

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:

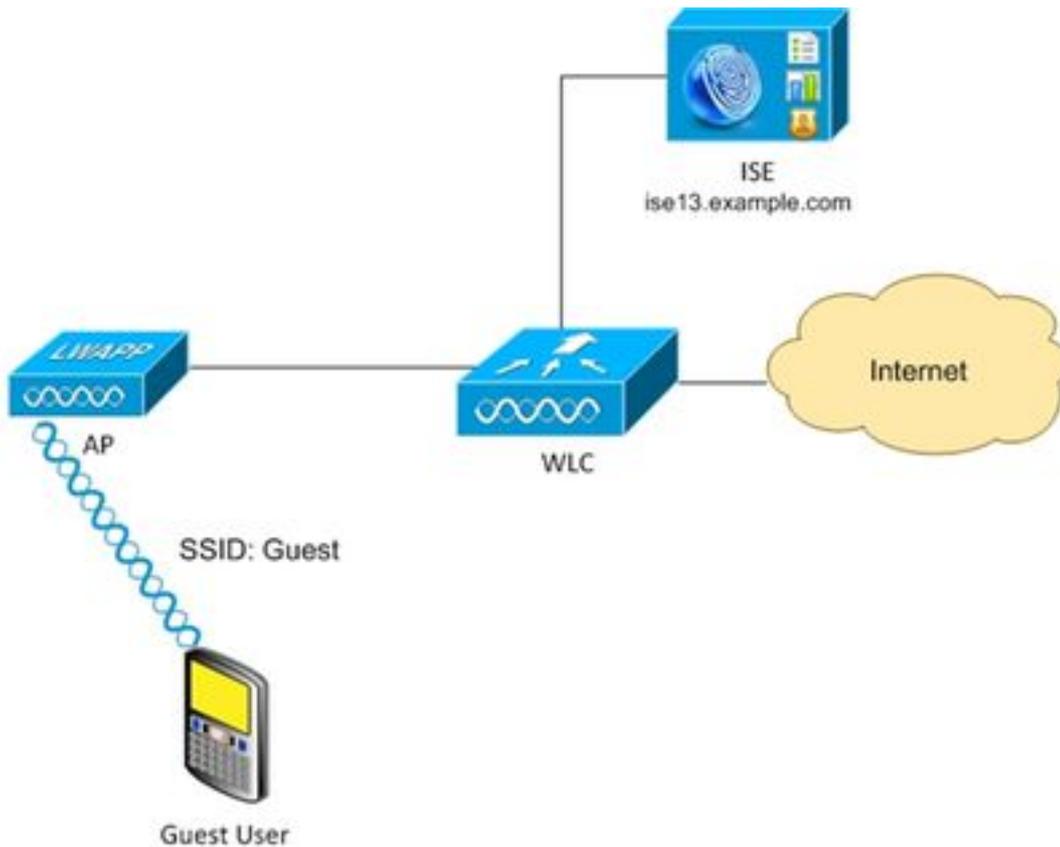
- Microsoft Windows 7

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

Configure

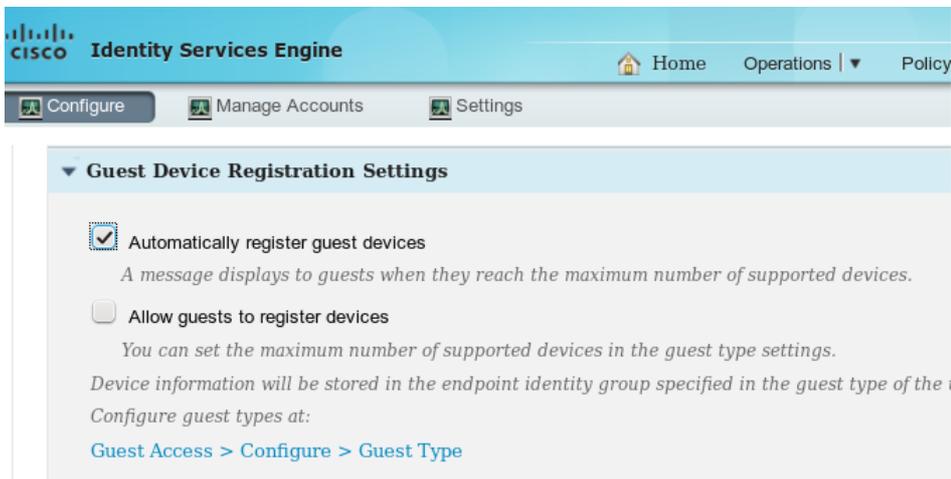
For basic guest access configuration please check references with configuration examples. This article focuses on Authorization Rules configuration and differences in the Authorization Conditions.

Network Diagram

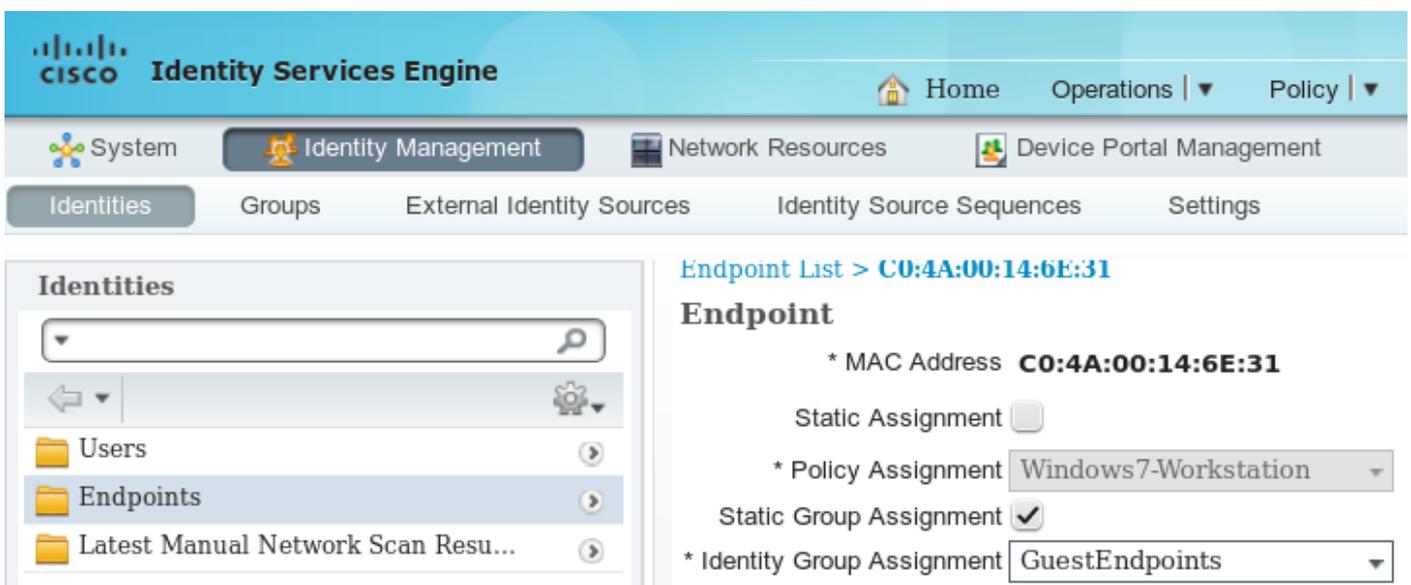


Permanent Access

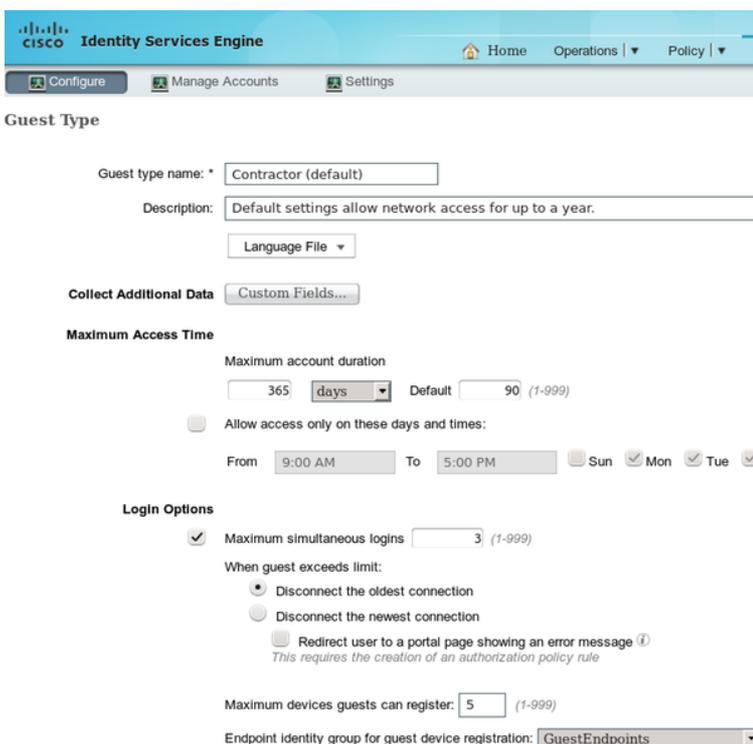
For ISE version 1.3 and newer after successful authentication on the guest portal with device registration enabled.



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 than guest) that setting is derived from the portal settings.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for Portal Settings. The top navigation bar includes Home, Operations, Policy, and Guest Access. Below the navigation bar are tabs for Configure, Manage Accounts, and Settings. The main content area is titled "Portal Settings" and contains the following configuration options:

- 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
- Employees using this portal as guests inherit login options from:** * Contractor (default)

Helpful links are provided for configuring certificates and authentication methods.

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.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for Authorization Policy. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. Below the navigation bar are tabs for Authentication, Authorization, Profiling, Posture, Client Provisioning, TrustSec, and Policy Elements. The main content area is titled "Authorization Policy" and contains the following configuration options:

- 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**

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

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.

Settings

- User Custom Attributes
- User Password Policy
- Endpoint Purge

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	Rule Name	Conditions (identity groups and/or other conditions)
Off	EnrolledRule	if DeviceRegistrationStatus Equals Registered

▼ **Purge**

Status	Rule Name	Conditions (identity groups and/or other conditions)
On	GuestEndpointsPurgeRule	if GuestEndpoints AND ElapsedDays Greater than 30
On	RegisteredEndpointsPurgeRule	if RegisteredDevices AND ElapsedDays Greater than 30

▼ **Schedule**

Purge endpoints from the identity table at a specific time

Schedule : Every at

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.

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 Expert go to Administration > Settings > Backups & Restore > Policy Expert Page

First Matched Rule Applies

▼ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
On	AuthenticatedGuest	if Wireless_MAD AND Network Access UserCase EQUALS Guest Flow	PermitAccess
On	RedirectToPortal	if Wireless_MAD	GuestPortal

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.

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 content area displays three summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). Below these is a table titled 'Show Live 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

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.

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 Suppliants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). Below the dashboard, there are options to 'Show Live Sessions', 'Add or Remove Columns', 'Refresh', and 'Reset Repeat Counts'. A table lists authentication sessions with columns for Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, Network Device, and Event. The table shows five sessions, with the most recent one (2015-08-14 22:10:19...) showing a successful authentication for the 'guest' identity group on endpoint 'C0:4A:00:14:6E:31' through the 'GuestPortal' profile.

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

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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface, similar to the previous one. It displays the same dashboard metrics (0 Misconfigured Suppliants, 0 Misconfigured Network Devices, 0 RADIUS Drops). The table below shows a sequence of authentication sessions for the same endpoint 'C0:4A:00:14:6E:31'. The sessions show a transition from a terminated session to a started session, followed by successful authentication and dynamic authorization, and finally a successful authentication through the 'GuestPortal' profile.

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...	✅				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

Temporary Access

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

A small screenshot of the Cisco Identity Services Engine (ISE) interface, showing the same dashboard and table structure as the previous screenshots. The table lists authentication sessions, with the most recent one showing a successful authentication for the 'guest' identity group on endpoint 'C0:4A:00:14:6E:31' through the 'GuestPortal' profile.

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

The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. 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. Three summary cards are displayed: Misconfigured Supplicants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). The main area shows a table of authentication events with columns for Time, Status, Det..., R..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event. The table contains 9 rows of log entries, showing a sequence of events for a 'guest' user, including session start, authorization success, and redirection to a portal.

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...				guest	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	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...				guest	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

Guest Flow condition is to 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.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for viewing endpoint attributes. The top navigation bar includes Home, Operations, Policy, Guest Access, and Admin. Below are sub-tabs: System, Identity Management, Network Resources, Device Portal Management, and pxGrid Services. The main area is titled 'Identities' and shows a list of attributes for a specific endpoint. The 'UseCase' attribute is highlighted as 'Guest Flow'.

Attribute	Value
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

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](#)