

Solucionar problemas comuns de acesso de convidados do ISE

Contents

[Introduction](#)

[Pré-requisito](#)

[Requirements](#)

[Componentes Utilizados](#)

[Fluxo de convidado](#)

[Guias comuns de implantação](#)

[Problemas encontrados com frequência](#)

[O redirecionamento para o Portal do Convidado não funciona](#)

[Falha na autorização dinâmica](#)

[Notificações SMS/EMAIL não enviadas](#)

[A página Gerenciar as Contas não está acessível](#)

[Práticas recomendadas de certificado do portal](#)

[Informações Relacionadas](#)

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

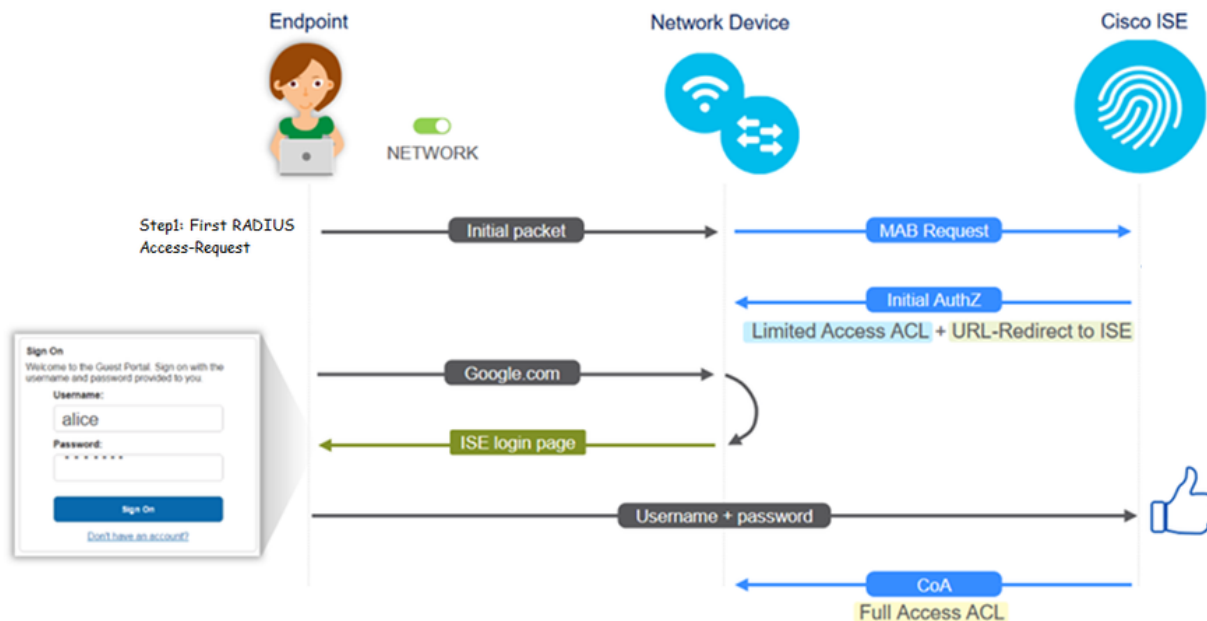
As informações neste documento são baseadas em Cisco ISE, versão 2.6 e:

- 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)

May 15, 2020 01:34:18.290 AM	testquest	84:96:91:26:DD:8D	Windows 10...	Guest Access	Guest Acces...	PermitAccess	10.106.37.15	DefaultNetwork...	TenOgablEber	User Identity Groups G	solumu26
May 15, 2020 01:34:18.289 AM		84:96:91:26:DD:8D						DefaultNetwork...			solumu26
May 15, 2020 01:34:14.446 AM	testquest	84:96:91:26:DD:8D					10.106.37.15			GuestType_Daily (defa	solumu26
May 15, 2020 01:22:50.904 AM		84:96:91:26:DD:8D	Intel-Device	Guest Acces...	Guest Acces...	Guest_redirect	10.106.37.15	DefaultNetwork...	TenOgablEber	Profiled	solumu26

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**:

```
questlab#sh auth sess int Tl/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: 0A6A2511000012652C64B014
      Acct Session ID: 0x0000124F
      Handle: 0x5E00014D
      Current Policy: POLICY_Tel/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
A2511000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbf9ce930a43142fe26b9d9577971de
  URL Redirect ACL: REDIRECT_ACL

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

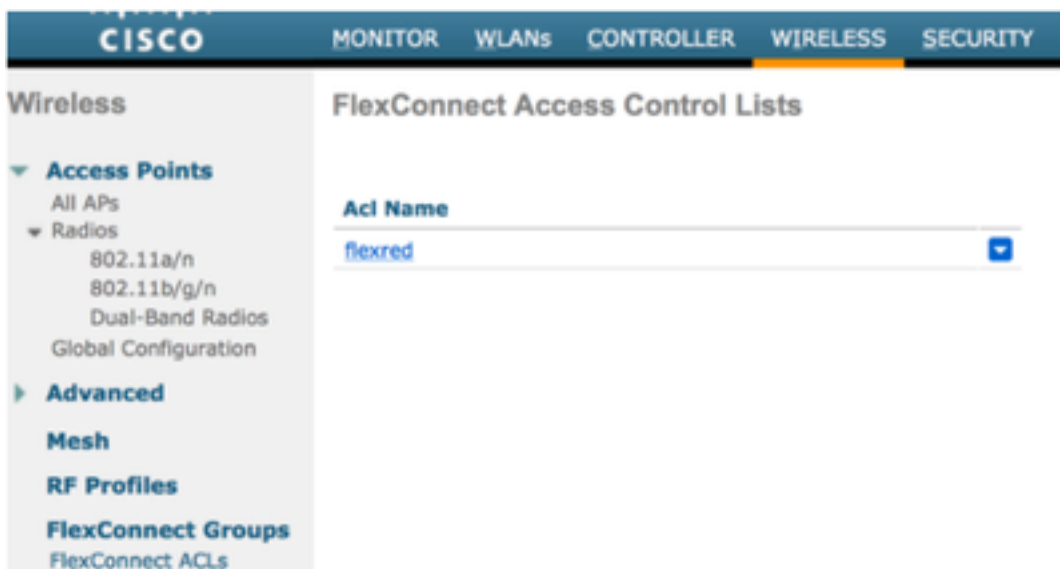
2. O status do cliente na Controladora de LAN Sem Fio (se houver acesso de convidado sem fio):
Monitor > Cliente > Endereço MAC

Security Information	
Security Policy Completed	No
Policy Type	N/A
Auth Key Mgmt	N/A
Encryption Cipher	None
EAP Type	N/A
SNMP NAC State	Access
Radius NAC State	CENTRAL_WEB_AUTH
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	cwa_redirect
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	<http://10.10.10.10:8443/portal/gateway?sessionId=0

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):

ip.addr==2.2.2.2

No.	Arrival Time	Source	Destination	Protocol	Info
190	May 18, 2020 14:29:13.49400500...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	May 18, 2020 14:29:13.49657400...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
192	May 18, 2020 14:29:13.49670300...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
194	May 18, 2020 14:29:13.69293900...	2.2.2.2	10.106.37.18	TCP	[TCP Dup ACK 191#1] 80 → 54571 [ACK] Seq=1 Ack=1 Win=4128 Len=0
218	May 18, 2020 14:29:16.34762700...	10.106.37.18	2.2.2.2	HTTP	GET / HTTP/1.1
219	May 18, 2020 14:29:16.35025300...	2.2.2.2	10.106.37.18	HTTP	HTTP/1.1 302 Page Moved
220	May 18, 2020 14:29:16.35047200...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [FIN, PSH, ACK] Seq=279 Ack=329 Win=3800 Len=0
221	May 18, 2020 14:29:16.35050600...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seq=329 Ack=280 Win=63962 Len=0
222	May 18, 2020 14:29:16.35064600...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [FIN, ACK] Seq=329 Ack=280 Win=63962 Len=0
224	May 18, 2020 14:29:16.35466100...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [ACK] Seq=280 Ack=330 Win=3800 Len=0

219 May 18, 2020 14:29:16.3502... 2.2.2.2 10.106.37.18 HTTP HTTP/1.1 302 Page Moved

> Frame 219: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits) on interface 0
 > Ethernet II, Src: Cisco_ca:0e:c5 (00:07:31:ca:0e:c5), Dst: IntelCor_26:dd:6d (b4:96:91:26:dd:6d)
 > Internet Protocol Version 4, Src: 2.2.2.2, Dst: 10.106.37.18
 > Transmission Control Protocol, Src Port: 80, Dst Port: 54571, Seq: 1, Ack: 329, Len: 278
 > Hypertext Transfer Protocol
 > HTTP/1.1 302 Page Moved\r\n
 Location: https://10.127.197.212:8443/portal/gateway?sessionId=046A2511000012652C648014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&token=66bbfce930a43142fe26b9d9577971de&redirect=http://2.2.2.2/\r\n
 Pragma: no-cache\r\n
 Cache-Control: no-cache\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.002626000 seconds]
 [Request in frame: 218]
 [Request URI: http://2.2.2.2/]

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:

The screenshot shows the Cisco WLC Management interface. The 'Management' tab is selected, and the 'HTTP-HTTPS Configuration' page is displayed. The configuration includes:

- HTTP Access: Enabled
- HTTPS Access: Enabled
- WebAuth SecureWeb: Enabled
- HTTPS Redirection: Disabled
- Web Session Timeout: 30 Minutes

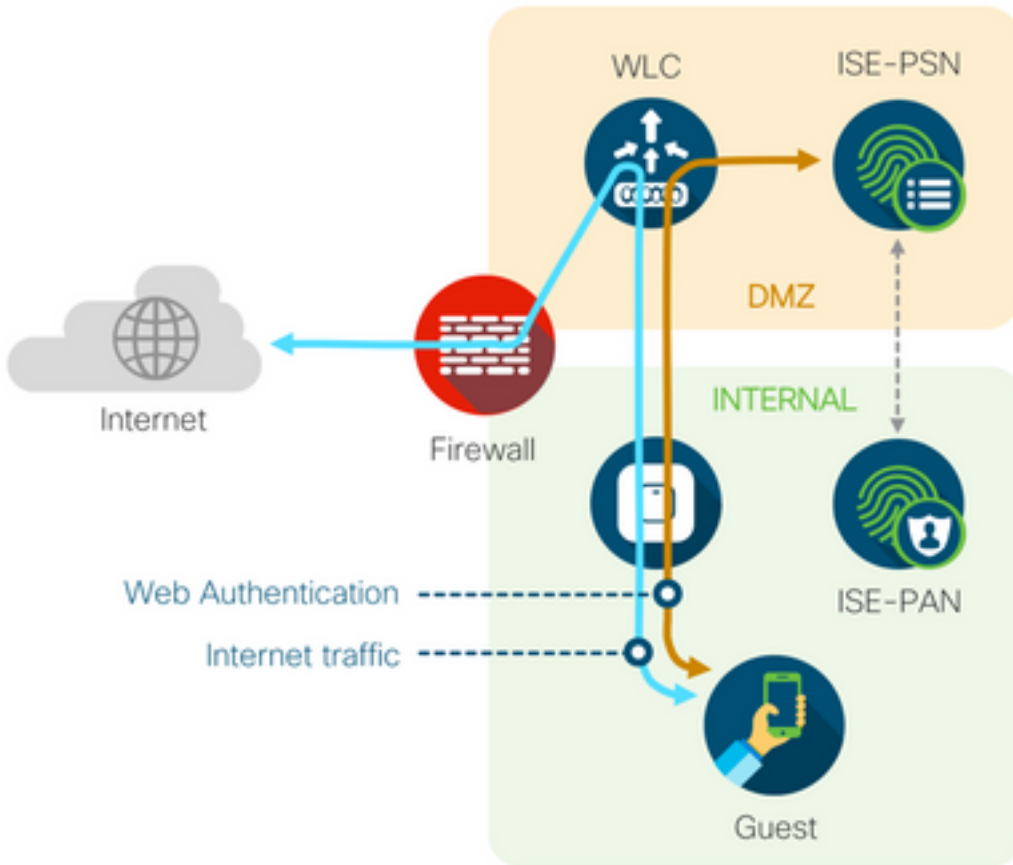
 The left sidebar shows navigation options: Summary, SNMP, HTTP-HTTPS (selected), Telnet-SSH, Serial Port, Local Management, and Users.

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:

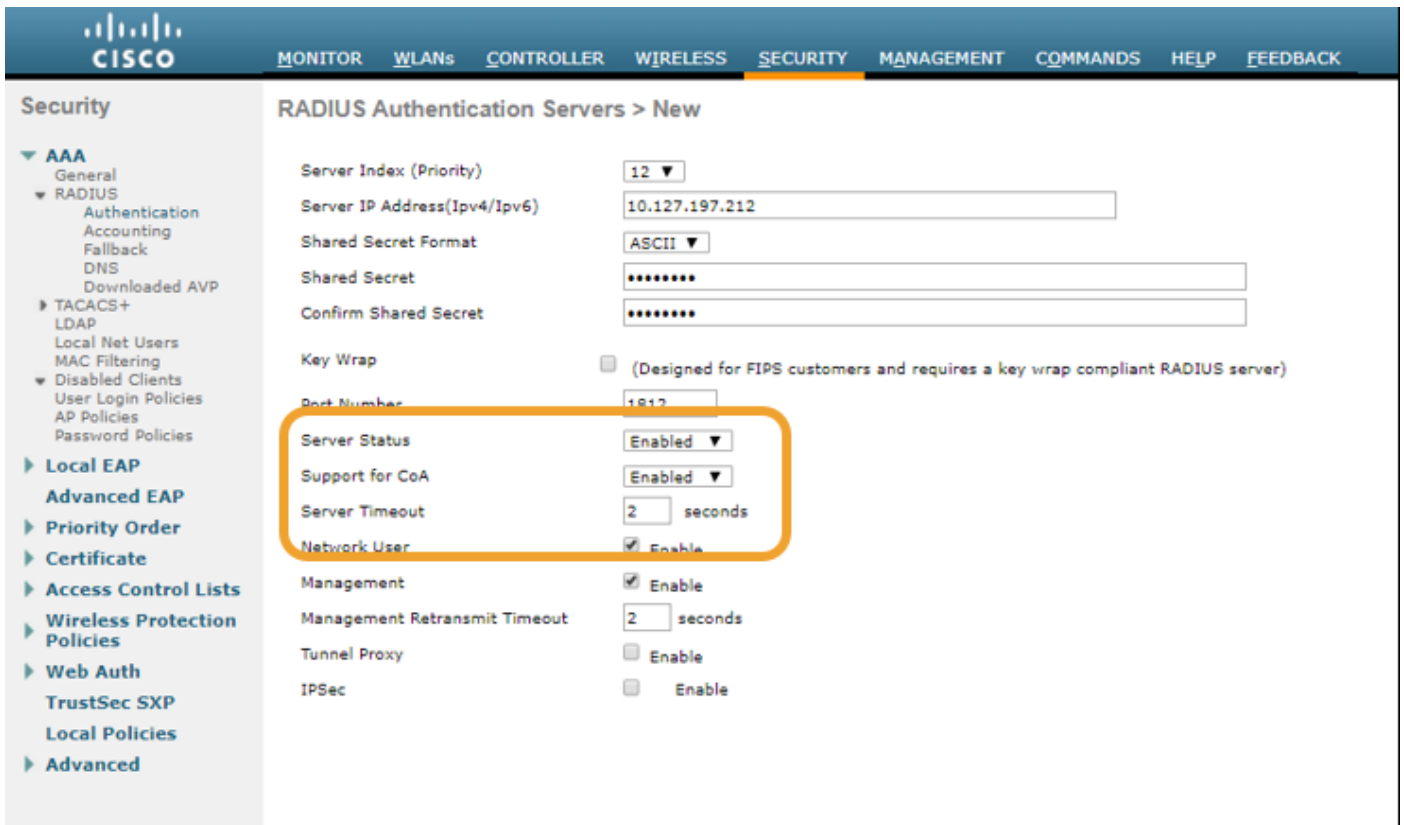
Overview	
Event	5417 Dynamic Authorization failed
Username	
Endpoint Id	MAC ADDRESS
Endpoint Profile	
Authorization Result	

Steps

- 11204 Received reauthenticate request
- 11220 Prepared the reauthenticate request
- 11100 RADIUS-Client about to send request - (port = 1700 , type = Cisco CoA)
- 11104 RADIUS-Client request timeout expired (🕒 Step latency=10003 ms)
- 11213 No response received from Network Access Device after sending a Dynamic Authorization request

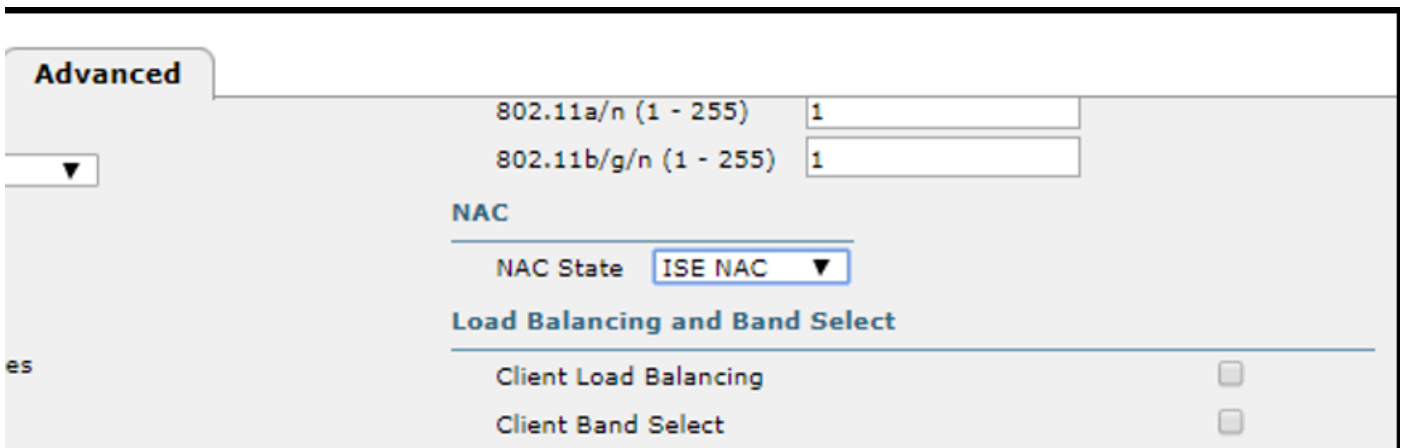
1. A Alteração de Autorização (CoA) deve ser ativada/configurada no NAD:

```
!
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**]

SMS Gateway Provider

SMS Gateway Provider Name: * **Global Default**

Select Provider Interface Type:

SMS Email Gateway

SMS HTTP API

URL: *

Data (Url encoded portion):

Use HTTP POST method for data portion

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.

Account Expiration Notification

Send account expiration notification days before account expires [?](#)

View messages in:

Email

Send a copy of the notification email to the Sponsor

Use customization from:

Messages:

Copy text from:

Send test email to me at:

[Configure SMTP server at: Work Centers > Guest Access > Administration > SMTP server](#)

SMS

Messages:

Copy text from:

(160 character limit per message)*Over 160 characters requires multiple messages.

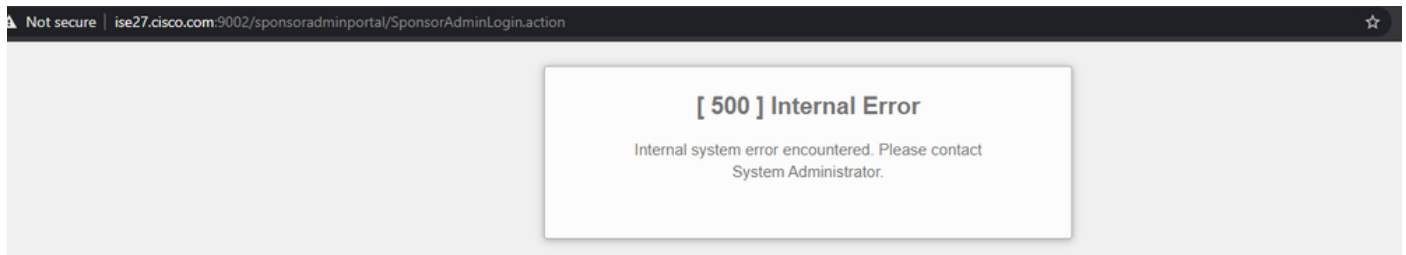
Send test SMS to me at:

[Configure SMS service provider at: Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

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.