

# Configurazione dell'accesso temporaneo e permanente per i guest ISE

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Accesso permanente](#)

[Rimozione endpoint per account guest](#)

[Accesso temporaneo](#)

[Comportamento disconnessione WLC](#)

[Verifica](#)

[Accesso permanente](#)

[Accesso temporaneo](#)

[Bug](#)

[Riferimenti](#)

[Discussioni correlate nella Cisco Support Community](#)

## Introduzione

In questo documento vengono descritti i diversi metodi di configurazione dell'accesso guest di Identity Services Engine (ISE). In base alle diverse condizioni nelle norme di autorizzazione:

- è possibile fornire l'accesso permanente alla rete (non è richiesta alcuna autenticazione successiva)
- è possibile fornire l'accesso temporaneo alla rete (è richiesta l'autenticazione guest dopo la scadenza della sessione)

Viene inoltre presentato il comportamento specifico del controller WLC (Wireless LAN Controller) per la rimozione delle sessioni insieme all'impatto sullo scenario di accesso temporaneo.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Implementazioni ISE e flussi guest
- Configurazione dei Wireless LAN Controller (WLC)

## Componenti usati

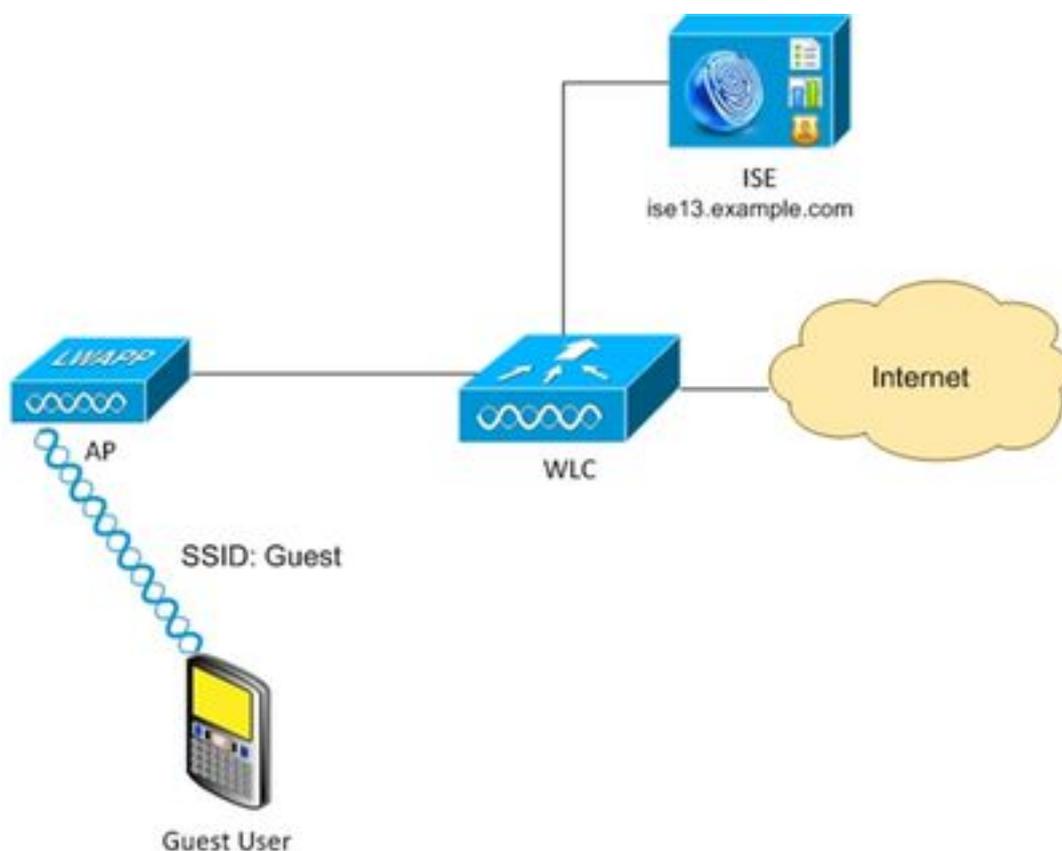
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- Cisco WLC versione 7.6 e successive
- Software ISE versione 1.3 e successive

## Configurazione

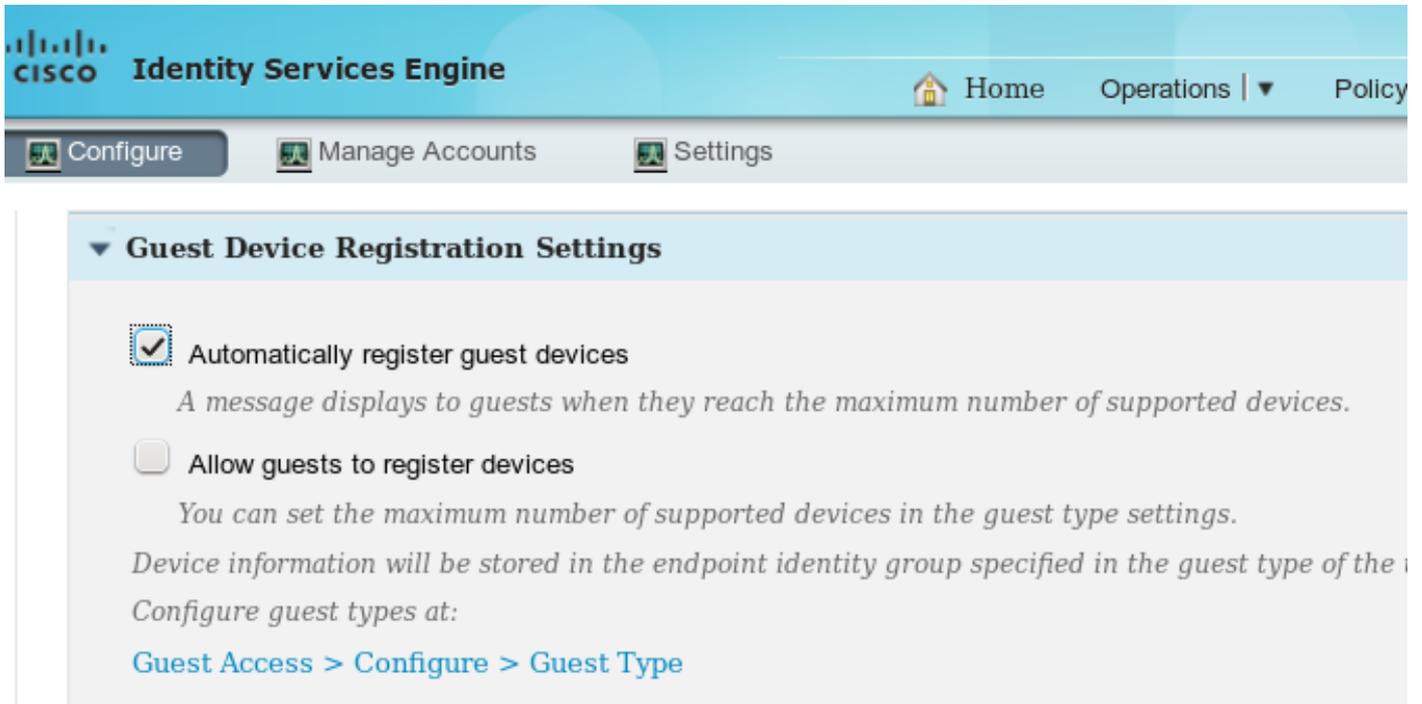
Per la configurazione di accesso guest di base, controllare i riferimenti con gli esempi di configurazione. In questo articolo vengono illustrate la configurazione delle regole di autorizzazione e le differenze nelle condizioni di autorizzazione.

## Esempio di rete

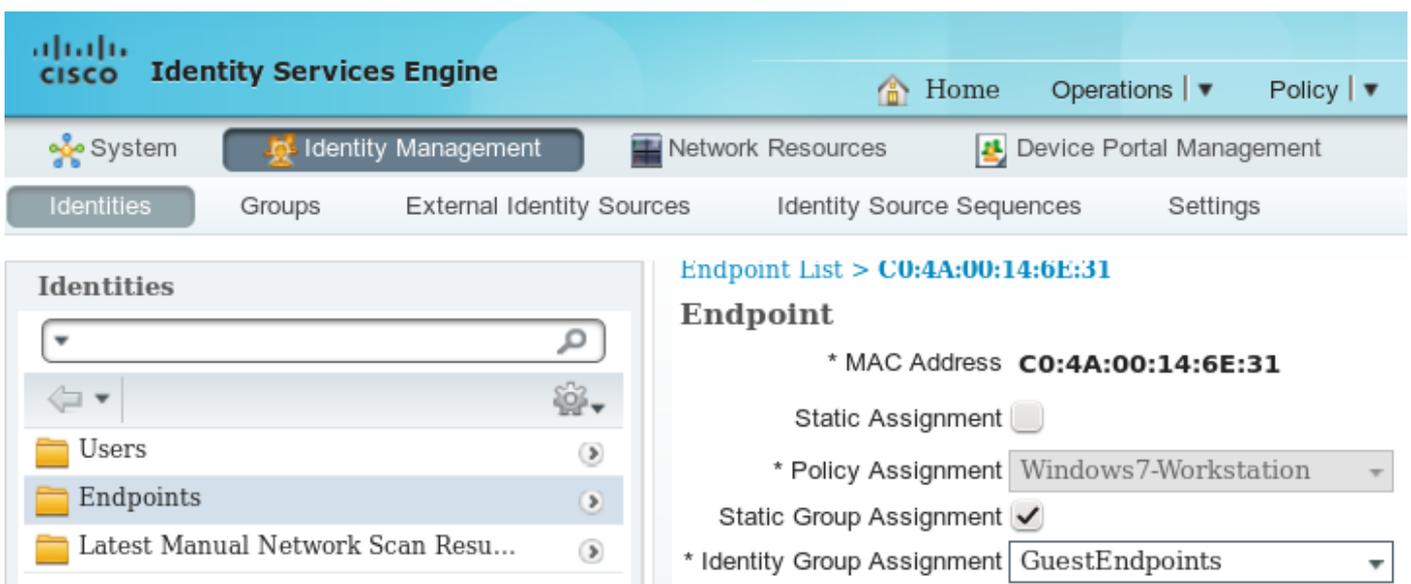


## Accesso permanente

Per ISE versione 1.3 e successive dopo l'autenticazione sul portale guest con la registrazione del dispositivo abilitata.



Il dispositivo endpoint (indirizzo MAC) è registrato in modo statico in un gruppo endpoint specifico (GuestEndpoints in questo esempio).



Il gruppo è derivato dal tipo Guest dell'utente, come illustrato in questa immagine.



## 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 si tratta di un utente aziendale (archivio identità diverso da guest), l'impostazione viene derivata dalle impostazioni del portale.

**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: \*

Di conseguenza, l'indirizzo MAC associato al guest appartiene sempre a quel gruppo di identità specifico. Non può essere modificato automaticamente (ad esempio dal servizio Profiler).

**Nota:** Per applicare i risultati del profiler è possibile utilizzare la condizione di autorizzazione EndPointPolicy.

Poiché il dispositivo appartiene sempre a un gruppo di identità dell'endpoint specifico, è possibile creare regole di autorizzazione basate su tale gruppo, come mostrato nell'immagine.

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

Dopo che un utente non è autenticato, l'autorizzazione corrisponde alla regola generica RedirectToPortal. Dopo il reindirizzamento al portale guest e l'autenticazione, l'endpoint viene

inserito nel gruppo di identità dell'endpoint specifico. Questo viene usato dalla prima condizione, più specifica. Tutte le autenticazioni successive dell'endpoint vengono eseguite sulla prima regola di autorizzazione e all'utente viene concesso l'accesso completo alla rete senza la necessità di ripetere l'autenticazione sul portale guest.

## Rimozione endpoint per account guest

Questa situazione potrebbe durare per sempre. Tuttavia, ad ISE 1.3 è stata introdotta la funzionalità Purge Endpoint. Con la configurazione predefinita.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. The left sidebar shows 'Settings' with 'Endpoint Purge' selected. 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 <b>GuestEndpoints</b> AND ElapsedDays Greater than 30
<input checked="" type="checkbox"/>	RegisteredEndPointsPurgeRule	if <b>RegisteredDevices</b> AND ElapsedDays Greater than 30

**Schedule**

Purge endpoints from the identity table at a specific time

Schedule : Every  at

Tutti gli endpoint utilizzati per l'autenticazione guest vengono rimossi dopo 30 giorni dalla creazione dell'endpoint. Di conseguenza, in genere dopo 30 giorni che l'utente guest tenta di accedere alla regola di autorizzazione RedirectToPortal riscontrata nella rete e viene reindirizzato per l'autenticazione.

**Nota:** La funzionalità di rimozione degli endpoint è indipendente dai criteri di rimozione degli account guest e dalla scadenza degli account guest.

**Nota:** In ISE 1.2 gli endpoint possono essere rimossi automaticamente solo quando si superano i limiti della coda interna del profiler. Verranno rimossi gli endpoint utilizzati meno di recente.

## Accesso temporaneo

Un altro metodo per l'accesso guest consiste nell'utilizzare la condizione Flusso guest.

**CISCO 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
✓	AuthenticatedGuest	if (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow )	then PermitAccess
✓	RedirectToPortal	if Wireless_MAB	then GuestPortal

Questa condizione sta verificando le sessioni attive su ISE e i relativi attributi. Se nella sessione è presente l'attributo che indica che in precedenza l'utente guest ha eseguito l'autenticazione con successo, la condizione viene soddisfatta. Dopo che ISE ha ricevuto un messaggio di interruzione dell'accounting Radius da NAD (Network Access Device), la sessione viene terminata e successivamente rimossa. In questa fase la condizione Accesso alla rete:UseCase = Flusso guest non è più soddisfatta. Di conseguenza, tutte le autenticazioni successive dell'endpoint raggiungono il reindirizzamento delle regole generiche per l'autenticazione guest.

**Nota:** Il flusso guest non è supportato quando l'utente viene autenticato tramite il portale HotSpot. Per questi scenari l'attributo UseCase è impostato su Ricerca host anziché su Flusso guest.

## Comportamento disconnessione WLC

Quando i client si disconnettono dalla rete wireless (ad esempio utilizzando il pulsante di disconnessione in Windows), invia un frame di deautenticazione. Ma questo viene omesso dal WLC e può essere confermato usando "debug client xxxx" - WLC non presenta debug quando il client si disconnette dalla WLAN. Di conseguenza sul client Windows:

- l'indirizzo ip viene rimosso dall'interfaccia
- interfaccia nello stato: supporto disconnesso

Tuttavia, sul WLC, lo stato è invariato (il client è ancora in stato RUN).

Progettato per WLC, la sessione viene rimossa quando

- accessi utente con timeout di inattività
- riscontri session-timeout
- se si utilizza la crittografia L2, quando l'intervallo di rotazione della chiave di gruppo raggiunge
- qualcos'altro fa sì che l'AP/WLC spenga il client (ad esempio, la radio dell'AP viene reimpostata, qualcuno chiude la WLAN, ecc.)

Con questo comportamento, la configurazione dell'accesso temporaneo dopo la disconnessione dell'utente dalla sessione WLAN non viene rimossa da ISE perché il WLC non l'ha mai cancellata (e non ha mai inviato il messaggio Radius Accounting Stop). Se la sessione non viene rimossa, ISE ricorda ancora la sessione precedente e la condizione di flusso guest è soddisfatta. Dopo la disconnessione e la riconnessione, l'utente dispone di accesso completo alla rete senza la

necessità di rieseguire l'autenticazione.

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 authentication sessions with columns for Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event. The table contains six rows of session data.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-08-15 00:28:36...			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

Ma se dopo la disconnessione l'utente si connette a una WLAN diversa, il WLC decide di cancellare la vecchia sessione. Viene inviato il comando Radius Accounting Stop, che rimuove la sessione. Se il client tenta di connettersi alla condizione di flusso guest WLAN originale non è soddisfatto e l'utente viene reindirizzato per l'autenticazione.

**Nota:** Il WLC configurato con MFP (Management Frame Protection) accetta il frame di deautenticazione crittografato dal client MFP CCXv5.

## Verifica

### Accesso permanente

Dopo il reindirizzamento al portale guest e la riuscita dell'autenticazione, ISE invia il messaggio CoA (Change of Authorization) per attivare la riautenticazione. Di conseguenza, è in corso la creazione della nuova sessione MAB (MAC Authentication Bypass). Questo endpoint temporale appartiene al gruppo di identità GuestEndpoints e corrisponde alla regola che fornisce l'accesso completo.

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 authentication sessions with columns for Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, Network Device, and Event. The table contains five rows of session data.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-08-14 22:25:45...			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

A questo punto l'utente wireless può disconnettersi, connettersi a diverse WLAN, quindi riconnettersi. Tutte le autenticazioni successive utilizzano l'identità basata sull'indirizzo MAC, ma incontrano la prima regola a causa dell'appartenenza dell'endpoint a un gruppo di identità specifico. L'accesso completo alla rete viene fornito senza autenticazione guest.

**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 | Client

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...			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

## Accesso temporaneo

L'inizio del secondo scenario (con condizione basata sul flusso guest) è lo stesso.

**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...			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

Tuttavia, dopo la rimozione della sessione per tutte le autenticazioni successive, il guest ha raggiunto la regola generica e viene nuovamente reindirizzato per l'autenticazione guest.

**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	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

La condizione di flusso guest viene soddisfatta quando sono presenti gli attributi corretti per la sessione. È possibile verificare questa condizione esaminando gli attributi dell'endpoint. Vengono

indicati i risultati dell'autenticazione guest.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Admin'. The main navigation bar has 'System', 'Identity Management', 'Network Resources', 'Device Portal Management', and 'pxGrid Services'. The 'Identities' tab is selected, and the 'Users' folder is expanded. The configuration details for the 'guest' user are displayed on the right side of the screen.

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

[CSCuu41157](#) ISE ENH CoA termina l'invio quando l'account guest viene rimosso o scade.

(richiesta di miglioramento per terminare le sessioni guest dopo la rimozione o la scadenza dell'account guest)

## Riferimenti

- [Guida per l'amministratore di Cisco ISE 1.3](#)
- [Guida per l'amministratore di Cisco ISE 1.4](#)
- [Esempio di configurazione di un hotspot ISE versione 1.3](#)
- [Esempio di configurazione di ISE Version 1.3 Self Registered Guest Portal](#)
- [Esempio di autenticazione Web centralizzata su WLC e ISE](#)
- [Esempio di autenticazione Web centrale con punti di accesso FlexConnect su un WLC con configurazione ISE](#)

- [Documentazione e supporto tecnico – Cisco Systems](#)