

ISE Guest tijdelijke en permanente toegang configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Permanente toegang](#)

[Endpoint Purge voor Guest Account](#)

[Tijdelijke toegang](#)

[WLC-gedrag van verbroken verbinding](#)

[Verifiëren](#)

[Permanente toegang](#)

[Tijdelijke toegang](#)

[Bugs](#)

[Referenties](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

In dit document worden verschillende methoden beschreven voor de toegangsconfiguratie van de Identity Services Engine (ISE). Op grond van verschillende voorwaarden in de vergunningsregels:

- permanente toegang tot het net is mogelijk (geen vereiste voor latere echtheidscontroles)
- tijdelijke toegang tot het netwerk kan worden verleend (hiervoor is de verificatie van de gast na afloop van de sessie vereist)

Ook het specifieke WLC-gedrag (Wireless LAN Controller) voor sessieverwijdering wordt langs de impact op een tijdelijk toegangsscenario gepresenteerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE-implementaties en Guest-stromen
- Configuratie van draadloze LAN-controllers (WLC's)

Gebruikte componenten

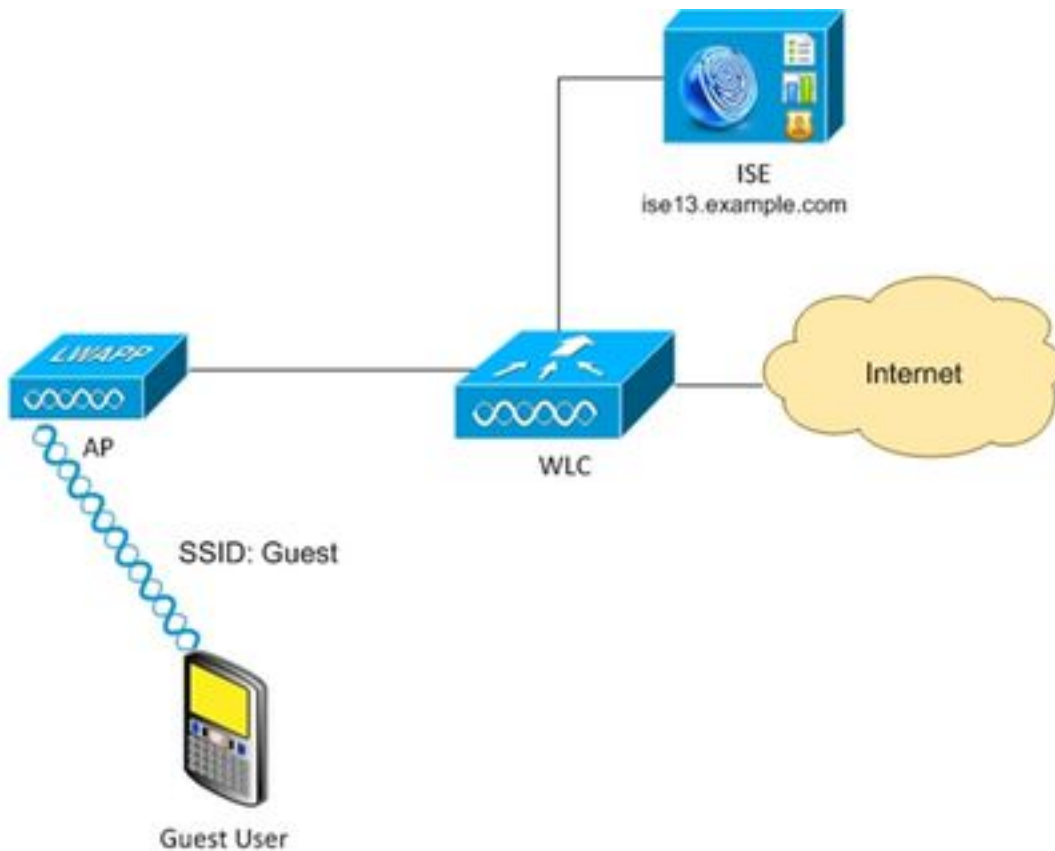
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Cisco WLC versie 7.6 en hoger
- ISE-software, versie 1.3 en hoger

Configureren

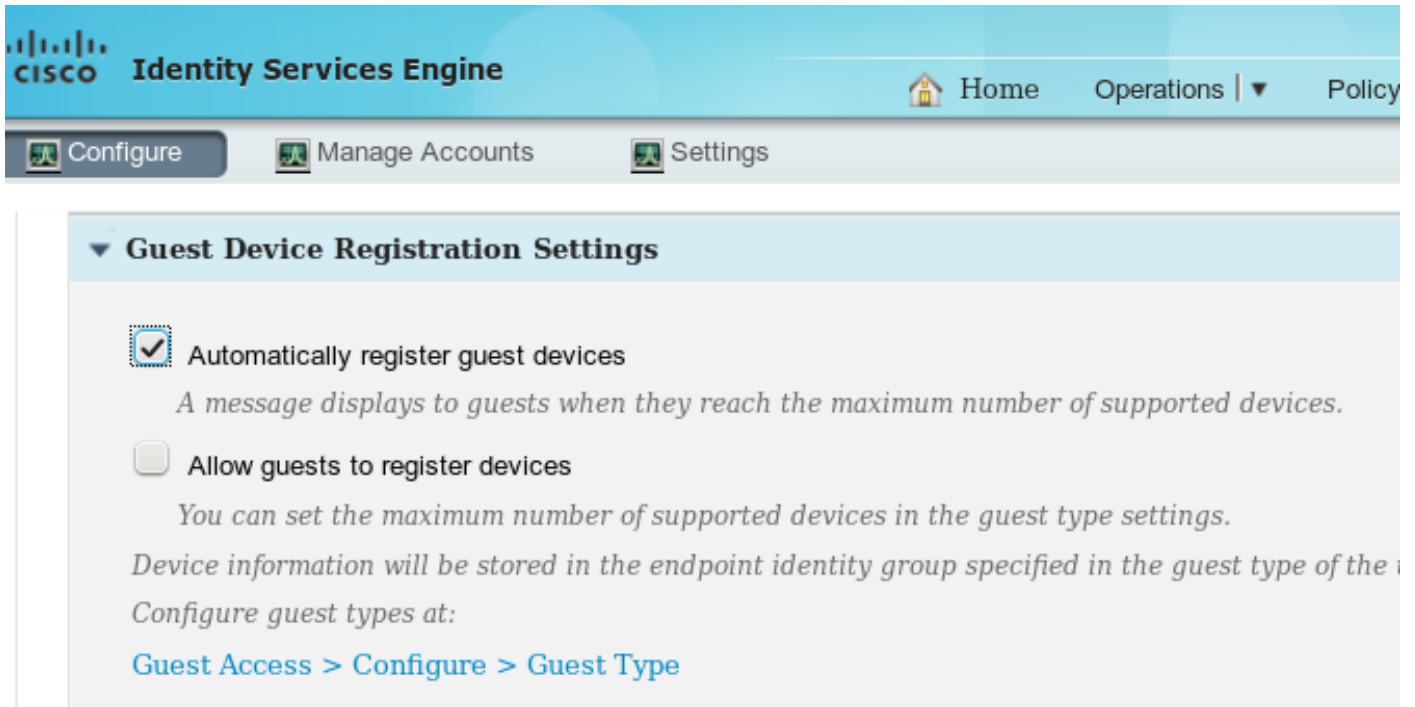
Voor basisconfiguratie van de toegang van een gast kunt u referenties met configuratievoorbeelden controleren. Dit artikel richt zich op de configuratie van de vergunningsregels en op verschillen in de vergunningsvoorwaarden.

Netwerkdigram

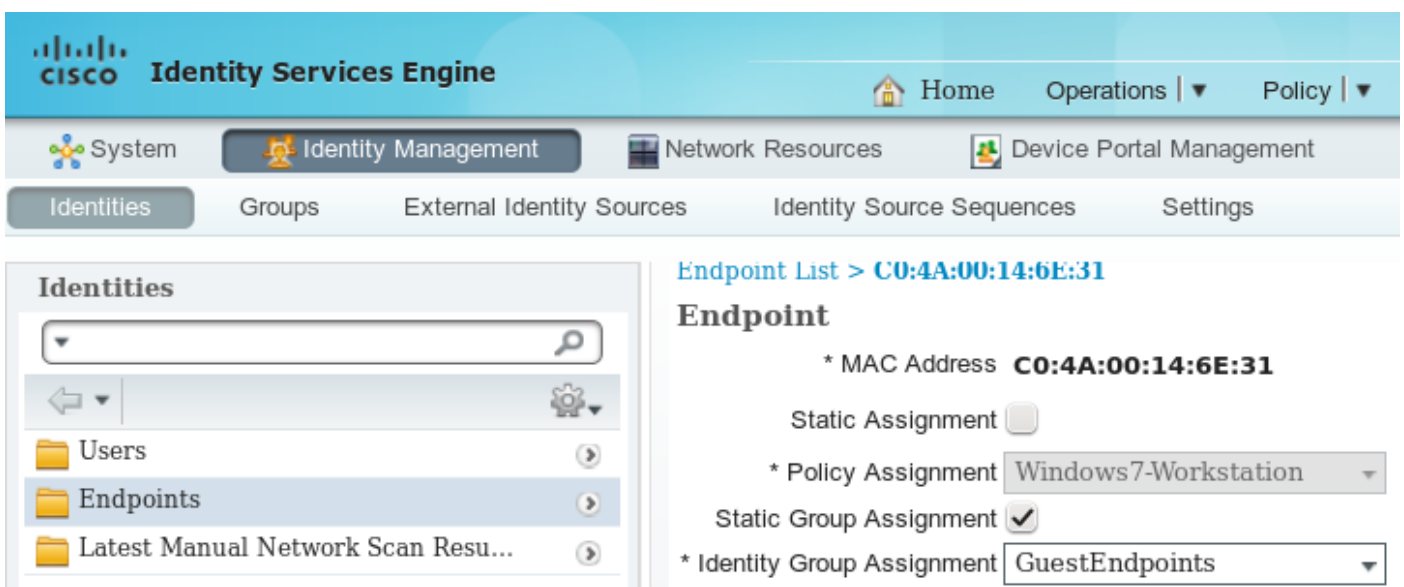


Permanente toegang

Voor ISE versie 1.3 en nieuwer na succesvolle authenticatie in het gastportaal met apparaatregistratie ingeschakeld.



Endpoint device (mac-adres) is statistisch geregistreerd in specifieke endpointgroepen (GuestEndpoints in dit voorbeeld).



Deze groep is afgeleid van het gasttype van de gebruiker, zoals in deze afbeelding wordt getoond.

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 ▾

Als het een zakelijke gebruiker is (identiteitswinkel andere dan gast) die instelling is afgeleid van de portal instellingen.

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: *

Als gevolg daarvan behoort het met de gast verbonden hoofdadres altijd tot die specifieke identiteitsgroep. Dit kan niet automatisch worden gewijzigd (bijvoorbeeld door Profiler Service).

Opmerking: Voor het toepassen van Profiler resultaten kan de voorwaarden van de EndPointPolicy autorisatie worden gebruikt.

Het weten dat het apparaat altijd deel uitmaakt van een specifieke eindpuntidentiteitsgroep is mogelijk om op basis daarvan goedkeuringsregels op te stellen, zoals in deze afbeelding wordt getoond.

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

Zodra een gebruiker niet echt is bevonden, komt de autorisatie overeen met generieke regel

RedirectToPortal. Na omleiding naar het gastportal en verificatie wordt het eindpunt geplaatst in de specifieke eindpuntidentiteitsgroep. Dat wordt gebruikt door de eerste, specifiekere voorwaarde. Alle latere authenticaties van dat eindpunt bereiken de eerste machtigingsregel en de gebruiker wordt volledige netwerktoegang verleend zonder de noodzaak om op het gastportaal opnieuw te authentifieren.

Endpoint Purge voor Guest Account

Deze situatie kan eeuwig duren. Maar in ISE 1.3 is Purge Endpoint functionaliteit geïntroduceerd. Met de standaardconfiguratie.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar contains a 'Settings' menu with options for 'User Custom Attributes', 'User Password Policy', and 'Endpoint Purge'. The main content area is titled 'Endpoint Purge' and includes the following sections:

- 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**: A table with one rule named 'EnrolledRule' with a status of 'Off' and the condition 'if DeviceRegistrationStatus Equals Registered'.
- Purge**: A table with two rules: 'GuestEndpointsPurgeRule' (status 'On', condition 'if GuestEndpoints AND ElapsedDays Greater than 30') and 'RegisteredEndpointsPurgeRule' (status 'On', condition 'if RegisteredDevices AND ElapsedDays Greater than 30').
- Schedule**: A section for scheduling purges, currently set to 'Everyday' at '03:00'.

Alle eindpunten die gebruikt worden voor gastverificatie worden na 30 dagen verwijderd (na het maken van eindpunt). Het resultaat is gewoonlijk na 30 dagen dat de gastgebruiker probeert om toegang te krijgen tot de autorisatieregels van RedirectToPortal en wordt opnieuw gericht voor authenticatie.

Opmerking: Endpoint Purge-functionaliteit is afhankelijk van het beleid voor het zuiveren van uw account en het aflopen van uw account.

Opmerking: In ISE 1.2 kunnen endpoints alleen automatisch worden verwijderd wanneer ze de limieten van de interne wachtrij voor profielen raken. Laatst gebruikte eindpunten worden dan verwijderd.

Tijdelijke toegang

Een andere methode voor gasttoegang is de Guest Flow conditie te gebruiken.

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

Die voorwaarde is het controleren van actieve sessies op ISE en het zijn eigenschappen. Als die sessie de eigenschap heeft die erop wijst dat de vorige gastgebruiker voor echt geauthentiseerd is voorwaarde wordt gematcht. Nadat ISE het bericht van de Voorbereiding van Radius van het Netwerk toegangsapparaat (NAD) ontvangt, wordt de sessie beëindigd en later verwijderd. In dat stadium is de conditie Network Access:UseCase = Guest Flow niet meer tevreden. Als resultaat hiervan bereikt alle verdere authenticaties van dat eindpunt generieke regel die omleiding voor gastauthenticatie.

Opmerking: Guest Flow wordt niet ondersteund wanneer de gebruiker geauthentiseerd is via het Hot Folder-portal. Voor die scenario's is de eigenschap UseCase ingesteld op Host Lookup in plaats van Guest Flow.

WLC-gedrag van verbroken verbinding

Nadat klanten van draadloos netwerk losmaakt (bijvoorbeeld het gebruiken van losconnect knop in Windows) verstuurt het een authenticatiekader. Maar die is weggelaten door de WLC en kan worden bevestigd met behulp van "debug client xxxx" - WLC levert geen debugs op wanneer client wordt losgekoppeld van WLAN. Als resultaat bij Windows client:

- IP-adres wordt uit de interface verwijderd
- de interface staat in : media losgekoppeld

Maar op WLC is de status onveranderd (client nog steeds in RUN-status).

Dat is het geplande ontwerp voor WLC, de sessie wordt verwijderd wanneer

- hits als gebruikers die geen toegang tot de ether hebben
- hits in de sessie
- als L2-encryptie wordt gebruikt, dan wanneer het groep key interval bereikt
- iets anders veroorzaakt dat AP/WLC de client afschoppen (bijvoorbeeld AP-radio resets, iemand sluit de WLAN, enz.)

Met dat gedrag en de tijdelijke toegangsconfiguratie nadat gebruikers hun verbindingen hebben verbroken van WLAN-sessie, wordt niet verwijderd van ISE omdat WLC deze nooit heeft geklaard (en nooit Radius Accounting Stop heeft verzonden). Als de sessie niet wordt verwijderd, herinnert ISE zich nog steeds oude sessie en is de toestand van de gastenstroom bevredigend. Na het afsluiten en opnieuw verbinden heeft de gebruiker volledige netwerktoegang zonder vereiste om

opnieuw te bevestigen.

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 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

Maar als een gebruiker die de verbinding met een ander WLAN heeft verbroken, beslist WLC om de oude sessie te wissen. Radius accounting Stop wordt verzonden en ISE verwijdert de sessie. Als de client probeert verbinding te maken met de oorspronkelijke WLAN-status is de gebruiker niet tevreden en wordt de gebruiker opnieuw gericht op verificatie.

Opmerking: WLC ingesteld met Management Frame Protection (MFP) accepteert versleuteld verificatiekader van CCXv5 MFP-client.

Verifiëren

Permanente toegang

Na omleiding naar het gastportaal en succesvolle authenticatie stuurt ISE een wijziging van de vergunning (CoA) om verificatie te starten. Als resultaat hiervan wordt er een nieuwe MAC Verificatie Bypass (MAB)-sessie gebouwd. Dit tijd-eindpunt behoort tot de identiteitsgroep van GuestEndpoints en de wedstrijdregel die volledige toegang verleent.

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 four metrics: 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 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

In dat stadium kan de draadloze gebruiker de verbinding verbroken, verbinding maken met verschillende WLAN's en vervolgens opnieuw aansluiten. Al die latere authenticaties gebruiken een identiteit gebaseerd op het mac-adres, maar slaan de eerste regel aan vanwege het eindpunt dat tot een specifieke identiteitsgroep behoort. Volledige netwerktoegang wordt geboden zonder gastverificatie.

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...					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

Tijdelijke toegang

Voor het tweede scenario (met conditie gebaseerd op Guest Flow) is het begin hetzelfde.

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

Maar nadat de sessie voor alle latere authenticaties is verwijderd, slaat gast algemene regels op en wordt opnieuw gericht voor gastauthenticatie.

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

De voorwaarde van de stroom van de gast is tevreden wanneer de juiste eigenschappen voor de zitting bestaan. Dat kan worden geverifieerd door te kijken naar de eigenschappen van het

eindpunt. Het resultaat van geslaagde verificatie van gasten wordt aangegeven.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for a Guest Flow. The page is divided into a left sidebar and a main content area. The sidebar contains a search bar and a list of categories: Users, Endpoints, and Latest Manual Network Scan Resu... The main content area displays a list of attributes and their values:

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 beëindigen de verzending van een gastaccount of het verlopen van het account.

(verzoek om versterking om gastsessies te beëindigen na verwijdering of beëindiging van de gastaccount)

Referenties

- [Cisco ISE 1.3 beheerdershandleiding](#)
- [Cisco ISE 1000 1000 1000 1000000000 SERIES BEHEERDERS](#)
- [ISE versie 1.3 Configuratievoorbeeld voor hotspotjes](#)
- [Configuratievoorbeeld van ISE versie 1.3, zelfgeregistreerd Guest Portal](#)
- [Central-webverificatie in het configuratievoorbeeld van WLC en ISE](#)
- [Central-webverificatie met FlexConnect APs op een WLC met ISE-configuratievoorbeeld](#)

- [Technische ondersteuning en documentatie – Cisco Systems](#)