Configurazione dell'accesso temporaneo e permanente per i guest ISE

Sommario

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:

- èpossibile fornire l'accesso permanente alla rete (non è richiesta alcuna autenticazione successiva)
- èpossibile 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

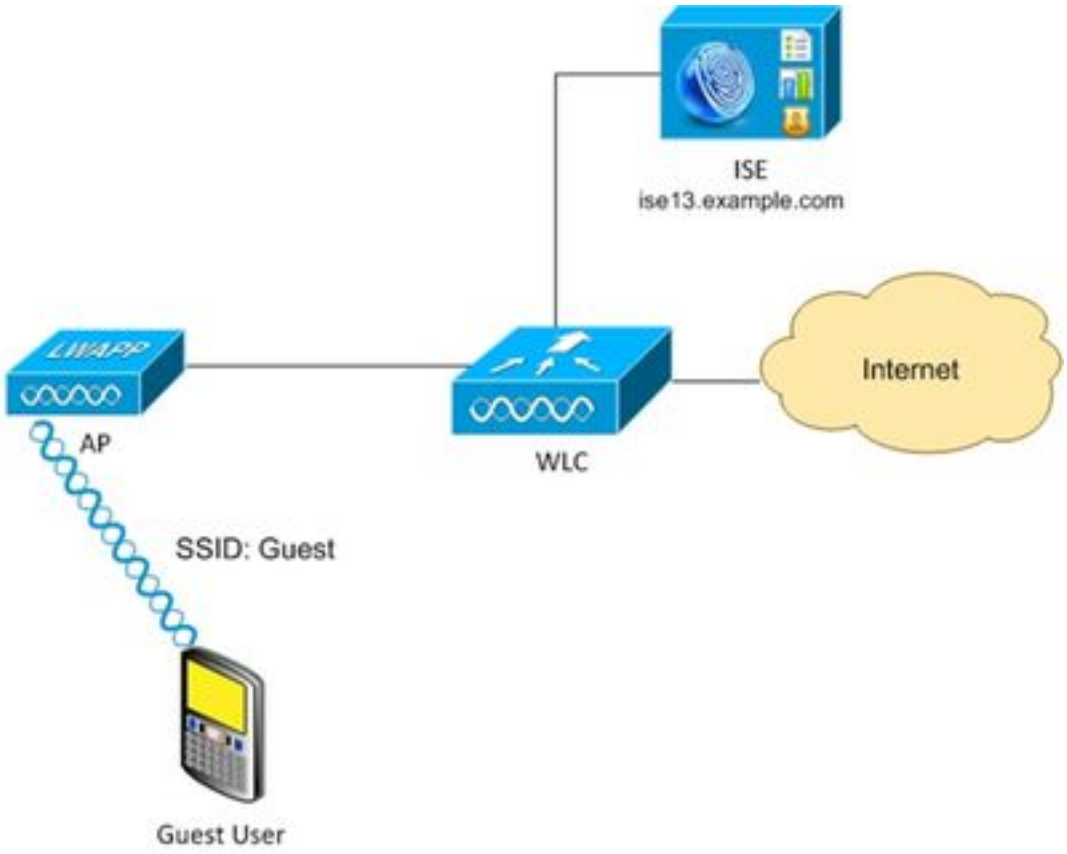
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Configurazione

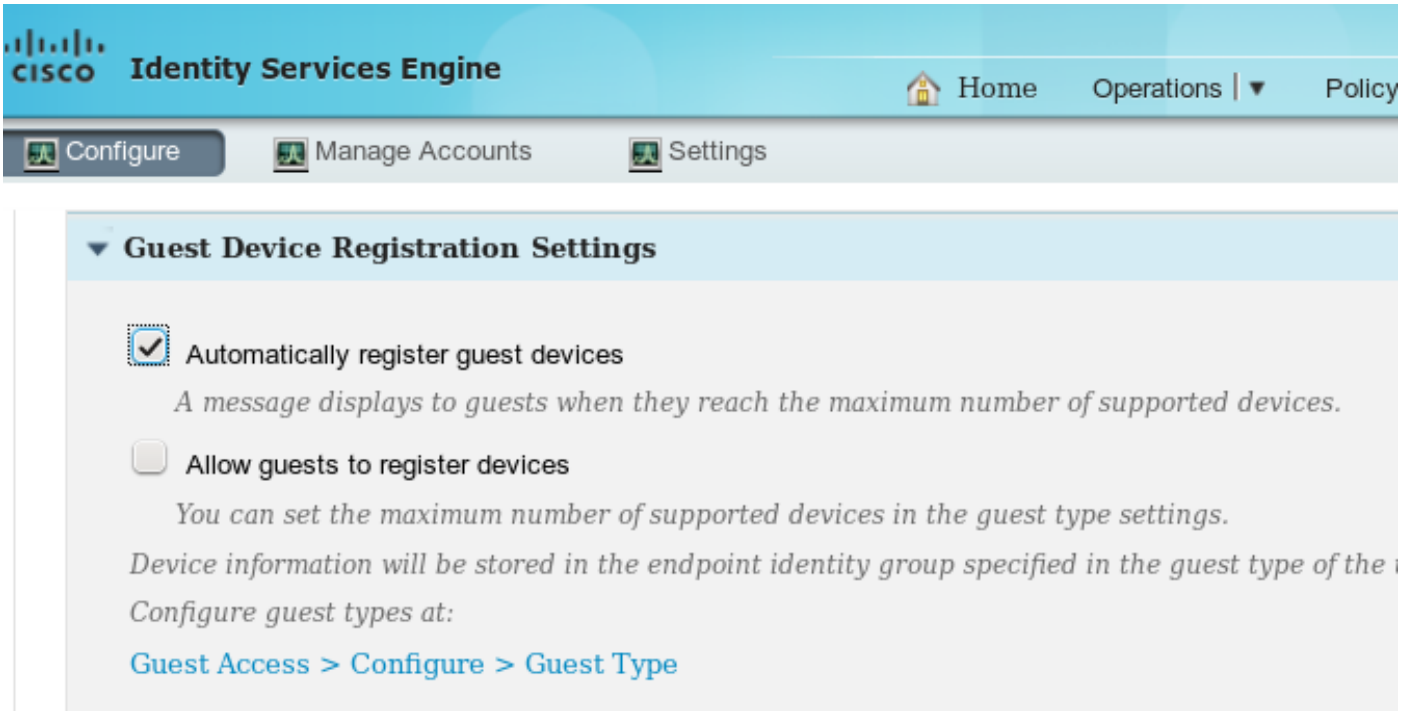
Per la configurazione di accesso guest di base, controllare i riferimenti con gli esempi di configurazione. In questo articolo vengono illustrate la configurazione delle regole di autorizzazione e le differenze nelle condizioni di autorizzazione.

Esempio di rete

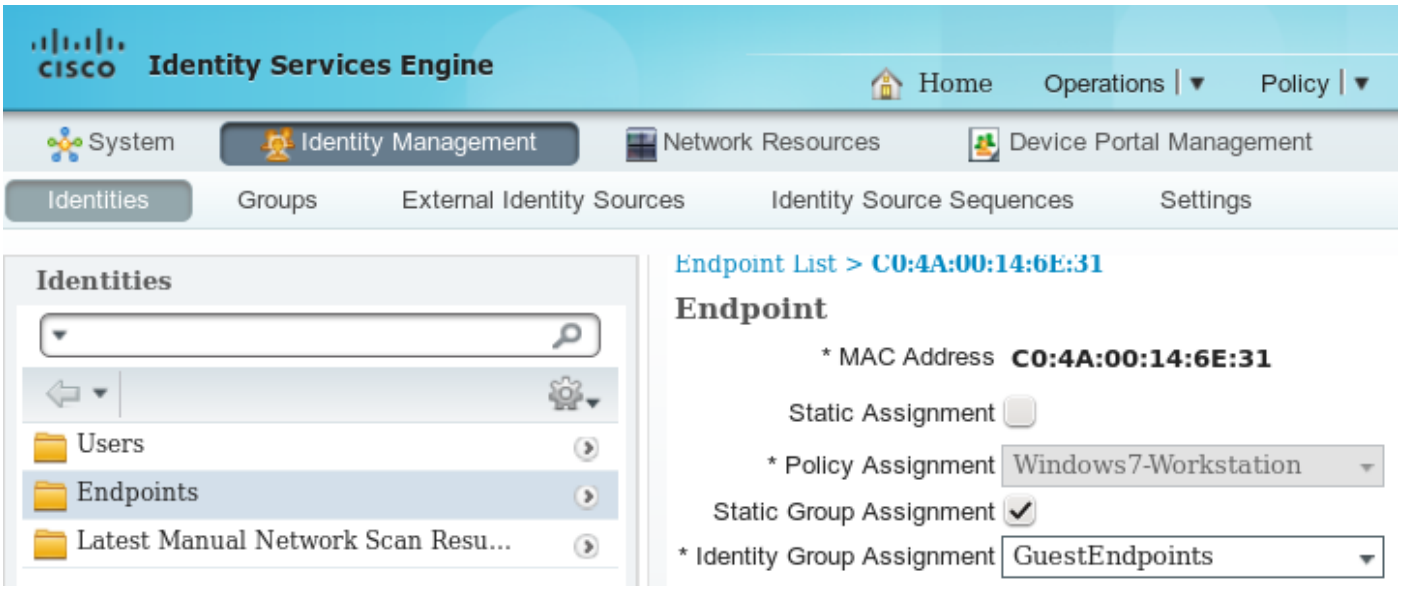


Accesso permanente

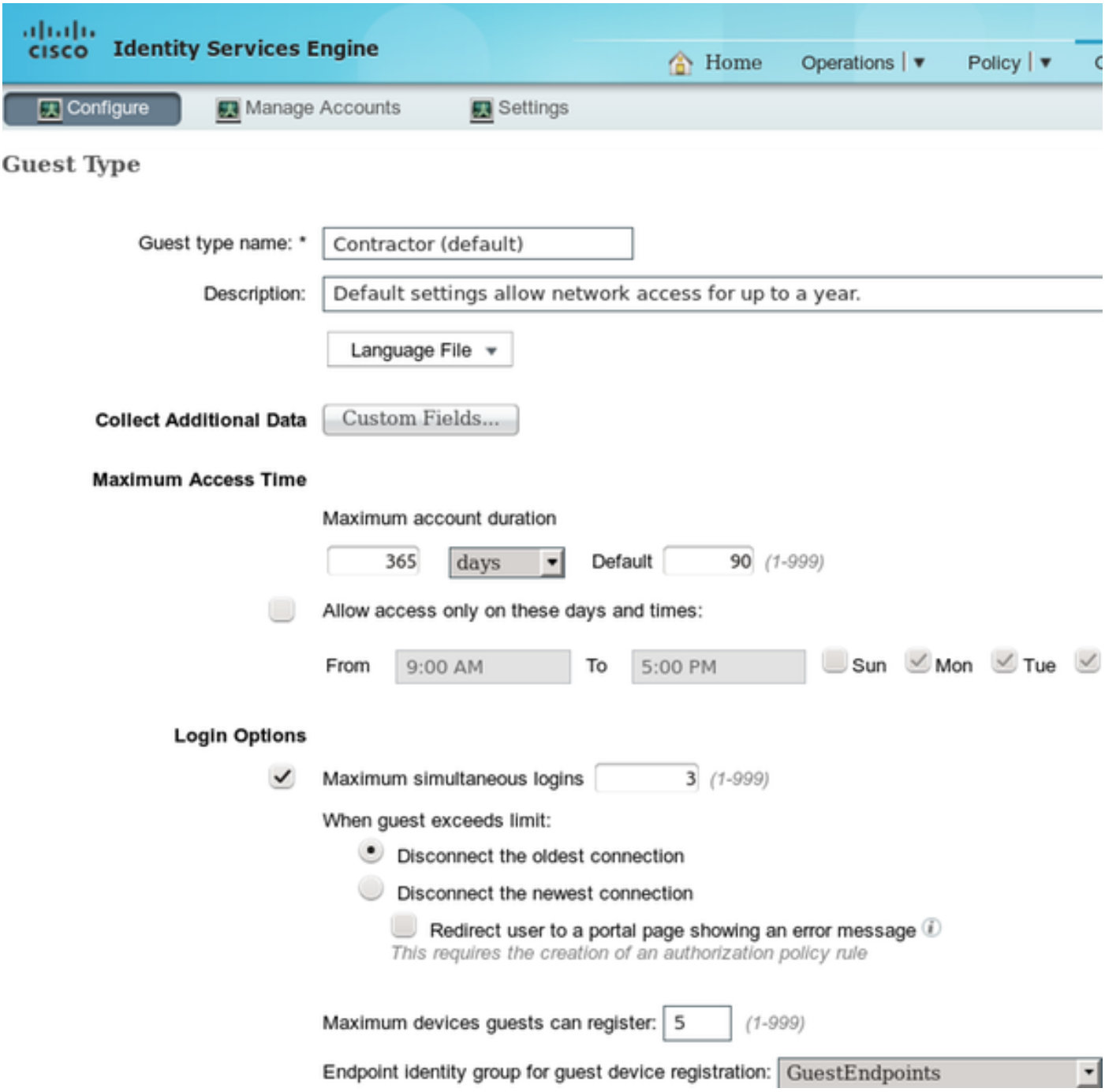
Per ISE versione 1.3 e successive dopo l'autenticazione sul portale guest con la registrazione del dispositivo abilitata.



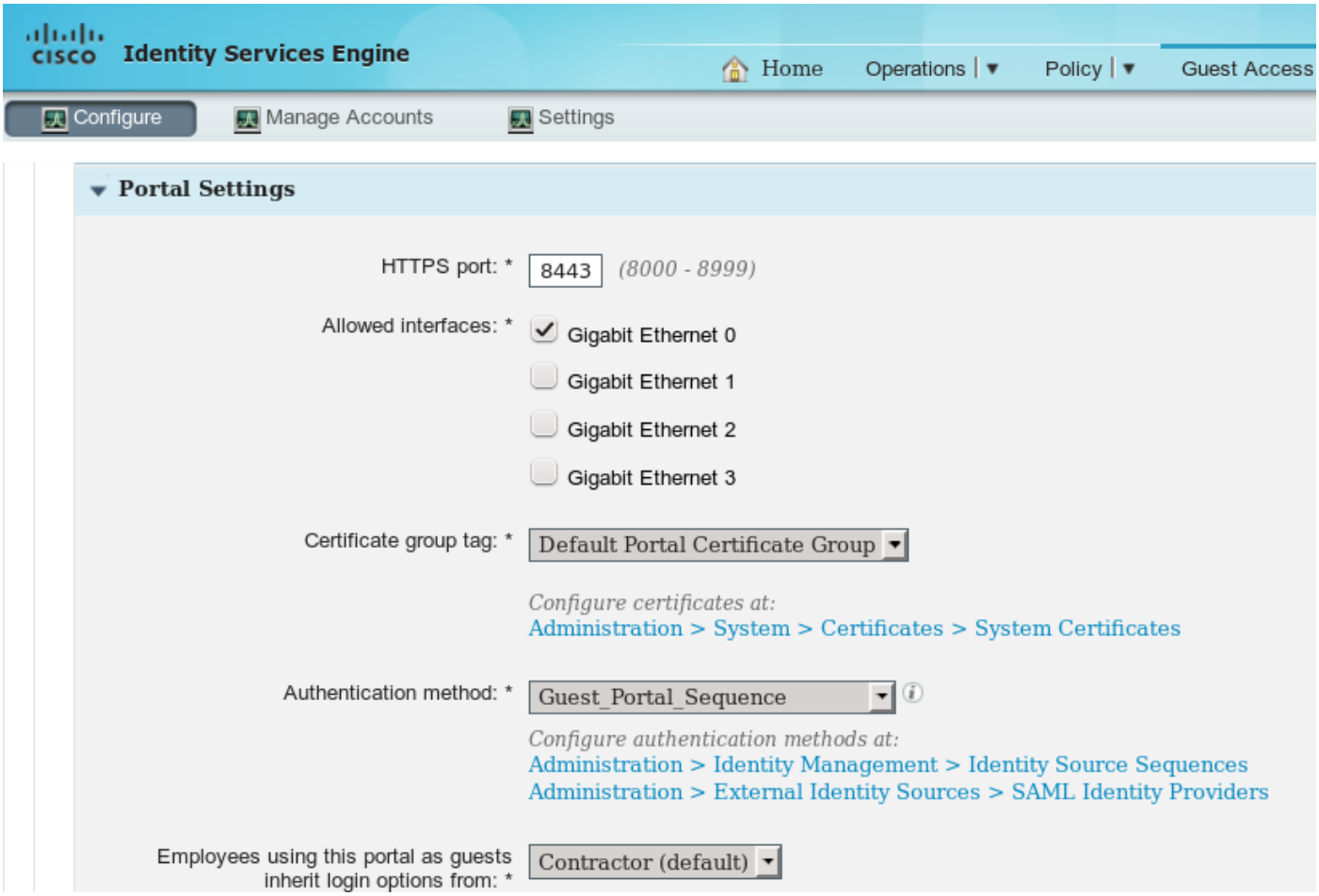
Il dispositivo endpoint (indirizzo MAC) è registrato in modo statico in un gruppo endpoint specifico (GuestEndpoints in questo esempio).



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



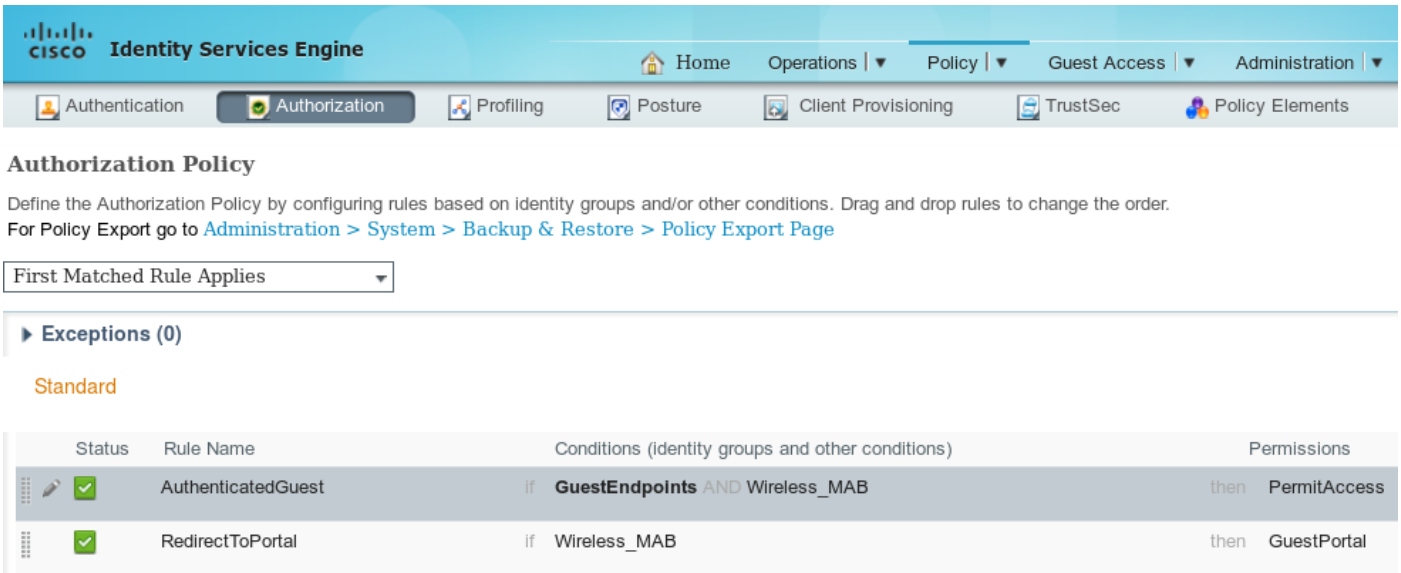
Se si tratta di un utente aziendale (archivio identità diverso da guest), l'impostazione viene derivata dalle impostazioni del portale.



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.

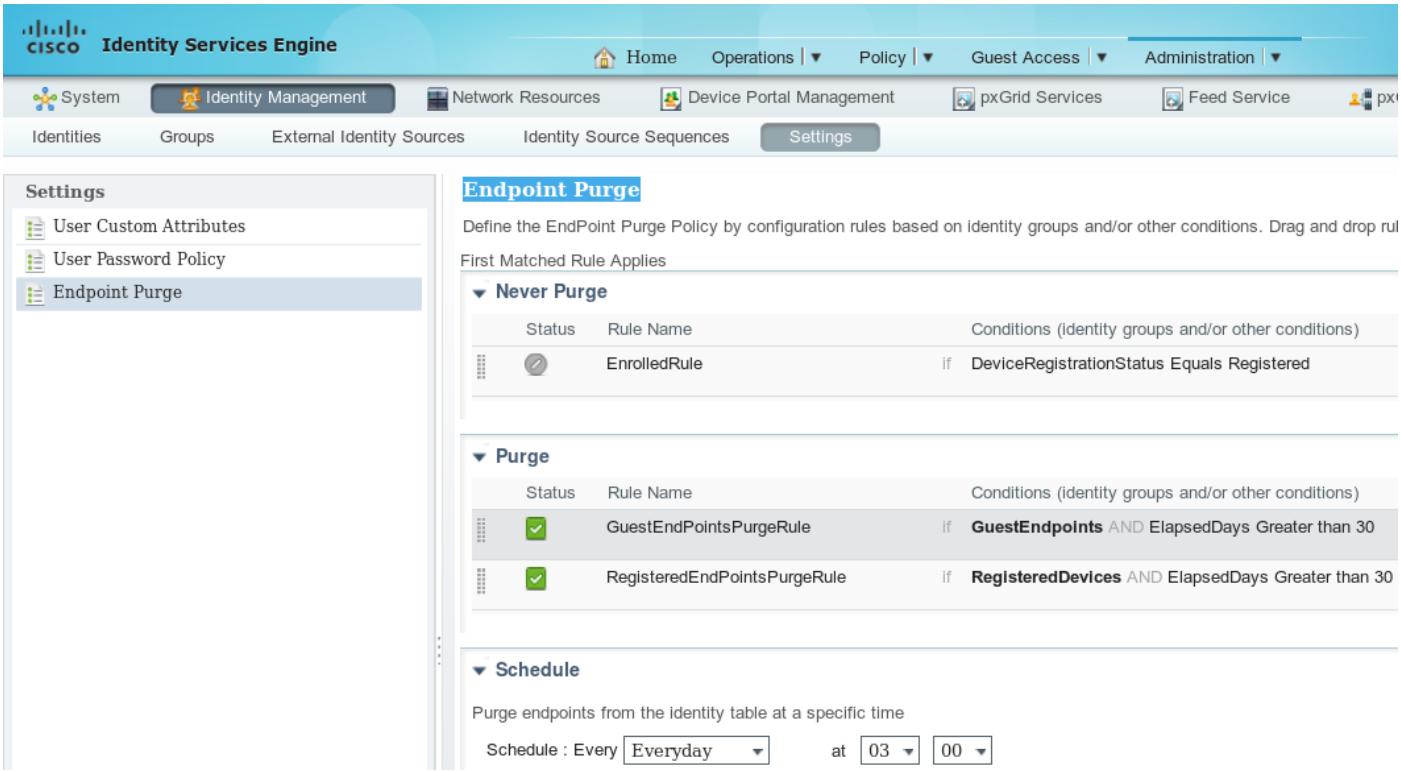


Dopo che un utente non è autenticato, l'autorizzazione corrisponde alla regola generica RedirectToPortal. Dopo il reindirizzamento al portale guest e l'autenticazione, l'endpoint viene

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.



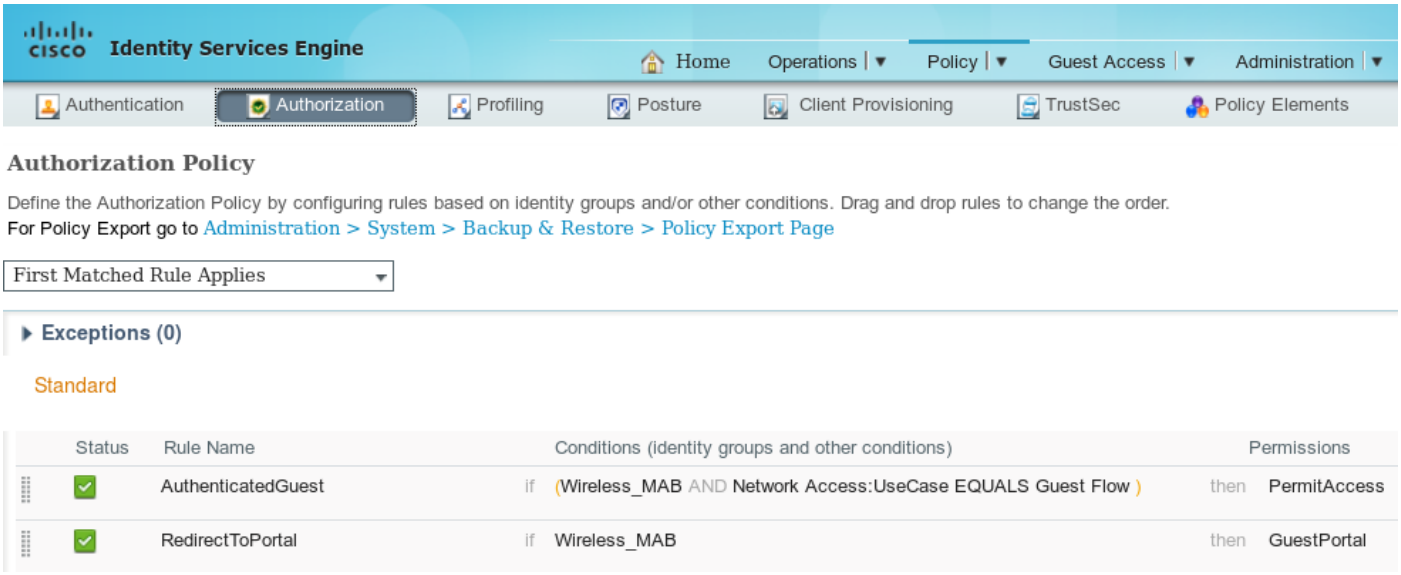
Tutti gli endpoint utilizzati per l'autenticazione guest vengono rimossi dopo 30 giorni dalla creazione dell'endpoint. Di conseguenza, in genere dopo 30 giorni che l'utente guest tenta di accedere alla regola di autorizzazione RedirectToPortal riscontrata nella rete e viene reindirizzato per l'autenticazione.

> **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.



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

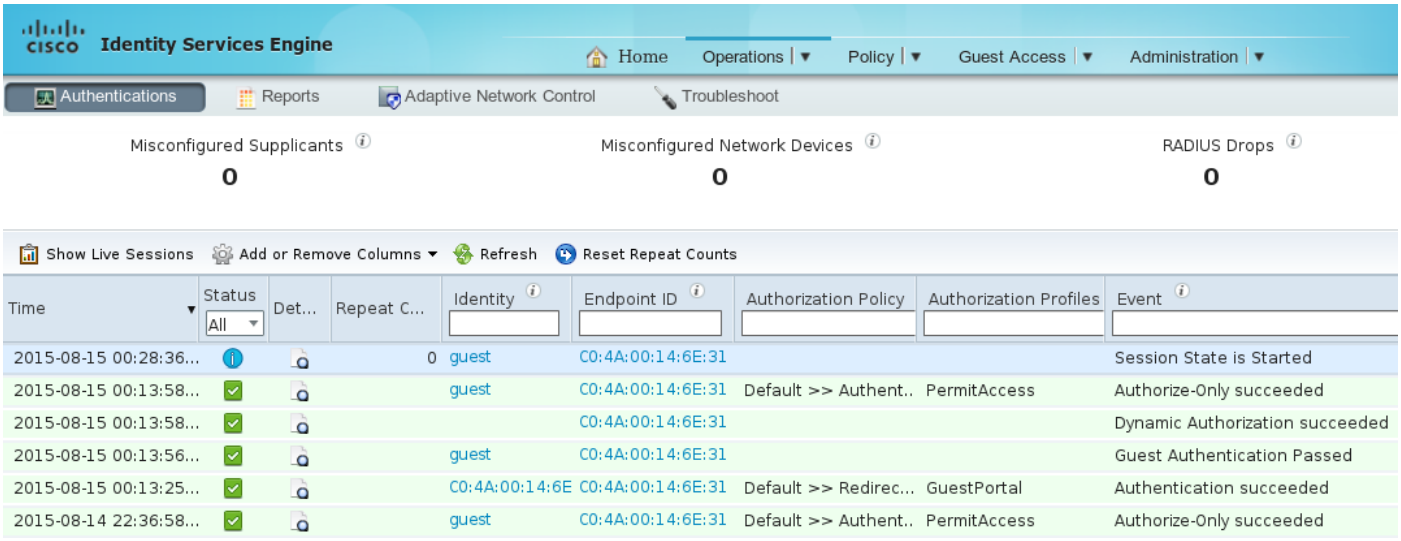
Tuttavia, sul WLC, lo stato è invariato (il client è ancora in stato RUN).

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.



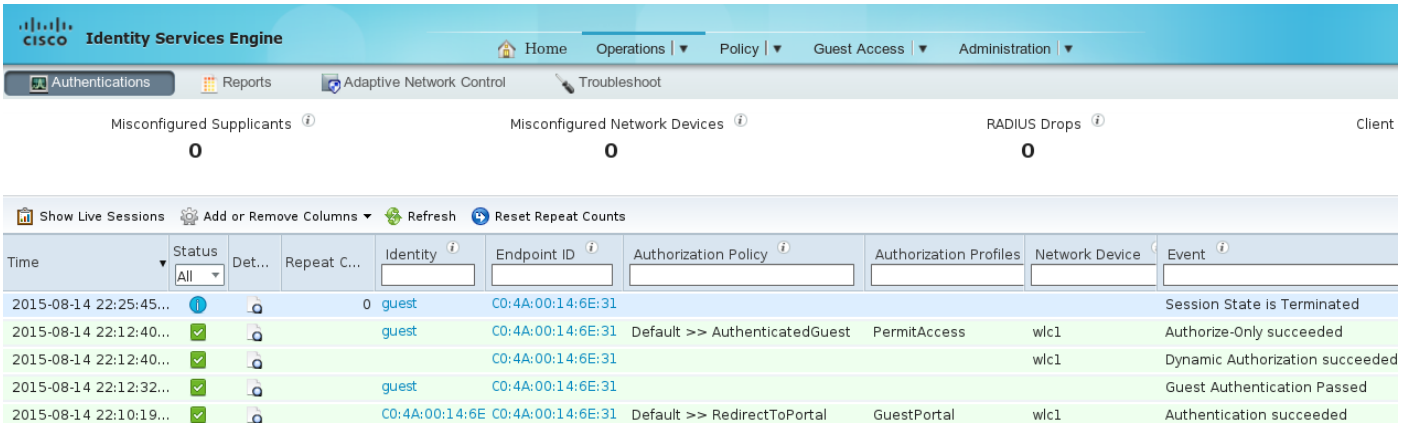
Ma se dopo la disconnessione l'utente si connette a una WLAN diversa, il WLC decide di cancellare la vecchia sessione. Viene inviato il comando Radius Accounting Stop, che rimuove la sessione. Se il client tenta di connettersi alla condizione di flusso guest WLAN originale non è soddisfatto e l'utente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

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

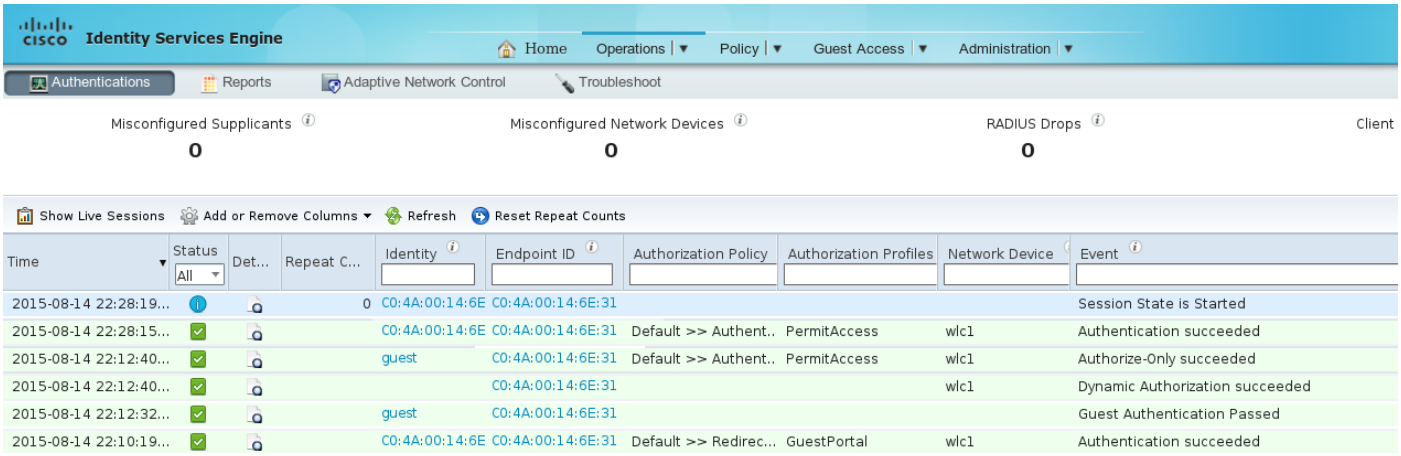
Verifica

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.

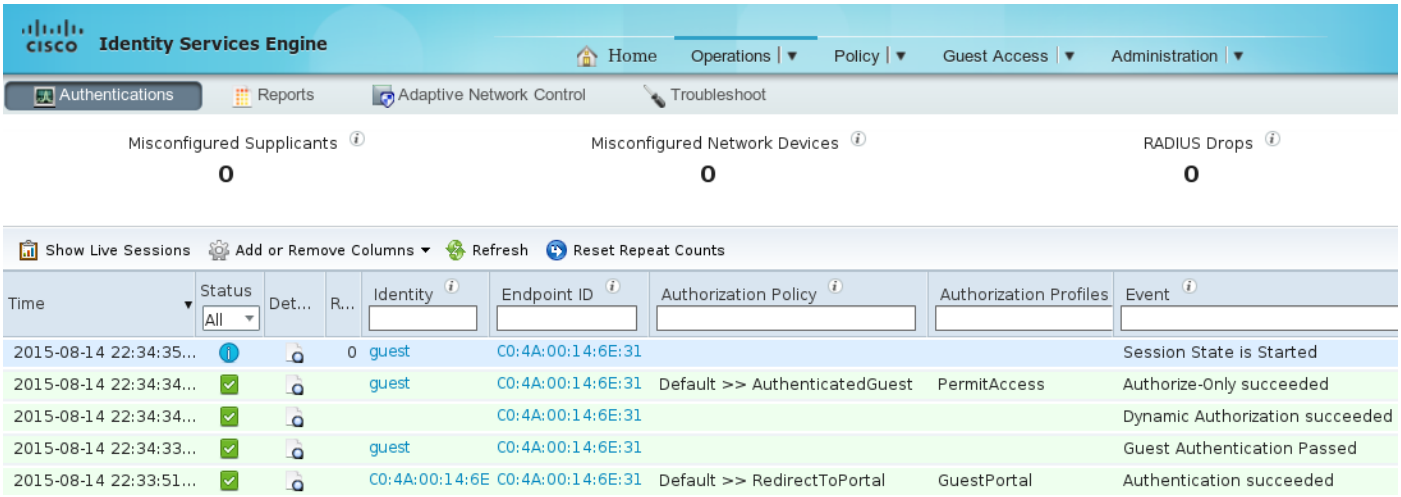


A questo punto l'utente wireless può disconnettersi, connettersi a diverse WLAN, quindi riconnettersi. Tutte le autenticazioni successive utilizzano l'identità basata sull'indirizzo MAC, ma incontrano la prima regola a causa dell'appartenenza dell'endpoint a un gruppo di identità specifico. L'accesso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

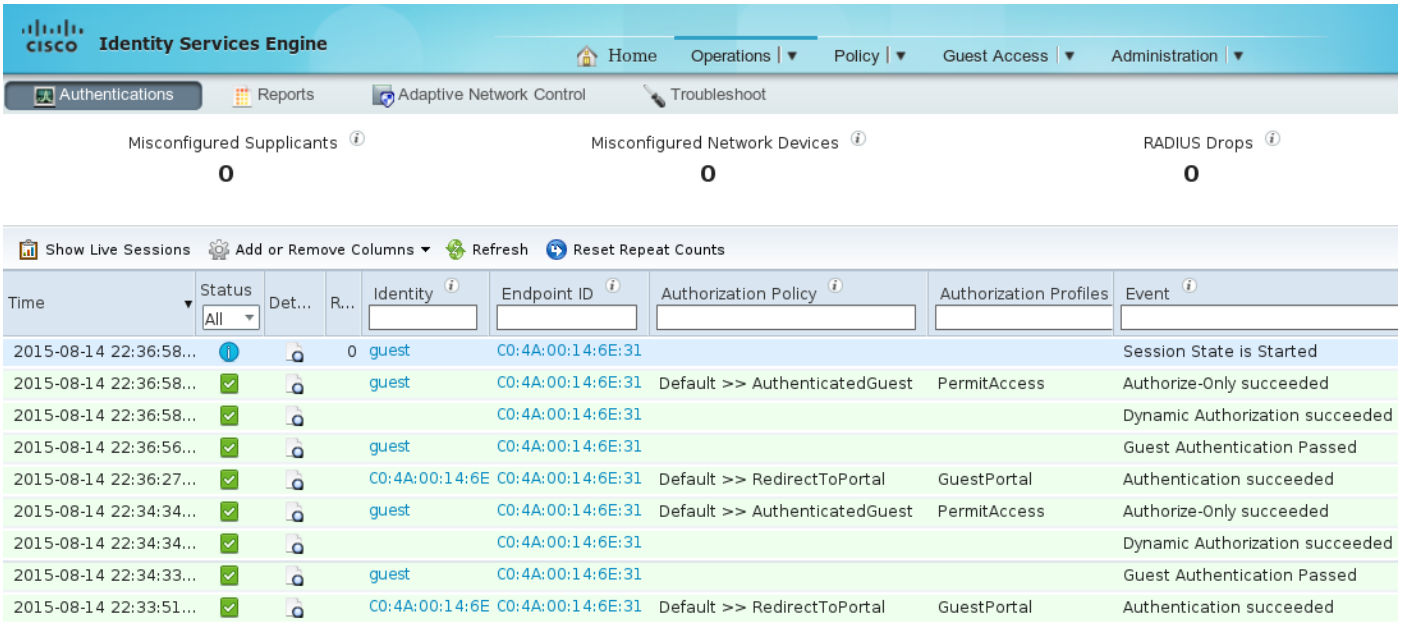


Accesso temporaneo

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

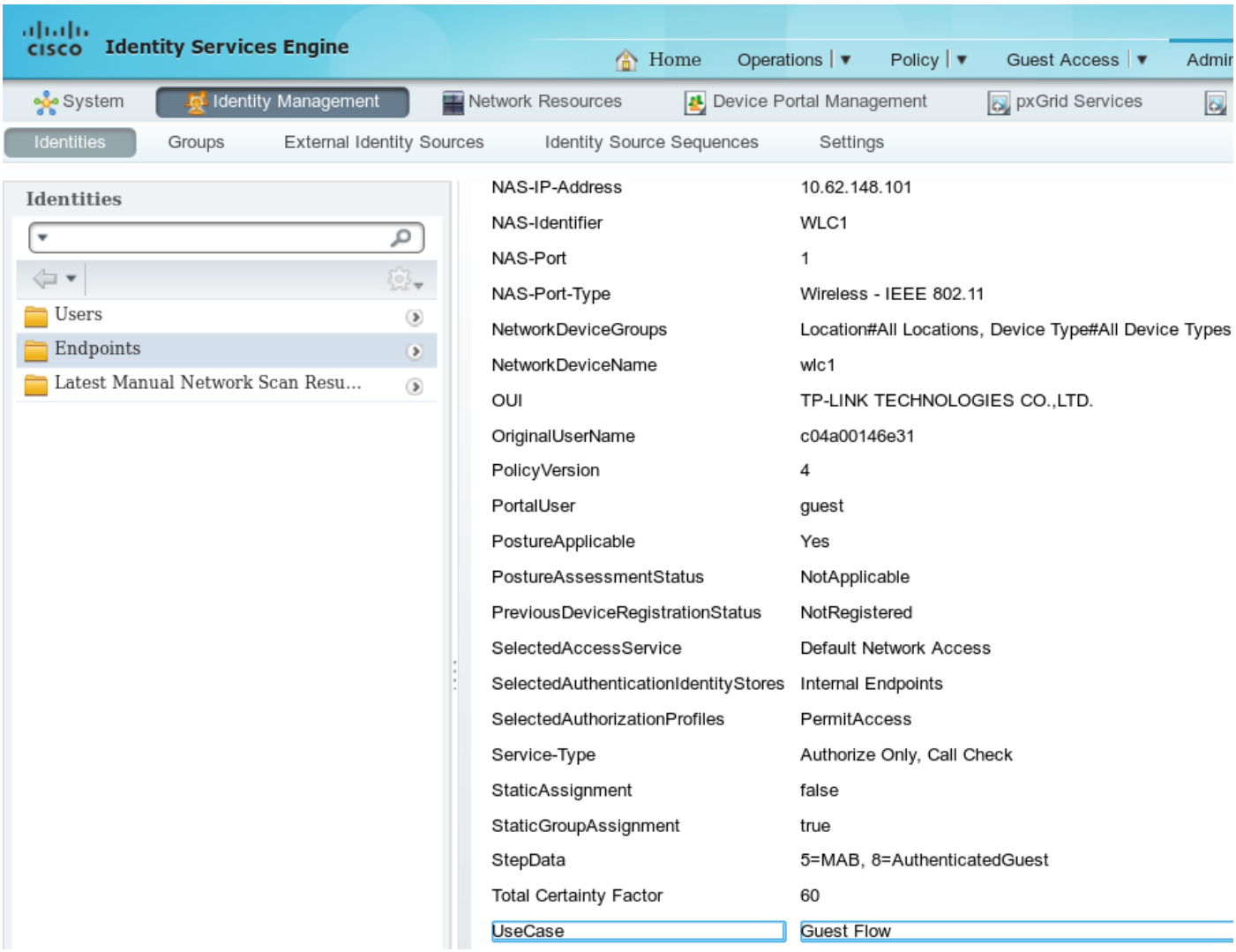


Tuttavia, dopo la rimozione della sessione per tutte le autenticazioni successive, il guest ha raggiunto la regola generica e viene nuovamente reindirizzato per l'autenticazione guest.



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.




```
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