

# Configurar o Portal de Convidado Autorregistrado do ISE

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Topologia e fluxo](#)

[Configurar](#)

[WLC](#)

[ISE](#)

[Verificar](#)

[Troubleshoot](#)

[Configuração opcional](#)

[Configurações de autorregistro](#)

[Configurações de login de convidado](#)

[Configurações de registro do dispositivo](#)

[Configurações de Conformidade do Dispositivo Convidado](#)

[Configurações de BYOD](#)

[Contas aprovadas pelo patrocinador](#)

[Entregar credenciais via SMS](#)

[Registro de dispositivo](#)

[Postura](#)

[BYOD](#)

[Alteração de VLAN](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como configurar e solucionar problemas dessa funcionalidade. Portal de convidado com registro automático, permite que os usuários convidados se registrem junto com os funcionários para usar suas credenciais do AD para obter acesso aos recursos da rede. Esse portal permite configurar e personalizar vários recursos.

## Prerequisites

## Requirements

A Cisco recomenda que você tenha experiência com a configuração do ISE e conhecimento básico destes tópicos:

- Implantações do ISE e fluxos de convidados

- Configuração de controladoras Wireless LAN (WLC)

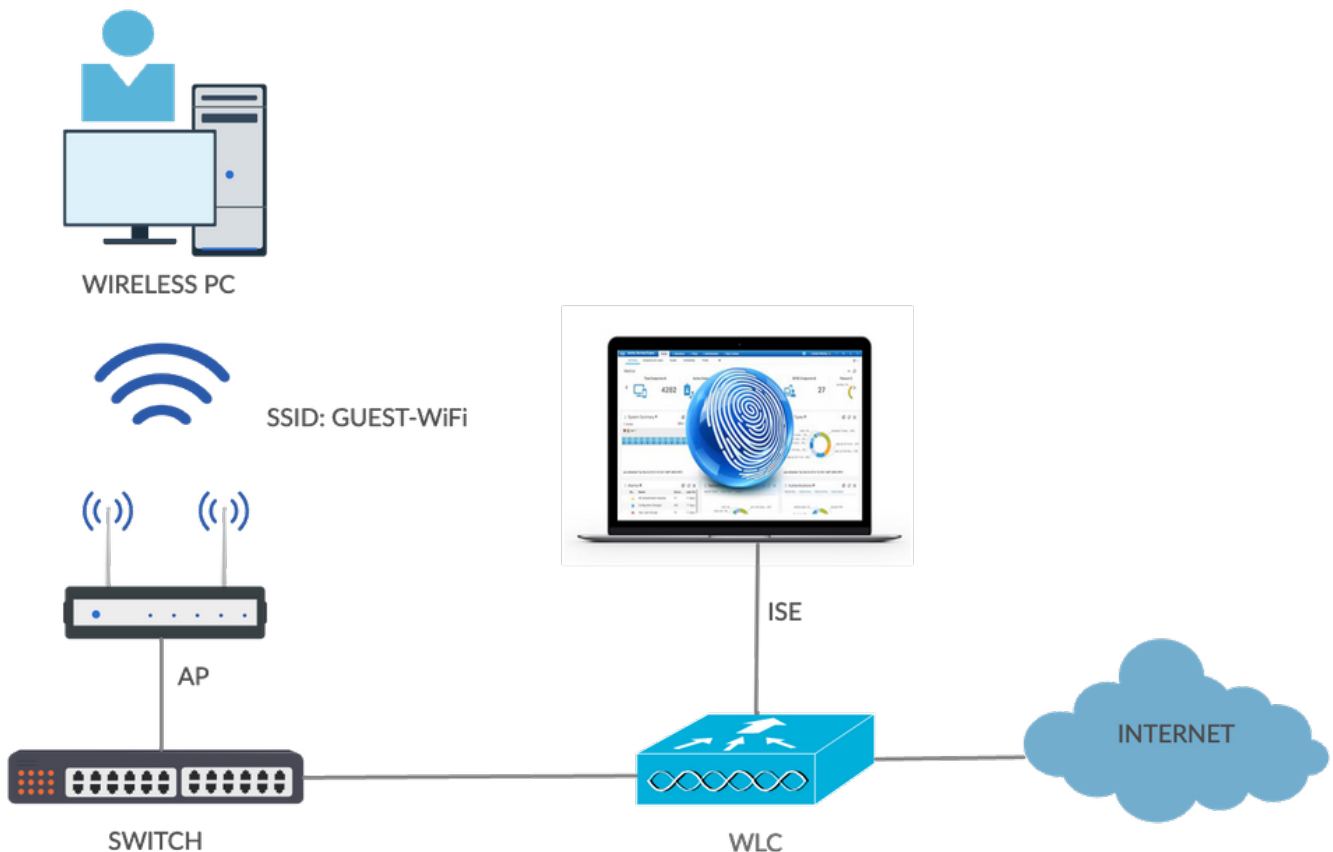
## Componentes Utilizados

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

- Microsoft Windows 10 Pro
- Cisco WLC 5508 com versão 8.5.135.0
- Software ISE, versão 3.0

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.

## Topologia e fluxo



Esse cenário apresenta várias opções disponíveis para usuários convidados quando eles executam o autorregistro.

Aqui está o fluxo geral:

**Etapa 1.** O usuário convidado está associado ao Service Set Identifier (SSID): WiFi para convidados. Esta é uma rede aberta com filtragem MAC com ISE para autenticação. Essa autenticação corresponde à segunda regra de autorização no ISE, e o perfil de autorização é redirecionado para o Portal de convidado autorregistrado. O ISE retorna um RADIUS Access-Accept com dois cisco-av-pair:

- url-redirect-acl (qual tráfego deve ser redirecionado e o nome da Access Control List (ACL) definida localmente na WLC)
- url-redirect (para onde redirecionar esse tráfego - para ISE)

**Etapa 2.** O usuário convidado é redirecionado para o ISE. Em vez de fornecer credenciais para fazer login, o usuário clica em **Registrar-se para Acesso de Convidado**. O usuário é redirecionado para uma página onde essa conta pode ser criada. Um código de registro secreto opcional pode ser ativado para limitar o privilégio de autorregistro a pessoas que conhecem esse valor secreto. Depois que a conta é criada, o usuário recebe credenciais (nome de usuário e senha) e faz login com essas credenciais.

**Etapa 3.** O ISE envia uma reautenticação RADIUS Change of Authorization (CoA) para a WLC. A WLC autentica novamente o usuário quando envia a solicitação de acesso RADIUS com o atributo Authorize-Only. O ISE responde com Access-Accept e Airespace ACL definidos localmente na WLC, que fornece acesso apenas à Internet (o acesso final para o usuário convidado depende da política de autorização).

**Note:** Sessões EAP (Extensible Authentication Protocol), o ISE deve enviar um CoA Terminate para disparar uma nova autenticação, pois a sessão EAP está entre o solicitante e o ISE. Mas para MAB (filtragem MAC), CoA Reauthenticate é suficiente; não há necessidade de desassociar/desautenticar o cliente sem fio.

**Etapa 4.** O usuário convidado tem o acesso desejado à rede.

Vários recursos adicionais, como postura e consumerização de TI (BYOD), podem ser ativados (discutidos posteriormente).

## Configurar

### WLC

1. Adicione o novo servidor RADIUS para Autenticação e Contabilização. Navegue para **Security > AAA > Radius > Authentication** para habilitar RADIUS CoA (RFC 3576).

**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
    - User Login Policies
    - AP Policies
    - Password Policies
- Local EAP
- Advanced EAP
- Priority Order
- Certificate
- Access Control Lists
  - Access Control Lists
  - CPU Access Control Lists
  - FlexConnect ACLs
  - Layer2 ACLs
  - URL ACLs

**RADIUS Authentication Servers > Edit**

Server Index: 2

Server Address(Ipv4/Ipv6): 10.106.32.25

Shared Secret Format: ASCII

Shared Secret: ...

Confirm Shared Secret: ...

Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number: 1812

Server Status: Enabled

Support for CoA: Enabled

Server Timeout: 2 seconds

Network User:  Enable

Management:  Enable

Management Retransmit Timeout: 2 seconds

Tunnel Proxy:  Enable

[Realm List](#)

IPsec:  Enable

Há uma configuração semelhante para Contabilização. Também é aconselhável configurar o WLC para enviar o SSID no atributo ID da estação chamada, que permite que o ISE configure regras flexíveis com base no SSID:

**Security**

- AAA
  - General
  - RADIUS
    - Authentication

**RADIUS Authentication Servers**

Auth Called Station ID Type: AP MAC Address:SSID

Use AES Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

**Security**

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP

**RADIUS Accounting Servers**

Acct Called Station ID Type: IP Address

MAC Delimiter: Hyphen

Network User	Tunnel Proxy	Server Index	Server Address(Ipv4/Ipv6)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	* 10.106.32.25

2. Na guia WLANs, crie a Guest-WiFi Wireless LAN (WLAN) e configure a interface correta. Defina a segurança da Camada 2 como **Nenhuma** com filtragem MAC. Em Servidores AAA (Security/Authentication, Authorization, and Accounting), selecione o endereço IP do ISE para Autenticação e Contabilização. Na guia Advanced, habilite **AAA Override** e defina o Network Admission Control (NAC) State como ISE NAC (suporte a CoA).

3. Navegue até **Segurança > Listas de Controle de Acesso > Listas de Controle de Acesso** e crie duas listas de acesso:

GuestRedirect, que permite o tráfego que não deve ser redirecionado e redireciona todo o

tráfego restante Internet, que é negada para redes corporativas e permitida para todas as outras

Aqui está um exemplo para a ACL GuestRedirect (é necessário excluir o tráfego de/para o ISE do redirecionamento):

Security

Access Control Lists > Edit

General

Access List Name: GuestRedirect

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.106.32.25 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.106.32.25 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

## ISE

1. Adicione a WLC como um dispositivo de acesso à rede em **Centros de trabalho > Acesso de convidado > Dispositivos de rede**.
2. Criar Grupo de Identidades de Ponto de Extremidade. Navegue até **Centros de trabalho > Acesso de convidado > Grupos de identidade > Grupos de identidade de endpoint**.

Cisco ISE

Work Centers · Guest Access

Overview | Identities | **Identity Groups** | Ext Id Sources | Administration | Network Devices | Portals & Components | Manage Accounts | Policy Elements

Identity Groups

Endpoint Identity Group List > New Endpoint Group

Endpoint Identity Group

\* Name: Cisco\_GuestEndpoints

Description:

Parent Group:

Submit Cancel

3. Crie um Tipo de Convidado navegando até **Centros de Trabalho > Acesso de Convidado > Portal e Componentes > Tipos de Convidado**. Consulte o grupo de identidade de endpoint criado anteriormente sob esse novo tipo de convidado e salve.

Guest Portals

**Guest Types**

Sponsor Groups

Sponsor Portals

**Guest type name: \***

Guest-Daily

**Description:**

Guest account access for 30 days

Language File ▼**Collect Additional Data**[Custom Fields...](#)**Maximum Access Time**

Account duration starts

 From first login From sponsor-specified date (or date of self-registration, if applicable)

Maximum account duration

5 days ▼ Default 1 (1-999) Allow access only on these days and times:From 9:00 AM To 5:00 PM  Sun  Mon  Tue  Wed  Thu  Fri  Sat +

Configure guest Account Purge Policy at:

[Work Centers](#) > [Guest Access](#) > [Settings](#) > [Guest Account Purge Policy](#)**Login Options** Maximum simultaneous logins 3 (1-999)

When guest exceeds limit:

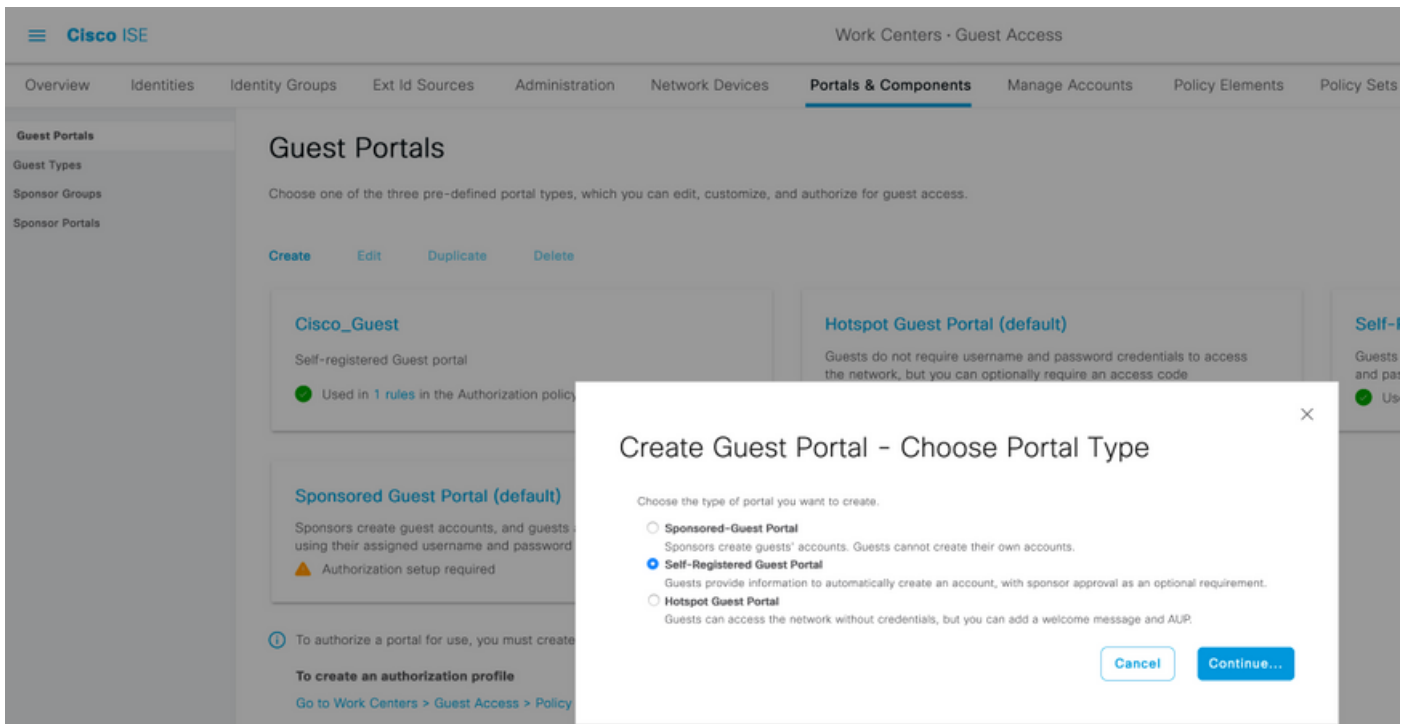
 Disconnect the oldest connection Disconnect the newest connection Redirect user to a portal page showing an error message ⓘ

This requires the creation of an authorization policy rule

Maximum devices guests can register: 5 (1-999)

Endpoint identity group for guest device registration: Cisco\_GuestEndpoints ▼ ⓘ

4. Crie um novo Tipo de Portal de Convidado: Portal de convidado com registro automático. Navegue até **Centros de trabalho > Acesso de convidado > Portais de convidado**.

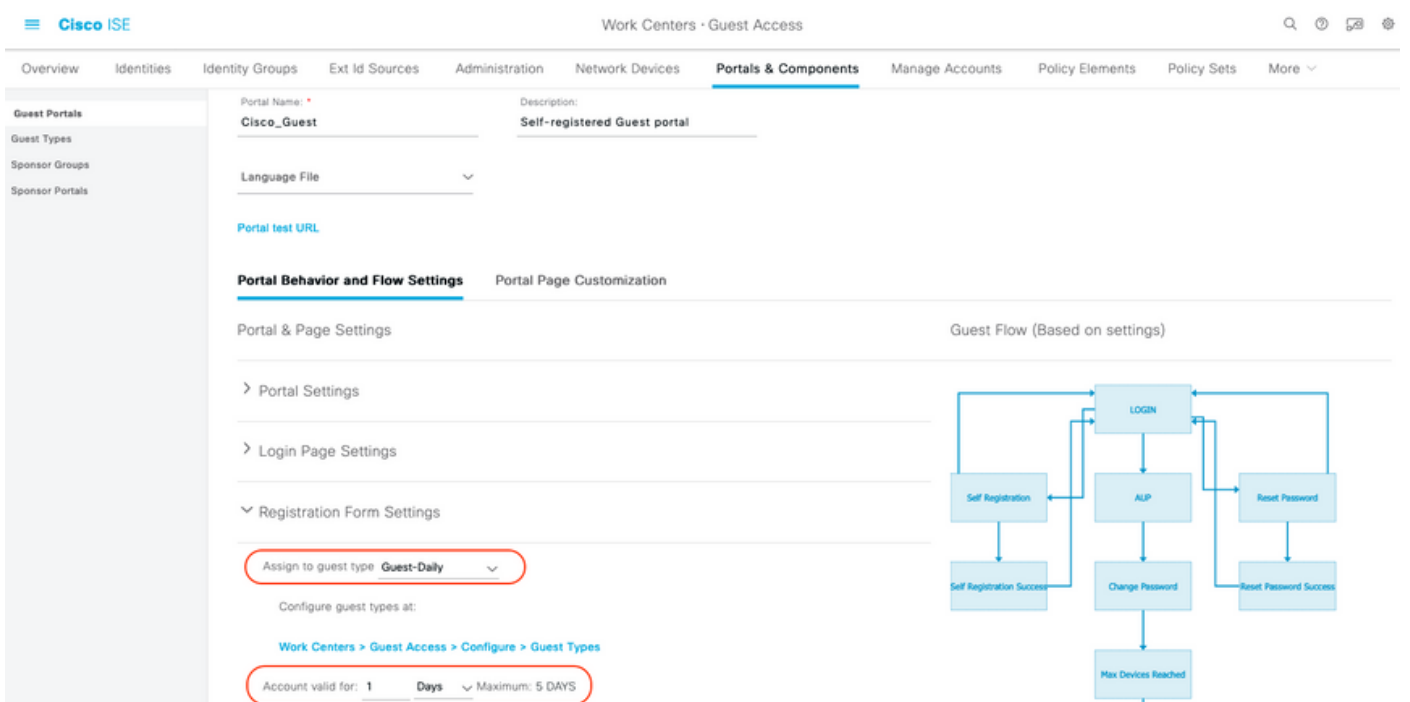


5. Escolha o nome do portal, consulte o Tipo de Convidado criado antes e envie as configurações de notificação de credenciais nas configurações do Formulário de Registro para enviar as credenciais por e-mail.

Consulte este documento sobre como configurar o servidor SMTP no ISE:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/216187-configure-secure-smtp-server-on-ise.html>

Deixe todas as outras configurações como padrão. Em Personalização da página do portal, todas as páginas apresentadas podem ser personalizadas. Por padrão, a conta Convidado é válida por 1 dia e pode ser estendida para o número de dias configurado no Tipo de Convidado específico.



6. Configure esses dois Perfis de Autorização Navegando até **Centros de Trabalho > Acesso de Convidado > Elementos de Política > Resultados > Perfis de Autorização**.

- Guest-Portal (com redirecionamento para o portal de convidado **Cisco\_Guest** e uma ACL de redirecionamento chamada **GuestRedirect**). Essa ACL GuestRedirect foi criada anteriormente na WLC.

The screenshot shows the Cisco ISE interface for configuring an Authorization Profile. The page title is "Work Centers - Guest Access" and the breadcrumb is "Policy Elements". The left sidebar shows navigation options: Overview, Identities, Identity Groups, Ext Id Sources, Administration, Network Devices, Portals & Components, Manage Accounts, and Policy Elements (selected). The main content area is titled "Authorization Profile" and contains the following fields:

- \* Name: Guest-Portal
- Description: Redirect to Self-registered guest portal
- \* Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:  ⓘ
- Agentless Posture:  ⓘ
- Passive Identity Tracking:  ⓘ

Below the configuration fields is a section for "Common Tasks":

- Web Redirection (CWA, MDM, NSP, CPP) ⓘ
- Centralized Web Auth:  (dropdown)
- ACL:  (dropdown)
- Value:  (dropdown)
- Display Certificates Renewal Message
- Static IP/Host name/FQDN
- Suppress Profiler CoA for endpoints in Logical Profile

- Permit\_Internet (com Airespace ACL igual à Internet)



Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components

Authorization Profiles > Permit\_internet

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

Airespace ACL Name

Airespace IPv6 ACL Name

ASA VPN

7. Modifique o Conjunto de Políticas denominado Default. O conjunto de políticas padrão é pré-configurado para acesso ao portal Convidado. Uma **política de autenticação** chamada MAB está presente, o que permite que a autenticação MAC Authentication Bypass (MAB) continue (não rejeite) para endereços Mac desconhecidos.

Cisco ISE Work Centers · Guest Access

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements **Policy Sets** More

Policy Sets → Default Reset Reset Polycyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	Wired_MAB Wireless_MAB	Internal Endpoints Options If Auth fail REJECT If User not found CONTINUE If Process fail DROP	0	

8. Navegue até **Política de autorização** na mesma página. Crie estas Regras de Autorização, conforme mostrado nesta imagem.

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
●	Wifi_Guest_Access	AND IdentityGroup-Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints Wireless_MAB	Permit_internet x	Select from list	0
●	Wifi_Redirect_to_Guest_Portal	AND Radius-Called-Station-ID CONTAINS Guest Wireless_MAB	Guest-Portal x	Select from list	0

Novos usuários quando associados ao SSID de convidado ainda não fazem parte de nenhum grupo de identidade e, portanto, correspondem à segunda regra e são redirecionados para o Portal de convidado.

Após o login bem-sucedido do usuário, o ISE envia um RADIUS CoA e o WLC executa a reautenticação. Dessa vez, a primeira regra de autorização é correspondida (à medida que o ponto final se torna parte do grupo de identidade do ponto final definido) e o usuário obtém o perfil de autorização Permit\_internet.

9. Também podemos fornecer Acesso Temporário aos Convidados usando a condição Fluxo de Convidado. Essa condição está verificando sessões ativas no ISE e é atribuída. Se essa sessão tiver o atributo indicando que o usuário convidado anterior foi autenticado com êxito, a condição será correspondida. Depois que o ISE recebe a mensagem Radius Accounting Stop do Network Access Device (NAD), a sessão é encerrada e removida posteriormente. Nesse estágio, a condição Acesso à rede:Caso de uso = Fluxo de convidado não é mais atendida. Como resultado, todas as autenticações subsequentes desse ponto final atingem o redirecionamento de regra genérica para autenticação de convidado.

Status	Rule Name	Conditions	Results		
			Profiles	Security Groups	Hits
●	Temporary_Guest_Access	AND Network Access-UseCase EQUALS Guest Flow Wireless_MAB	Permit_internet x	Select from list	1
○	Permanent_Guest_Access	AND IdentityGroup-Name EQUALS Endpoint Identity Groups: Cisco_GuestEndpoints Wireless_MAB	Permit_internet x	Select from list	2
●	Wifi_Redirect_to_Guest_Portal	AND Radius-Called-Station-ID CONTAINS Guest Wireless_MAB	Guest-Portal x	Select from list	3

**Note:** Ao mesmo tempo, você pode usar o acesso de convidado temporário ou o acesso de convidado permanente, mas não ambos.

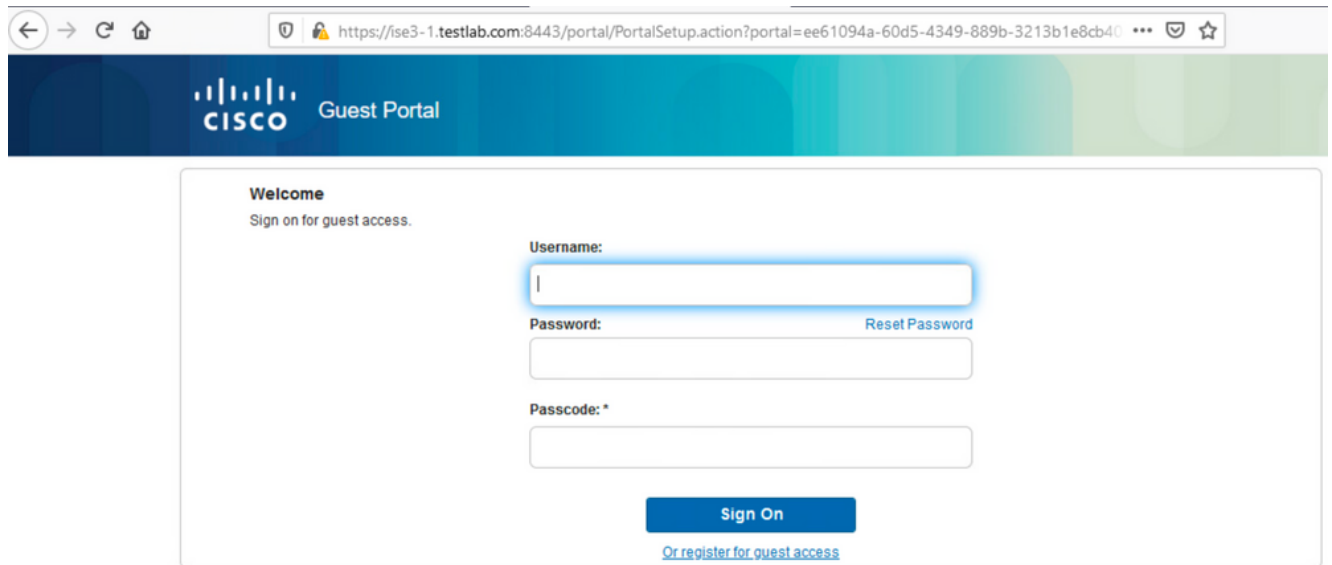
Consulte este documento para obter informações detalhadas sobre a configuração de acesso temporário e permanente de convidados do ISE.

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200273-Configure-ISE-Guest-Temporary-and-Perman.html>

## Verificar

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

1. Depois de associar-se ao SSID de convidado e digitar uma URL, você será redirecionado para a página Portal de convidado, como mostrado na imagem.



The image shows a web browser window displaying the Cisco Guest Portal. The browser's address bar shows the URL: <https://ise3-1.testlab.com:8443/portal/PortalSetup.action?portal=ee61094a-60d5-4349-889b-3213b1e8cb40>. The page header features the Cisco logo and the text "Guest Portal". The main content area is titled "Welcome" and includes the instruction "Sign on for guest access." Below this, there are three input fields: "Username:" (with a blue highlight), "Password:" (with a "Reset Password" link), and "Passcode: \*". A blue "Sign On" button is positioned below the input fields, and a link "Or register for guest access" is located at the bottom of the form.

2. Como você ainda não tem credenciais, escolha a opção **Registrar para acesso de convidado**. Você verá o formulário de registro para criar a conta. Se a opção Código de registro foi habilitada na configuração do Portal de convidado, esse valor de segredo será necessário (isso garante que somente as pessoas com permissões corretas tenham permissão para se registrarem automaticamente).

https://ise3-1.testlab.com:8443/portal/SelfRegistration.action?from=LOGIN 80%

**CISCO** Guest Portal

**Registration**  
Please complete this registration form:

Registration Code\*  
8015

Username  
guest1

First name  
Poonam

Last name  
Garg

Email address\*  
poongarg@cisco.com

Mobile number  
+91 0000000000

Company  
Cisco

Person being visited(email)  
abc@cisco.com

Reason for visit  
Personal

**Register** **Cancel**

Activati  
Go.to.Set

3. Se houver qualquer problema com a senha ou com a política do usuário, navegue para **Centros de Trabalho > Acesso de Convidado > Configurações > Política de Nome de Usuário de Convidado** para alterar as configurações. Aqui está um exemplo:

Overview Identities Identity Groups Ext Id Sources Administration Network Devices Portals & Components Manage Accounts Policy Elements **More** ▾

Guest Account Purge Policy  
Custom Fields  
Guest Email Settings  
Guest Locations and SSIDs  
**Guest Username Policy**  
Guest Password Policy  
DHCP & DNS Services  
Logging

### Guest Username Policy

Configure username requirements that will be enforced for guest usernames. Usernames are not case sensitive.

**Username Length**

Minimum username length:\*  (1-64 characters)

**Username Criteria for Known Guests**

If data is available, base username on:

First name and last name  
 Email address

**Characters Allowed in Randomly-Generated Usernames**

Alphabetic:  ▾ ABCDEFGHIJKLMNOPQRSTUVWXYZ

Minimum alphabetic:  (0-64)

Numeric:  ▾ 23456789

Minimum numeric:  (0-64)

Special:  ▾

Minimum special:  (0-64)

4. Após a criação bem-sucedida da conta, você recebe as credenciais (senha gerada de acordo com as políticas de senha de convidado) e o usuário convidado recebe a notificação de e-mail se ela estiver configurada:

https://fise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF\_REGISTRATION

**CISCO** Guest Portal guest1 ⓘ

**Account Created**

Choose how to receive your login information, by text or email. Email Me attempts left:5

You can only click the button 5 times.

**Username:** guest1  
**Password:** 3154  
**First name:** Poonam  
**Last name:** Garg  
**Email:** poongarg@cisco.com  
**Mobile number:** +910000000000  
**Company:** Cisco  
**Location:** India  
**SMS provider:** Global Default  
**Person being visited (email):** abc@cisco.com  
**Reason being visited:** Personal

## Your Guest Account Credentials



ise@testlab.com <ise@testlab.com>

Today at 9:47 AM

To: Poonam Garg (poongarg)



Hello Poonam,  
Your guest account details:  
Username: guest1  
Password: 3154  
First Name: Poonam  
Last Name: Garg  
Mobile Number:+910000000000  
Valid From: 2020-11-07 09:43:50  
Valid To: 2020-11-08 09:43:50  
Person being visited: [abc@cisco.com](mailto:abc@cisco.com)  
Reason for visit: Personal

5. Clique em **Sign On** e forneça as credenciais (uma senha de acesso adicional poderá ser necessária se for configurada no Portal do Convidado; esse é outro mecanismo de segurança que permite que somente aqueles que conhecem a senha façam login).

Welcome  
Sign on for guest access.

Username:  
guest1

Password: [Reset Password](#)  
.....

Passcode: \*  
8015

[Sign On](#)

[Or register for guest access](#)

6. Quando bem-sucedido, uma Política de Uso Aceitável (AUP) opcional pode ser apresentada (se configurada no Portal do Convidado). O usuário recebe uma opção de alteração de senha e o banner pós-login (também configurável no Portal do convidado) também pode ser exibido.

Browser address bar: <https://ise3-1.testlab.com:8443/portal/LoginSubmit.action?from=LOGIN>

**CISCO Guest Portal** guest1

**Acceptable Use Policy**  
Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco Systems website.

**Accept** **Decline**

Browser address bar: <https://ise3-1.testlab.com:8443/portal/AupSubmit.action?from=AUP>

**CISCO Guest Portal** guest1

**Change Password**  
You are required to change your password now. Please enter a new password.

Current password:

New password:

Confirm password:

**Submit**

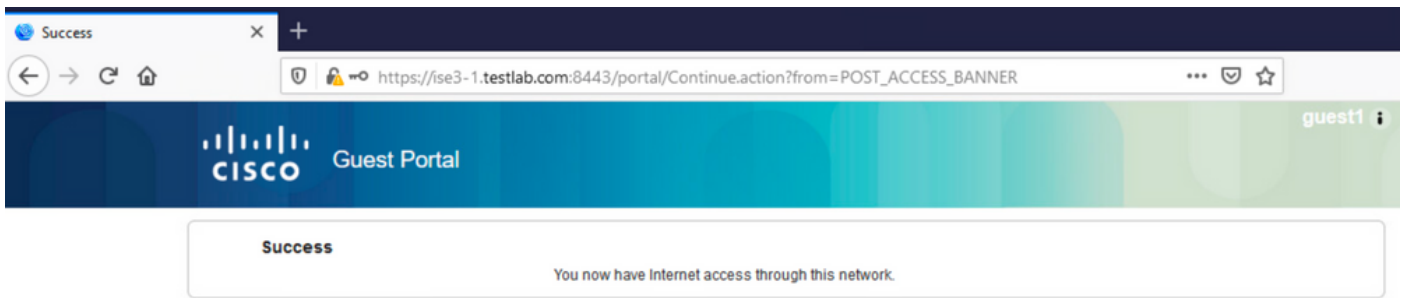
Browser address bar: [https://ise3-1.testlab.com:8443/portal/ChangePwd.action?from=CHANGE\\_PASSWORD](https://ise3-1.testlab.com:8443/portal/ChangePwd.action?from=CHANGE_PASSWORD)

**CISCO Guest Portal** guest1

**Welcome Message**  
Click **Continue** to connect to the network.  
You're very close to gaining network access.

**Continue**

7. A última página (Banner pós-login) confirma que o acesso foi concedido:



## Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Nesse estágio, o ISE apresenta esses logs em **Operations > RADIUS > Live Logs**, como mostrado na imagem.

Time	Status	Details	Identity	Endpoint ID	Authenticat...	Authorization Policy	Authorization P...	IP Address	Identity Group	Event
Nov 07, 2020 04:17:32.46...	<span style="color: blue;">●</span>		guest1	D0:37:45:89:EF:64	Default	Default >> Permanent_Guest_Access	Permit_Internet	10.106.32.2...		Session State is Started
Nov 07, 2020 04:17:32.42...	<span style="color: green;">■</span>		guest1	D0:37:45:89:EF:64	Default	Default >> Permanent_Guest_Access	Permit_Internet		User Identity Groups:GuestType_Guest-Daily	Authorize-Only succeeded
Nov 07, 2020 04:17:32.39...	<span style="color: green;">■</span>			D0:37:45:89:EF:64						Dynamic Authorization succeeded
Nov 07, 2020 04:16:14.85...	<span style="color: green;">■</span>		guest1	D0:37:45:89:EF:64				10.106.32.2...	GuestType_Guest-Daily	Guest Authentication Passed
Nov 07, 2020 03:43:30.75...	<span style="color: green;">■</span>			D0:37:45:89:EF:64	Default >> MAB	Default >> Wifi_Redirect_to_Guest_Portal	Guest-Portal		Profiled	Authentication succeeded

Aqui está o fluxo:

- O usuário convidado encontra a segunda regra de autorização (Wifi\_Redirect\_to\_Guest\_Portal) e é redirecionado para o Guest-Portal (**Autenticação bem-sucedida**).
- O convidado é redirecionado para autorregistro. Após o login bem-sucedido (com a conta recém-criada), o ISE envia a CoA Reauthenticate, que é confirmada pela WLC (**Autorização dinâmica bem-sucedida**).
- A WLC executa uma nova autenticação com o atributo Authorize-Only e o nome da ACL é retornado (**Authorize-Only successful**). O convidado recebe o acesso correto à rede.

Os Relatórios (**Operações > Relatórios > Convidado > Relatório Mestre de Convidado**) também confirmam que:

Logged At	Guest User Name	MAC Address	IP Address	Operation	Sponsor User Name
2020-11-07 04:17:01.1...	guest1	D0:37:45:89:EF:64	10.106.32.254	Password Change	guest1
2020-11-07 04:16:33.9...	guest1	D0:37:45:89:EF:64	10.106.32.254	AUP	
2020-11-07 04:13:51.0...	guest1	D0:37:45:89:EF:64	10.106.32.254	Add	SelfRegistration

Um usuário patrocinador (com privilégios corretos) pode verificar o status atual de um usuário convidado.



Este exemplo confirma que a conta foi criada e que o usuário fez login no portal:

The screenshot displays the Cisco Sponsor Portal interface. At the top left is the Cisco logo and the text 'Sponsor Portal'. At the top right, a user is logged in as 'test123'. Below the header, there are several action buttons: 'Create Accounts', 'Manage Accounts (1)', 'Pending Accounts (0)', and 'Notices (0)'. A secondary row of buttons includes 'Resend', 'Extend', 'Edit', 'Suspend', 'Reinstate', 'Delete', 'Reset Password', and 'Print'. The main content area shows a detailed view of a user account for 'guest1'. The user's information is as follows:

Username:	guest1
Password:	.....
First name:	Poonam
Last name:	Garg
Email address:	poongarg@cisco.com
Company:	Cisco
Mobile number:	+910000000000
Person being visited (email):	abc@cisco.com
Reason for visit:	Personal
Guest type:	Guest-Daily
SMS provider:	Global Default
From date (yyyy-mm-dd):	2020-11-07 09:43
To date (yyyy-mm-dd):	2020-11-08 09:43
Location:	India
SSID:	
Language:	English
Group tag:	
Time left:	0D 22H 48M
State:	Active

At the bottom of the user details section, there is a 'Done' button.

## Configuração opcional

Para cada estágio desse fluxo, diferentes opções podem ser configuradas. Tudo isso é configurado de acordo com o Portal de convidado em **Centros de trabalho > Acesso de convidado > Portais e componentes > Portais de convidado > Nome do portal > Editar > Comportamento do portal e Configurações de fluxo**. As configurações mais importantes incluem:

### Configurações de autorregistro

- Tipo de convidado - Descreve por quanto tempo a conta ficará ativa, as opções de expiração de senha, as horas de login e as opções (mistura de Perfil de tempo e Função de convidado)
- Código de registro - Se ativado, somente os usuários que sabem o código secreto têm permissão para fazer o autorregistro (deve fornecer a senha quando a conta for criada)
- AUP - Aceitar política de uso durante autorregistro
- O requisito para o patrocinador aprovar/ativar a conta de convidado.

### Configurações de login de convidado

- Código de acesso - Se habilitado, somente os usuários convidados que souberem o código secreto poderão fazer login.
- AUP - Aceite a Política de Uso durante o autorregistro.

- Opção de alteração de senha.

## Configurações de registro do dispositivo

- Por padrão, o dispositivo é registrado automaticamente.

## Configurações de Conformidade do Dispositivo Convidado

- Permite uma postura dentro do fluxo.

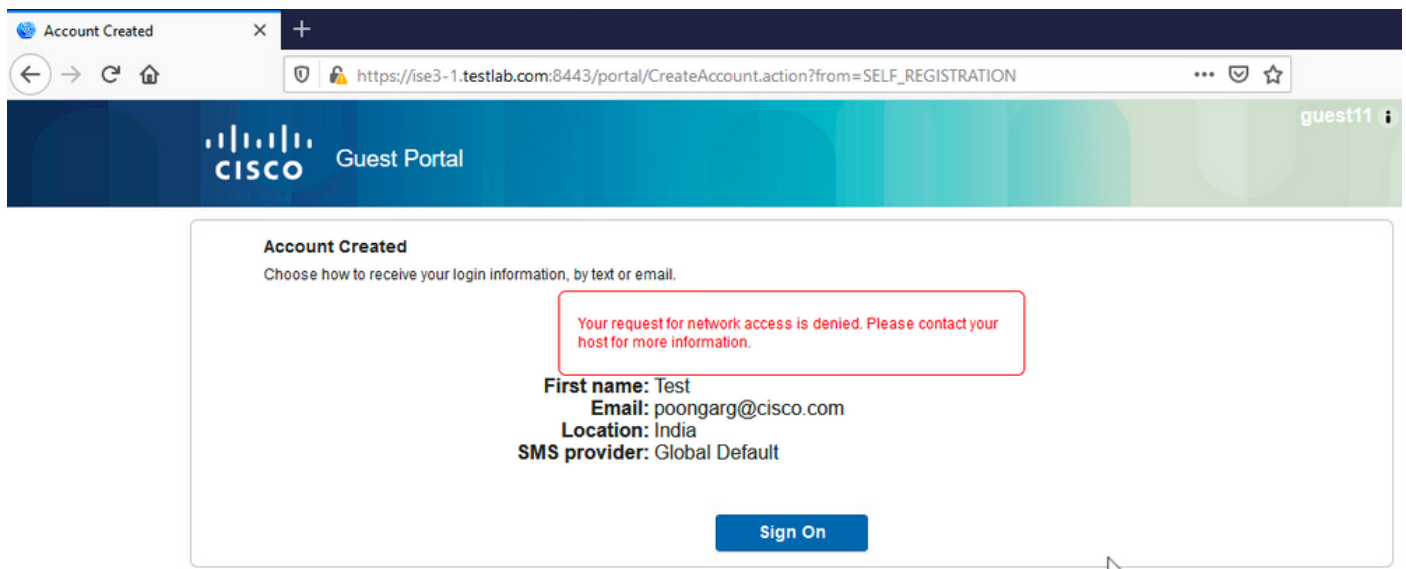
## Configurações de BYOD

- Permite que os usuários corporativos que usam o portal como convidados registrem seus dispositivos pessoais.

## Contas aprovadas pelo patrocinador

Se a opção **Exigir que os convidados sejam aprovados** estiver selecionada em **Configurações do formulário de registro**, a conta criada pelo convidado deverá ser aprovada por um patrocinador. Este recurso pode usar o e-mail para enviar uma notificação ao patrocinador (para aprovação da conta do convidado):

Se o servidor SMTP estiver configurado incorretamente, a conta não será criada:



O log do guest.log confirma que há um problema com o envio da Notificação de Aprovação para o e-mail do Patrocinador quando o servidor SMTP está configurado incorretamente:

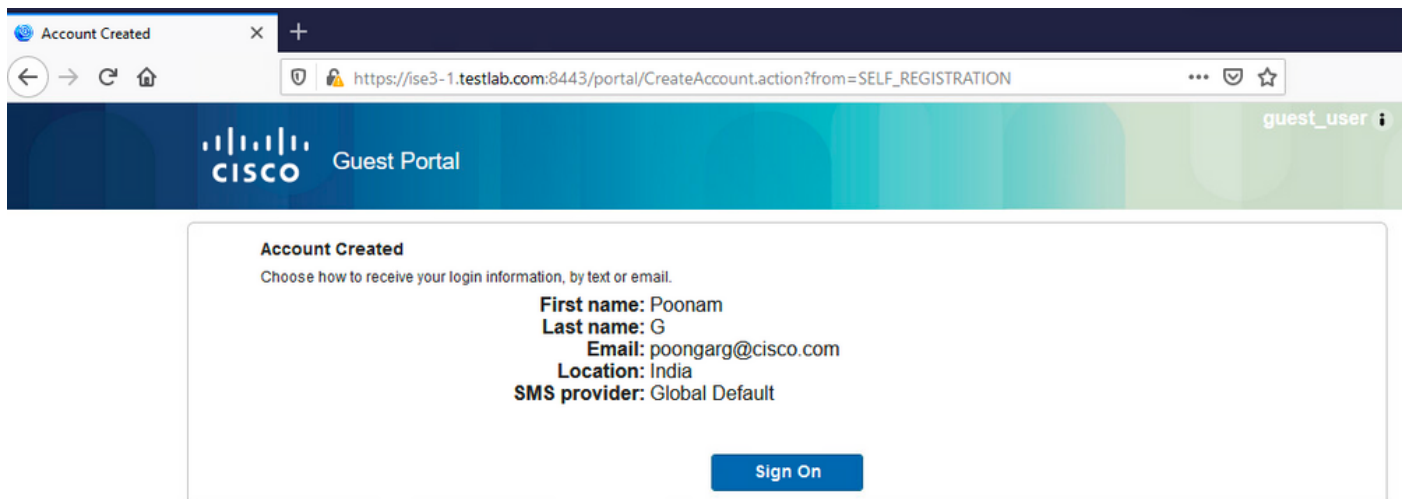
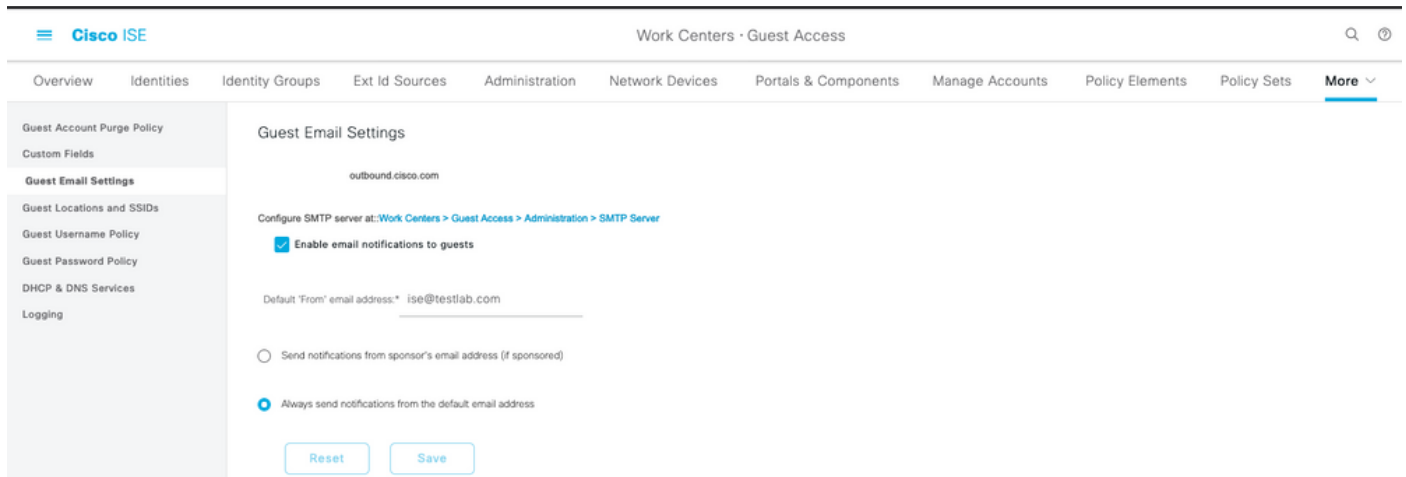
```
2020-11-07 07:16:38,547 ERROR [GUEST_ACCESS_SMTTP_RETRY_THREAD] []
cpm.guestaccess.apiservices.util.SmtplibMsgRetryThreadUtil --:- An exception occurred while sending
email :
javax.mail.MessagingException: Could not connect to SMTP host: outbound.cicso.com, port: 25,
response: 421
```

```
2020-11-07 07:16:38,547 ERROR [https-jsse-nio-10.106.32.25-8443-exec-1] []
cpm.guestaccess.apiservices.notification.NotificationService --:- sendApprovalNotification
```

com.cisco.cpm.guestaccess.exception.GuestAccessSystemException:

com.cisco.cpm.guestaccess.exception.GuestAccessSystemException: Unable to send mail. Failure occurred

Quando você tiver a configuração de e-mail e servidor SMTP adequada, a conta será criada:



Depois de ativar a opção **Exigir que os convidados sejam aprovados**, os campos de nome de usuário e senha são automaticamente removidos da seção **Incluir essas informações na página de Êxito do autorregistro**. É por isso que, quando a aprovação do patrocinador é necessária, as credenciais para usuários convidados não são exibidas por padrão na página da Web que apresenta informações para mostrar que a conta foi criada. Em vez disso, eles devem ser entregues por SMS (Short Message Services, serviços de mensagens curtas) ou e-mail. Esta opção deve ser habilitada na seção **Enviar notificação de credencial mediante aprovação usando** (marcar email/SMS).

Um e-mail de notificação é entregue ao responsável:

## Guest Approval Request



ise@testlab.com <ise@testlab.com>

Today at 1:07 PM

To: Poonam Garg (poongarg)



Please approve (or deny) this self-registering guest. The guest provided the following information:

Username: guest\_user

First Name: Poonam

Last Name: G

[Approve](#)

[Deny](#)

O patrocinador clica no link Aprovação e faz login no portal Patrocinador e a conta é aprovada:



Guest (guest\_user) has been approved.

[Help](#)

A partir desse ponto, o usuário convidado pode fazer login (com as credenciais recebidas por e-mail ou SMS).

Em resumo, há três endereços de e-mail usados nesse fluxo:

- Endereço "De" da notificação. Isso é definido estaticamente ou obtido da conta do patrocinador e usado como o endereço De para: notificação ao patrocinador (para aprovação) e detalhes da credencial para o convidado. Isso é configurado em **Centros de trabalho > Acesso de convidado > Configurações > Configurações de e-mail de convidado**.
- Endereço "Para" da notificação. Isso é usado para notificar o patrocinador de que recebeu uma conta para aprovação. Isso é configurado no Portal do convidado em **Centros de trabalho > Acesso do convidado > Portais do convidado > Portais e componentes > Nome do portal > Configurações do formulário de registro > Exigir que os convidados sejam aprovados > Enviar solicitação de aprovação por e-mail para**.
- Endereço "Para" do convidado. Isso é fornecido pelo usuário convidado durante o registro. Se **Enviar notificação de credencial mediante aprovação usando Email** estiver selecionado, o e-mail com detalhes de credencial (nome de usuário e senha) será entregue ao convidado.

## Entregar credenciais via SMS

As credenciais de convidado também podem ser fornecidas por SMS. Estas opções devem ser configuradas:

1. Escolha o provedor de serviços SMS em Configurações do Formulário de Registro:

SMS Service Provider

Guests can choose from these SMS providers:

- Global Default
- T-Mobile
- ATT
- Verizon
- ClickatellViaSMTP
- Orange
- Inmobile
- TheRingRingCompany
- Sprint
- NaaS

Guest see providers list only if multiple are selected

Configure SMS providers at:

[Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

2. Verifique a **notificação de credencial de envio mediante aprovação usando**: Caixa de seleção **SMS**.

Send credential notification upon approval using:

- Email
- SMS

3. Em seguida, o usuário convidado é solicitado a escolher o provedor disponível ao criar uma conta:

### Registration

Please complete this registration form:

Registration Code\*

8015

Username

Guest13

First name

Poonam

Last name

Email address\*

poongarg@cisco.com

Mobile number\*

+91 9999999999

Company

SMS provider\*

NaaS
ATT
Global Default
NaaS

4. Um SMS é entregue com o provedor escolhido e o número de telefone:

https://ise3-1.testlab.com:8443/portal/CreateAccount.action?from=SELF\_REGISTRATION

guest13

**CISCO** Guest Portal

**Account Created**  
Choose how to receive your login information, by text or email.

**First name:** Poonam  
**Email:** poongarg@cisco.com  
**Mobile number:** +919999999999  
**Location:** India  
**SMS provider:** NaaS

Sign On

5. Você pode configurar Provedores de SMS em **Administração > Sistema > Configurações > Gateway SMS**.

## Registro de dispositivo

Se a opção **Permitir que convidados registrem dispositivos** for selecionada depois que um usuário convidado fizer login e aceitar a AUP, você poderá registrar dispositivos:

## Guest Device Registration Settings

Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers](#) > [Guest Access](#) > [Configure](#) > [Guest Types](#)

**Device Registration**

You can add a maximum of 5 devices. Enter a device ID and device description. The device ID is the MAC address or Wi-Fi address of the device. It is an alphanumeric ID in this format: A1:B3:E5:19:6F:BB

Device ID \*

D0:37:45:89:EF:64

Device Description \*

Add Save, Continue

Cancel, Continue

Manage Devices (1)

D0:37:45:89:EF:64	Delete
-------------------	--------

Observe que o dispositivo já foi adicionado automaticamente (ele está na lista Gerenciar dispositivos). Isso porque **Registrar automaticamente os dispositivos convidados** foram selecionados.

## Postura

Se a opção **Exigir conformidade do dispositivo convidado** estiver selecionada, os usuários convidados serão provisionados com um Agente que executa a postura (NAC/Web Agent) depois

que fizerem login e aceitarem a AUP (e, opcionalmente, realizarem o registro do dispositivo). O ISE processa as regras de provisionamento do cliente para decidir qual agente deve ser provisionado. Em seguida, o agente que é executado na estação executa a postura (de acordo com as regras de postura) e envia os resultados ao ISE, que envia a reautenticação do CoA para alterar o status de autorização, se necessário.

As possíveis regras de autorização podem ser semelhantes a:

Guest_Complaint	AND	IdentityGroup-Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints	Wireless_MAB	Radius-Called-Station-ID CONTAINS Guest	Session-PostureStatus EQUALS Compliant	PermitAccess
Permanent_Guest_Access	AND	IdentityGroup-Name EQUALS Endpoint Identity Groups:Cisco_GuestEndpoints	Wireless_MAB	Radius-Called-Station-ID CONTAINS Guest		Limited_Access
Wifi_Redirect_to_Guest_Portal	AND			Radius-Called-Station-ID CONTAINS Guest	Wireless_MAB	Guest-Portal

Os primeiros usuários novos que encontrarem a regra Guest\_Authenticate serão redirecionados para o portal Autoregistrar Convidado. Depois que o usuário se registra e faz login, o CoA altera o status de autorização e o usuário recebe acesso limitado para executar postura e correção. Somente depois que o NAC Agent é provisionado e a estação está em conformidade, o CoA altera novamente o status de autorização para fornecer acesso à Internet.

Os problemas típicos de postura incluem a falta de regras corretas de provisionamento do cliente:



Isso também pode ser confirmado se você examinar o arquivo **guest.log**:

```
2020-11-09 09:23:32,157 ERROR [https-jsse-nio-10.106.32.25-8443-exec-7] []
guestaccess.flowmanager.step.guest.ClientProvStepExecutor -:guest18:- CP Response is not
successful, status=NO_POLICY
```

## BYOD

Se a opção **Permitir que os funcionários usem dispositivos pessoais na rede** estiver selecionada, os usuários corporativos que usam este portal poderão passar pelo fluxo de BYOD e registrar dispositivos pessoais. Para usuários convidados, essa configuração não altera nada.

O que significa "funcionários que usam o portal como convidados"?



Por padrão, os portais de convidado são configurados com o armazenamento de identidade **Guest\_Portal\_Sequence**:

▼ Portal Settings

---

HTTPS port: \* 8443 (8000 - 8999)

Allowed interfaces: \* Make selections in one or both columns based on your PSN configurations.

If bonding is not configured on a PSN, use: ⓘ	If bonding is configured on a PSN, use: ⓘ
<input checked="" type="checkbox"/> Gigabit Ethernet 0	<input checked="" type="checkbox"/> Bond 0 Uses Gigabit Ethernet <b>0</b> as <b>primary</b> , <b>1</b> as <b>backup</b> .
<input type="checkbox"/> Gigabit Ethernet 1	<input type="checkbox"/> Bond 1 Uses Gigabit Ethernet <b>2</b> as <b>primary</b> , <b>3</b> as <b>backup</b> .
<input type="checkbox"/> Gigabit Ethernet 2	<input type="checkbox"/> Bond 2 Uses Gigabit Ethernet <b>4</b> as <b>primary</b> , <b>5</b> as <b>backup</b> .
<input type="checkbox"/> Gigabit Ethernet 3	
<input type="checkbox"/> Gigabit Ethernet 4	
<input type="checkbox"/> Gigabit Ethernet 5	

Certificate group tag: \* Default Portal Certificate Group ▼

Configure certificates at:  
[Work Centers > Guest Access > Administration > System Certificates](#)

Authentication method: \* Guest\_Portal\_Sequence ▼ ⓘ

Configure authentication methods at:  
[Work Centers > Guest Access > Identities > Identity Source Sequences](#)

Esta é a sequência de armazenamento interno que tenta os Usuários Internos primeiro (antes de Usuários Convidados) e depois as credenciais do AD. Como as configurações Avançadas devem continuar para o próximo armazenamento na sequência quando um armazenamento de identidade selecionado não puder ser acessado para autenticação, um Funcionário com credenciais internas ou credenciais do AD poderá fazer logon no portal.

Overview **Identities** Identity Groups Ext Id Sources Administration Network Devices Portals & Components

Endpoints  
Network Access Users  
**Identity Source Sequences**

### Identity Source Sequence

\* Name: Guest\_Portal\_Sequence

Description: A built-in Identity Sequence for the Guest Portal

### Certificate Based Authentication

Select Certificate Authentication Profile

### Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
	Guest Users
	All_AD_Join_Points

Quando estiver nesse estágio no portal do convidado, o usuário fornecerá as credenciais definidas no armazenamento de Usuários Internos ou no Active Directory e o redirecionamento de BYOD ocorrerá:

BYOD Welcome  
Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

The following system was detected

**Windows**

Was your device detected incorrectly?

Select your Device

Windows

**Start**

Dessa forma, os usuários corporativos podem executar o BYOD para dispositivos pessoais.

Quando, em vez de credenciais de Usuários internos/AD, as credenciais de Usuários convidados

são fornecidas, o fluxo normal continua (sem BYOD).

## Alteração de VLAN

Ele permite executar o ativeX ou um miniaplicativo Java, que dispara o DHCP para liberar e renovar. Isso é necessário quando o CoA aciona a alteração de VLAN para o endpoint. Quando MAB é usado, o endpoint não está ciente de uma alteração de VLAN. Uma solução possível é alterar a VLAN (versão/renovação do DHCP) com o NAC Agent. Outra opção é solicitar um novo endereço IP por meio do miniaplicativo retornado na página da Web. Um atraso entre a liberação/CoA/renovação pode ser configurado. Esta opção não tem suporte em dispositivos móveis.

## Informações Relacionadas

- [Serviços de postura no Guia de configuração do Cisco ISE](#)
- [https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin\\_guide/b\\_ISE\\_admin\\_3\\_0/b\\_ISE\\_admin\\_30\\_overview.html](https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin_guide/b_ISE_admin_3_0/b_ISE_admin_30_overview.html)Cisco Guia do administrador do ISE 1.3
- [BYOD sem fio com Identity Services Engine](#)
- [Exemplo de suporte SCEP do ISE para configuração de BYOD](#)
- [Exemplo de configuração da autenticação da Web central no WLC e no ISE](#)
- [Exemplo de configuração de autenticação da Web central com APs FlexConnect em uma WLC com ISE](#)
- [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.