

Acceso temporal y permanente del invitado de la configuración ISE

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Acceso permanente](#)

[Purgación del punto final para las cuentas de invitado](#)

[Acceso temporario](#)

[Comportamiento de la desconexión del WLC](#)

[Verificación](#)

[Acceso permanente](#)

[Acceso temporario](#)

[Bug](#)

[Referencias](#)

[Discusiones relacionadas de la comunidad del soporte de Cisco](#)

Introducción

Este documento describe los métodos distintos para la configuración del acceso de invitado del Identity Services Engine (ISE). De acuerdo con diversas condiciones en las reglas de la autorización:

- el acceso permanente a la red puede ser proporcionado (ningún requisito para las autenticaciones subsiguientes)
- el Acceso temporario a la red puede ser proporcionado (requiriendo la autenticación del invitado después de que expire la sesión)

También el comportamiento específico del regulador del Wireless LAN (WLC) para el retiro de la sesión se presenta a lo largo del impacto en el escenario del Acceso temporario.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Implementaciones ISE y flujos del invitado
- Configuración de los reguladores del Wireless LAN (WLCs)

Componentes Utilizados

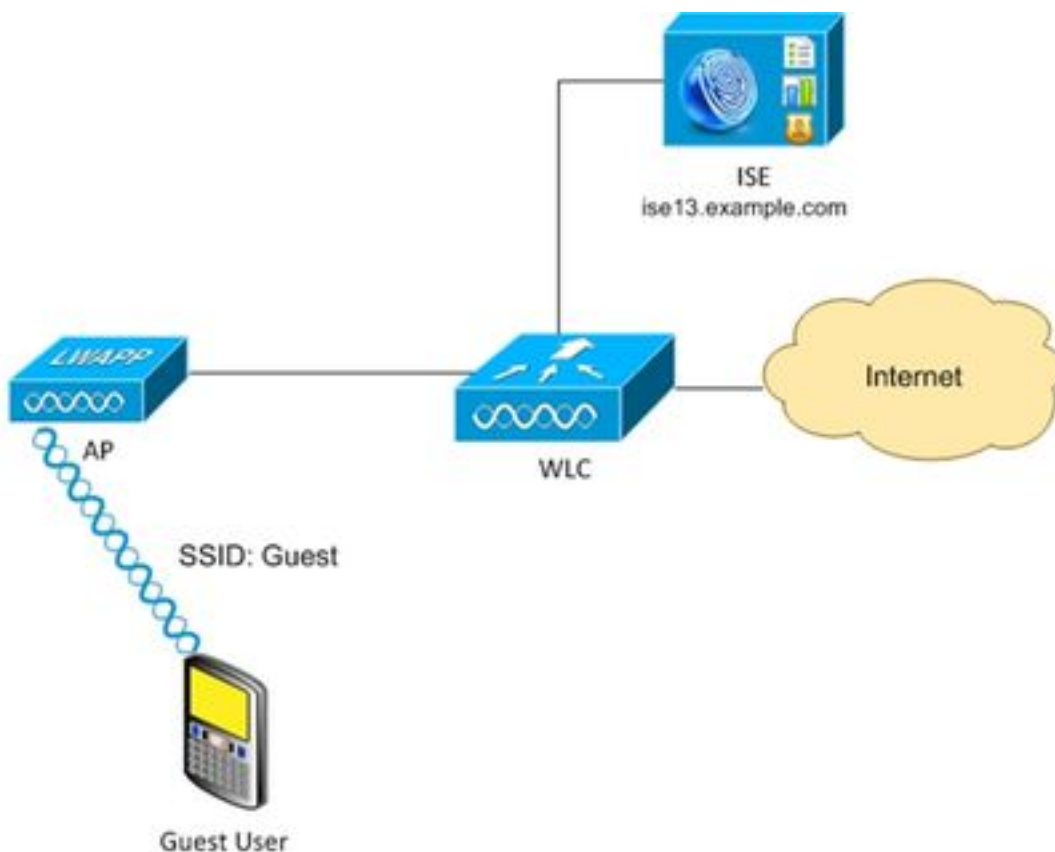
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Versión 7.6 y posterior del WLC de Cisco
- Software ISE, versión 1.3 y posterior

Configurar

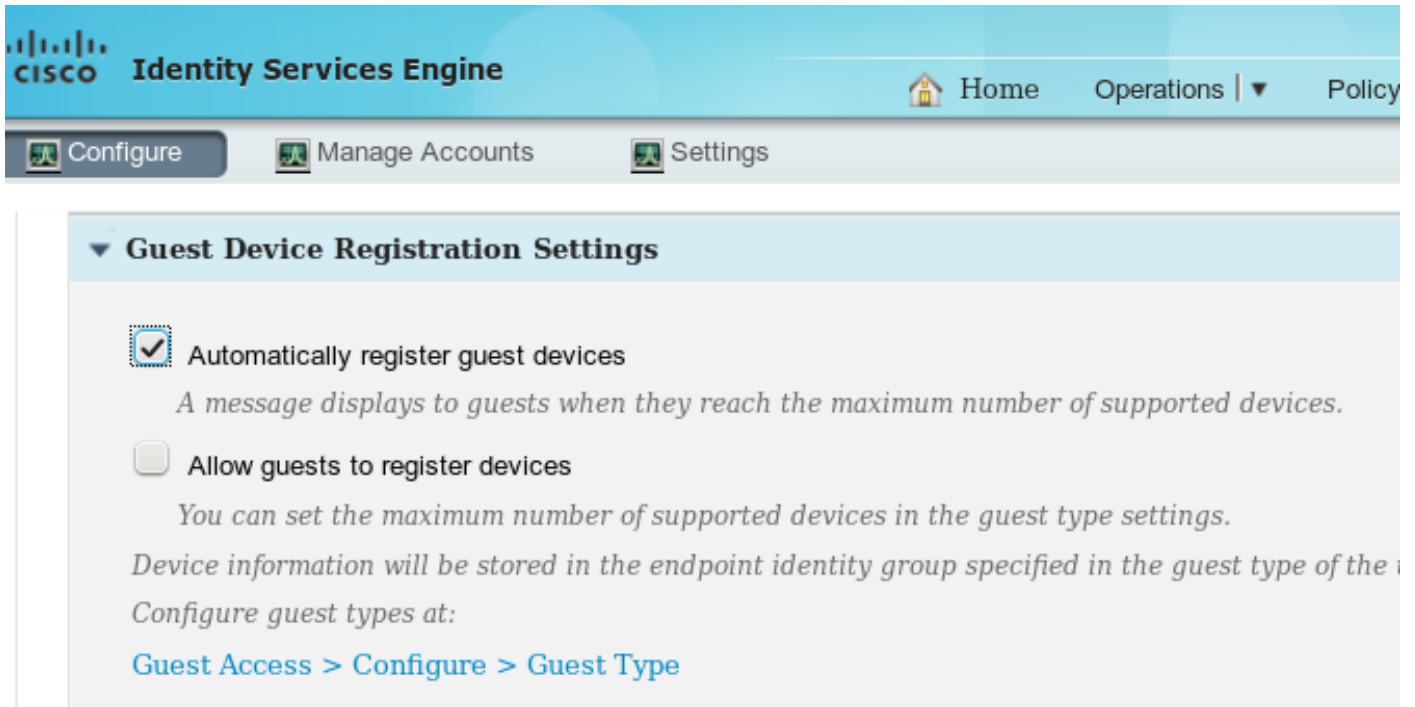
Para la configuración básica del acceso de invitado marque por favor las referencias con los ejemplos de configuración. Este artículo se centra en las reglas configuración y diferencias de la autorización en las condiciones de la autorización.

Diagrama de la red

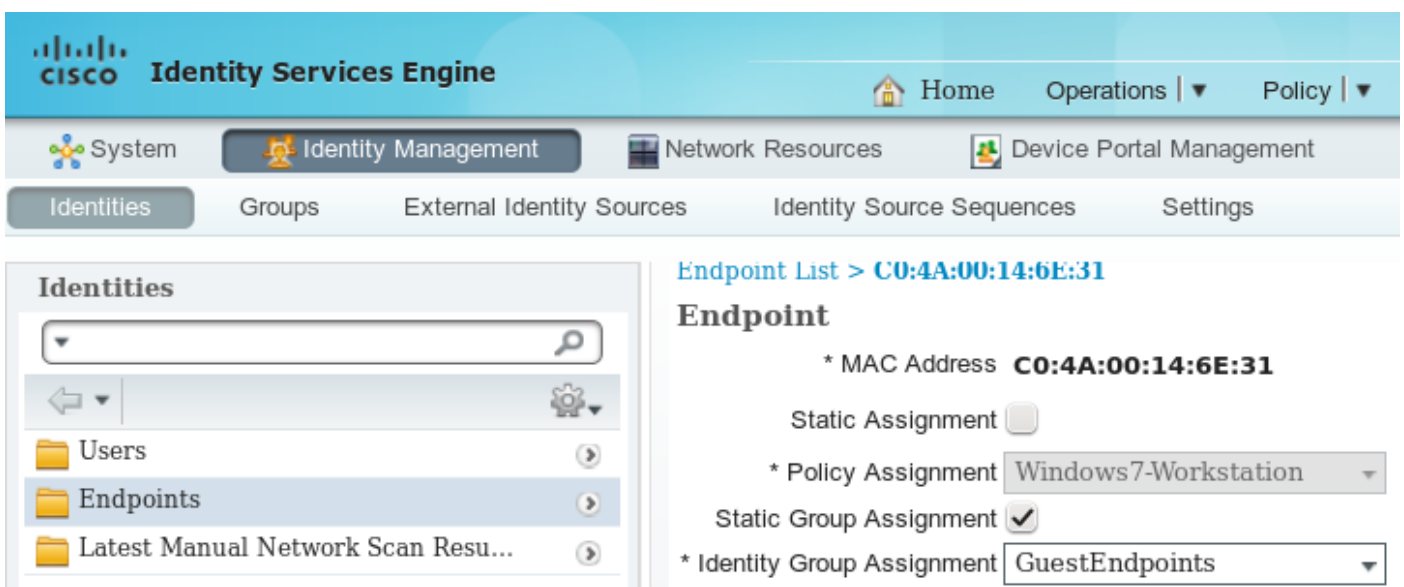


Acceso permanente

Para la versión 1.3 posterior ISE después de la autenticación satisfactoria en el portal del invitado con el registro del dispositivo habilitado.



El dispositivo de punto final (MAC address) se registra estáticamente en el grupo específico del punto final (GuestEndpoints en este ejemplo).



Derivan a ese grupo del tipo del invitado del usuario, tal y como se muestra en de esta imagen.

Guest Type

Guest type name: * Contractor (default)

Description: Default settings allow network access for up to a year.

Language File

Collect Additional Data Custom Fields...

Maximum Access Time

Maximum account duration

365 days Default 90 (1-999)

Allow access only on these days and times:

From 9:00 AM To 5:00 PM Sun Mon Tue

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 (i)
This requires the creation of an authorization policy rule

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

Endpoint identity group for guest device registration: GuestEndpoints

Si es usuario corporativo (almacén de la identidad el otro entonces invitado) esa configuración se deriva de las configuraciones porta.

Identity Services Engine

Home | Operations | Policy | Guest Access

Configure | Manage Accounts | Settings

Portal Settings

HTTPS port: * (8000 - 8999)

Allowed interfaces: *

- Gigabit Ethernet 0
- Gigabit Ethernet 1
- Gigabit Ethernet 2
- Gigabit Ethernet 3

Certificate group tag: *

Configure certificates at:
[Administration > System > Certificates > System Certificates](#)

Authentication method: * ⓘ

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: *

Como consecuencia el MAC address asociado al invitado pertenece siempre a ese grupo específico de la identidad. Eso no puede ser cambiada automáticamente (por ejemplo por el servicio del Profiler).

Note: Para aplicar la condición de la autorización de EndPointPolicy de los resultados del Profiler puede ser utilizada.

Sabiendo que el dispositivo pertenece siempre al grupo específico de la identidad del punto final que es posible construir las reglas de la autorización basadas en ésta, tal y como se muestra en de esta imagen.

Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

Authentication | **Authorization** | Profiling | Posture | Client Provisioning | TrustSec | Policy Elements

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
<input checked="" type="checkbox"/>	AuthenticatedGuest	if GuestEndpoints AND Wireless_MAB	then PermitAccess
<input checked="" type="checkbox"/>	RedirectToPortal	if Wireless_MAB	then GuestPortal

Una vez que no autentican a un usuario, la autorización hace juego la regla genérica RedirectToPortal. Después del cambio de dirección al portal y a la autenticación del invitado, el punto final se pone en el grupo específico de la identidad del punto final. Eso es utilizada por el primer, una condición más específica. Todas las autenticaciones subsiguientes de ese punto final golpean la primera regla de la autorización y el usuario es acceso a la red completo proporcionado sin la necesidad de reautenticar en el portal del invitado.

Purgación del punto final para las cuentas de invitado

Esta situación podía durar para siempre. Pero en el punto final de la purgación ISE 1.3 se han introducido las funciones. Con la configuración predeterminada.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The main menu shows 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', and 'Feed Service'. The 'Settings' section is expanded, showing 'User Custom Attributes', 'User Password Policy', and 'Endpoint Purge'. The 'Endpoint Purge' configuration page is active, with the following details:

- Endpoint Purge**: 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: Off
 - Rule Name: EnrolledRule
 - Conditions: if DeviceRegistrationStatus Equals Registered
- Purge**:
 - Status: On
 - Rule Name: GuestEndpointsPurgeRule
 - Conditions: if GuestEndpoints AND ElapsedDays Greater than 30
 - Status: On
 - Rule Name: RegisteredEndpointsPurgeRule
 - Conditions: if RegisteredDevices AND ElapsedDays Greater than 30
- Schedule**:
 - Purge endpoints from the identity table at a specific time
 - Schedule: Every Everyday at 03:00

Todos los puntos finales usados para la autenticación del invitado se quitan después de 30 días (de la creación del punto final). Como consecuencia después de 30 días el Usuario invitado que intenta a la red de acceso golpea la regla de la autorización de RedirectToPortal y se reorienta generalmente para la autenticación.

Note: Las funciones de la purgación del punto final son independiente de la expiración de la directiva y de la cuenta de invitado de la purgación de la cuenta de invitado.

Note: En ISE 1.2 los puntos finales podían ser quitados automáticamente solamente al golpear los límites de cola internos del profiler. Entonces menos puntos finales usados recientemente se están quitando.

Acceso temporario

Otro método para el acceso de invitado es utilizar la condición de flujo del invitado.

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 la condición está marcando a las sesiones activas en el ISE y ella es atributos. Si esa sesión tiene el atributo que indica que el Usuario invitado ha autenticado previamente con éxito condicione se corresponde con. Después de que el ISE reciba el mensaje de la parada de las estadísticas del radio del dispositivo de acceso a la red (NAD), la sesión se termina y posterior quitó. En esa etapa el acceso a la red de la condición: UseCase = el flujo del invitado no se satisface más. Como consecuencia todas las autenticaciones subsiguientes de ese punto final golpean la regla genérica que reorienta para la autenticación del invitado.

Note: Flujo del invitado no soportado cuando autentican al usuario vía el portal del hotspot. Para esos escenarios el atributo de UseCase se fija a las operaciones de búsqueda del host en vez del flujo del invitado.

Comportamiento de la desconexión del WLC

Después de que las desconexiones de los clientes de la red inalámbrica (por ejemplo usando el botón disconnect en Windows) él envíen la trama del deauthentication. Pero eso es omitida por el WLC y se puede confirmar usando “el xxxx del cliente del debug” - el WLC no presenta ningún debug cuando el cliente está desconectando de la red inalámbrica (WLAN). Como consecuencia en el cliente de Windows:

- el IP Address se quita de la interfaz
- la interfaz está en el estado: media desconectados

Pero en el WLC el estatus es sin cambios (todavía cliente en el estado de FUNCIONAMIENTO).

Se quita ése es diseño previsto para el WLC, la sesión cuando

- golpes del tiempo de inactividad del usuario
- golpes del sesión-descanso
- si usa el cifrado L2, entonces cuando el intervalo de la rotación de la clave del grupo golpea
- el algo más hace el AP/WLC golpear al cliente con el pie de (e.g. las restauraciones de la radio AP, alguien apagan el WLAN, el etc.)

Con esa configuración del comportamiento y del Acceso temporario después de que las desconexiones del usuario de la sesión de la red inalámbrica (WLAN) no se quiten del ISE porque el WLC nunca ha borrado lo (y la parada nunca enviada de las estadísticas del radio). Si la sesión no se quita, el ISE todavía recuerda que la vieja condición de flujo de la sesión y del invitado está

satisfecha. Después del usuario de la desconexión y de la reconexión tenga acceso a la red completo sin el requisito de reauthenticate.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, and Administration. Below these are sub-tabs: Authentications, Reports, Adaptive Network Control, and Troubleshoot. The main dashboard displays three metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). Below the dashboard is a table of live sessions with columns for Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event. The table contains several rows of session data, including successful authentications and session terminations.

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

Pero si después de que el usuario de la desconexión conecte con diversa red inalámbrica (WLAN), después el WLC decide a borrar la vieja sesión. Se envía la parada de las estadísticas del radio y el ISE quita la sesión. Si los intentos del cliente a conectar con la condición de flujo original del invitado de la red inalámbrica (WLAN) no se satisfacen y reorientan al usuario para la autenticación.

Note: El WLC configurado con la protección del capítulo de la Administración (MFP) valida la trama cifrada del deauthentication del cliente CCXv5 MFP.

Verificación

Acceso permanente

Después del cambio de dirección al portal y a la autenticación satisfactoria del invitado el ISE envía el cambio de la autorización (CoA) de accionar el reauthentication. Como consecuencia la nueva sesión de puente de la autenticación de MAC (MAB) se está construyendo. Este punto final del tiempo pertenece al grupo de la identidad de GuestEndpoints y hace juego la regla que proporciona al acceso total.

The screenshot shows the Cisco Identity Services Engine (ISE) interface with a 'Client' label on the right. The dashboard metrics are: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), and Client. Below the dashboard is a table of live sessions with columns for Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, Network Device, and Event. The table contains several rows of session data, including successful authentications and session terminations.

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

En ese usuario de red inalámbrica de la etapa puede desconectar, conectar con diversos WLAN, después volver a conectar. Todas esas autenticaciones subsiguientes utilizan la identidad basada

en el MAC address, pero golpean la primera regla debido al punto final que pertenece al grupo específico de la identidad. El acceso a la red completo se proporciona sin la autenticación del invitado.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, and Administration. Below these are sub-tabs: Authentications, Reports, Adaptive Network Control, and Troubleshoot. A summary bar shows: Misconfigured Supplicants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). The main table displays live sessions with columns: Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, Network Device, and Event.

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

Acceso temporario

Para el segundo principio del escenario (con la condición basada en el flujo del invitado) es lo mismo.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are navigation tabs: Home, Operations, Policy, Guest Access, and Administration. Below these are sub-tabs: Authentications, Reports, Adaptive Network Control, and Troubleshoot. A summary bar shows: Misconfigured Supplicants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). The main table displays live sessions with columns: Time, Status, Det..., R..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event.

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

Pero después de que la sesión se quite para todas las autenticaciones subsiguientes, el invitado golpeó la regla genérica y se reorienta otra vez para la autenticación del invitado.

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...			0	guest	CO:4A:00:14:6E:31			Session State is Started
2015-08-14 22:36:58...				guest	CO:4A:00:14:6E:31	Default >> AuthenticatedGuest	PermitAccess	Authorize-Only succeeded
2015-08-14 22:36:58...					CO:4A:00:14:6E:31			Dynamic Authorization succeeded
2015-08-14 22:36:56...				guest	CO:4A:00:14:6E:31			Guest Authentication Passed
2015-08-14 22:36:27...				CO:4A:00:14:6E:31	CO:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded
2015-08-14 22:34:34...				guest	CO:4A:00:14:6E:31	Default >> AuthenticatedGuest	PermitAccess	Authorize-Only succeeded
2015-08-14 22:34:34...					CO:4A:00:14:6E:31			Dynamic Authorization succeeded
2015-08-14 22:34:33...				guest	CO:4A:00:14:6E:31			Guest Authentication Passed
2015-08-14 22:33:51...				CO:4A:00:14:6E:31	CO:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded

Satisfagan al invitado que es la condición de flujo cuando los atributos correctos son existentes para la sesión. Eso puede ser verificada mirando los atributos del punto final. El resultado de la autenticación acertada del invitado se indica.

CISCO Identity Services Engine

Home | Operations | Policy | Guest Access | Administration

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Identities

- Users
- Endpoints
- Latest Manual Network Scan Resu...

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

Bug

El CoA [CSCuu41157](#) ISE ENH termina envía encendido el retiro o el vencimiento de la cuenta de invitado.

(pedido de mejora de terminar las sesiones del invitado después del retiro o del vencimiento de la cuenta de invitado)

Referencias

- [Guía de administradores de Cisco ISE 1.3](#)
- [Guía de administradores de Cisco ISE 1.4](#)
- [Ejemplo de configuración del hotspot de la versión 1.3 ISE](#)
- [Ejemplo de configuración registrado uno mismo del portal del invitado de la versión 1.3 ISE](#)
- [Autenticación Web central en el ejemplo de configuración del WLC y ISE](#)
- [Autenticación Web central con FlexConnect AP en un WLC con el ejemplo de configuración ISE](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)