

ISE ゲストの一時および永続的なアクセスの設定

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[常置アクセス](#)

[ゲスト アカウントのためのエンド ポイント ページ](#)

[一時アクセス](#)

[WLC 接続解除動作](#)

[確認](#)

[常置アクセス](#)

[一時アクセス](#)

[バグ](#)

[参考資料](#)

[Cisco サポート コミュニティ - 特集対話](#)

概要

この資料は Identity Services Engine (ISE) ゲスト アクセス設定用の異なった方法を記述したものです。承認規則の異なる条件に基づく:

- ネットワークへの常置アクセスは提供することができます (それに続く認証のための要件無し)
- ネットワークへの一時アクセスは提供することができます (セッションが切れた後ゲスト認証を必要とします)

またセッション削除のための特定のワイヤレス LAN コントローラ (WLC) 動作は一時アクセスシナリオの影響に沿って示されます。

前提条件

要件

次の項目に関する知識が推奨されます。

- ISE の導入およびゲスト フロー
- ワイヤレス LAN コントローラ (WLC) の設定

使用するコンポーネント

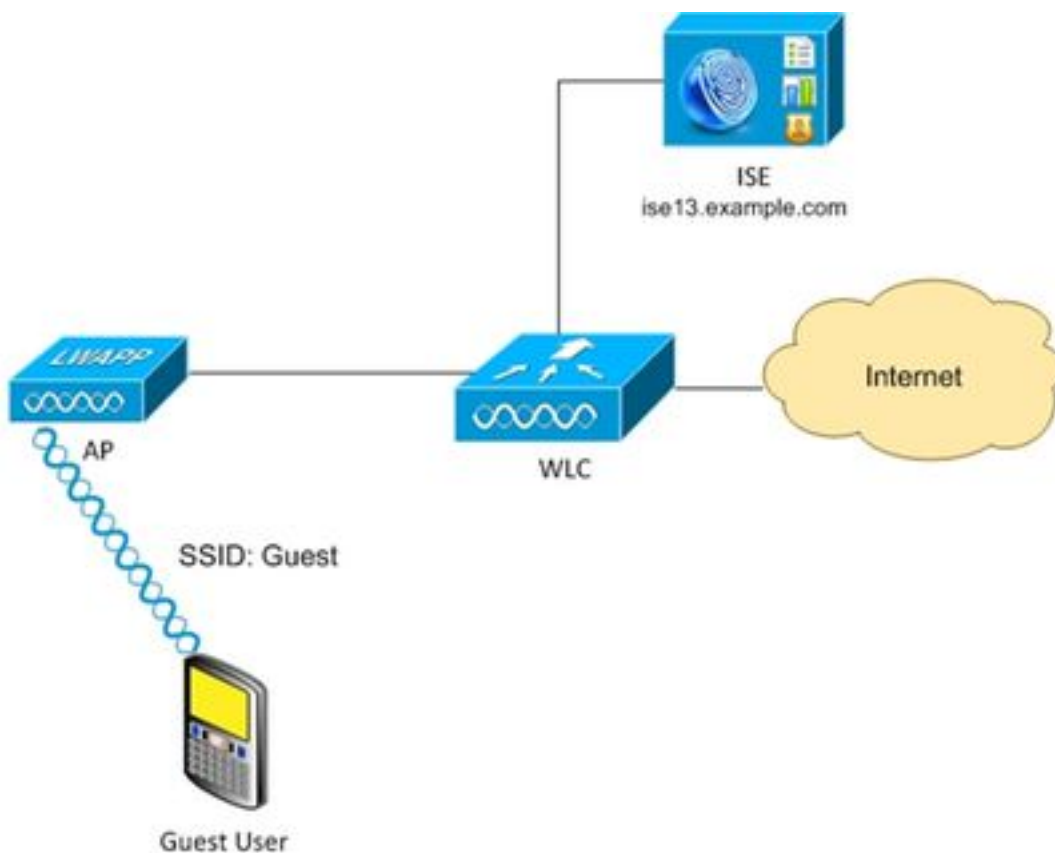
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Microsoft Windows 7
- Cisco WLC バージョン 7.6 以降
- ISE ソフトウェア バージョン 1.3 以降

設定

基本的なゲスト アクセス設定に関しては設定例と参照をチェックして下さい。この技術情報は許可状態の承認規則設定および違いに焦点を合わせます。

ネットワーク図



常置アクセス

デバイス登録がイネーブルの状態です。ゲスト ポータルの認証の成功の後の ISE バージョン 1.3 およびそれ以降に関しては。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below it are tabs for 'Configure', 'Manage Accounts', and 'Settings'. The main content area is titled 'Guest Device Registration Settings'. It features two radio button options: 'Automatically register guest devices' (which is selected) and 'Allow guests to register devices'. Below these options are explanatory text blocks and a link to 'Configure guest types at: Guest Access > Configure > Guest Type'.

エンドポイント デバイス (MAC アドレス) は特定のエンド ポイント グループ (この例の GuestEndpoints) で静的に登録されています。

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an endpoint. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below it are tabs for 'System', 'Identity Management', 'Network Resources', and 'Device Portal Management'. Under 'Identity Management', there are sub-tabs for 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The main content area is titled 'Endpoint List > C0:4A:00:14:6E:31'. It shows the 'Endpoint' configuration for the MAC address C0:4A:00:14:6E:31. The configuration includes: 'Static Assignment' (unchecked), '* Policy Assignment' (Windows7-Workstation), 'Static Group Assignment' (checked), and '* Identity Group Assignment' (GuestEndpoints).

そのグループはこのイメージに示すようにユーザのゲスト型から、得られます。



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: ▾

それが企業ユーザ（識別ストア他のそしてゲスト）ならその設定は門脈設定から得られます。

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: *

その結果ゲストと関連付けられる MAC アドレスはその特定の識別グループに常に属します。それは自動的に変更することができません（たとえばプロファイラー サービスによって）。

注: プロファイラー結果 EndPointPolicy 許可状態を適用することは使用することができます。

デバイスがによってそれに基づいて承認規則を構築することは可能性のあるである特定のエンドポイント識別グループに常に属することをこのイメージに示すように確認します。

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

ユーザが認証されなければ、許可は汎用ルール RedirectToPortal と一致します。ゲスト ポータルおよび認証へのリダイレクションの後で、エンドポイントは特定のエンドポイント識別グループ

プに置かれます。それは第 1 によって、特定の状態使用されます。そのエンド ポイントのすべてのそれ続く認証は最初の承認規則を見つけ、ユーザはゲスト ポータルで再認証する必要なしに提供された完全なネットワーク アクセスです。

ゲスト アカウントのためのエンド ポイント ページ

この状況は永久に持続する可能性があります。しかし ISE 1.3 ページ エンド ポイントで機能性をもたらされました。デフォルト 設定を使って。

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 the Settings menu with options for User Custom Attributes, User Password Policy, and Endpoint Purge. 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 to the list below.

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

ゲスト認証に使用するすべてのエンド ポイントは 30 日以降に取除かれます (エンド ポイント作成から)。その結果通常 30 日ゲストユーザの後でネットワーク ヒット RedirectToPortal 承認規則にアクセスを試みることは認証のためにリダイレクトされ。

注: エンド ポイント パージ機能性はゲスト アカウント パージ ポリシーおよびゲスト アカウント有効期限の依存しないです。

注: ISE 1.2 でエンド ポイントは内部プロファイラー キュー制限を見つけるときだけだけ自動的に取除くことができます。それから最も少なく最近使用されたエンド ポイントは取除かれています。

一時アクセス

ゲスト アクセスにおけるもう一つの方式はゲスト フロー条件を使用することです。

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

条件は ISE およびそのアクティブセッションをチェックしていること属性です。以前にゲストユーザは認証に成功したことをそのセッションに示す属性があったら一致されます調節して下さい。ISE がネットワーク アクセス デバイス (NAD) から Radius アカウンティング停止メッセージを受け取った後、セッションは取除かれる終えられたおよびそれ以降です。それステージ条件ネットワーク アクセス: UseCase = ゲスト フローはもう満たされません。その結果そのエンドポイントのすべてのそれに続く認証はゲスト認証のためにリダイレクトする汎用ルールを見つけます。

注: ユーザがホットスポット ポータルによって認証される時サポートされないゲスト フロー。それらのシナリオに関しては UseCase 属性はゲスト フローの代りにホスト ルックアップに設定されます。

WLC 接続解除動作

クライアントが無線ネットワークから切断された後 (たとえば Windows の Disconnect ボタンを使用して) deauthentication フレームを送信します。しかしそれは WLC で省略され、「デバッグクライアントを使用して xxxx」確認することができます-クライアントが WLAN から切断されているとき WLC はデバッグを示しません。その結果 Windows クライアントで:

- IP アドレスはインターフェイスから削除されます
- インターフェイスは状態にあります: 切られるメディア

しかし WLC でステータスは不変です (走行状態のまだクライアント)。

それは WLC のための計画設計、セッション取除かれます時です

- ユーザアイドルタイムアウト ヒット
- セッション タイムアウト ヒット
- L2 暗号化を使用している、場合 Group 鍵回転間隔が見つかる時
- 何か他のものにより AP/WLC はクライアントをを離れて蹴ります (例えば AP Radio リセットは、誰か WLAN、等をシャットダウンします)

その動作および一時アクセス設定を使ってずっと WLC が決してそれクリアしていないので WLAN セッションからのユーザ切断が ISE から取除かれなかった後 (および決して送信された Radius アカウンティング停止を)。セッションが取除かれない場合、ISE はまだ古いセッションおよびゲスト フロー条件が満足することを覚えています。切断および再接続ユーザの後で再認証すべき要件なしで完全なネットワーク アクセスを持って下さい。

Cisco Identity Services Engine									
Misconfigured Supplicants ⁱ		Misconfigured Network Devices ⁱ				RADIUS Drops ⁱ			
0		0				0			
Show Live Sessions Add or Remove Columns Refresh Reset Repeat Counts									
Time	Status	Det...	Repeat C...	Identity ⁱ	Endpoint ID ⁱ	Authorization Policy	Authorization Profiles	Event ⁱ	
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	

しかし切断ユーザが別の WLAN に接続した後、そして WLC は古いセッションを解決することになります。Radius アカウンティング停止は送信され、ISE はセッションを取除きます。によってフロー条件満足しないおよびクライアントがオリジナル WLAN ゲストに接続することを試みればユーザは認証のためにリダイレクトされます。

注: 管理フレーム保護 (MFP) で設定される WLC は CCXv5 MFP クライアントからの暗号化された deauthentication フレームを受け入れます。

確認

常置アクセス

再認証を誘発する許可 (CoA) のゲスト ポータルおよび認証の成功 ISE 送信変更へのリダイレクションの後。その結果新しい MAC 認証バイパス (MAB) セッションは構築されています。今回エンドポイントは GuestEndpoints 識別グループに属し、一致はフルアクセスの提供を支配します。

Cisco Identity Services Engine									
Misconfigured Supplicants ⁱ		Misconfigured Network Devices ⁱ				RADIUS Drops ⁱ		Client	
0		0				0			
Show Live Sessions Add or Remove Columns Refresh Reset Repeat Counts									
Time	Status	Det...	Repeat C...	Identity ⁱ	Endpoint ID ⁱ	Authorization Policy ⁱ	Authorization Profiles	Network Device	Event ⁱ
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

そのステージ無線ユーザで切り、異なる WLAN に接続し、そして再接続できます。それらのそれらに続く認証はすべて MAC アドレスに基づいて識別を使用しますが特定の識別グループに属するエンドポイントが理由で最初のルールを見つけます。完全なネットワーク アクセスはゲスト認証なしで提供されます。

Time	Status	Det...	Repeat C...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Network Device	Event
2015-08-14 22:28:19...	i		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

一時アクセス

第2シナリオ(ゲストフローに基づく条件が)始まりに関しては同じはあります。

Time	Status	Det...	R...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-08-14 22:34:35...	i		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

しかしセッションがすべてのそれに続く認証のために取除かれた後、ゲストは汎用ルールを見つけ、ゲスト認証のために再度リダイレクトされます。

Time	Status	Det...	R...	Identity	Endpoint ID	Authorization Policy	Authorization Profiles	Event
2015-08-14 22:36:58...	i		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

ゲストはフロー条件によってがある正しい属性がセッションのために存在しているとき満足します。それはエンドポイント属性を検知することによって確認することができます。正常なガス

ト認証の結果は示されません。

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

バグ

[CSCuu41157](#) ISE ENH CoA はゲスト アカウント削除または終止の送信を終えます。

(ゲスト アカウント削除か終止の後でゲスト セッションを終了する機能拡張要求)

参考資料

- [Cisco ISE 1.3 アドミニストレータ ガイド](#)
- [Cisco ISE 1.4 管理者ガイド](#)
- [ISE バージョン 1.3 ホットスポットの設定例](#)
- [ISE バージョン 1.3 の自己登録したゲスト ポータルの設定例](#)
- [WLC と ISE での中央 Web 認証の設定例](#)
- [ISE を搭載した WLC 上で FlexConnect AP を使用した中央 Web 認証の設定例](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)