

Konfigurieren des temporären und permanenten ISE-Gastzugriffs

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Permanenter Zugriff](#)

[Endpunktlöschung für Gastkonten](#)

[Temporärer Zugriff](#)

[WLC-Trennungsverhalten](#)

[Überprüfen](#)

[Permanenter Zugriff](#)

[Temporärer Zugriff](#)

[Bug](#)

[Referenzen](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Dokument werden verschiedene Methoden für die Identity Services Engine (ISE)-Gastzugriffskonfiguration beschrieben. Basierend auf unterschiedlichen Bedingungen in Autorisierungsregeln:

- permanenter Netzwerkzugriff ist möglich (keine nachträgliche Authentifizierung erforderlich)
- temporärer Zugriff auf das Netzwerk möglich ist (Gastauthentifizierung nach Ablauf der Sitzung erforderlich)

Neben den Auswirkungen auf das Szenario des temporären Zugriffs wird auch ein bestimmtes Verhalten des Wireless LAN Controller (WLC) für die Sitzungsentfernung dargestellt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- ISE-Bereitstellungen und Gastdatenströme
- Konfiguration der Wireless LAN Controller (WLCs)

Verwendete Komponenten

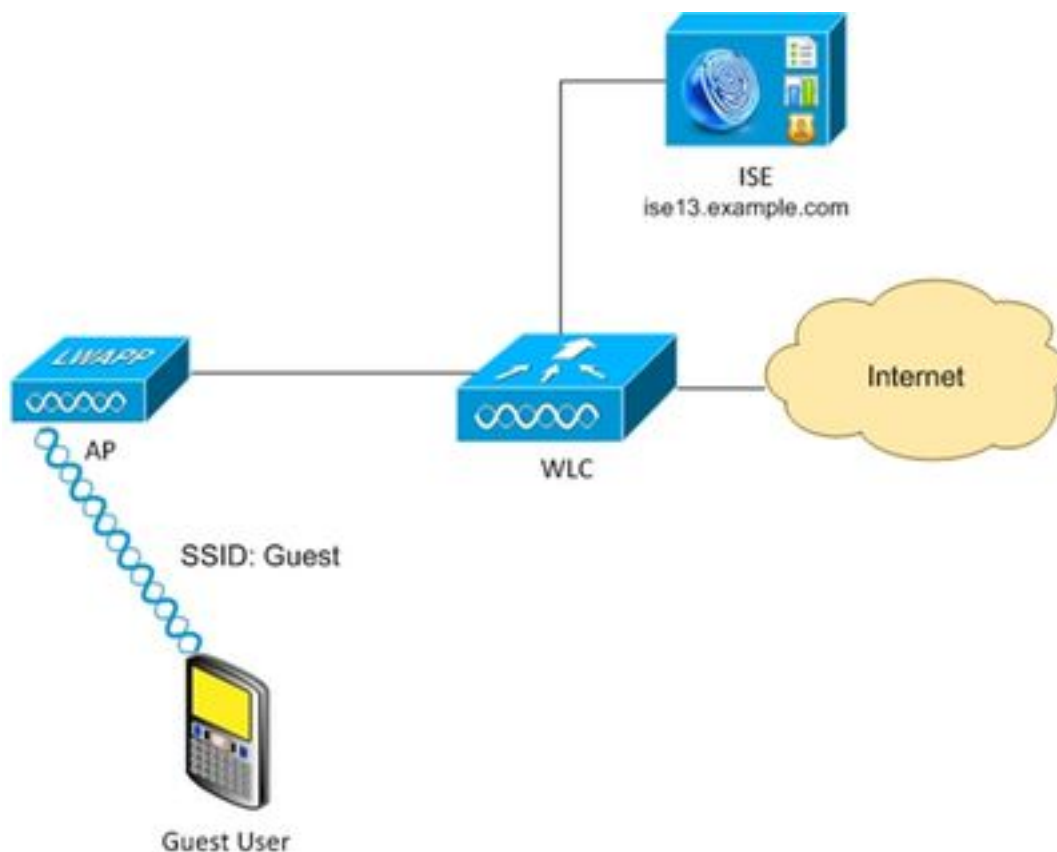
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco WLC 7.6 oder höher
- ISE Software, Version 1.3 und höher

Konfigurieren

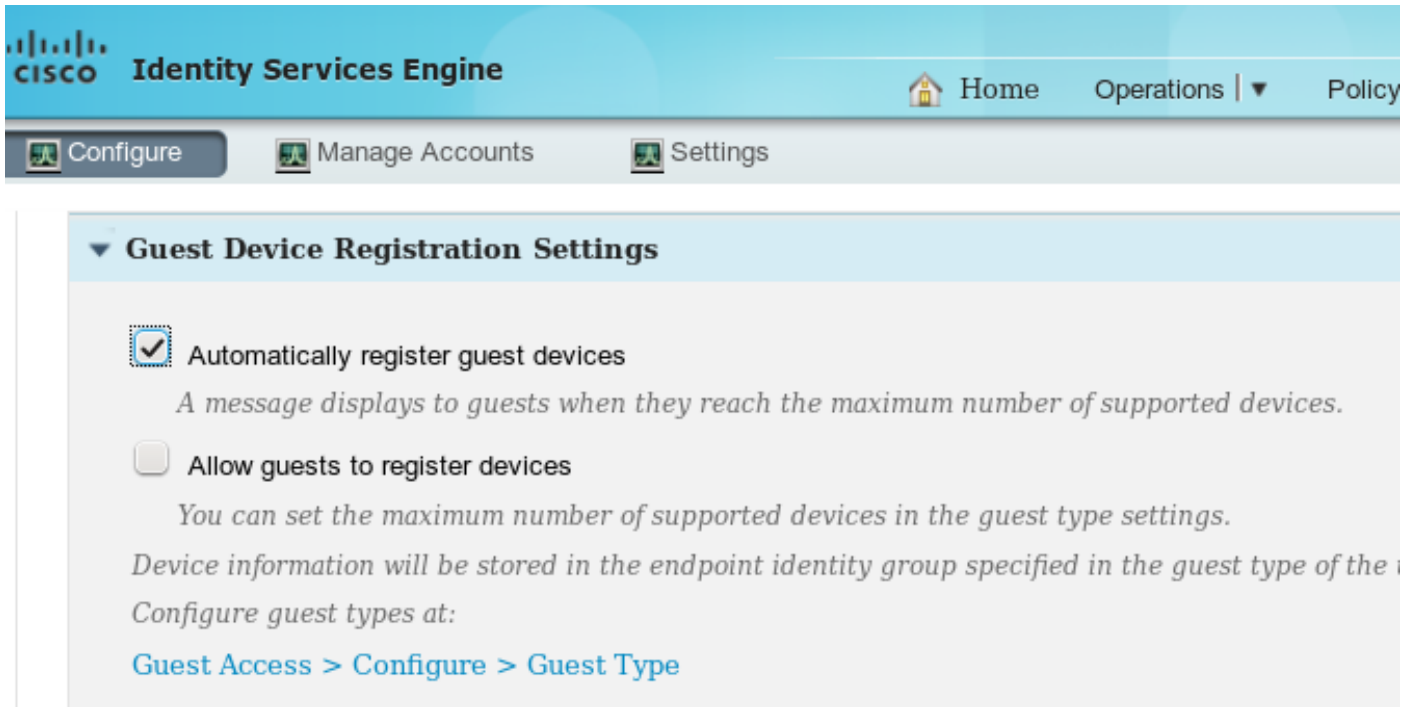
Eine grundlegende Konfiguration für den Gastzugriff finden Sie in den Referenzen mit Konfigurationsbeispielen. Dieser Artikel behandelt die Konfiguration von Autorisierungsregeln und Unterschiede in den Autorisierungsbedingungen.

Netzwerkdiagramm

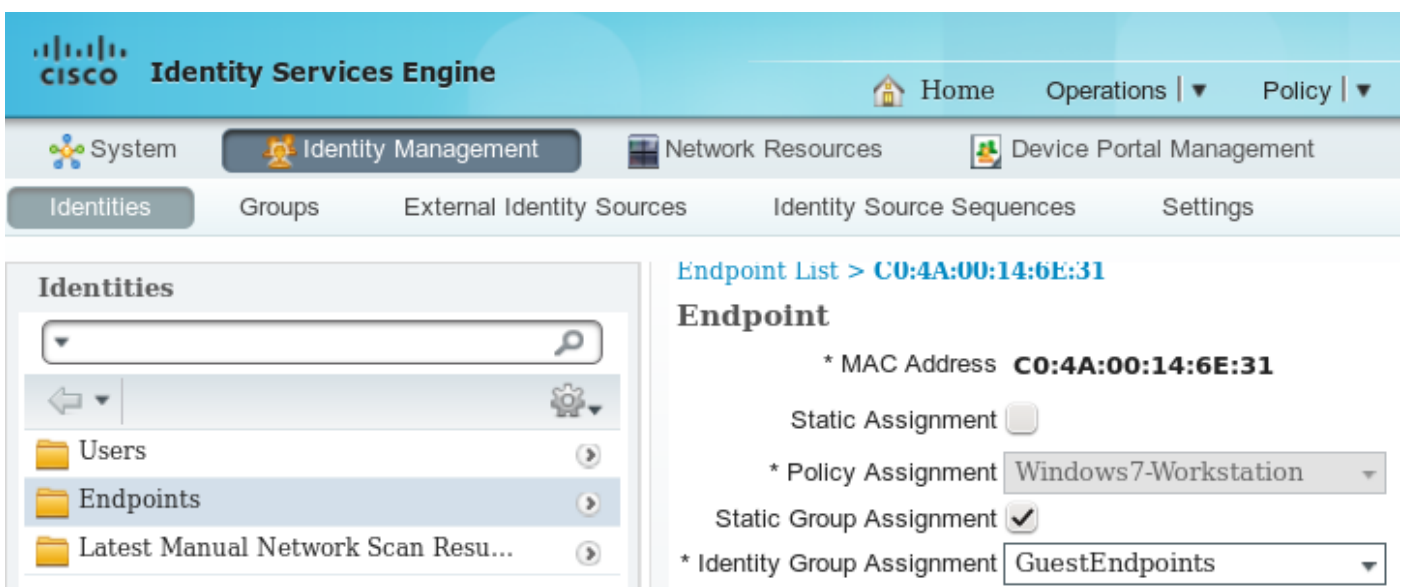


Permanenter Zugriff

Für ISE Version 1.3 und höher nach erfolgreicher Authentifizierung auf dem Gastportal mit aktivierter Geräteregistrierung.



Endgerät (MAC-Adresse) ist statisch in einer bestimmten Endpunktgruppe registriert (in diesem Beispiel GuestEndpoints).



Diese Gruppe wird vom Gasttyp des Benutzers abgeleitet, wie in diesem Bild gezeigt.



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: ▾

Wenn es sich um einen Firmenbenutzer (Identitätsspeicher mit Ausnahme von Gast) handelt, wird diese Einstellung von den Portaleinstellungen abgeleitet.

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: *

Folglich gehört die dem Gast zugeordnete MAC-Adresse immer zu dieser spezifischen Identitätsgruppe. Das kann nicht automatisch geändert werden (z.B. durch Profiler Service).

Hinweis: Zum Anwenden von Profilerergebnissen kann eine EndPointPolicy-Autorisierungsbedingung verwendet werden.

Da das Gerät immer zu einer bestimmten Endpunkt-Identitätsgruppe gehört, können auf dieser Grundlage Autorisierungsregeln erstellt werden, wie in diesem Bild gezeigt.

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

Wenn ein Benutzer nicht authentifiziert wurde, stimmt die Autorisierung mit der generischen Regel RedirectToPortal überein. Nach der Umleitung zum Gastportal und der Authentifizierung wird der

Endpunkt in der spezifischen Endpunkt-Identitätsgruppe platziert. Das wird von der ersten, spezifischeren Bedingung verwendet. Alle nachfolgenden Authentifizierungen dieses Endpunkts treffen auf die erste Autorisierungsregel, und der Benutzer erhält vollständigen Netzwerkzugriff, ohne dass eine erneute Authentifizierung im Gastportal erforderlich ist.

Endpunktlöschung für Gastkonten

Diese Situation könnte ewig andauern. In ISE 1.3 wurde jedoch die Funktion "Endgeräte entfernen" eingeführt. Mit der Standardkonfiguration.

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 GuestEndpoints AND ElapsedDays Greater than 30
<input checked="" type="checkbox"/>	RegisteredEndPointsPurgeRule	if RegisteredDevices AND ElapsedDays Greater than 30

Schedule

Purge endpoints from the identity table at a specific time

Schedule : Every at

Alle Endpunkte, die für die Gastauthentifizierung verwendet werden, werden nach 30 Tagen (von der Erstellung des Endpunkts an) entfernt. Daher trifft ein Gastbenutzer, der versucht, auf das Netzwerk zuzugreifen, in der Regel nach 30 Tagen auf die RedirectToPortal-Autorisierungsregel und wird zur Authentifizierung umgeleitet.

Hinweis: Die Funktion zum Zurücksetzen von Endpunkten ist unabhängig von der Richtlinie zum Zurücksetzen von Gastkonten und dem Ablauf von Gastkonten.

Hinweis: In der ISE 1.2 konnten Endpunkte nur dann automatisch entfernt werden, wenn die internen Warteschlangenbeschränkungen für Profiler eingehalten wurden. Dann werden die zuletzt verwendeten Endgeräte entfernt.

Temporärer Zugriff

Eine weitere Methode für den Gastzugriff ist die Verwendung des Gastdatenflusszustands.

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

Diese Bedingung besteht darin, aktive Sitzungen auf der ISE und deren Attribute zu überprüfen. Wenn diese Sitzung über das Attribut verfügt, das angibt, dass der zuvor erfolgreich authentifizierte Gastbenutzer zugeordnet wurde. Nachdem die ISE die RADIUS Accounting Stopp-Nachricht vom Network Access Device (NAD) erhält, wird die Sitzung beendet und später entfernt. In dieser Phase ist die Bedingung Netzwerkzugriff:UseCase = Guest Flow nicht mehr erfüllt. Infolgedessen treffen alle nachfolgenden Authentifizierungen dieses Endpunkts auf die generische Regelumleitung für die Gastauthentifizierung.

Hinweis: Guest Flow wird nicht unterstützt, wenn der Benutzer über das HotSpot-Portal authentifiziert wird. In diesen Szenarien ist das UseCase-Attribut auf Host Lookup anstatt auf Guest Flow festgelegt.

WLC-Trennungverhalten

Nachdem Clients die Verbindung zum Wireless-Netzwerk getrennt haben (z. B. über die Trenntaste in Windows) sendet sie einen deauthentifizierten Frame. Dies wird vom WLC jedoch weggelassen und kann mit dem Befehl "debug client xxxx" bestätigt werden. WLC zeigt keine Debugging-Meldungen an, wenn der Client die Verbindung zum WLAN trennt. Als Ergebnis auf Windows-Client:

- IP-Adresse wird von der Schnittstelle entfernt
- Schnittstelle ist in Status: Medien getrennt

Auf dem WLC ist der Status jedoch unverändert (der Client befindet sich noch im RUN-Status).

Das geplante Design für WLC sieht vor, dass die Sitzung entfernt wird, wenn

- Timeout-Treffer im Leerlauf
- Sitzungs-Timeout-Treffer
- Wenn L2-Verschlüsselung verwendet wird, dann wenn das Rotationsintervall für die Gruppenschlüssel erreicht wird
- Ein anderer Grund führt dazu, dass der Access Point/WLC den Client ausschaltet (z. B. Zurücksetzen der AP-Funkverbindung, Herunterfahren des WLAN usw.)

Mit diesem Verhalten und der Konfiguration des temporären Zugriffs, nachdem der Benutzer die Verbindung von der WLAN-Sitzung getrennt hat, wird diese nicht aus der ISE entfernt, da der

WLC diesen Vorgang nie gelöscht hat (und keinen Radius Accounting Stopp gesendet hat). Wenn die Sitzung nicht entfernt wird, speichert die ISE weiterhin die alte Sitzung und die Bedingung für den Gastfluss ist erfüllt. Nach dem Trennen der Verbindung und der erneuten Verbindung hat der Benutzer uneingeschränkten Netzwerkzugriff, ohne dass eine erneute Authentifizierung erforderlich ist.

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 events.

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

Wenn der Benutzer nach dem Trennen der Verbindung jedoch eine Verbindung zu einem anderen WLAN herstellt, entscheidet der WLC, die alte Sitzung zu löschen. Radius Accounting Stopp wird gesendet, und die ISE entfernt die Sitzung. Wenn der Client versucht, eine Verbindung zum ursprünglichen Zustand des WLAN-Gastdatenflusses herzustellen, ist dieser nicht zufrieden und der Benutzer wird zur Authentifizierung umgeleitet.

Hinweis: WLC, konfiguriert mit Management Frame Protection (MFP), akzeptiert verschlüsselte deauthentifizierte Frames vom CCXv5 MFP-Client.

Überprüfen

Permanenter Zugriff

Nach der Umleitung zum Gastportal und erfolgreicher Authentifizierung sendet die ISE CoA (Change of Authorization), um eine erneute Authentifizierung auszulösen. Infolgedessen wird eine neue MAB-Sitzung (MAC Authentication Bypass) erstellt. Dieser Zeitendpunkt gehört zur Identitätsgruppe GuestEndpoints und stimmt mit einer Regel überein, die vollständigen Zugriff bereitstellt.

The screenshot shows the Cisco Identity Services Engine (ISE) interface with the same navigation and dashboard as the previous screenshot. 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 events.

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-08-14 22:25:45...	i		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 dieser Phase kann der Wireless-Benutzer die Verbindung trennen, eine Verbindung zu verschiedenen WLANs herstellen und dann die Verbindung wieder herstellen. Alle diese nachfolgenden Authentifizierungen verwenden die Identität basierend auf der MAC-Adresse, treffen aber die erste Regel, weil der Endpunkt zu einer bestimmten Identitätsgruppe gehört. Der vollständige Netzwerkzugriff wird ohne Gastauthentifizierung bereitgestellt.

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 area displays three summary cards: Misconfigured Suppliants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). Below these 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.

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

Temporärer Zugriff

Für das zweite Szenario (mit einer Bedingung, die auf Guest Flow basiert) ist der Beginn identisch.

The screenshot shows the Cisco Identity Services Engine (ISE) interface, similar to the first one. It displays three summary cards: Misconfigured Suppliants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). Below these is a table of live sessions with columns for Time, Status, Det..., R..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event.

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

Nachdem die Sitzung jedoch für alle nachfolgenden Authentifizierungen entfernt wurde, trifft der Gast die generische Regel und wird erneut zur Gastauthentifizierung umgeleitet.

The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. At the top, there are navigation tabs for Home, Operations, Policy, Guest Access, and Administration. Below these are buttons for Authentications, Reports, Adaptive Network Control, and Troubleshoot. Three summary cards are displayed: Misconfigured Suppliants (0), Misconfigured Network Devices (0), and RADIUS Drops (0). The main area features a table with columns for Time, Status, Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event. The table contains several rows of session logs, including authentication successes and failures.

Time	Status	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...	✓		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:31	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...	✓		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:31	CO:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded

Die Bedingung für den Gastfluss ist erfüllt, wenn die richtigen Attribute für die Sitzung vorhanden sind. Dies lässt sich durch die Betrachtung von Endgeräteattributen überprüfen. Das Ergebnis der erfolgreichen Gastauthentifizierung wird angezeigt.

The screenshot shows the Cisco Identity Services Engine (ISE) Identity Management section. The left sidebar contains a tree view with folders for Users, Endpoints, and Latest Manual Network Scan Resu... The main area displays a list of attributes and their values for a specific session.

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 wird bei Entfernung oder Ablauf eines Gastkontos beendet.

(Erweiterungsanfrage zur Beendigung von Gastsitzungen nach Entfernung oder Ablauf eines Gastkontos)

Referenzen

- [Cisco ISE 1.3 Administratorhandbuch](#)
- [Cisco ISE 1.4 Administratorhandbuch](#)
- [Konfigurationsbeispiel für ISE-Version 1.3 Hotspot](#)
- [Konfigurationsbeispiel für das selbst registrierte Gastportal der ISE-Version 1.3](#)
- [Zentrale Webauthentifizierung im Konfigurationsbeispiel für WLC und ISE](#)
- [Zentrale Webauthentifizierung mit FlexConnect-APs auf einem WLC mit ISE-Konfigurationsbeispiel](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)