

Configurez Access provisoire et permanent d'invité ISE

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Diagramme du réseau](#)

[Access permanent](#)

[Purge de point final pour des comptes d'invité](#)

[Access provisoire](#)

[Comportement de débranchement WLC](#)

[Vérifiez](#)

[Access permanent](#)

[Access provisoire](#)

[Bogues](#)

[Références](#)

[Cisco relatif prennent en charge des discussions de la Communauté](#)

Introduction

Ce document décrit des différentes méthodes pour la configuration d'accès invité du Cisco Identity Services Engine (ISE). Basé sur différentes conditions dans des règles d'autorisation :

- l'accès permanent au réseau peut être fourni (aucune condition requise pour des authentications ultérieures)
- l'accès provisoire au réseau peut être fourni (exigeant l'authentification d'invité après que la session expire)

Également le comportement Sans fil spécifique du contrôleur LAN (WLC) pour la suppression de session est présenté le long de l'incidence sur le scénario provisoire d'accès.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Déploiements ISE et écoulements d'invité
- Configuration des contrôleurs LAN Sans fil (WLCs)

Composants utilisés

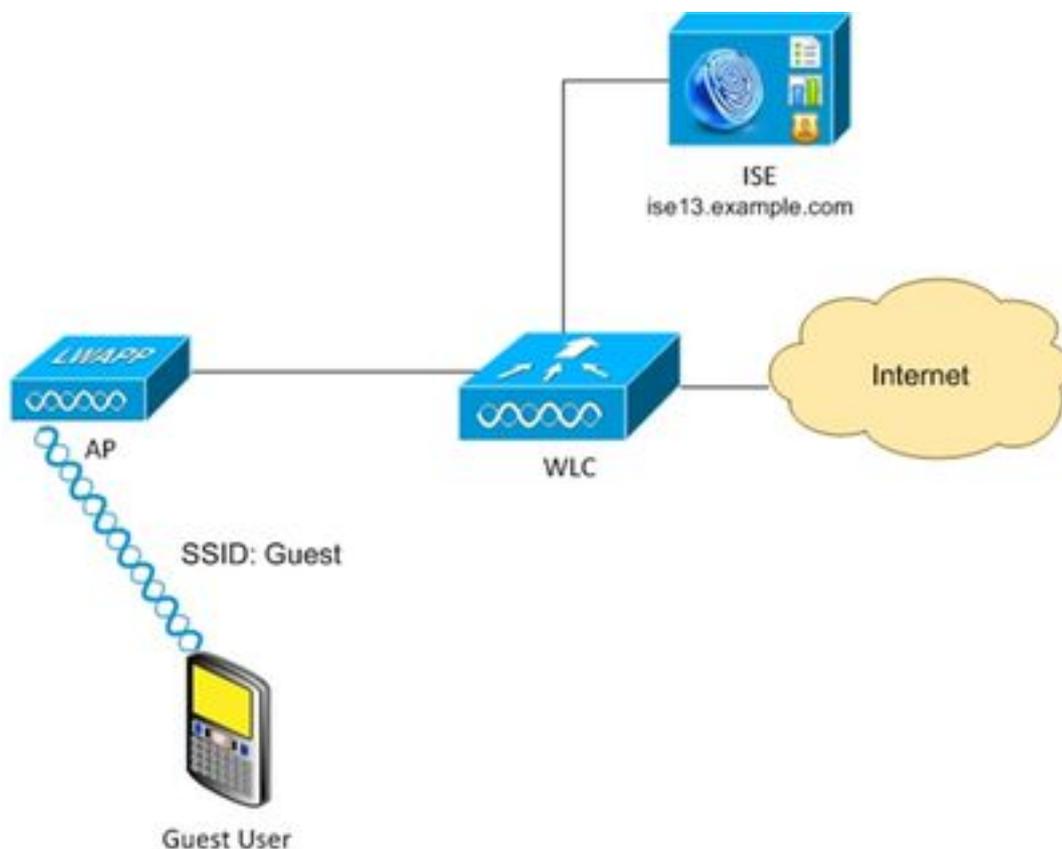
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Version 7.6 et ultérieures de Cisco WLC
- Logiciel ISE, version 1.3 et ultérieures

Configurez

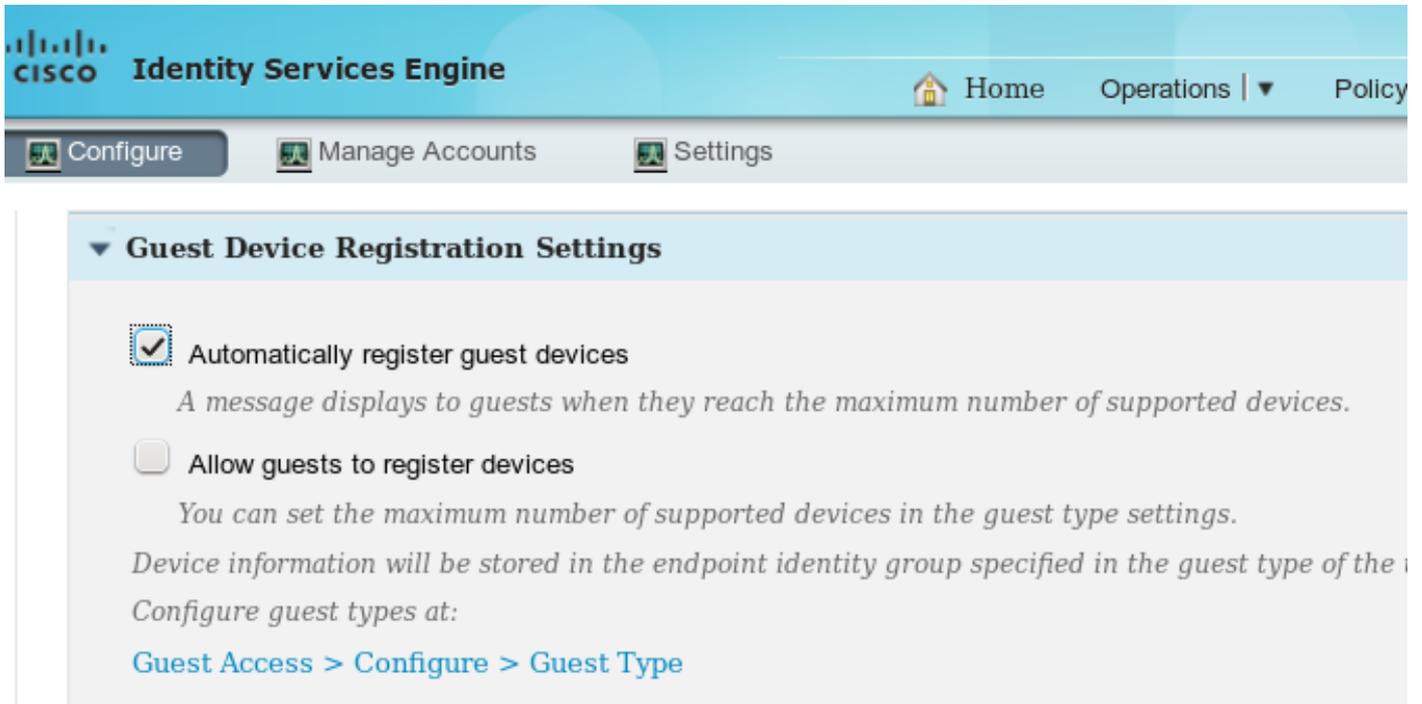
Pour la configuration de base d'accès invité vérifiez s'il vous plaît les références avec des exemples de configuration. Cet article se concentre sur des règles configuration et différences d'autorisation en conditions d'autorisation.

Diagramme du réseau

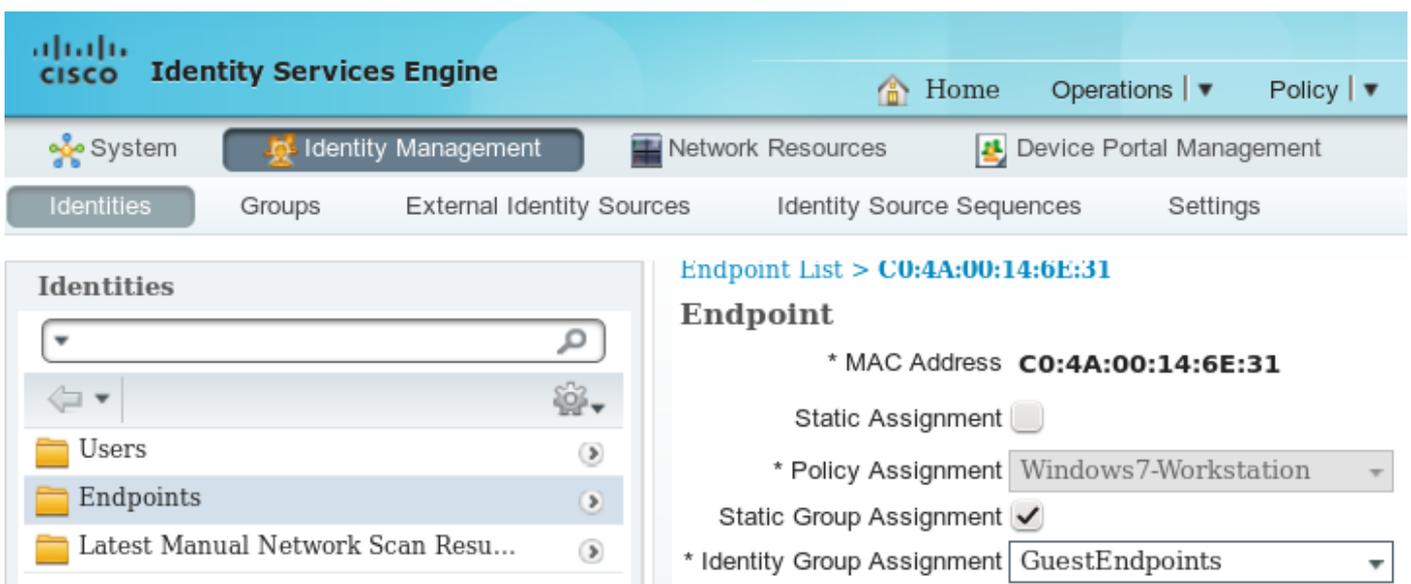


Access permanent

Pour la version 1.3 et plus récentes ISE après l'authentification réussie sur le portail d'invité avec l'enregistrement de périphérique activé.



Le périphérique d'extrémité (MAC address) est statiquement enregistré dans le groupe spécifique de point final (GuestEndpoints dans cet exemple).



Ce groupe est dérivé du type d'invité de l'utilisateur, suivant les indications de cette image.



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: ▾

Si c'est un utilisateur en entreprise (mémoire d'identité l'autre puis invité) cette configuration est dérivée des configurations portales.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for Portal Settings. The main configuration area includes:

- 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
 - 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:** * Contractor (default)

En conséquence le MAC address associé avec l'invité appartient toujours à ce groupe spécifique d'identité. Cela ne peut pas être changé automatiquement (par exemple par service de profileur).

Note: Pour appliquer l'état d'autorisation d'EndPointPolicy de résultats de profileur peut être utilisée.

Sachant que le périphérique appartient toujours au groupe spécifique d'identité de point final qu'il est possible d'établir des règles d'autorisation basées sur celle, suivant les indications de cette image.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for Authorization Policy. The main configuration area includes:

- 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

Une fois qu'un utilisateur n'est pas authentifié, l'autorisation apparie la règle générique

RedirectToPortal. Après redirection au portail et à l'authentification d'invité, le point final est placé dans le groupe spécifique d'identité de point final. Cela est utilisé par le premier, une condition plus spécifique. Toutes les authentifications ultérieures de ce point final frappe la première règle d'autorisation et l'utilisateur est plein accès au réseau fourni sans nécessité d'authentifier à nouveau sur le portail d'invité.

Purge de point final pour des comptes d'invité

Cette situation a pu durer pour toujours. Mais dans le point final de purge ISE 1.3 la fonctionnalité a été introduite. Avec la configuration par défaut.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes Home, Operations, Policy, Guest Access, and Administration. The main menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, and Feed Service. 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

Tous les points finaux utilisés pour l'authentification d'invité sont retirés après 30 jours (de la création de point final). En conséquence habituellement après utilisateur d'invité de 30 jours essayer d'accéder à la règle d'autorisation de RedirectToPortal de hit de réseau et est réorienté pour l'authentification.

Note: La fonctionnalité de purge de point final est indépendant d'expiration de stratégie de purge de compte d'invité et de compte d'invité.

Note: Dans ISE 1.2 des points finaux ont pu être retirés automatiquement seulement en frappant des limites internes de file d'attente de profileur. Alors moins points finaux utilisés récemment sont retirés.

Access provisoire

Une autre méthode pour l'accès invité est d'utiliser l'état d'écoulement d'invité.

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

Que la condition vérifie des sessions actives là-dessus ISE et est des attributs. Si cette session a l'attribut indiquant que précédemment l'utilisateur d'invité a authentifié avec succès conditionnez est apparié. Après qu'ISE reçoive le message de comptabilité d'arrêt de Radius du périphérique d'accès au réseau (NAD), la session est terminée et plus tard retirée. À cette étape l'accès au réseau de condition : UseCase = écoulement d'invité n'est plus satisfait. En conséquence toutes les authentifications ultérieures de ce point final frappe la règle générique réorientant pour l'authentification d'invité.

Note: Écoulement d'invité non pris en charge quand l'utilisateur est authentifié par l'intermédiaire du portail de point névralgique. Pour ces scénarios l'attribut d'UseCase est placé à la consultation d'hôte au lieu de l'écoulement d'invité.

Comportement de débranchement WLC

Après que les démonter de clients du réseau Sans fil (par exemple utilisant le bouton de débranchement dans Windows) il envoie la trame de deauthenticaton. Mais cela est omis par le WLC et peut être confirmé utilisant « mettent au point le client xxxx » - WLC présente l'aucun met au point quand le client déconnecte du WLAN. En conséquence sur le client Windows :

- l'IP address est retiré de l'interface
- l'interface est dans l'état : medias déconnectés

Mais sur WLC l'état est inchangé (client toujours dans l'état de PASSAGE).

C'est conception prévue pour WLC, la session est retirée quand

- hit de veille de délai d'attente d'utilisateur
- hit de session-timeout
- si utilisant le cryptage L2, puis quand l'intervalle de rotation de clé de groupe frappe
- autre chose fait donner un coup de pied l'AP/WLC le client outre de (par exemple les remises par radio AP, quelqu'un arrêtent le WLAN, etc.)

Avec ces comportement et configuration provisoire d'accès après que des démonter d'utilisateur de la session WLAN ne soit pas enlevés d'ISE parce que WLC n'a jamais effacé lui (et l'arrêt de comptabilité non jamais envoyé de Radius). Si la session n'est pas retirée, ISE se souvient toujours la vieille session et l'état d'écoulement d'invité est satisfait. Après déconnexion et reconnexion l'utilisateur ont le plein accès au réseau sans condition requise d'authentifier à

nouveau.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there is a navigation bar with 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, there are tabs for 'Authentications', 'Reports', 'Adaptive Network Control', and 'Troubleshoot'. The main area displays three summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), and 'RADIUS Drops' (0). Below these, there are controls for 'Show Live Sessions', 'Add or Remove Columns', 'Refresh', and 'Reset Repeat Counts'. The main table lists session events with columns for Time, Status, Det..., Repeat C..., Identity, Endpoint ID, Authorization Policy, Authorization Profiles, and Event.

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

Mais si après que l'utilisateur de déconnexion se connecte au WLAN différent, puis WLC décide d'effacer la vieille session. L'arrêt de comptabilité de Radius est envoyé et ISE retire la session. Si les essais de client à connecter à l'état d'écoulement d'origine d'invité WLAN n'est pas satisfait et l'utilisateur est réorienté pour l'authentification.

Note: WLC configuré avec le Management Frame Protection (MFP) reçoit la trame chiffrée de deauthentication du client CCXv5 MFP.

Vérifiez

Access permanent

Après redirection à l'authentification portale et réussie d'invité ISE envoie la modification de l'autorisation (CoA) de déclencher la réauthentification. En conséquence la nouvelle session de dérivation d'authentification MAC (MAB) est établie. Ce point final de temps appartient au groupe d'identité de GuestEndpoints et les correspondances ordonnent fournir l'accès complet.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there is a navigation bar with 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below this, there are tabs for 'Authentications', 'Reports', 'Adaptive Network Control', and 'Troubleshoot'. The main area displays three summary cards: 'Misconfigured Supplicants' (0), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (0), and 'Client'. Below these, there are controls for 'Show Live Sessions', 'Add or Remove Columns', 'Refresh', and 'Reset Repeat Counts'. The main table lists session events 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 22:25:45...			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

À cette étape l'utilisateur de sans fil peut se déconnecter, se connecter à différents WLAN, puis rebrancher. Toutes ces authentifications ultérieures utilisent l'identité basée sur le MAC address, mais frappent la première règle en raison du point final appartenant au groupe spécifique d'identité. Le plein accès au réseau est fourni sans authentification d'invité.

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...				guest	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

Access provisoire

Pour le deuxième scénario (dans la condition étant basé sur l'écoulement d'invité) le début est identique.

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

Mais après que la session soit retirée pour toutes les authentifications ultérieures, l'invité a frappé la règle générique et est de nouveau réorienté pour l'authentification d'invité.

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

L'invité que l'état d'écoulement est soit satisfait quand les attributs corrects sont existants pour la

session. Cela peut être vérifié en regardant des attributs de point final. Le résultat de l'authentification réussie d'invité sont indiqués.

Attribute	Value
NAS-IP-Address	10.62.148.101
NAS-Identifiant	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
```

Bogues

Le CoA [CSCuu41157](#) ISE ENH se terminent envoient en fonction la suppression ou l'échéance de compte d'invité.

(demande d'amélioration de terminer des sessions d'invité après suppression ou échéance de compte d'invité)

Références

- [Guide d'administrateurs de Cisco ISE 1.3](#)
- [Guide d'administrateurs de Cisco ISE 1.4](#)
- [Exemple de configuration de point névralgique de version 1.3 ISE](#)
- [Exemple enregistré par individu de configuration portails d'invité de version 1.3 ISE](#)
- [Authentification Web centrale exemple sur WLC et ISE configuration](#)

- [Authentification Web centrale avec FlexConnect aps sur un WLC avec l'exemple de configuration ISE](#)
- [Support et documentation techniques - Cisco Systems](#)