Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Configure](#)
[Network Diagram](#)
[Permanent Access](#)
[Endpoint Purge for Guest Accounts](#)
[Temporary Access](#)
[WLC Disconnect Behavior](#)
[Verify](#)
[Permanent Access](#)
[Temporary Access](#)
[Bugs](#)
[References](#)
[Related Cisco Support Community Discussions](#)

Introduction

This document describes different methods for Identity Services Engine (ISE) Guest access configuration. Based on different conditions in authorization rules:

- permanent access to the network can be provided (no requirement for subsequent authentications)
- temporary access to the network can be provided (requiring guest authentication after session expires)

Also specific Wireless LAN Controller (WLC) behavior for session removal is presented along the impact on temporary access scenario.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ISE deployments and Guest flows
- Configuration of Wireless LAN Controllers (WLCs)

Components Used

The information in this document is based on these software and hardware versions:

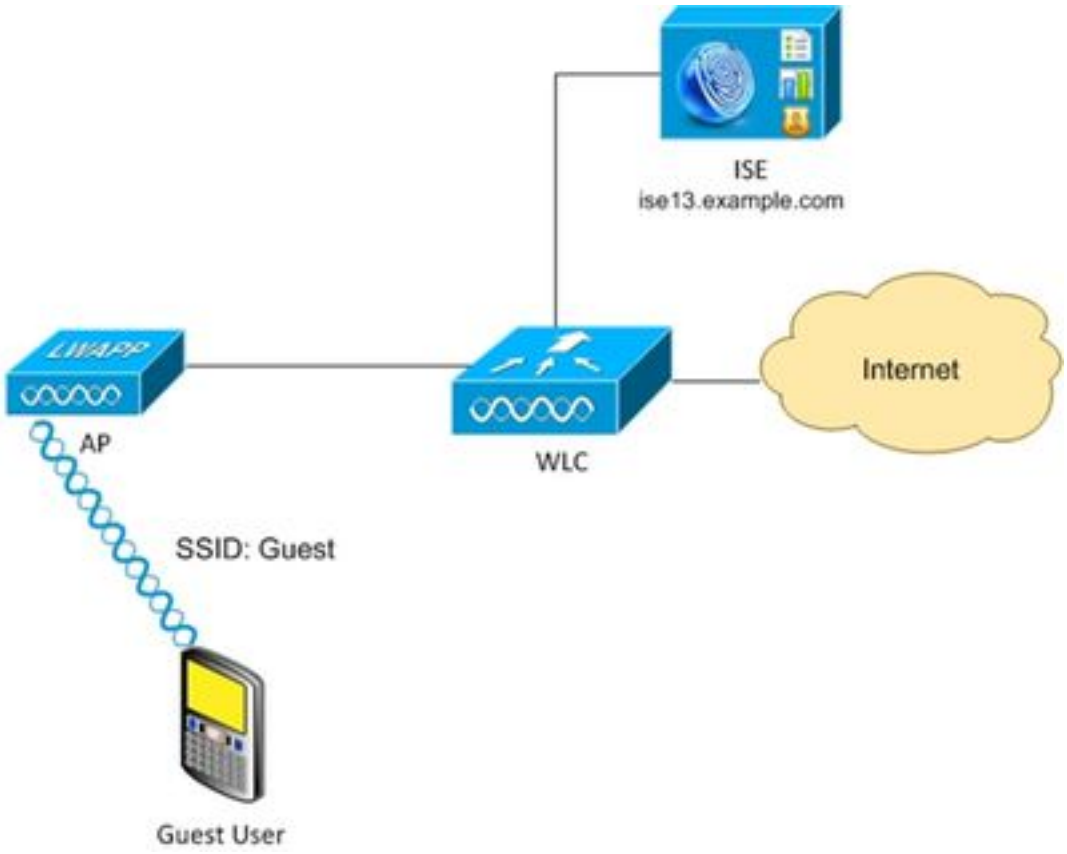
- Microsoft Windows 7

- Cisco WLC Version 7.6 and Later
- ISE Software, Version 1.3 and Later

Configure

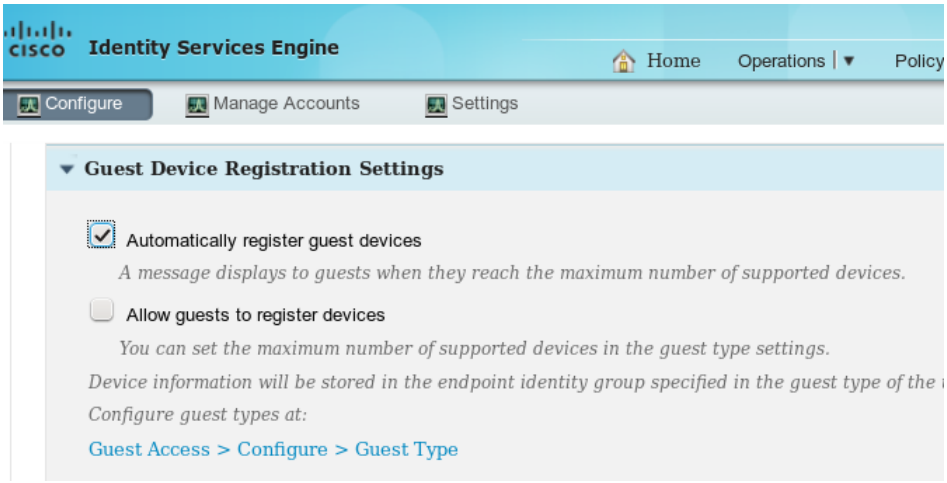
For basic guest access configuration please check references with configuration examples. This article focuses on Authorization Rules configuration and differences in the Authorization Conditions.

Network Diagram

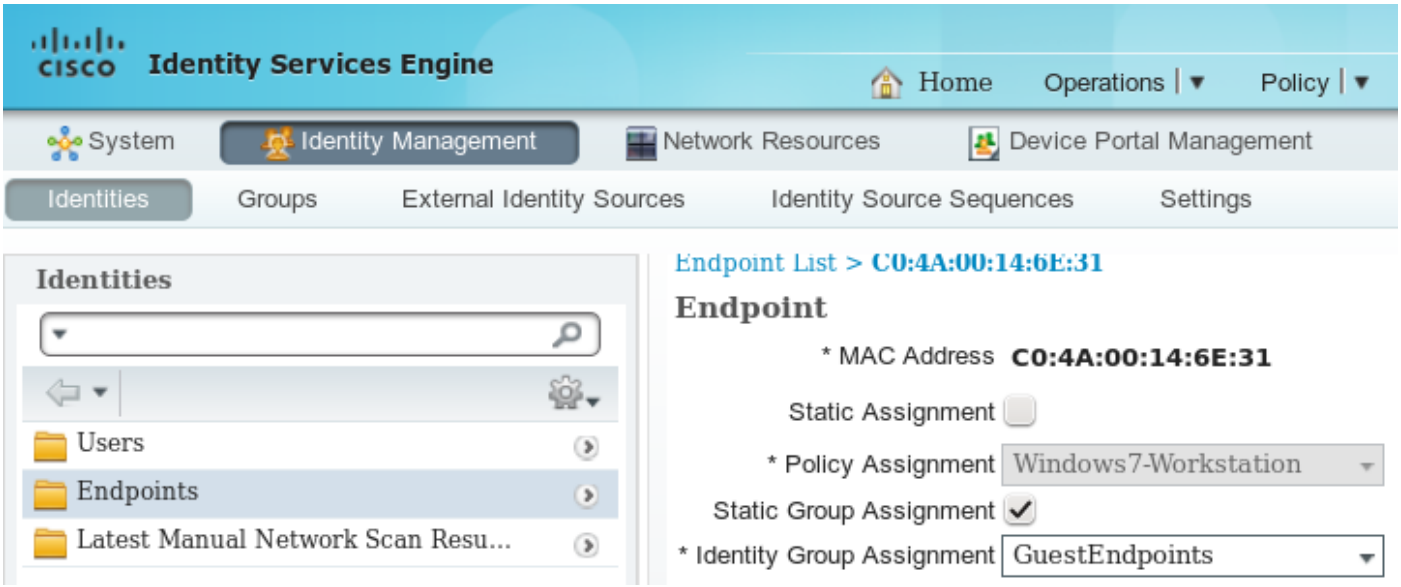


Permanent Access

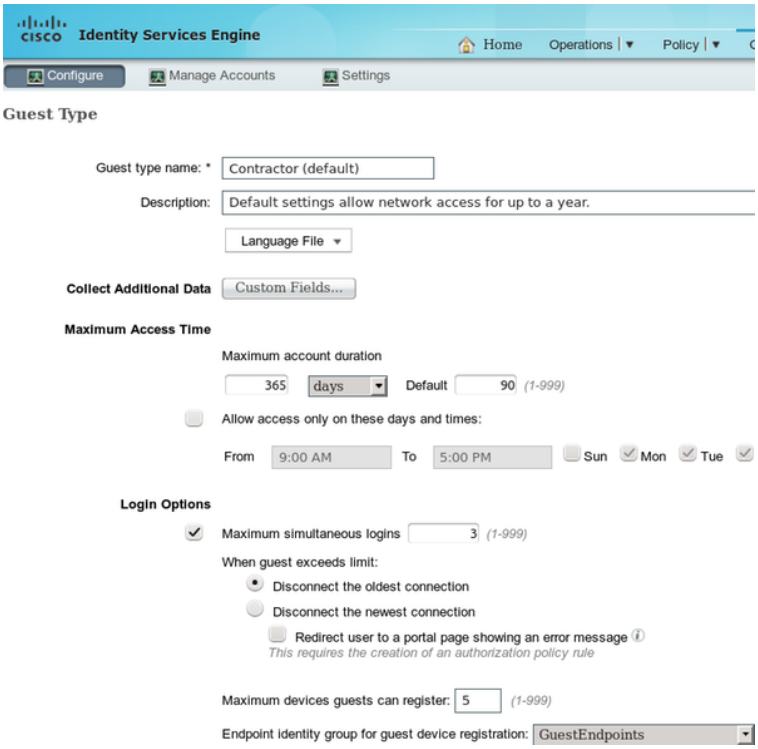
For ISE version 1.3 and newer after successful authentication on the guest portal with device registration enabled.



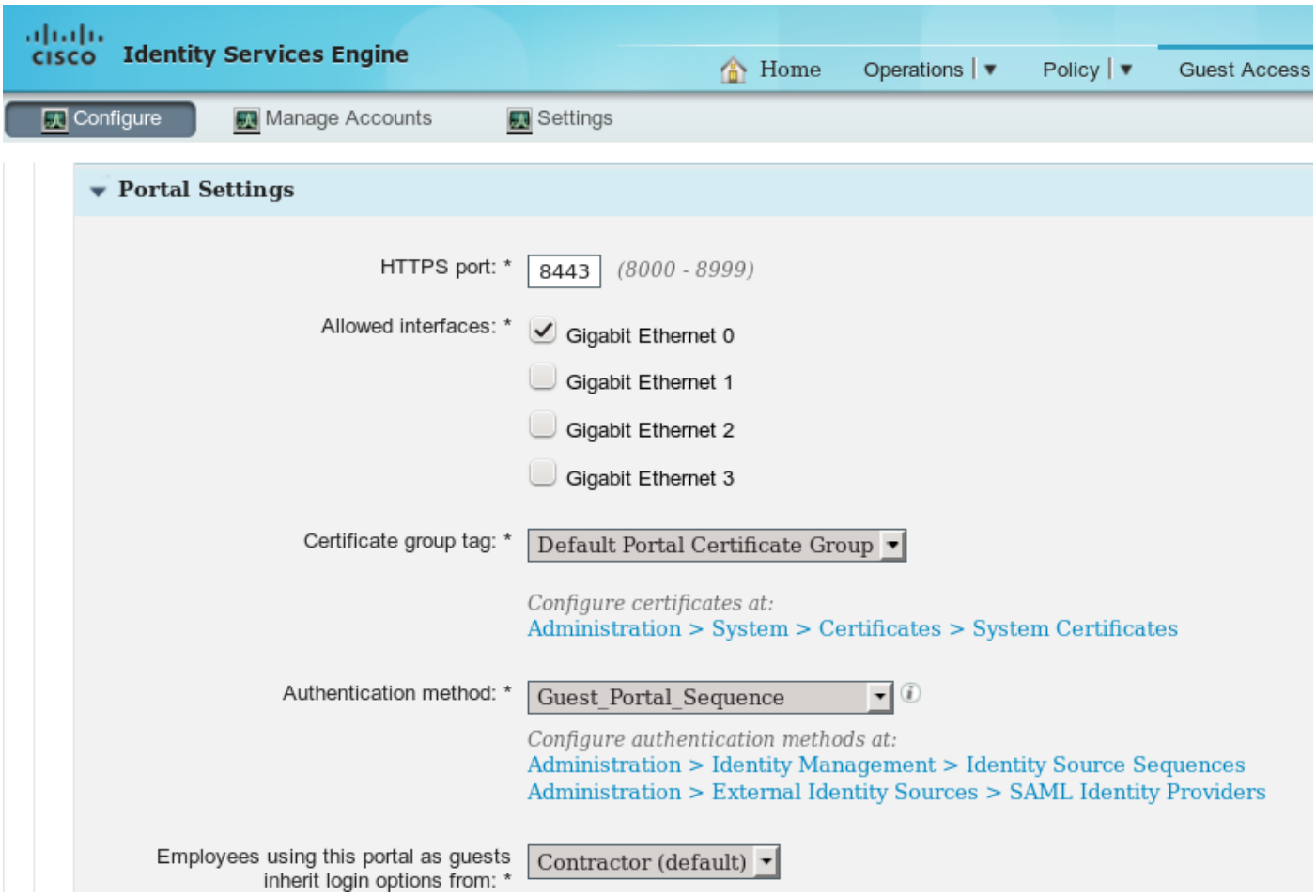
Endpoint device (mac address) is statically registered in specific endpoint group (GuestEndpoints in this example).



That group is derived from the Guest Type of the user, as shown in this image.



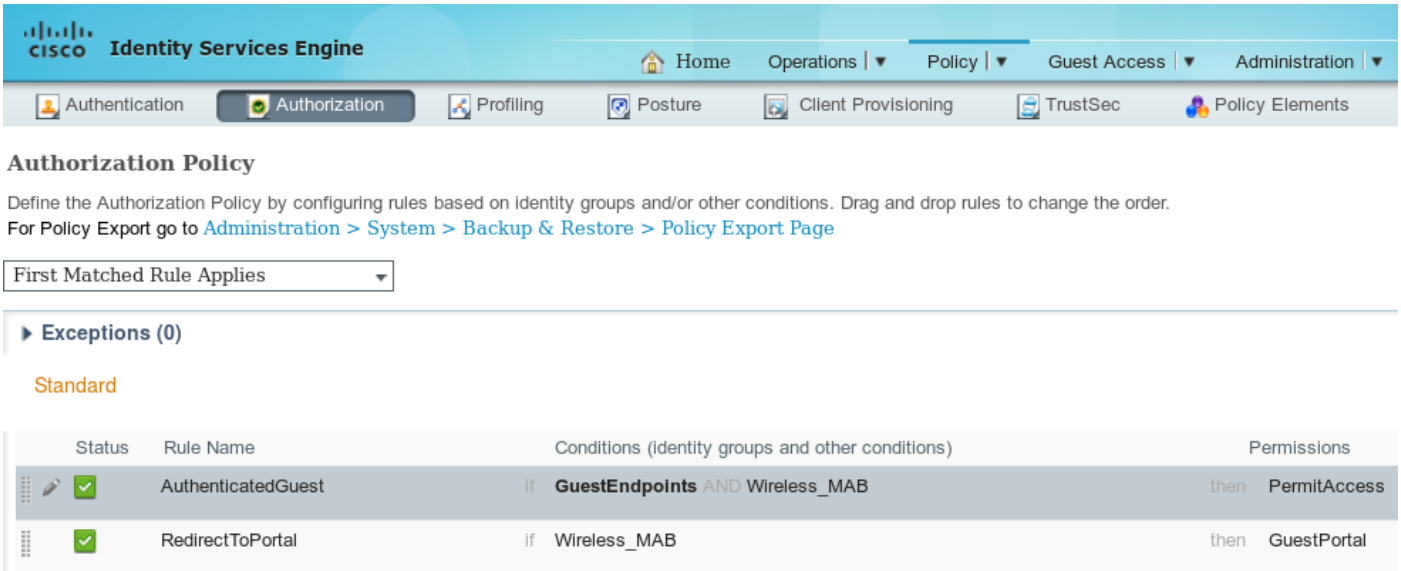
If it is a corporate user (identity store other then guest) that setting is derived from the portal settings.



As a result mac address associated with the guest always belongs to that specific identity group. That can not be changed automatically (for example by Profiler service).

Note: To apply Profiler results EndPointPolicy authorization condition can be used.

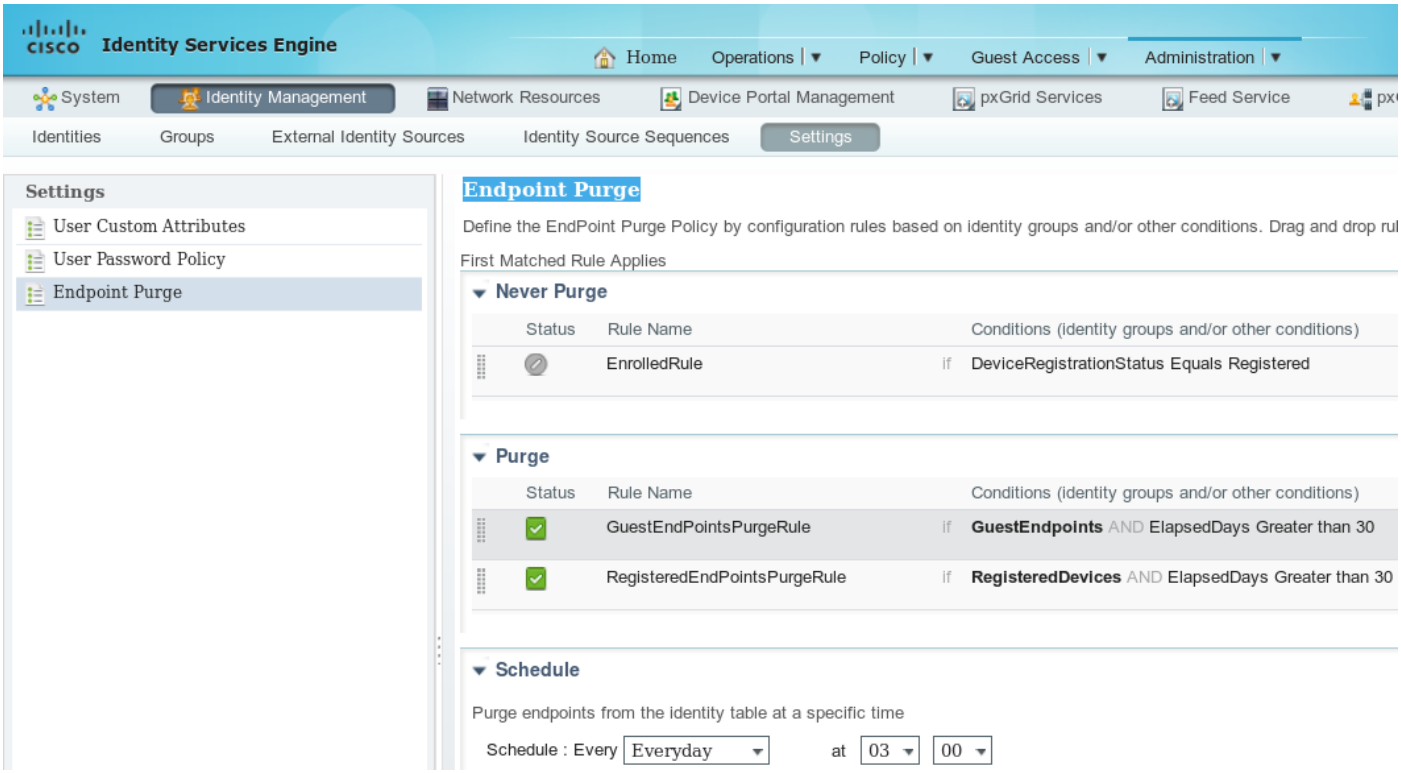
Knowing that device always belong to specific endpoint identity group it is possible to build authorization rules based on that, as shown in this image.



Once a user is not authenticated, authorization matches generic rule RedirectToPortal. After redirection to the guest portal and authentication, endpoint is placed in the specific endpoint identity group. That is used by the first, more specific condition. All subsequent authentications of that endpoint hits the first authorization rule and the user is provided full network access without the need to re-authenticate on the guest portal.

Endpoint Purge for Guest Accounts

This situation could last forever. But in ISE 1.3 Purge Endpoint functionality has been introduced. With the default configuration.



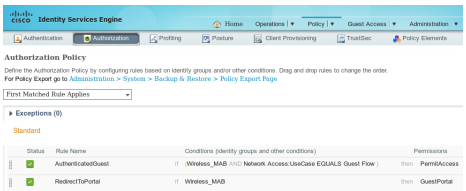
All endpoints used for guest authentication are removed after 30 days (from endpoint creation). As a result usually after 30 days guest user trying to access network hits RedirectToPortal authorization rule and is redirected for authentication.

> **Note**: Endpoint Purge functionality is independent of Guest Account Purge Policy and Guest Account Expiration.

> **Note**: In ISE 1.2 endpoints could be removed automatically only when hitting internal profiler queue limits. Then least recently used endpoints are being removed.

Temporary Access

Another method for guest access is to use Guest Flow condition.



That condition is checking active sessions on ISE and it's attributes. If that session has the attribute indicating that previously guest user has authenticated successfully condition is matched. After ISE receives Radius Accounting Stop message from Network Access Device (NAD), session is terminated and later removed. At that stage the condition Network Access:UseCase = Guest Flow is not satisfied anymore. As a result all subsequent authentications of that endpoint hits generic rule redirecting for guest authentication.

> **Note**: Guest Flow not supported when user is authenticated via HotSpot portal. For those scenarios UseCase attribute is set to Host Lookup instead of Guest Flow.

WLC Disconnect Behavior

After clients disconnects from wireless network (for example using disconnect button in Windows) it sends deauthentication frame. But that is omitted by the WLC and can be confirmed using "debug client xxxx" - WLC presents no debugs when client is disconnecting from WLAN. As a result on Windows client:

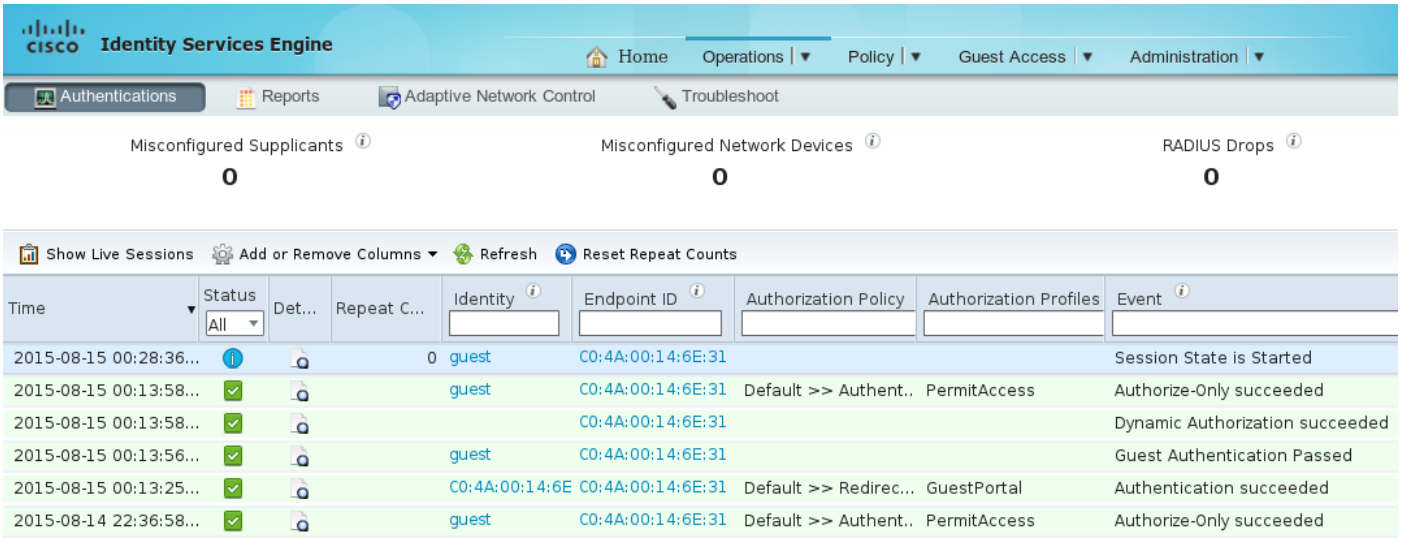
- ip address is removed from the interface
- interface is in state: media disconnected

But on WLC the status is unchanged (client still in RUN state).

That is planned design for WLC, the session is removed when

- user idle timeout hits
- session-timeout hits
- if using L2 encryption, then when the group key rotation interval hits
- something else causes the AP/WLC to kick the client off (e.g. AP radio resets, someone shuts down the WLAN, etc.)

With that behavior and temporary access configuration after user disconnects from WLAN session is not removed from ISE because WLC has never cleared it (and never sent Radius Accounting Stop). If session is not removed, ISE still remembers old session and Guest Flow condition is satisfied. After disconnection and reconnection user have full network access without requirement to reauthenticate.



But if after disconnection user connects to different WLAN, then WLC decides to clear old session. Radius Accounting Stop is sent and ISE removes the session. If the client tries to connect to

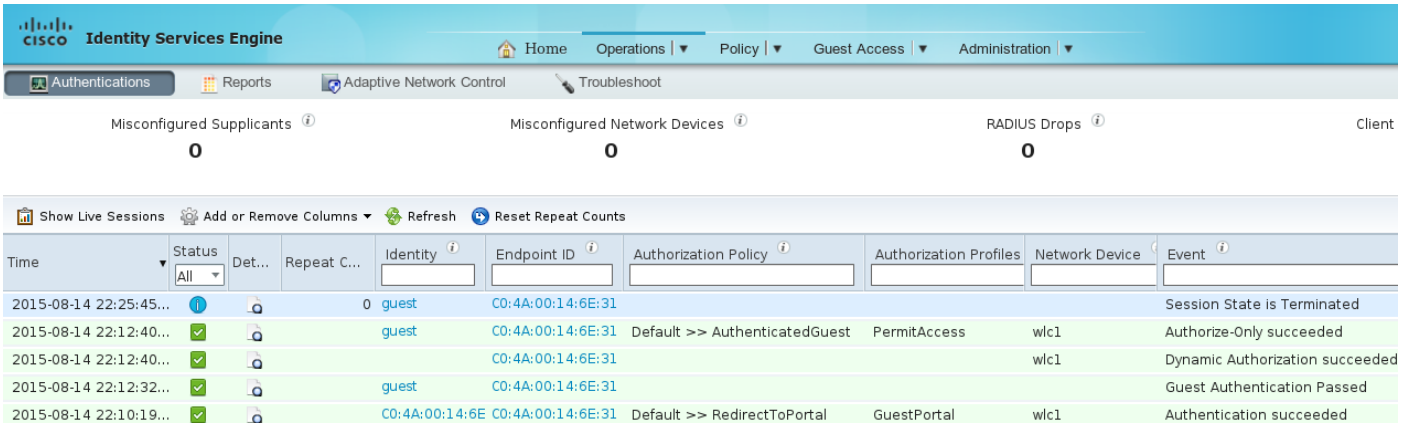
original WLAN Guest Flow condition is not satisfied and user is redirected for authentication.

> **Note**: WLC configured with Management Frame Protection (MFP) accepts encrypted deauthentication frame from CCXv5 MFP client.

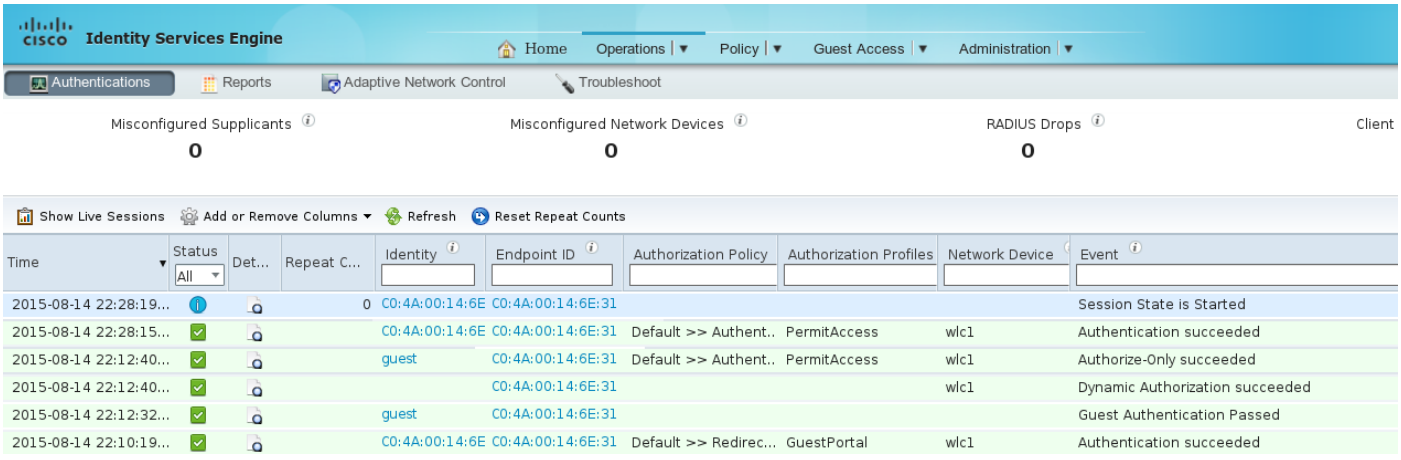
Verify

Permanent Access

After redirection to the guest portal and successful authentication ISE sends Change of Authorization (CoA) to trigger reauthentication. As a result new MAC Authentication Bypass (MAB) session is being built. This time endpoint belongs to GuestEndpoints identity group and matches rule providing full access.

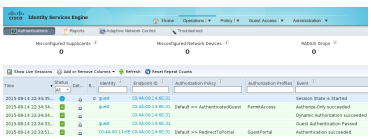


At that stage wireless user can disconnect, connect to different WLANs, then reconnect. All those subsequent authentications use identity based on mac address, but hits the first rule because of endpoint belonging to specific identity group. Full network access is provided without guest authentication.

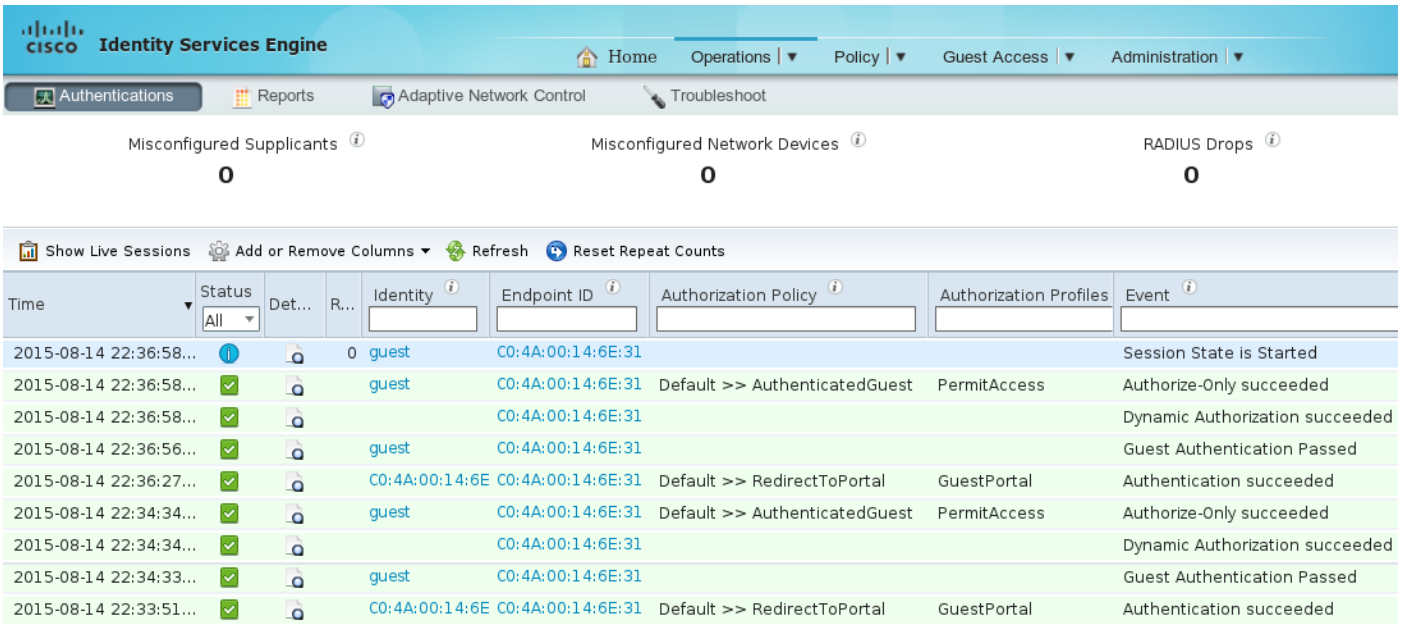


Temporary Access

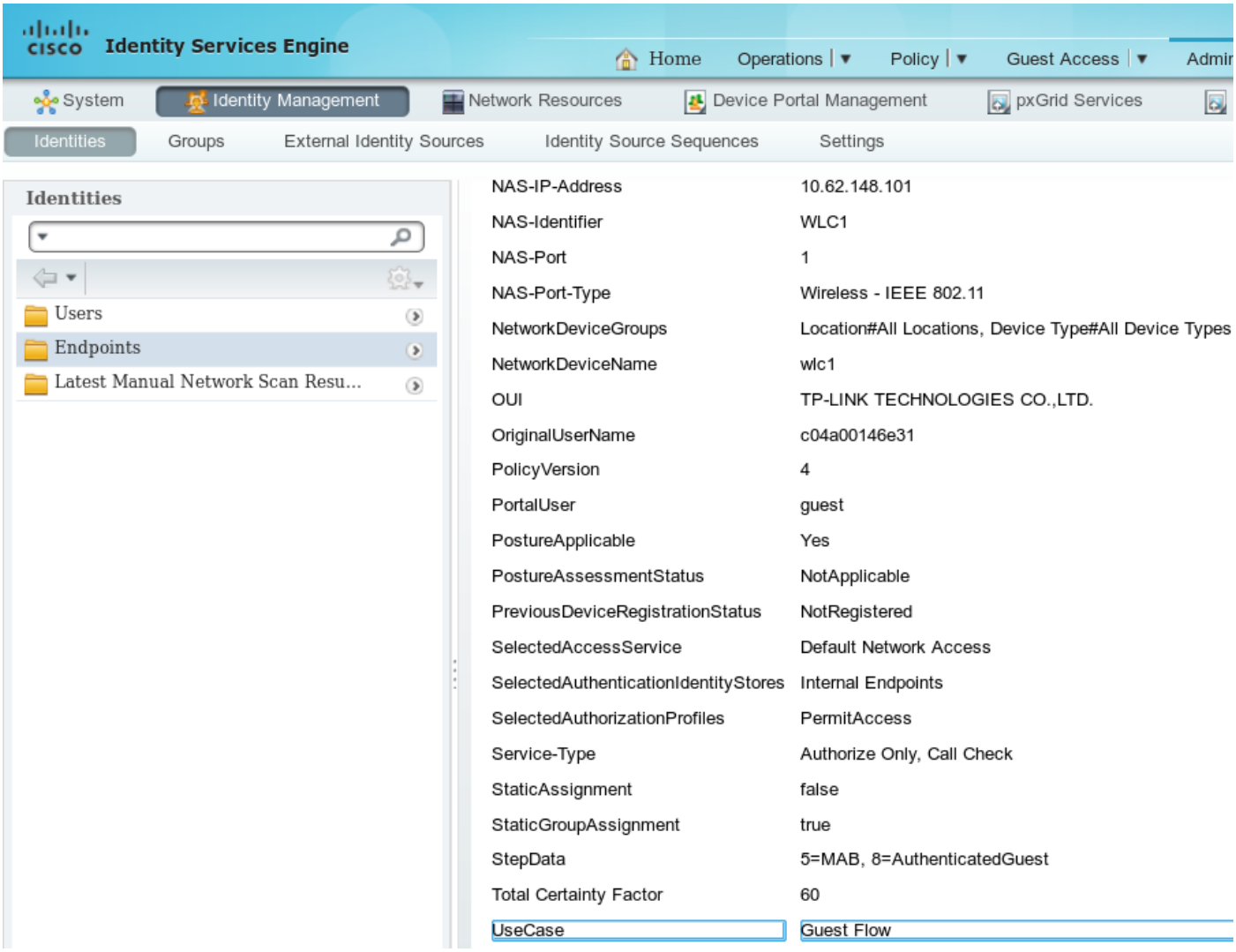
For the second scenario (with condition based on Guest Flow) beginning is the same.



But after the session is removed for all subsequent authentications, guest hit generic rule and is again redirected for guest authentication.



Guest Flow condition is be satisfied when the correct attributes are existing for the session. That can be verified by looking at endpoint attributes. The result of successful guest authentication are indicated.



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

Bugs

CSCuu41157 ISE ENH CoA terminate send on guest account removal or expiry.

(enhancement request to terminate guest sessions after guest account removal or expiry)

References

- **Cisco ISE 1.3 Administrators Guide**
- **Cisco ISE 1.4 Administrators Guide**
- **ISE Version 1.3 Hotspot Configuration Example**
- **ISE Version 1.3 Self Registered Guest Portal Configuration Example**
- **Central Web Authentication on the WLC and ISE Configuration Example**
- **Central Web Authentication with FlexConnect APs on a WLC with ISE Configuration Example**
- **Technical Support & Documentation - Cisco Systems**