

Configurar o acesso provisório e permanente do convidado ISE

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Acesso permanente](#)

[Remoção do valor-limite para contas do convidado](#)

[Acesso temporário](#)

[O WLC desliga o comportamento](#)

[Verificar](#)

[Acesso permanente](#)

[Acesso temporário](#)

[Erros](#)

[Referências](#)

[Cisco relacionado apoia discussões da comunidade](#)

Introdução

Este documento descreve métodos diferentes para a configuração do acesso do convidado do Identity Services Engine (ISE). Baseado em condições diferentes em regras da autorização:

- o acesso permanente à rede pode ser fornecido (nenhuma exigência para autenticações subsequente)
- o acesso temporário à rede pode ser fornecido (exigindo a autenticação do convidado depois que a sessão expira)

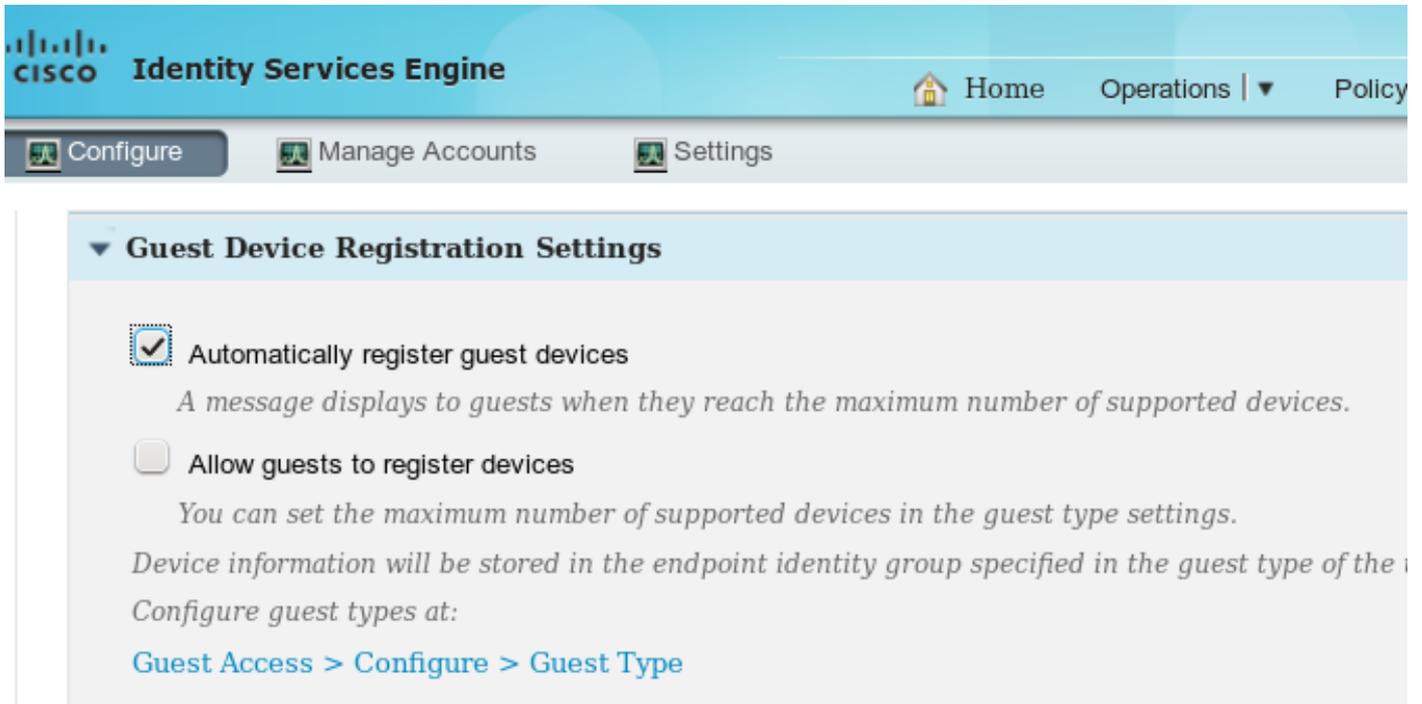
O comportamento específico do controlador do Wireless LAN (WLC) para a remoção da sessão é apresentado igualmente ao longo do impacto na encenação do acesso temporário.

Pré-requisitos

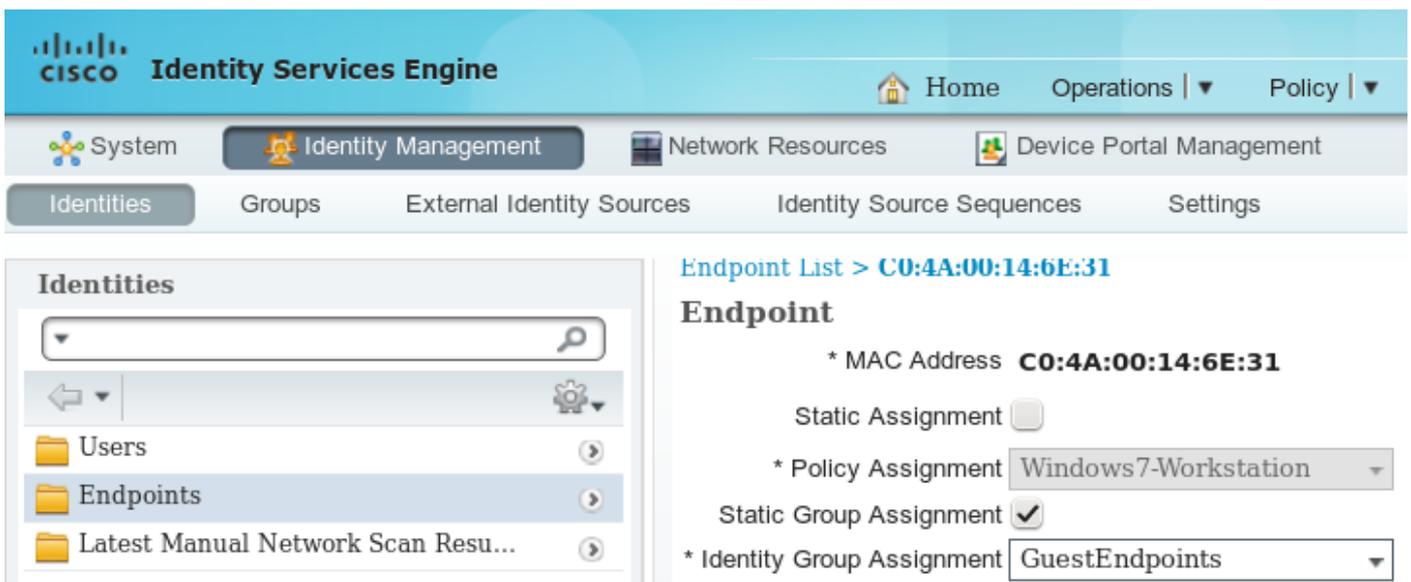
Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Disposições ISE e fluxos do convidado
- Configuração dos controladores do Wireless LAN (WLC)



O dispositivo de ponto final (MAC address) é registrado estaticamente no grupo específico do valor-limite (GuestEndpoints neste exemplo).



Esse grupo é derivado do tipo do convidado do usuário, segundo as indicações desta imagem.



Guest Type

Guest type name: *

Description:

▾

Collect Additional Data

Maximum Access Time

Maximum account duration

▾ Default (1-999)

Allow access only on these days and times:

From To Sun Mon Tue

Login Options

Maximum simultaneous logins (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: (1-999)

Endpoint identity group for guest device registration: ▾

Se é um usuário corporativo (loja da identidade o outro então convidado) esse ajuste é derivado dos ajustes portais.

The screenshot shows the 'Portal Settings' configuration page in the Cisco Identity Services Engine. The page includes the following settings:

- HTTPS port:** * 8443 (8000 - 8999)
- Allowed interfaces:** *
 - Gigabit Ethernet 0
 - Gigabit Ethernet 1
 - Gigabit Ethernet 2
 - Gigabit Ethernet 3
- Certificate group tag:** * Default Portal Certificate Group
- Authentication method:** * Guest Portal Sequence
 - Configure authentication methods at:
 - [Administration > Identity Management > Identity Source Sequences](#)
 - [Administration > External Identity Sources > SAML Identity Providers](#)
- Employees using this portal as guests inherit login options from:** * Contractor (default)

Em consequência o MAC address associado com o convidado pertence sempre a esse grupo específico da identidade. Isso não pode ser mudado automaticamente (por exemplo pelo serviço do perfilador).

Note: Para aplicar a condição da autorização de EndPointPolicy dos resultados do perfilador pode ser usada.

Sabendo que o dispositivo pertence sempre ao grupo que específico da identidade do valor-limite é possível construir as regras da autorização baseadas naquela, segundo as indicações desta imagem.

The screenshot shows the 'Authorization Policy' configuration page in the Cisco Identity Services Engine. The page includes the following elements:

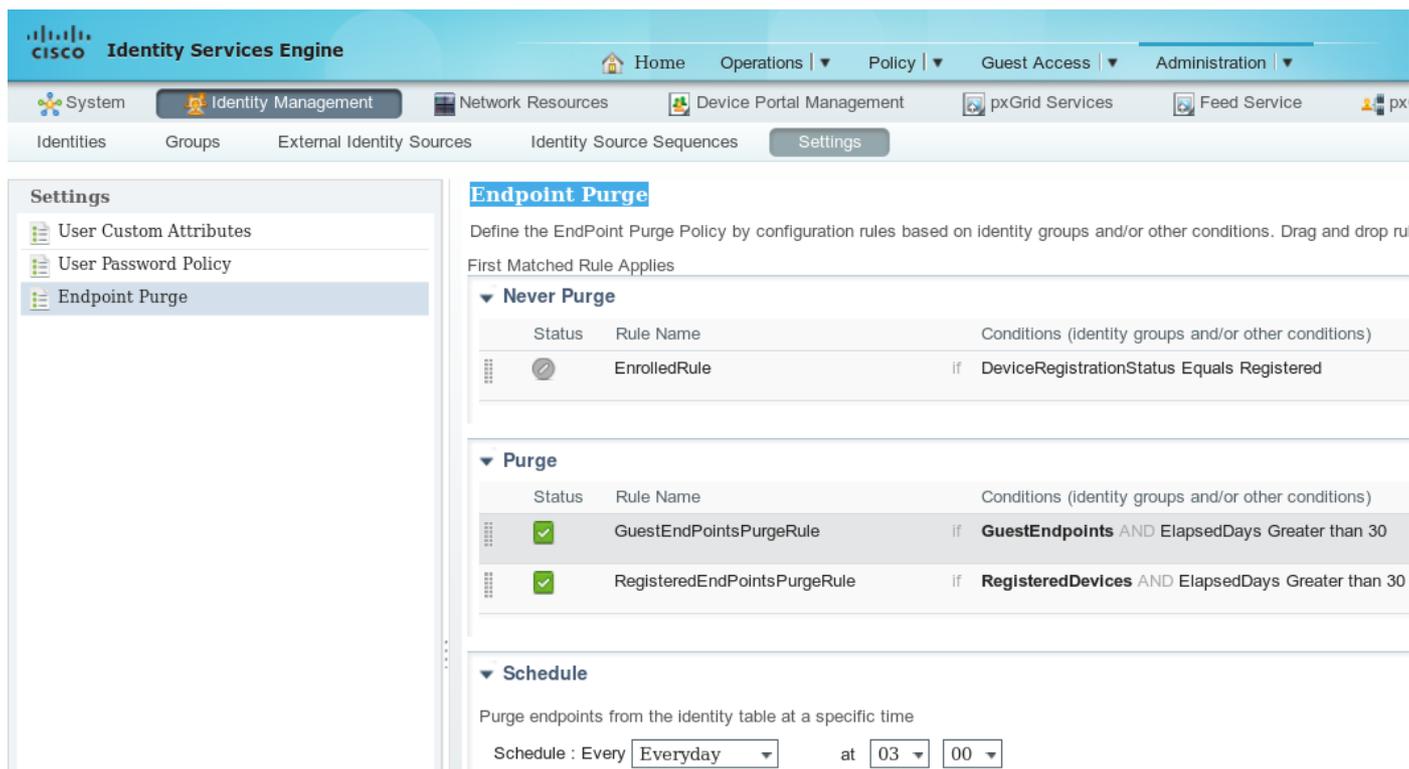
- Navigation:** Home, Operations, Policy, Guest Access, Administration.
- Menu:** Authentication, Authorization (selected), Profiling, Posture, Client Provisioning, TrustSec, Policy Elements.
- Section Header:** Authorization Policy
- Description:** Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)
- First Matched Rule Applies:** First Matched Rule Applies
- Exceptions (0):** Standard
- Table:**

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	AuthenticatedGuest	if GuestEndpoints AND Wireless_MAB	then PermitAccess
<input checked="" type="checkbox"/>	RedirectToPortal	if Wireless_MAB	then GuestPortal

Uma vez que um usuário não é autenticado, a autorização combina a regra genérica RedirectToPortal. Após a reorientação ao portal e à autenticação do convidado, o valor-limite é colocado no grupo específico da identidade do valor-limite. Isso é usado pelo primeiro, uma circunstância mais específica. Todas as autenticações subseqüente desse valor-limite batem a primeira regra da autorização e o usuário é acesso de rede completo fornecido sem a necessidade de autenticar novamente no portal do convidado.

Remoção do valor-limite para contas do convidado

Esta situação podia durar para sempre. Mas no valor-limite da remoção ISE 1.3 a funcionalidade foi introduzida. Com a configuração padrão.



The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The 'Administration' menu is expanded, showing 'Settings'. The left sidebar lists 'Settings' with sub-items: 'User Custom Attributes', 'User Password Policy', and 'Endpoint Purge'. The main content area is titled 'Endpoint Purge' and contains the following configuration details:

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rule

First Matched Rule Applies

Never Purge

Status	Rule Name	Conditions (identity groups and/or other conditions)
<input type="radio"/>	EnrolledRule	if DeviceRegistrationStatus Equals Registered

Purge

Status	Rule Name	Conditions (identity groups and/or other conditions)
<input checked="" type="checkbox"/>	GuestEndpointsPurgeRule	if GuestEndpoints AND ElapsedDays Greater than 30
<input checked="" type="checkbox"/>	RegisteredEndpointsPurgeRule	if RegisteredDevices AND ElapsedDays Greater than 30

Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every at

Todos os valores-limite usados para a autenticação do convidado são removidos após 30 dias (da criação do valor-limite). Em consequência após 30 dias o usuário convidado que tenta à rede de acesso bate a regra da autorização de RedirectToPortal e é reorientado geralmente para a autenticação.

Note: A funcionalidade da remoção do valor-limite é independente da expiração da política da remoção da conta do convidado e da conta do convidado.

Note: Em ISE 1.2 os valores-limite podiam ser removidos automaticamente somente ao bater limites de fila internos do perfilador. Os valores-limite o mais menos recentemente usados estão sendo removidos então.

Acesso temporário

Um outro método para o acesso do convidado é usar a condição de fluxo do convidado.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	AuthenticatedGuest	if (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow)	then PermitAccess
✓	RedirectToPortal	if Wireless_MAB	then GuestPortal

Que a circunstância está verificando sessões ativa no ISE e nela é atributos. Se essa sessão tem o atributo que indica que previamente o usuário convidado autenticou com sucesso condicione é combinado. Depois que o ISE recebe a mensagem da parada da contabilidade do raio do dispositivo do acesso de rede (NAD), a sessão está terminada e removida mais tarde. Nessa fase o acesso de rede da circunstância: UseCase = o fluxo do convidado não são satisfeitos anymore. Em consequência todas as autenticações subseqüente desse valor-limite batem a regra genérica que reorienta para a autenticação do convidado.

Note: Fluxo do convidado não apoiado quando o usuário for autenticado através do portal do ponto quente. Para aquelas encenações o atributo de UseCase é ajustado à consulta do host em vez do fluxo do convidado.

O WLC desliga o comportamento

Depois que as desconexões dos clientes da rede Wireless (por exemplo usando o botão disconnect em Windows) ele enviam o quadro do deauthentication. Mas isso é omitido pelo WLC e pode ser utilização confirmada “debuga o cliente xxxx” - o WLC apresenta o nenhum debuga quando o cliente está desligando do WLAN. Em consequência no cliente do Windows:

- o endereço IP de Um ou Mais Servidores Cisco ICM NT é removido da relação
- a relação está no estado: media desligados

Mas no WLC o estado é inalterado (cliente ainda no estado de CORRIDA).

Aquele for projeto de planeamento para o WLC, a sessão é removido quando

- batidas do idle timeout do usuário
- batidas do sessão-intervalo
- se usando a criptografia L2, então quando o intervalo da rotação da chave do grupo bater
- algo faz com mais que o AP/WLC retroceda o cliente fora de (por exemplo as restaurações do rádio AP, alguém fecham o WLAN, etc.)

Com essa configuração do comportamento e do acesso temporário depois que as desconexões do usuário da sessão WLAN não são removidas do ISE porque o WLC nunca cancelou o (e a parada nunca enviada da contabilidade do raio). Se a sessão não é removida, o ISE ainda recorda que a condição de fluxo velha da sessão e do convidado está satisfeita. Após o usuário da desconexão e da reconexão tenha o acesso de rede completo sem exigência reauthenticate.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-08-15 00:28:36...	i		0	guest	C0:4A:00:14:6E:31			Session State is Started
2015-08-15 00:13:58...	✓			guest	C0:4A:00:14:6E:31	Default >> Authent..	PermitAccess	Authorize-Only succeeded
2015-08-15 00:13:58...	✓				C0:4A:00:14:6E:31			Dynamic Authorization succeeded
2015-08-15 00:13:56...	✓			guest	C0:4A:00:14:6E:31			Guest Authentication Passed
2015-08-15 00:13:25...	✓				C0:4A:00:14:6E C0:4A:00:14:6E:31	Default >> Redirec...	GuestPortal	Authentication succeeded
2015-08-14 22:36:58...	✓			guest	C0:4A:00:14:6E:31	Default >> Authent..	PermitAccess	Authorize-Only succeeded

Mas se depois que o usuário da desconexão conecta ao WLAN diferente, a seguir o WLC decide cancelar a sessão velha. A parada da contabilidade do raio é enviada e o ISE remove a sessão. Se as tentativas do cliente a conectar à condição de fluxo original do convidado WLAN não são satisfeitas e o usuário está reorientado para a autenticação.

Note: O WLC configurado com proteção do quadro do Gerenciamento (MFP) aceita o quadro cifrado do deauthentication do cliente CCXv5 MFP.

Verificar

Acesso permanente

Após a reorientação ao portal e à autenticação bem sucedida do convidado o ISE envia a mudança da autorização (CoA) provocar o reauthentication. Em consequência a sessão nova do desvio da autenticação de MAC (MAB) está sendo construída. Este valor-limite do tempo pertence ao grupo da identidade de GuestEndpoints e os fósforos ordenam o fornecimento do acesso direto.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-08-14 22:25:45...	i		0	guest	C0:4A:00:14:6E:31				Session State is Terminated
2015-08-14 22:12:40...	✓			guest	C0:4A:00:14:6E:31	Default >> AuthenticatedGuest	PermitAccess	wlc1	Authorize-Only succeeded
2015-08-14 22:12:40...	✓				C0:4A:00:14:6E:31			wlc1	Dynamic Authorization succeeded
2015-08-14 22:12:32...	✓			guest	C0:4A:00:14:6E:31				Guest Authentication Passed
2015-08-14 22:10:19...	✓				C0:4A:00:14:6E C0:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	wlc1	Authentication succeeded

Nesse usuário Wireless da fase pode desligar, conectar aos WLAN diferentes, a seguir reconectar. Todas aquelas autenticações subseqüente usam a identidade baseada no MAC address, mas batem a primeira regra devido ao valor-limite que pertence ao grupo específico da identidade. O acesso de rede completo é fornecido sem a autenticação do convidado.

Cisco Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentications | Reports | Adaptive Network Control | Troubleshoot

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 0

Show Live Sessions | Add or Remove Columns | Refresh | Reset Repeat Counts

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-08-14 22:28:19...	i		0	C0:4A:00:14:6E	C0:4A:00:14:6E:31				Session State is Started
2015-08-14 22:28:15...	✓			C0:4A:00:14:6E	C0:4A:00:14:6E:31	Default >> Authent..	PermitAccess	wlc1	Authentication succeeded
2015-08-14 22:12:40...	✓			guest	C0:4A:00:14:6E:31	Default >> Authent..	PermitAccess	wlc1	Authorize-Only succeeded
2015-08-14 22:12:40...	✓			guest	C0:4A:00:14:6E:31			wlc1	Dynamic Authorization succeeded
2015-08-14 22:12:32...	✓			guest	C0:4A:00:14:6E:31				Guest Authentication Passed
2015-08-14 22:10:19...	✓			C0:4A:00:14:6E	C0:4A:00:14:6E:31	Default >> Redirec...	GuestPortal	wlc1	Authentication succeeded

Acesso temporário

Para o segundo começo da encenação (com a circunstância baseada no fluxo do convidado) é o mesmo.

Cisco Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentications | Reports | Adaptive Network Control | Troubleshoot

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 0

Show Live Sessions | Add or Remove Columns | Refresh | Reset Repeat Counts

Time	Status	Det...	R...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-08-14 22:34:35...	i		0	guest	C0:4A:00:14:6E:31			Session State is Started
2015-08-14 22:34:34...	✓			guest	C0:4A:00:14:6E:31	Default >> AuthenticatedGuest	PermitAccess	Authorize-Only succeeded
2015-08-14 22:34:34...	✓				C0:4A:00:14:6E:31			Dynamic Authorization succeeded
2015-08-14 22:34:33...	✓			guest	C0:4A:00:14:6E:31			Guest Authentication Passed
2015-08-14 22:33:51...	✓			C0:4A:00:14:6E	C0:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded

Mas depois que a sessão é removida para todas as autenticações subsequente, o convidado bateu a regra genérica e foi reorientado outra vez para a autenticação do convidado.

Cisco Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentications | Reports | Adaptive Network Control | Troubleshoot

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 0

Show Live Sessions | Add or Remove Columns | Refresh | Reset Repeat Counts

Time	Status	Det...	R...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-08-14 22:36:58...	i		0	guest	C0:4A:00:14:6E:31			Session State is Started
2015-08-14 22:36:58...	✓			guest	C0:4A:00:14:6E:31	Default >> AuthenticatedGuest	PermitAccess	Authorize-Only succeeded
2015-08-14 22:36:58...	✓				C0:4A:00:14:6E:31			Dynamic Authorization succeeded
2015-08-14 22:36:56...	✓			guest	C0:4A:00:14:6E:31			Guest Authentication Passed
2015-08-14 22:36:27...	✓			C0:4A:00:14:6E	C0:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded
2015-08-14 22:34:34...	✓			guest	C0:4A:00:14:6E:31	Default >> AuthenticatedGuest	PermitAccess	Authorize-Only succeeded
2015-08-14 22:34:34...	✓				C0:4A:00:14:6E:31			Dynamic Authorization succeeded
2015-08-14 22:34:33...	✓			guest	C0:4A:00:14:6E:31			Guest Authentication Passed
2015-08-14 22:33:51...	✓			C0:4A:00:14:6E	C0:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded

O convidado a condição de fluxo que é seja satisfeito quando os atributos corretos são existentes

para a sessão. Isso pode ser verificado olhando atributos do valor-limite. O resultado da autenticação bem sucedida do convidado é indicado.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The main content area displays a list of attributes and their values for a selected identity. The 'UseCase' attribute is highlighted with a blue box and set to 'Guest Flow'.

NAS-IP-Address	10.62.148.101
NAS-Identifier	WLC1
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Location#All Locations, Device Type#All Device Types
NetworkDeviceName	wlc1
OUI	TP-LINK TECHNOLOGIES CO.,LTD.
OriginalUserName	c04a00146e31
PolicyVersion	4
PortalUser	guest
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
PreviousDeviceRegistrationStatus	NotRegistered
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	Internal Endpoints
SelectedAuthorizationProfiles	PermitAccess
Service-Type	Authorize Only, Call Check
StaticAssignment	false
StaticGroupAssignment	true
StepData	5=MAB, 8=AuthenticatedGuest
Total Certainty Factor	60
UseCase	Guest Flow

```
PortalUser guest  
StepData 5=MAB, 8=AuthenticatedGuest  
UseCase Guest Flow
```

Erros

O CoA [CSCuu41157](#) ISE ENH termina envia sobre a remoção ou a expiração da conta do convidado.

(requisição de aprimoramento terminar sessões do convidado após a remoção ou a expiração da conta do convidado)

Referências

- [Guia de administradores de Cisco ISE 1.3](#)
- [Guia de administradores de Cisco ISE 1.4](#)
- [Exemplo de configuração do ponto quente da versão 1.3 ISE](#)
- [Exemplo de configuração registrado auto do portal do convidado da versão 1.3 ISE](#)
- [Autenticação da Web central no exemplo de configuração WLC e ISE](#)

- [Autenticação da Web central com FlexConnect AP em um WLC com exemplo de configuração ISE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)