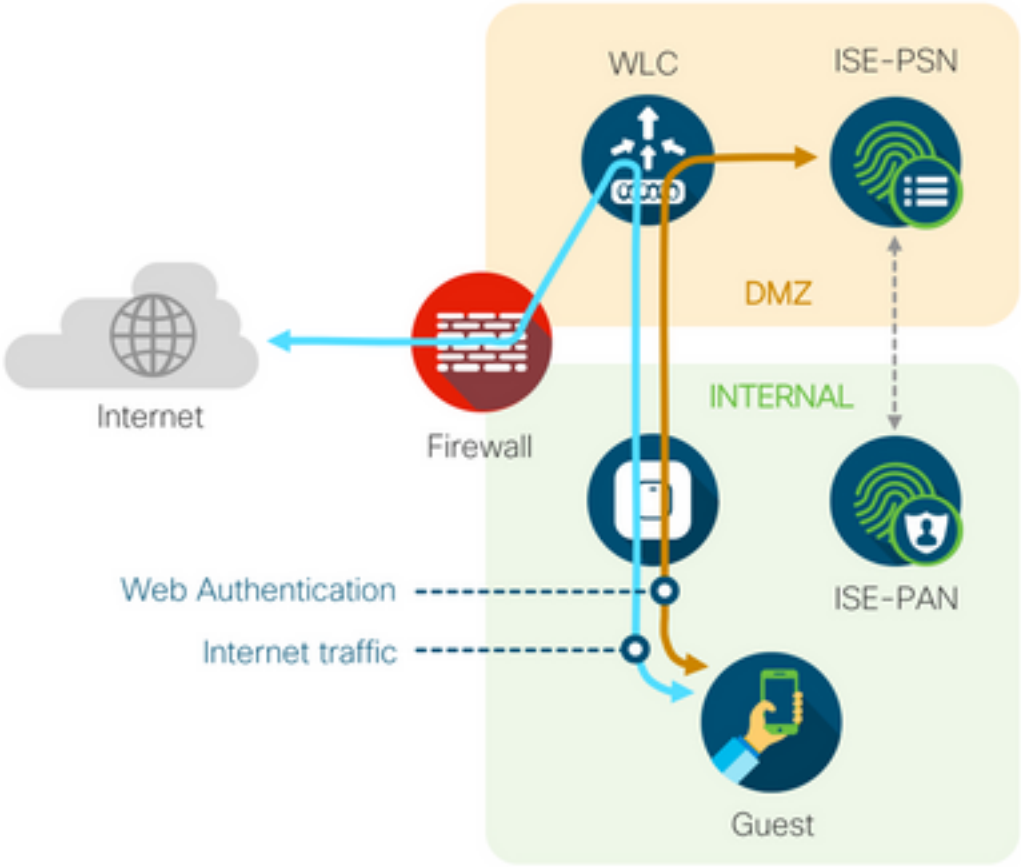
Na WLC:

8. Se a WLC estiver em uma configuração de âncora estrangeira, verifique:

Etapa 1. O status do cliente deve ser o mesmo em ambas as WLCs.

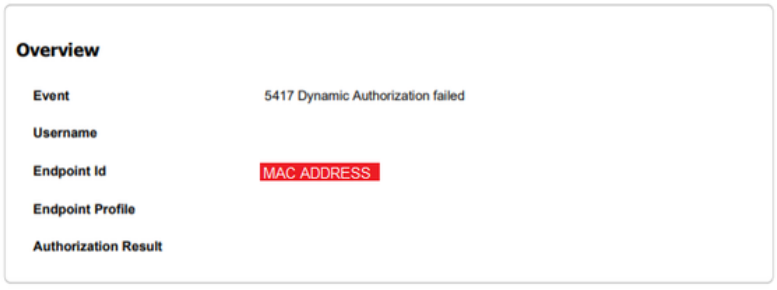
Etapa 2. A URL de redirecionamento deve ser vista em ambas as WLCs.

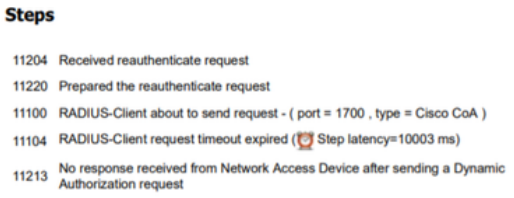
Etapa 3. A Contabilização RADIUS deve ser desabilitada na WLC âncora.



Falha na autorização dinâmica

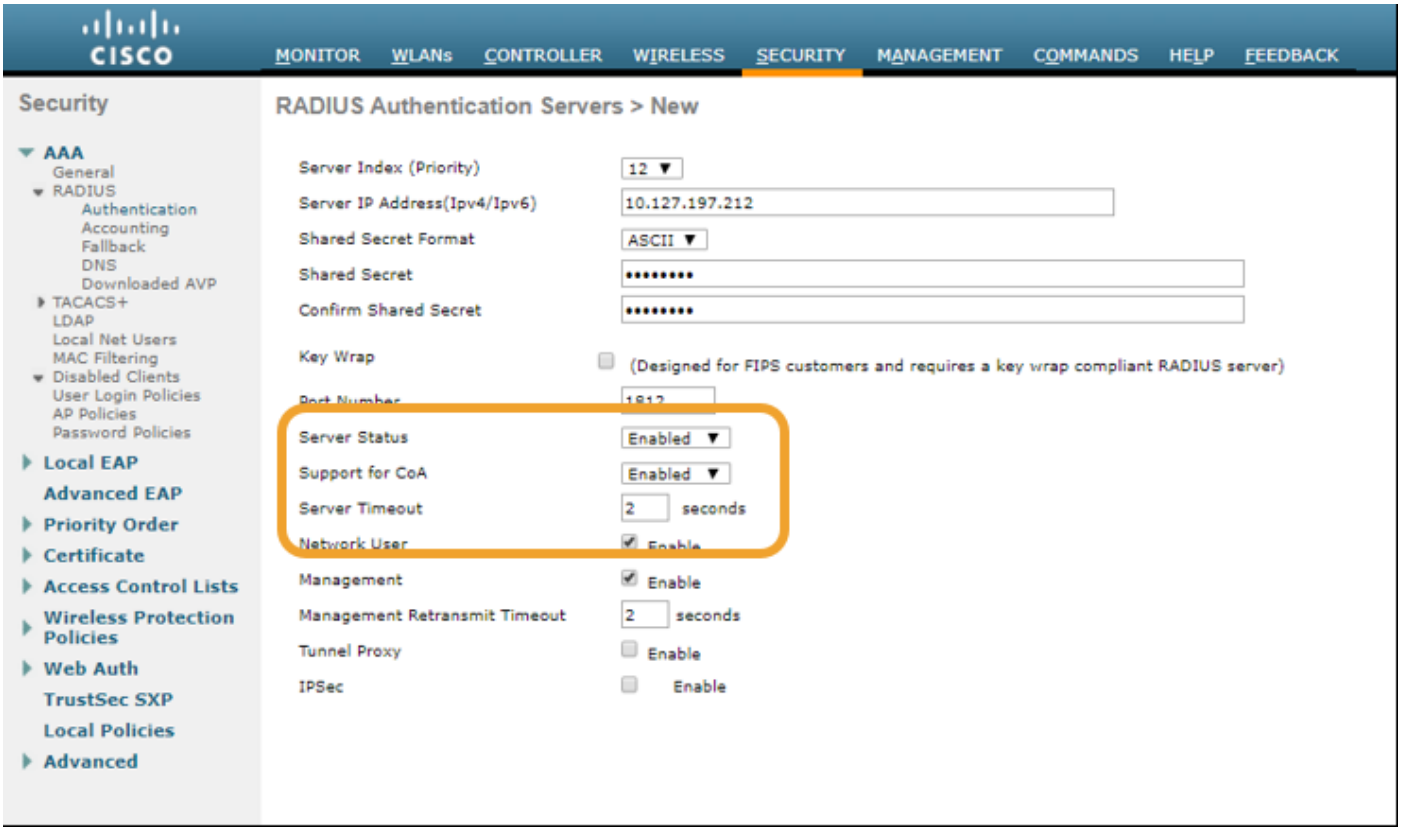
Se o usuário final puder acessar o portal do convidado e efetuar login com êxito, a próxima etapa será uma alteração de autorização, para conceder acesso total do convidado ao usuário. Se isso não funcionar, você verá uma falha de autorização dinâmica nos registros ao vivo do ISE Radius. Para corrigir o problema, verifique:





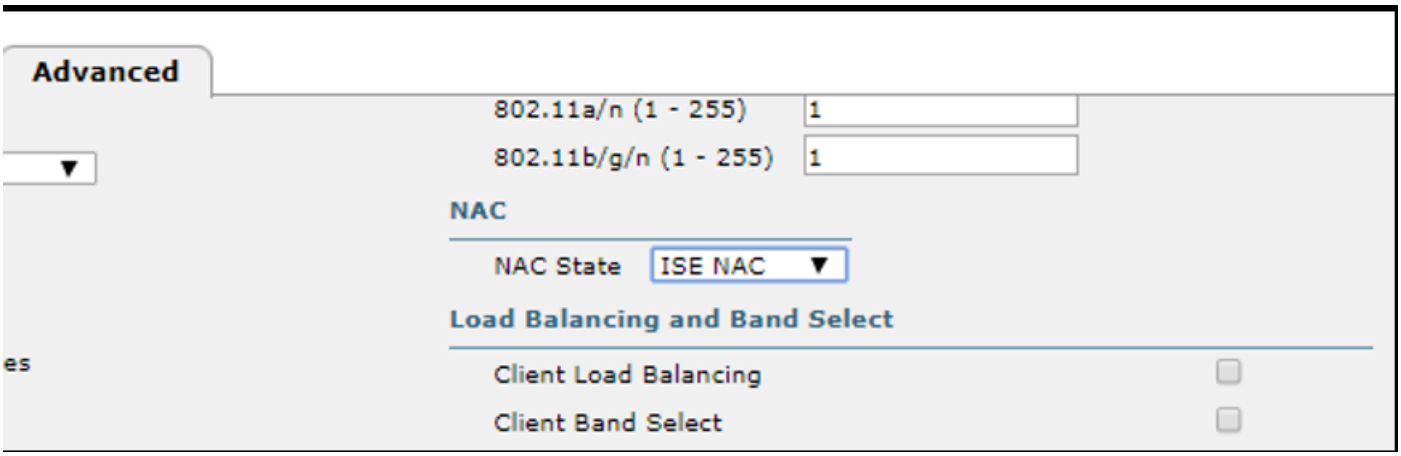
1. A Alteração de Autorização (CoA) deve ser ativada/configurada no NAD:

```
!
aaa server radius dynamic-author
 client 10.127.197.209 server-key cisco123
 client 10.127.197.212 server-key cisco123
!
```



2. A porta UDP 1700 deve ser permitida no firewall.

3. O estado NAC na WLC está incorreto. Em Advanced settings on **WLC GUI > WLAN**, altere o estado do NAC para ISE NAC.

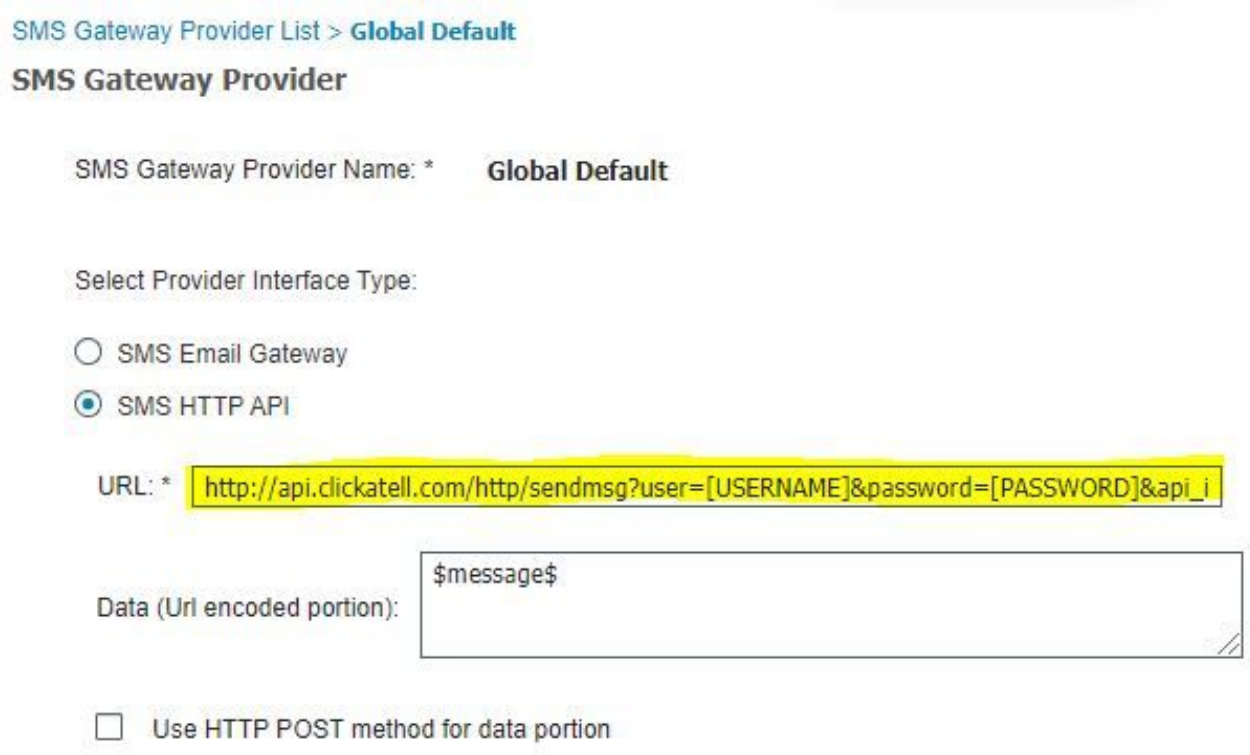


Notificações SMS/EMAIL não enviadas

1. Verifique a configuração de SMTP em **Administração > Sistema > Configurações > SMTP**.

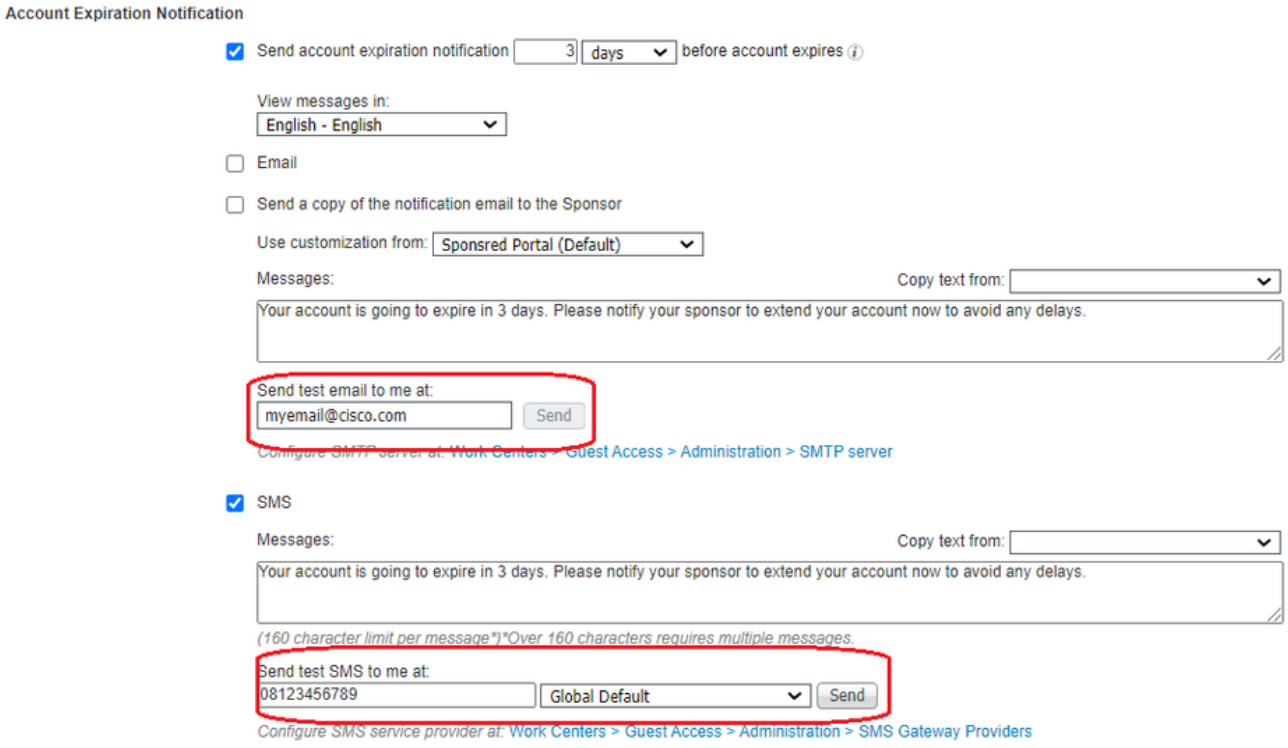
2. Verifique a API para gateways SMS/E-mail fora do ISE:

Teste a(s) URL(s) fornecida(s) pelo fornecedor em um cliente API ou navegador, substitua as variáveis como nomes de usuário, senhas, número de celular e teste a acessibilidade. [**Administração > Sistema > Configurações > Gateways SMS**]



Como alternativa, se você testar nos grupos de patrocinadores do ISE [**Workcenters > Guest Access > Portals and Components > Guest Types**], faça uma captura de pacote no ISE e no gateway SMS/SMTP para verificar se

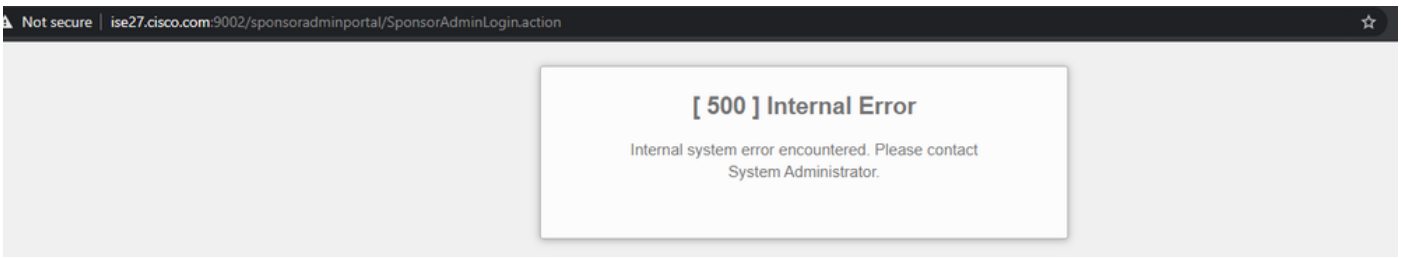
1. O pacote de solicitação chega ao servidor sem ser adulterado.
2. O servidor ISE tem as permissões/privilégios recomendados pelo fornecedor para que o gateway processe essa solicitação.



A página Gerenciar as Contas não está acessível

1. No botão **Workcenters > Guest Access > Manage accounts**, o administrador do ISE redireciona

para o FQDN do ISE na porta 9002 para acessar o portal do patrocinador:



2. Verifique se o FQDN é resolvido pela estação de trabalho a partir da qual o Portal do Patrocinador é acessado com o comando **nslookup <FQDN do ISE PAN>**.

3. Verifique se a porta TCP 9002 do ISE está aberta no CLI do ISE com o comando **show ports | incluir 9002**.

Práticas recomendadas de certificado do portal

- Para uma experiência de usuário perfeita, o certificado usado para portais e funções de administrador deve ser assinado por uma Autoridade de Certificação pública conhecida (exemplo: GoDaddy, DigiCert, VeriSign, etc.), geralmente confiável por navegadores (exemplo: Google Chrome, Firefox, etc.).

- Não é recomendável usar o IP estático para o redirecionamento de convidados, pois isso torna o IP privado do ISE visível a todos os usuários. A maioria dos fornecedores não fornece certificados assinados por terceiros para IP privado.

- Quando você passa do ISE 2.4 p6 para p8 ou p9, há um bug conhecido: ID de bug da Cisco CSCvp75207, em que as caixas **Trust for authentication within ISE** e **Trust for client authentication e Syslog** devem ser verificadas manualmente após o upgrade do patch. Isso garante que o ISE envie toda a cadeia de certificados para o fluxo TLS quando o portal do convidado for acessado.

Se essas ações não resolverem problemas de acesso de convidados, entre em contato com o TAC com um pacote de suporte coletado com instruções do documento: Debugs to enable on ISE.

Informações Relacionadas

- Suporte técnico e downloads da Cisco

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.