

配置ISE訪客臨時和永久訪問

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[永久訪問](#)

[訪客帳戶的終端清除](#)

[臨時訪問](#)

[WLC結束通話行為](#)

[驗證](#)

[永久訪問](#)

[臨時訪問](#)

[錯誤](#)

[參考資料](#)

[相關思科支援社群討論](#)

簡介

本文檔介紹身份服務引擎(ISE)訪客訪問配置的不同方法。根據授權規則中的不同條件：

- 可以提供對網路的永久訪問（無需進行後續身份驗證）
- 可以提供對網路的臨時訪問（需要在會話過期後進行訪客身份驗證）

此外，還會結合對臨時存取案例的影響，提供作業階段移除的特定無線LAN控制器(WLC)行為。

必要條件

需求

思科建議您瞭解以下主題：

- ISE部署和訪客流量
- 無線區域網路控制器(WLC)的組態

採用元件

本文中的資訊係根據以下軟體和硬體版本：

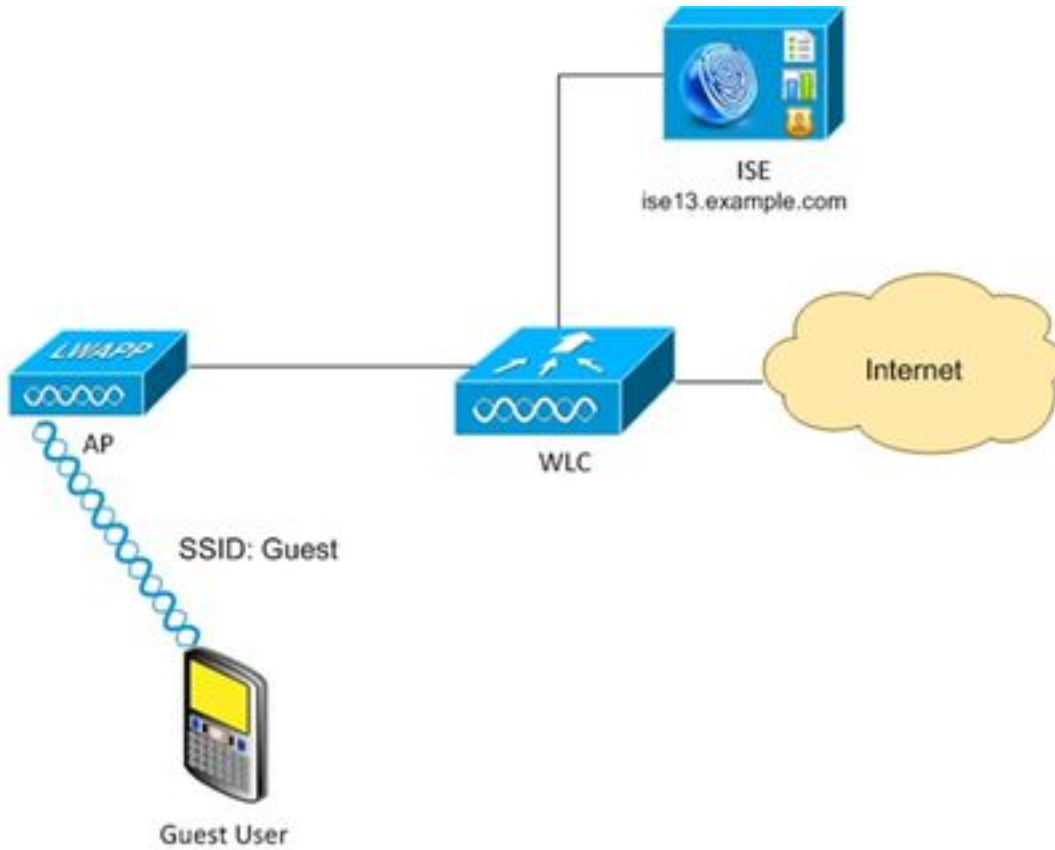
- Microsoft Windows 7
- Cisco WLC版本7.6及更高版本

- ISE軟體1.3版及更高版本

設定

有關基本訪客訪問配置，請通過配置示例檢查參考。本文重點介紹授權規則配置以及授權條件之間的差異。

網路圖表



永久訪問

在啟用了裝置註冊的訪客門戶上成功身份驗證後，對於ISE版本1.3及更高版本。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below it, there 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, there is explanatory text and a link to 'Guest Access > Configure > Guest Type'.

終端裝置 (mac地址) 在特定終端組 (本示例中為GuestEndpoints) 中靜態註冊。

The screenshot displays the Cisco Identity Services Engine (ISE) interface for managing endpoints. The top navigation bar shows 'Home', 'Operations', and 'Policy'. Below it, there 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 > CO:4A:00:14:6E:31'. It shows the 'Endpoint' configuration for the MAC address CO:4A:00:14:6E:31. The configuration includes: 'Static Assignment' (unchecked), '* Policy Assignment' (Windows7-Workstation), 'Static Group Assignment' (checked), and '* Identity Group Assignment' (GuestEndpoints).

該組是從使用者的Guest Type派生的，如下圖所示。

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 ⁽ⁱ⁾
This requires the creation of an authorization policy rule

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration:

如果是企業使用者（身份儲存不是訪客），則該設定是從門戶設定派生的。

The screenshot shows the 'Portal Settings' configuration page in the Cisco Identity Services Engine. The settings are as follows:

- 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)

因此，與訪客關聯的MAC地址始終屬於該特定身份組。不能自動更改（例如Profiler服務）。

附註：若要應用Profiler結果，可使用EndPointPolicy授權條件。

如果知道裝置始終屬於特定終端身份組，則可能基於該身份組構建授權規則，如下圖所示。

The screenshot shows the 'Authorization Policy' configuration page in the Cisco Identity Services Engine. The policy is named 'AuthenticatedGuest' and has the following configuration:

- First Matched Rule Applies:** First Matched Rule Applies
- Exceptions (0):** Standard
- Policy Rules:**

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

使用者未通過身份驗證後，授權將匹配通用規則RedirectToPortal。重定向到訪客門戶並進行身份驗證後，終端被置於特定終端身份組中。這是第一個更具體的情況。該端點的所有後續認證均滿足第一授權規則，並且向使用者提供完全的網路訪問，而無需在訪客門戶上重新進行認證。

訪客帳戶的終端清除

這種情況可能會永遠持續下去。但在ISE 1.3中引入了清除端點功能。使用預設配置。

Endpoint Purge

Define the EndPoint Purge Policy by configuration rules based on identity groups and/or other conditions. Drag and drop rules to change the order. 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

用於訪客身份驗證的所有終端將在30天後刪除（從終端建立）。因此，通常在30天後，嘗試訪問網路的訪客使用者會命中RedirectToPortal授權規則，然後重定向以進行身份驗證。

附註：終端清除功能獨立於訪客帳戶清除策略和訪客帳戶過期。

附註：在ISE 1.2中，只有在達到內部探查器隊列限制時，才能自動刪除端點。然後刪除最近最少使用的終結點。

臨時訪問

訪客訪問的另一種方法是使用訪客流條件。

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
On	AuthenticatedGuest	if (Wireless_MAB AND Network Access:UseCase EQUALS Guest Flow)	then PermitAccess
On	RedirectToPortal	if Wireless_MAB	then GuestPortal

該條件檢查ISE上的活動會話及其屬性。如果該會話具有指示先前訪客使用者已成功通過身份驗證的屬性，則匹配條件。ISE收到來自網路接入裝置(NAD)的Radius記帳停止消息後，會話被終止並隨後刪除。在此階段，不再滿足Network Access:UseCase = Guest Flow的條件。結果，該端點的所有後續驗證都命中通用規則重定向到訪客驗證。

附註： 使用者通過HotSpot門戶進行身份驗證時不支援訪客流。對於這些情況，UseCase屬性設定為Host Lookup而不是Guest Flow。

WLC結束通話行為

客戶端與無線網路斷開連線後（例如，在Windows中使用disconnect按鈕），它會傳送取消身份驗證幀。但是，WLC會省略這一點，可以使用「debug client xxxx」確認這一點 — WLC在客戶端從WLAN斷開連線時不會顯示調試。因此，在Windows客戶端上：

- ip address is removed from the interface
- 介面處於狀態：媒體已斷開連線

但是在WLC上，狀態沒有變更（使用者端仍處於RUN狀態）。

這是WLC的規劃設計，在以下情況下會刪除會話：

- 使用者空閒超時命中數
- session-timeout hits
- 如果使用L2加密，則當組金鑰輪替間隔命中時
- 其他情況會導致AP/WLC關閉客戶端（例如AP無線電重置、有人關閉WLAN等）

使用此行為和使用者從WLAN會話斷開後的臨時訪問配置不會從ISE中刪除，因為WLC從未清除它（並且從未傳送Radius記帳停止）。如果未刪除會話，ISE仍會記住舊會話，並且滿足訪客流條件。斷開連線並重新連線後，使用者無需重新驗證即可獲得完整的網路訪問許可權。

The screenshot displays 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 content area shows 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 several rows of session data, including timestamps, status indicators (green checkmarks), and event descriptions like 'Session State is Started', 'Authorize-Only succeeded', 'Dynamic Authorization succeeded', 'Guest Authentication Passed', and 'Authentication succeeded'.

但是，如果使用者在斷開連線後連線到不同的WLAN，則WLC會決定清除舊作業階段。傳送Radius記帳停止，ISE刪除會話。如果使用者端嘗試連線到原始WLAN Guest Flow條件未獲滿足，系統會將使用者重新導向以進行驗證。

附註： 配置有管理幀保護(MFP)的WLC接受來自CCXv5 MFP客戶端的加密解除身份驗證幀。

驗證

永久訪問

重定向到訪客門戶並成功進行身份驗證後，ISE傳送授權更改(CoA)以觸發重新身份驗證。因此，正在構建新的MAC身份驗證繞行(MAB)會話。此時間終結點屬於GuestEndpoints身份組並匹配提供完全訪問許可權的規則。

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, 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

在此階段，無線使用者可以斷開連線，連線到不同的WLAN，然後重新連線。所有後續身份驗證都使用基於MAC地址的身份，但由於終端屬於特定身份組，而命中了第一個規則。提供完全網路訪問而無需來賓身份驗證。

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, Network Device, and Event. The table contains six rows of session data.

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

臨時訪問

對於第二個方案（條件基於訪客流），開始處相同。

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	CO:4A:00:14:6E:31			Session State is Started
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	CO:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded

但在刪除所有後續身份驗證的會話後，訪客會點選通用規則，然後再次重定向以進行訪客身份驗證。

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	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	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	CO:4A:00:14:6E:31	Default >> RedirectToPortal	GuestPortal	Authentication succeeded

如果會話存在正確的屬性，則滿足訪客流條件。可以通過檢視端點屬性來驗證。指示成功的訪客身份驗證的結果。

Identity Services Engine

Home | Operations | Policy | Guest Access | Admin

System | Identity Management | Network Resources | Device Portal Management | pxGrid Services

Identities | Groups | External Identity Sources | Identity Source Sequences | Settings

Identities

- Users
- Endpoints
- Latest Manual Network Scan Resu...

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

錯誤

[CSCuu41157](#) ISE ENH CoA terminate send on guest account removal or expiry.

(在訪客帳戶刪除或到期後終止訪客會話的增強請求)

參考資料

- [思科ISE 1.3管理員指南](#)
- [思科ISE 1.4管理員指南](#)
- [ISE版本1.3熱點配置示例](#)
- [ISE版本1.3自註冊訪客門戶配置示例](#)
- [WLC 和 ISE 的中央 Web 驗證的組態範例](#)
- [使用ISE的WLC上使用FlexConnect AP進行中央Web身份驗證的配置示例](#)
- [技術支援與文件 - Cisco Systems](#)