身份服務引擎訪客門戶本地Web身份驗證配置示例

目錄

簡介

本檔案介紹如何使用思科身分識別服務引擎(ISE)訪客門戶設定本地Web驗證(LWA)。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- Cisco無線LAN控制器(WLC)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ISE版本1.4

- WLC版本7.4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

本文檔介紹LWA的配置。但是，思科建議您儘可能將集中式Web身份驗證(CWA)與ISE一起使用。LWA是優先選擇還是唯一選擇的情況有幾種，因此這是這些情況的配置示例。

設定

LWA要求在WLC上提供某些前提條件和主要配置，並在ISE上提供一些所需更改。

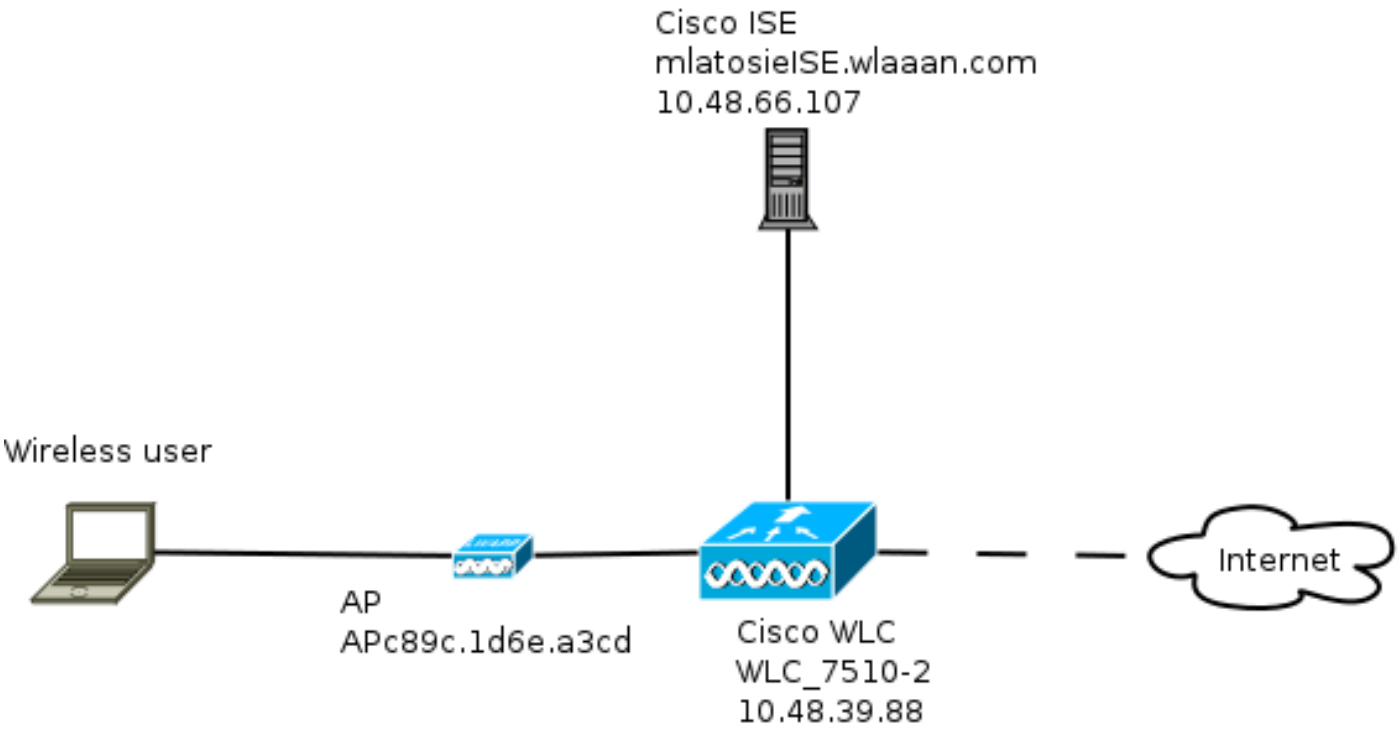
在涵蓋這些內容之前，這裡是ISE的LWA流程概述。

使用ISE訪客門戶的LWA流程

1. 瀏覽器嘗試獲取網頁。
2. WLC會攔截HTTP(S)要求並將其重新導向到ISE。
   HTTP重定向報頭中儲存了若干關鍵資訊。以下是重新導向URL的範例：
   https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9#&ui-state=dialog?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
   從示例URL中，您可以看到使用者嘗試訪問「yahoo.com」。 URL還包含有關無線區域網路(WLAN)名稱(mlatosie_LWA)以及使用者端和存取點(AP)MAC位址的資訊。在範例URL中，**1.1.1.1**是WLC，**mlatosieise.wlaan.com**是ISE伺服器。
3. 使用者會看到ISE訪客登入頁面並輸入使用者名稱和密碼。
4. ISE根據其配置的身份序列執行身份驗證。
5. 瀏覽器再次重新定向。這一次，它向WLC提交憑證。瀏覽器提供使用者在ISE中輸入的使用者名稱和密碼，無需使用者進行任何額外互動。以下是對WLC的GET要求範例。
   獲取
   /login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0
   同樣地，其中還包括原始URL(**yahoo.com**)、使用者名稱(**mlatosie@cisco.com**)和密碼(**ityh**)。
   附註：雖然此處可以看到URL，但實際請求是通過安全套接字層(SSL)（由HTTPS表示）提交的，並且難以攔截。
6. WLC使用RADIUS根據ISE驗證使用者名稱和密碼並允許存取。
7. 系統會將使用者重新導向到指定的入口網站。如需詳細資訊，請參閱本檔案的「**將外部ISE設定為webauth URL**」一節。

網路圖表

下圖描述了本示例中使用的裝置的邏輯拓撲。



配置先決條件

要使LWA流程正常運行，客戶端需要能夠獲得：

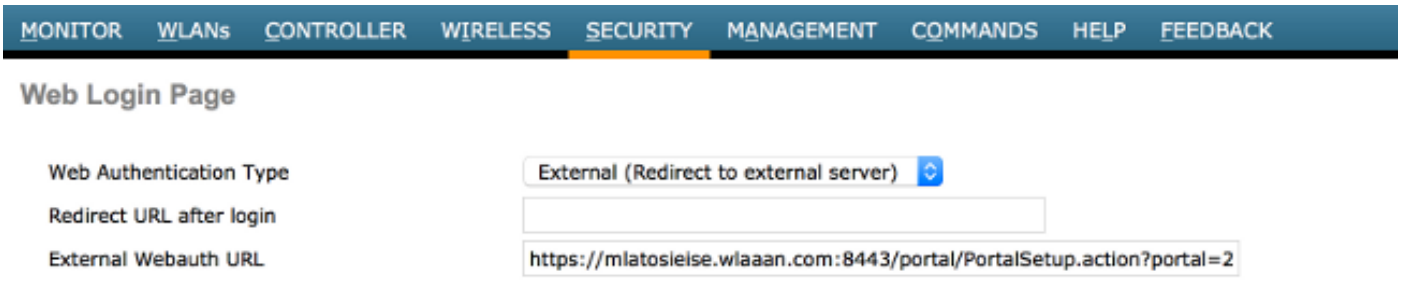
- IP地址和網路掩碼配置
- 預設路由
- 網域名稱系統(DNS)伺服器

所有這些都可以隨DHCP或本地配置一起提供。DNS解析需要正常工作，LWA才能正常工作。

設定WLC

將外部ISE配置為全域性的Webauth URL

在**Security > Web Auth > Web Login Page**下，您可以訪問此資訊。

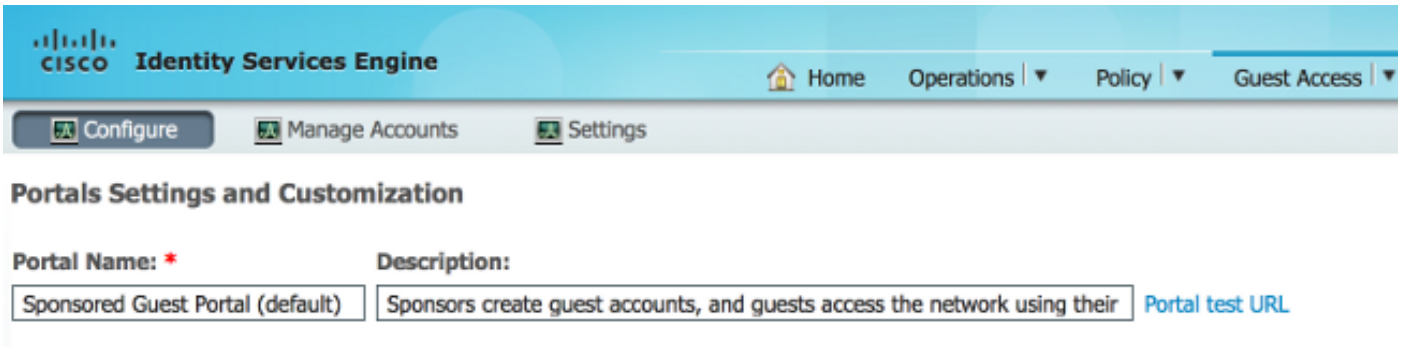


> **附註**：此示例使用外部Webauth URL，取自ISE版本1.4。如果您有不同的版本，請參閱配置指南以瞭解應該配置的內容。

也可以按WLAN配置此設定。它隨後位於特定的WLAN安全設定中。這些將覆蓋全域性設定。

要查詢特定門戶的正確URL，請選擇**ISE > Guest Policy > Configure > your specific portal**。按一下

右鍵「門戶測試URL」中的連結，然後選擇**複製連結位置**。



在此範例中，完整URL為：https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9

設定存取控制清單(ACL)

若要使Web驗證生效，應定義允許的流量。請判斷是應使用FlexConnect ACL還是應使用普通ACL。FlexConnect AP使用FlexConnect ACL，而使用集中交換的AP使用普通ACL。

要瞭解特定AP以何種模式運行，請選擇**Wireless** > Access points，然後選擇**AP name > AP Mode**下拉框。典型的部署是**local**或**FlexConnect**。

在**Security > Access Control Lists**下，選擇**FlexConnect ACL**或**ACLs**。在此示例中，允許所有UDP流量，以便專門允許DNS交換和到ISE的流量(10.48.66.107)。

General

Access List Name	FLEX_GUEST
Deny Counters	634752

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	Any	Any	Any	208398
2	Permit	10.48.66.107 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	32155
3	Permit	0.0.0.0 / 0.0.0.0	10.48.66.107 / 255.255.255.255	TCP	Any	Any	Any	Any	24532

此範例使用FlexConnect，因**此**FlexConnect和標準ACL都已定義。

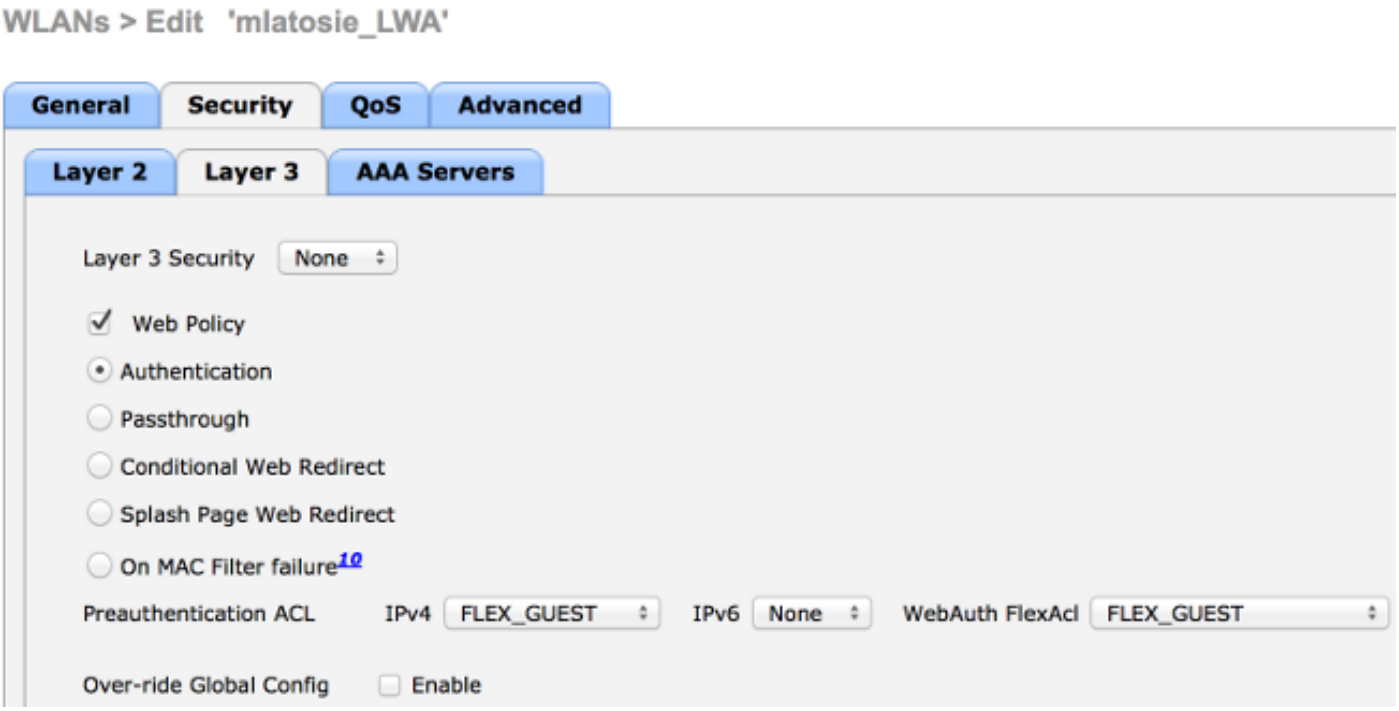
此行為在與WLC 7.4控制器相關的Cisco錯誤ID CSCue68065中記錄。在WLC 7.5上不再需要此功能，因為您只需一個FlexACL，再也不需要標準ACL

為LWA配置服務集識別符號(SSID)

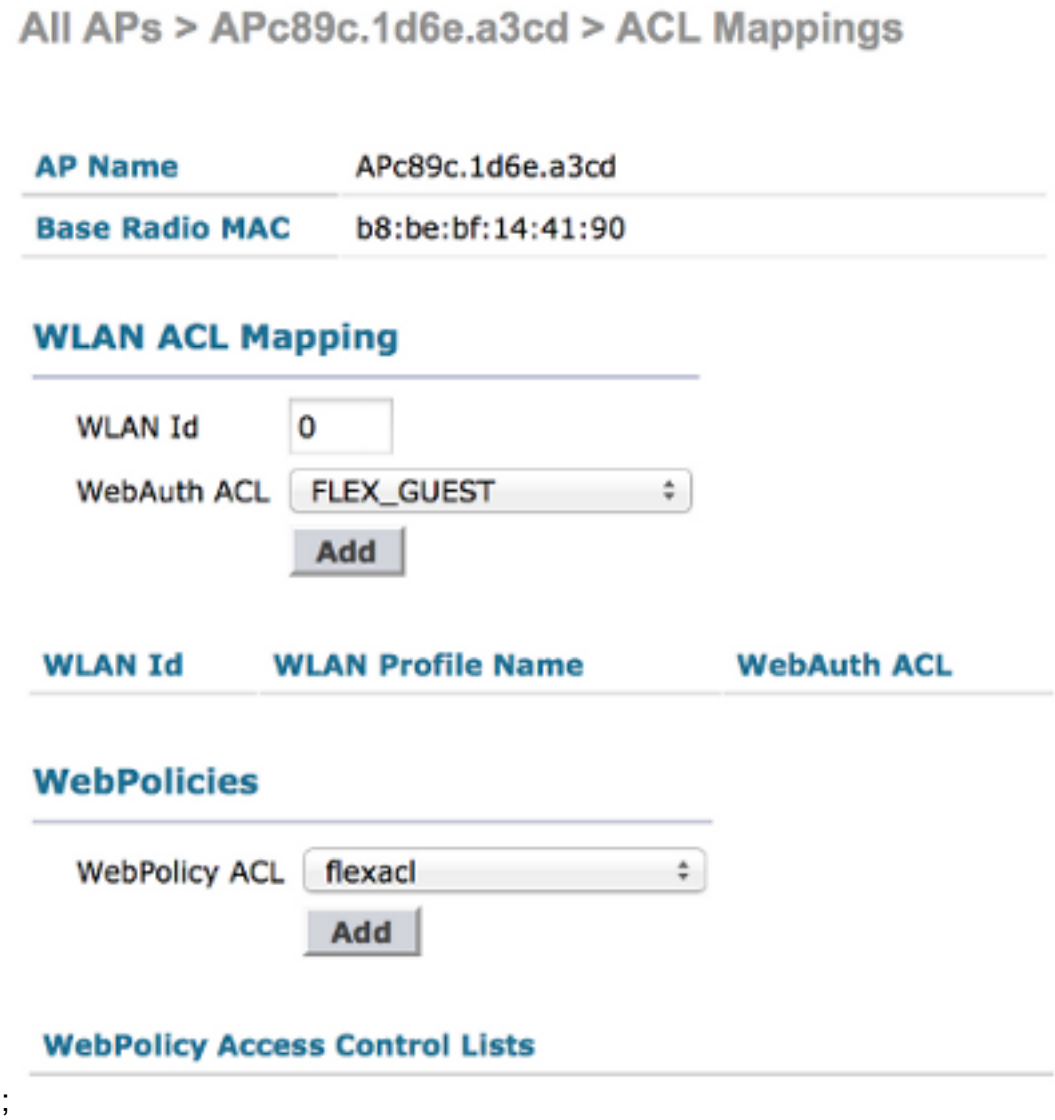
在**WLANs**下，選擇要編輯的**WLAN ID**。

Web Auth組態

套用上一步中定義的相同ACL並啟用Web驗證。



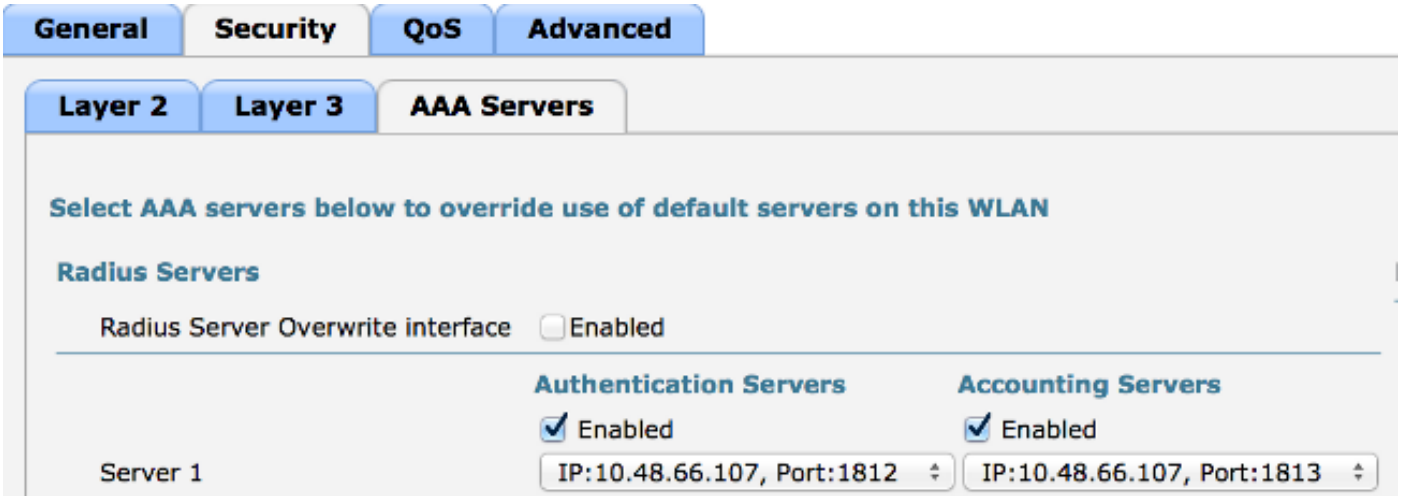
附註：如果使用FlexConnect的本地交換功能，則需要在AP級別上新增ACL對映。可從**Wireless > Access Points**下找到此項。選擇適當的**AP名稱> FlexConnect >外部Web身份驗證ACL**。



;

驗證、授權及記帳(AAA)伺服器組態

在本示例中，身份驗證和記帳伺服器都指向以前定義的ISE伺服器。



附註：Advanced索引標籤下的預設值不需要附加。

配置ISE

ISE配置包含幾個步驟。

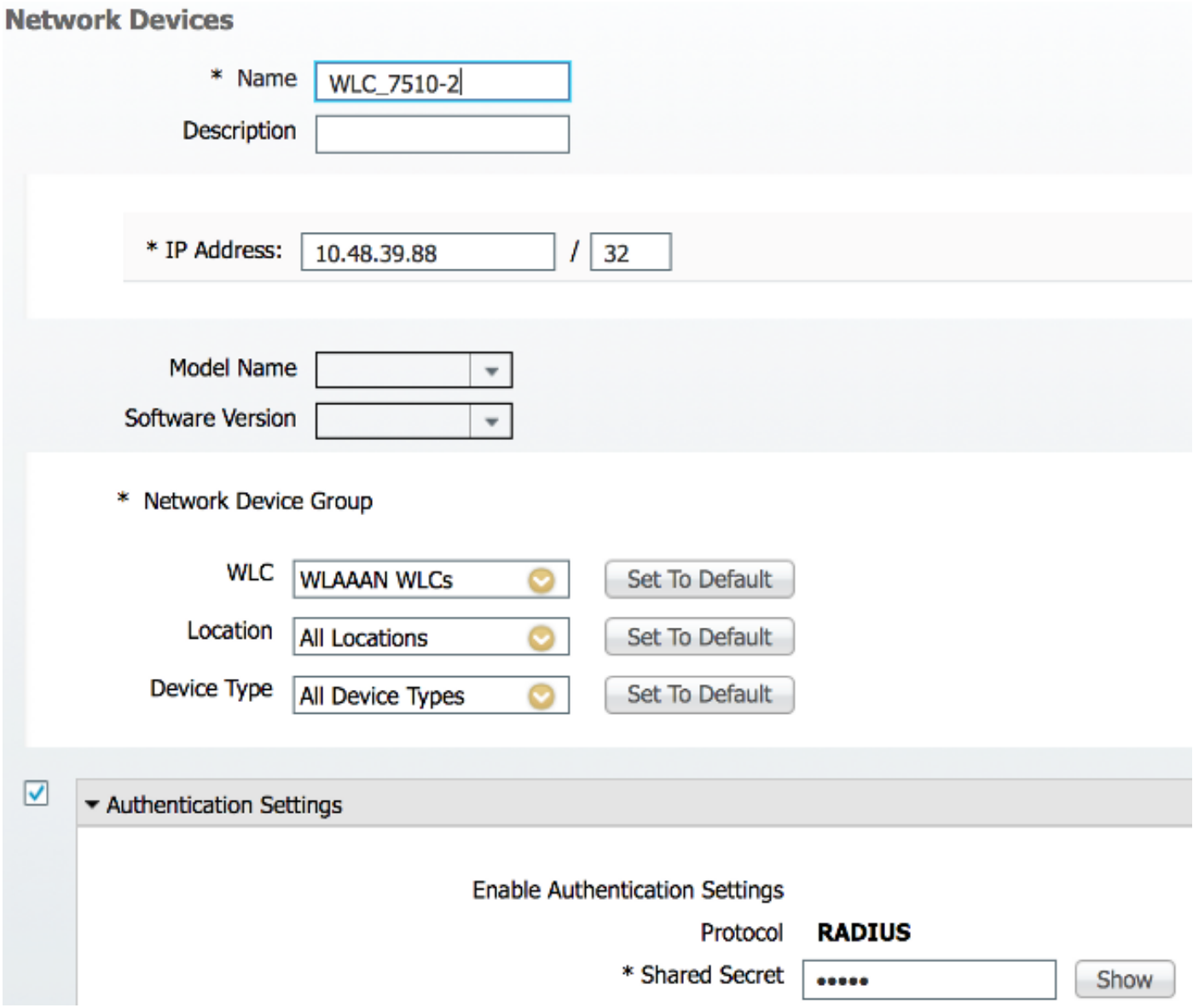
首先，將裝置定義為網路裝置。

然後，確儲存在適用於此交換的身份驗證和授權規則。

定義網路裝置

在Administration > Network Resources > Network Devices下，填充以下欄位：

- 裝置名稱
- 裝置IP地址
- **身份驗證設定>共用金鑰**

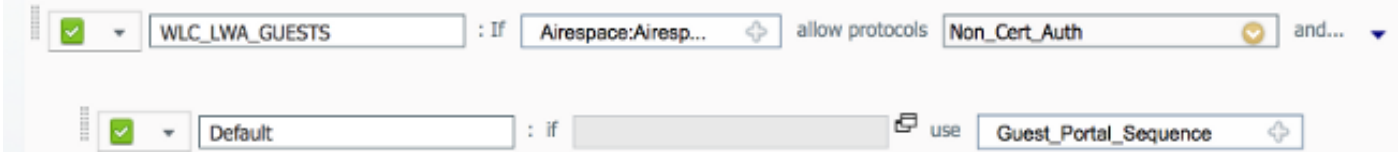


配置身份驗證策略

在**Policy > Authentication**下，新增新的身份驗證策略。

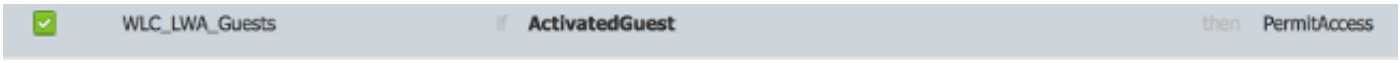
此示例使用以下引數：

- 名稱:**WLC_LWA_Guests**
- 條件： **Airespace:Airespace-Wlan-Id。此條件與先前在WLC上定義的WLAN mlatosie_LWA** ID 3匹配。
- {optional}它允許不需要證書**Non_Cert_Auth**的身份驗證協定，但可以使用預設值。
- Guest_Portal_Sequence，定義使用者是本地定義的訪客使用者。



配置授權策略和結果

在**Policy > Authorization**下定義新策略。它可以是非常基本的策略，例如：

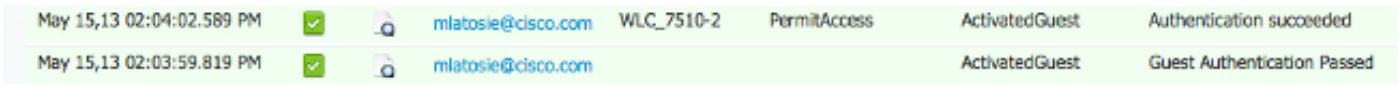


此配置取決於ISE的整體配置。此示例經過有針對性的簡化。

驗證

在ISE上，管理員可以在**Operations > Authentications**下監控即時會話並對其進行故障排除。

應看到兩個身份驗證。第一個身份驗證來自ISE上的訪客門戶。第二個身份驗證是從WLC到ISE的訪問請求。



您可以點選**Authentication Detail Report**圖示以驗證選擇了哪些授權策略和身份驗證策略。

在WLC上，管理員可以在**Monitor > Client**下監**控客戶端**。

以下是正確進行驗證的使用者端範例：

疑難排解

思科建議您儘可能通過客戶端運行調試。

通過CLI，這些調試提供了有用的資訊：

```
debug client MA:CA:DD:RE:SS

debug web-auth redirect enable macMA:CA:DD:RE:SS

debug aaa all enable
```

相關資訊

- 思科ISE 1.x配置指南
- Cisco WLC 7.x配置指南
- 技術支援與文件 - Cisco Systems