

使用交換機和身份服務引擎進行中央Web身份驗證的配置示例

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[概觀](#)

[建立可下載ACL](#)

[建立授權配置檔案](#)

[建立身份驗證規則](#)

[建立授權規則](#)

[啟用IP續訂 \(可選 \)](#)

[交換器組態 \(摘錄 \)](#)

[交換機配置 \(完全 \)](#)

[HTTP Proxy組態](#)

[有關交換機SVI的重要說明](#)

[有關HTTPS重新導向的重要附註](#)

[最終結果](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文說明如何藉助身份服務引擎(ISE)為連線到交換機的有線客戶端配置中央Web身份驗證。

中央Web驗證的概念與本地Web驗證相反，本地Web驗證是交換器本身上的常見Web驗證。在系統中，當dot1x/mab發生故障時，交換機將故障轉移到webauth配置檔案並將客戶端流量重定向到交換機上的網頁。

中央Web驗證提供將中央裝置作為Web門戶 (例如ISE) 的可能性。與通常的本地Web驗證相比，主要區別在於它與mac/dot1x驗證一起被移動到第2層。概念也不同于radius伺服器 (在本範例中為ISE) 返回特殊屬性，以指示交換器必須發生Web重新導向。此解決方案的優勢在於可消除Web驗證啟動所需的任何延遲。從全球範圍看，如果radius伺服器不知道使用者端站台的MAC位址 (但也可使用其他條件)，伺服器會傳回重新導向屬性，且交換器會授權該站 (透過MAC驗證略過[MAB])，但會放置存取清單，將Web流量重新導向入口網站。使用者登入到訪客門戶後，可以通過CoA (授權更改) 退回交換機埠，以便進行新的第2層MAB身份驗證。然後ISE會記住它是webauth使用者並向該使用者應用第2層屬性 (如動態VAN分配)。ActiveX元件還可以強制客戶端PC刷新其IP地址。

必要條件

需求

思科建議您瞭解以下主題：

- 身分識別服務引擎 (ISE)
- Cisco IOS®^{交換器}配置

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎(ISE)版本1.1.1
- 執行軟體版本12.2.55SE3的Cisco Catalyst 3560系列交換器

附註：其他Catalyst交換器型號的步驟相似或相同。您可以對Catalyst的所有Cisco IOS軟體版本使用這些步驟，除非另有說明。

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。

設定

概觀

ISE配置由以下五個步驟組成：

1. [建立可下載存取控制清單\(ACL\)](#)。
2. [建立授權配置檔案](#)。
3. [建立身份驗證規則](#)。
4. [建立授權規則](#)。
5. [啟用IP續訂（可選）](#)。

建立可下載ACL

這不是強制步驟。通過中央webauth設定檔傳回的重新導向ACL會判斷哪些流量（HTTP或HTTPS）重新導向到ISE。可下載ACL允許您定義允許哪些流量。您通常應該允許DNS、HTTP(S)和8443，並拒絕其餘情況。否則，交換器會重新導向HTTP流量，但允許其他通訊協定。

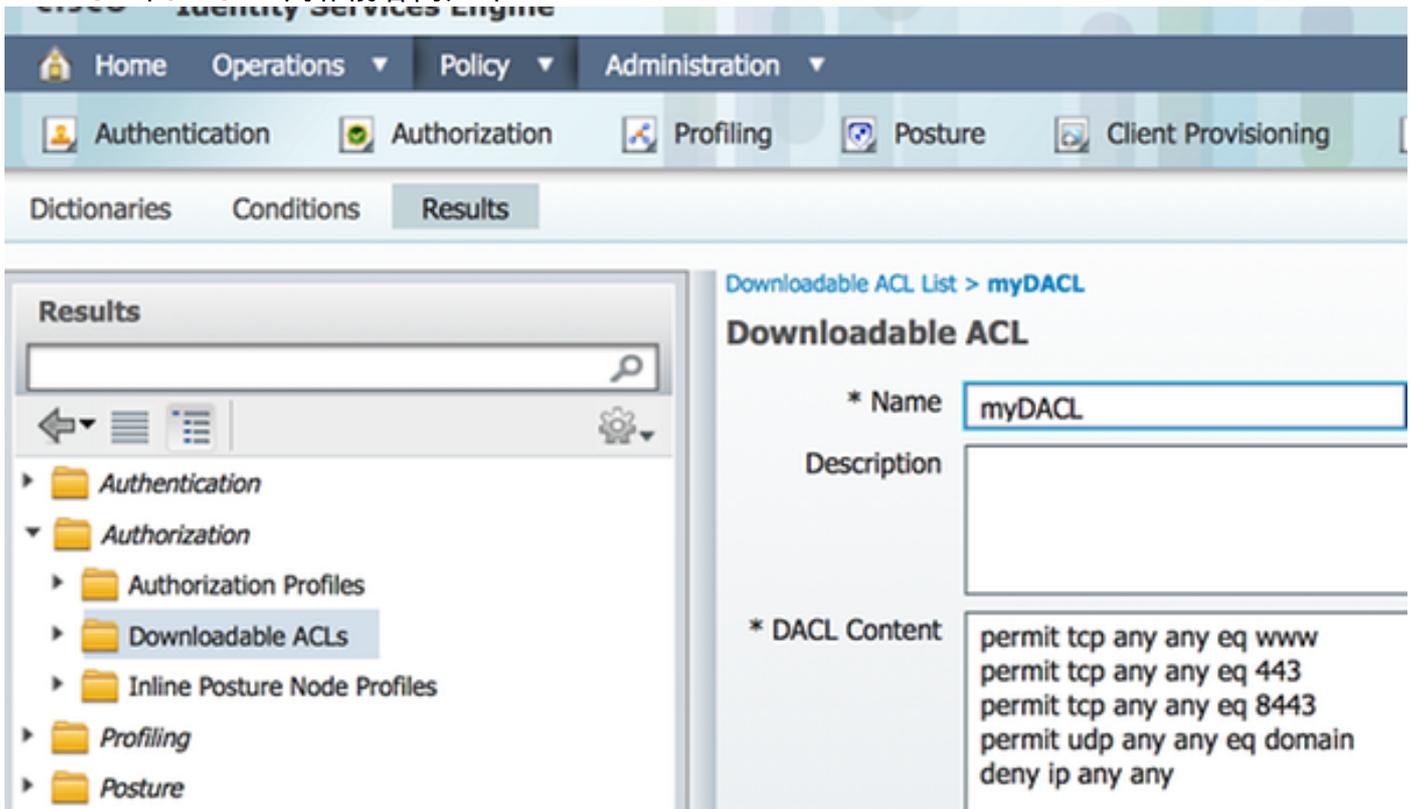
完成以下步驟即可建立可下載ACL：

1. 按一下**Policy**，然後按一下**Policy Elements**。
2. 按一下「**Results**」。
3. 展開**Authorization**，然後按一下**Downloadable ACLs**。
4. 按一下**Add**按鈕以建立一個新的可下載ACL。
5. 在**Name**欄位中，輸入DAACL的名稱。此範例使用**myDAACL**。

此圖顯示典型的DAACL內容，允許：

- DNS — 解析ISE門戶主機名

- HTTP和HTTPS — 允許重定向
- TCP埠8443 — 用作訪客門戶埠

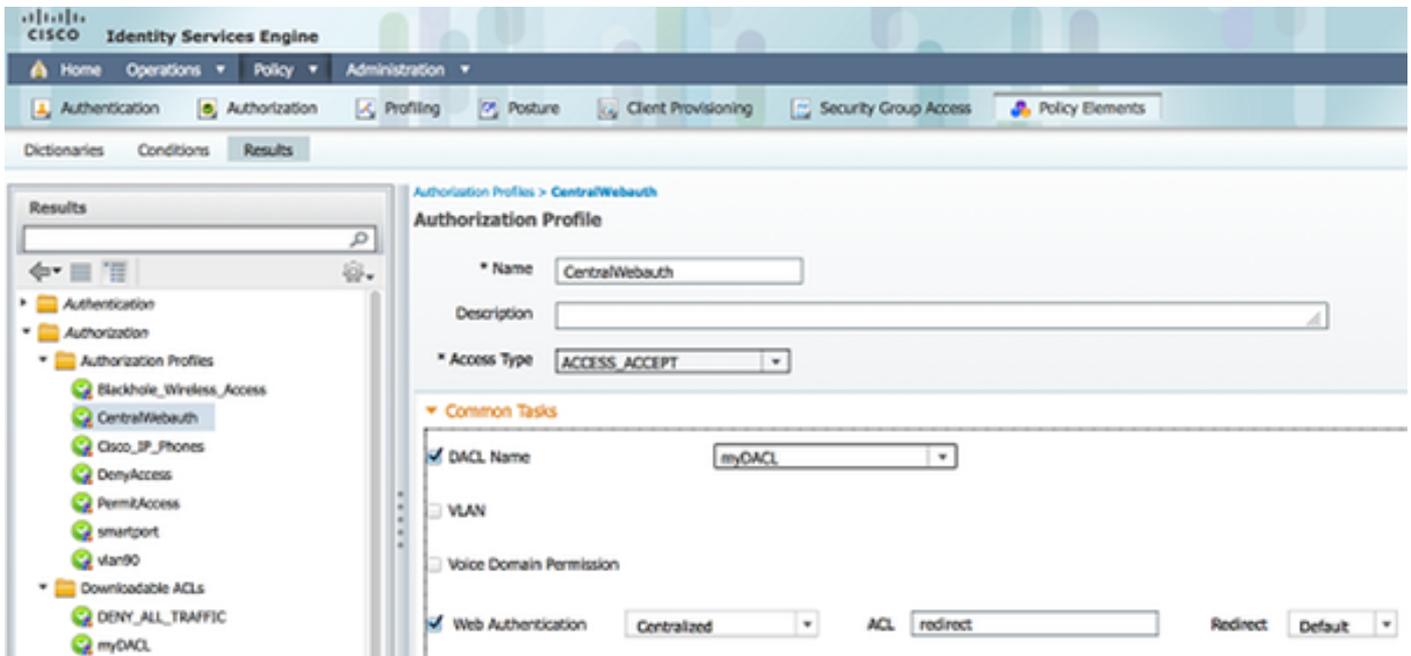


建立授權配置檔案

完成以下步驟以建立授權配置檔案：

1. 按一下**Policy**，然後按一下**Policy Elements**。
2. 按一下「**Results**」。
3. 展開**Authorization**，然後按一下**Authorization profile**。
4. 按一下**Add**按鈕，為中央webauth建立一個新的授權設定檔。
5. 在「**Name**」欄位中，輸入設定檔的名稱。此範例使用 *CentralWebauth*。
6. 從Access Type下拉選單中選擇**ACCESS_ACCEPT**。
7. 選中**Web Authentication**覈取方塊，然後從下拉選單中選擇**Centralized**。
8. 在ACL欄位中，輸入交換器上ACL的名稱，該名稱會定義要重新導向的流量。此範例使用 *redirect*。
9. 從Redirect下拉選單中選擇**Default**。
10. 如果決定在交換器上使用DACL而不是靜態連線埠ACL，請勾選**DACL**名稱，然後從下拉式清單中選擇**myDACL**。

Redirect屬性定義ISE看到預設Web門戶還是ISE管理員建立的自定義Web門戶。例如，此範例中的 *redirect* ACL會在從使用者端到任何位置的HTTP或HTTPS流量上觸發重新導向。ACL是在此配置示例稍後的交換機上定義的。

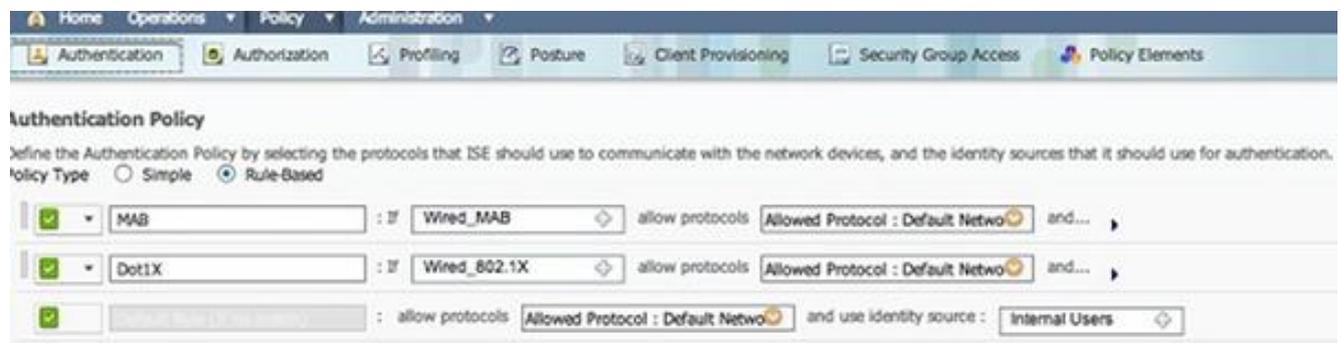


建立身份驗證規則

完成以下步驟，即可使用驗證設定檔建立驗證規則：

1. 在Policy (策略) 選單下，按一下**Authentication**。

此圖顯示如何配置身份驗證策略規則的示例。在此示例中，配置了一個在檢測到MAB時觸發的規則。



2. 輸入身份驗證規則的名稱。本示例使用**MAB**。
3. 在If條件欄位中選擇加號(+)圖示。
4. 選擇**複合條件**，然後選擇**Wired_MAB**。
5. 按一下位於**和...**旁邊的**箭頭**，以進一步擴展規則。
6. 按一下Identity Source欄位中的**+**圖示，然後選擇**Internal endpoints**。
7. 從「If user not found」下拉選單中選擇**Continue**。

此選項允許通過webauth對裝置進行身份驗證（即使裝置的MAC地址未知）。Dot1x使用者端仍可以使用其憑證進行驗證，因此不應關注此組態。

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should

Policy Type Simple Rule-Based

Internal Endpoints

Identity Source: Internal Endpoints

Options

If authentication failed: Reject

If user not found: Continue

If process failed: Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

建立授權規則

現在，在授權策略中有幾個規則需要配置。當PC接通電源時，它會通過MAB;假設不知道MAC位址，因此傳回webauth和ACL。此MAC未知規則顯示在此映像中，並在本節中配置：

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	2nd AUTH	if Network Access:UseCase EQUALS Guest Flow	then vlan90
<input checked="" type="checkbox"/>	IS-a-GUEST	if IdentityGroup:Name EQUALS Guest	then PermitAccess
<input checked="" type="checkbox"/>	MAC not known	if Network Access:AuthenticationStatus EQUALS UnknownUser	then CentralWebAuth

完成以下步驟以建立授權規則：

1. 建立新規則並輸入名稱。此示例使用未知的MAC。
2. 按一下條件欄位中的加號(+)圖示，並選擇建立新條件。
3. 展開expression下拉選單。
4. 選擇Network Access，然後展開它。
5. 按一下AuthenticationStatus，然後選擇Equals運算子。
6. 在右側欄位中選擇UnknownUser。
7. 在General Authorization頁面上，選擇Authorization Profile(Authorization Profile)(位於單詞右側)。

即使使用者 (或MAC) 未知，此步驟也允許ISE繼續。

現在，登入頁面將顯示未知使用者。但是，一旦他們輸入憑證，他們就會再次在ISE上收到身份驗證請求；因此，如果使用者是訪客使用者，則必須使用滿足的條件配置另一個規則。在本示例中，如果使用UseridentityGroup equals Guest，則假定所有來賓均屬於此組。

8. 按一下位於MAC未知規則結尾的操作按鈕，然後選擇在上方插入新規則。

附註：此新規則位於MAC未知規則之前非常重要。

9. 輸入新規則的名稱。此範例使用IS-a-GUEST。
10. 選擇與訪客使用者匹配的條件。

此示例使用InternalUser:IdentityGroup Equals Guest，因為所有訪客使用者都繫結到Guest組

(或您在發起人設定中配置的另一個組)。

11. 在結果框 (然後位於單詞右側) 中選擇**PermitAccess**。

當使用者在Login頁面上獲得授權時，ISE在交換機埠上重新啟動第2層身份驗證，然後出現新的MAB。在此場景中，不同之處在於，為ISE設定了不可見標誌，以記住它是訪客身份驗證使用者。此規則是第2次AUTH，條件是*Network Access:UseCase Equals GuestFlow*。使用者透過webauth進行驗證，且交換器連線埠重新設定為新的MAB時，就會符合此條件。可以指定任何您喜歡的屬性。此示例分配一個配置檔案vlan90，以便使用者在其第二個MAB身份驗證中分配了VLAN 90。

12. 按一下**Actions** (位於IS-a-GUEST規則末尾)，然後選擇**Insert new rule above**。

13. 在名稱欄位中輸入**2nd AUTH**。

14. 在條件欄位中，按一下加號(+)圖示，然後選擇建立新條件。

15. 選擇**Network Access**，然後按一下**UseCase**。

16. 選擇**Equals**作為運算子。

17. 選擇**GuestFlow**作為正確的運算元。

18. 在授權頁面上，點選加號(+)圖示(位於*then*旁邊)，為您的規則選擇結果。

在本範例中，已指派預先設定的設定檔(vlan90);本檔案沒有顯示此組態。

您可以選擇**Permit Access**選項或建立自定義配置檔案以返回您喜歡的VLAN或屬性。

啟用IP續訂 (可選)

如果分配VLAN，最後一步是客戶端PC更新其IP地址。此步驟由Windows客戶端的訪客門戶實現。如果您之前沒有為第2個AUTH規則設定VLAN，則可以跳過此步驟。

如果您分配了VLAN，請完成以下步驟以啟用IP續訂：

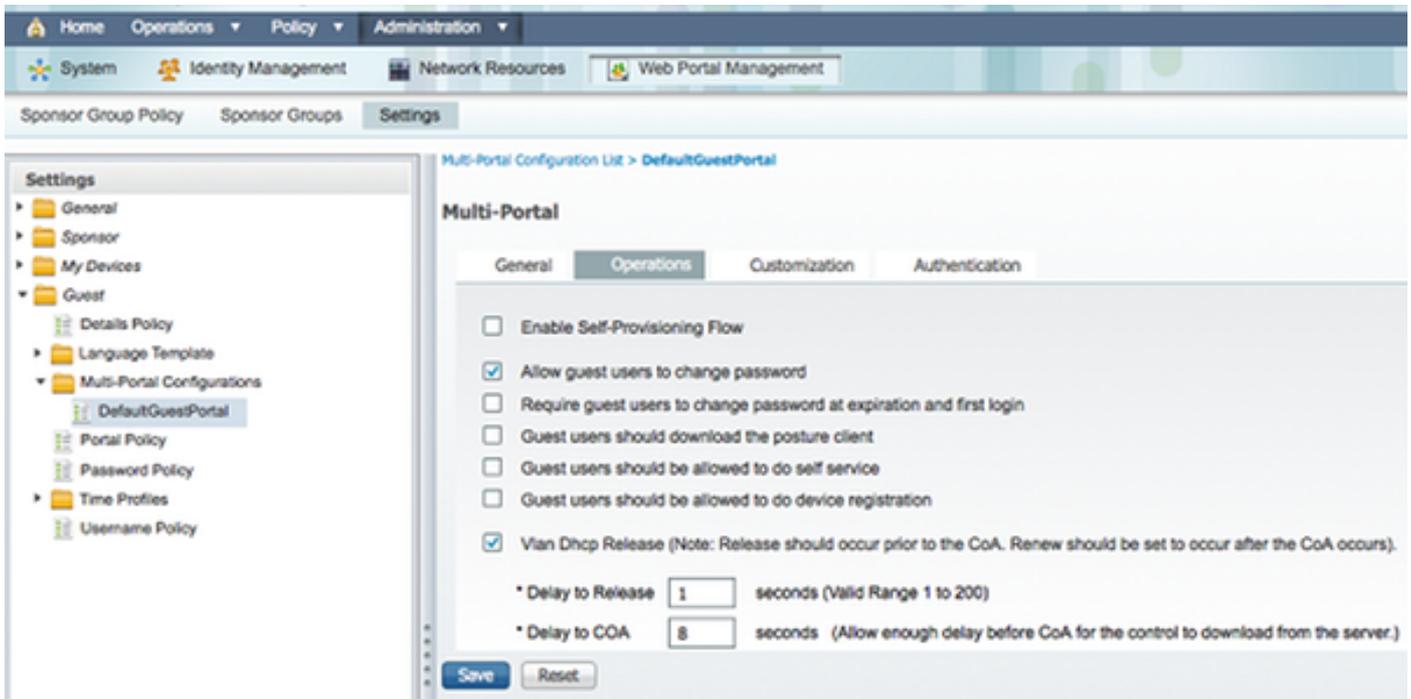
1. 按一下**Administration**，然後按一下**Guest Management**。

2. 按一下「**Settings**」。

3. 展開**Guest**，然後展開**Multi-Portal Configuration**。

4. 按一下**DefaultGuestPortal**或您可能已建立的自定義門戶的名稱。

5. 按一下**Vlan DHCP 釋放覈取方塊**。 **附註**：此選項僅適用於Windows客戶端。



交換器組態 (摘錄)

本節簡短介紹交換器組態。如需完整組態，請參閱[交換器組態 \(完整 \)](#)。

此示例顯示一個簡單的MAB配置。

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

VLAN 100是提供完全網路連線的VLAN。應用並定義預設連線埠ACL(命名為*webauth*)，如下所示：

```
ip access-list extended webauth
permit ip any any
```

此範例組態會提供完整網路存取許可權，即使使用者未通過驗證；因此，您可能希望限制未經驗證的使用者訪問。

在此配置中，HTTP和HTTPS瀏覽在沒有身份驗證（根據其他ACL）的情況下無法運行，因為ISE配置為使用重定向ACL(命名重定向)。交換器上的定義如下：

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

必須在交換器上定義此存取清單，才能定義交換器會在哪些流量上執行重新導向。(在*permit*中匹配。) 在本範例中，使用者端傳送的任何HTTP或HTTPS流量都會觸發Web重新導向。此範例也會拒絕

ISE IP位址，因此到ISE的流量會進入ISE，而不會在循環中重新導向。(在此案例中，deny不會封鎖流量；它只是不會重定向流量。) 如果您使用異常的HTTP埠或Proxy，則可以新增其他埠。

另一種可能性是允許HTTP訪問某些網站並重定向其他網站。例如，如果您在ACL中定義僅允許內部Web伺服器，則使用者端可以在未驗證的情況下瀏覽Web，但會在嘗試存取內部Web伺服器時遭遇重新導向。

最後一步是在交換機上允許CoA。否則，ISE無法強制交換機重新驗證客戶端。

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

交換器需要以下命令才能根據HTTP流量重新導向：

```
ip http server
```

根據HTTPS流量重新導向需要以下命令：

```
ip http secure-server
```

這些命令也很重要：

```
radius-server vsa send authentication
radius-server vsa send accounting
```

如果使用者尚未通過驗證，則**show authentication session int <interface num>**傳回以下輸出：

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address: 000f.b049.5c4b
    IP Address: 192.168.33.201
    User-Name: 00-0F-B0-49-5C-4B
    Status: Authz Success
    Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
ACS ACL: xACSACLx-IP-myDACL-51519b43
URL Redirect ACL: redirect
URL Redirect: https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
Session timeout: N/A
Idle timeout: N/A
Common Session ID: C0A82102000002D8489E0E84
Acct Session ID: 0x000002FA
Handle: 0xF60002D9
```

Runnable methods list:

```
Method   State
mab      Authc Success
```

附註：儘管成功進行MAB身份驗證，但重定向ACL是因為ISE不知道該MAC地址。

交換機配置 (完全)

本節列出完整的交換機配置。省略了一些不必要的介面和命令列；因此，此示例配置應僅供參考，不應複製。

Building configuration...

```
Current configuration : 6885 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$xqtx$VPsZHbpGmLyH/EOObPpla.
!
aaa new-model
!
!
aaa group server radius newGroup
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization exec default none
aaa authorization network default group radius
!
!
!
!
aaa server radius dynamic-author
client 192.168.131.1 server-key cisco
!
aaa session-id common
clock timezone CET 2 0
system mtu routing 1500
vtp interface Vlan61
udld enable

nmosp enable
ip routing
ip dhcp binding cleanup interval 600
!
!
ip dhcp snooping
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-1351605760
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1351605760
revocation-check none
rsa-keypair TP-self-signed-1351605760
!
!
crypto pki certificate chain TP-self-signed-1351605760
certificate self-signed 01
```

30820245 308201AE A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31333531 36303537 3630301E 170D3933 30333031 30303033
35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33353136
30353736 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B068 86D31732 E73D2FAD 05795D6D 402CE60A B93D4A88 C98C3F54 0982911D
D211EC23 77734A5B 7D7E5684 388AD095 67354C95 92FD05E3 F3385391 8AB9A866
B5925E04 A846F740 1C9AC0D9 6C829511 D9C5308F 13C4EA86 AF96A94E CD57B565
92317B2E 75D6AB18 04AC7E14 3923D3AC 0F19BC6A 816E6FA4 5F08CDA5 B95D334F
DA410203 010001A3 6D306B30 0F060355 1D130101 FF040530 030101FF 30180603
551D1104 11300F82 0D69696C 796E6173 2D333536 302E301F 0603551D 23041830
16801457 D1216AF3 F0841465 3DDDD4C9 D08E06C5 9890D530 1D060355 1D0E0416
041457D1 216AF3F0 8414653D DDD4C9D0 8E06C598 90D5300D 06092A86 4886F70D
01010405 00038181 0014DC5C 2D19D7E9 CB3E8ECE F7CF2185 32D8FE70 405CAA03

```
dot1x system-auth-control
dot1x critical eapol
!
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
!
spanning-tree mode pvst
spanning-tree logging
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-200 priority 24576
!
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
!
interface FastEthernet0/2
switchport access vlan 33
switchport mode access
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
!
interface Vlan33
ip address 192.168.33.2 255.255.255.0
!
ip default-gateway 192.168.33.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.33.1
!
ip access-list extended MY_TEST
permit ip any any
ip access-list extended redirect
deny ip any host 192.168.131.1
permit tcp any any eq www
permit tcp any any eq 443
ip access-list extended webAuthList
permit ip any any
```

```
!  
ip sla enable reaction-alerts  
logging esm config  
logging trap warnings  
logging facility auth  
logging 10.48.76.31  
snmp-server community c3560public RO  
snmp-server community c3560private RW  
snmp-server community private RO  
radius-server host 192.168.131.1 auth-port 1812 acct-port 1813 key cisco  
radius-server vsa send authentication  
radius-server vsa send accounting  
!  
!  
!  
privilege exec level 15 configure terminal  
privilege exec level 15 configure  
privilege exec level 2 debug radius  
privilege exec level 2 debug aaa  
privilege exec level 2 debug  
!  
line con 0  
line vty 0 4  
exec-timeout 0 0  
password Ciscol23  
authorization commands 1 MyTacacs  
authorization commands 2 MyTacacs  
authorization commands 15 MyTacacs  
authorization exec MyTacacs  
login authentication MyTacacs  
line vty 5 15  
!  
ntp server 10.48.76.33  
end
```

HTTP Proxy組態

如果對使用者端使用HTTP Proxy，則表示使用者端：

- 為HTTP協定使用非常規埠
- 將所有流量傳送到代理

要使交換機偵聽非常規埠（例如8080），請使用以下命令：

```
ip http port 8080  
ip port-map http port 8080
```

您還需要配置所有客戶端以繼續使用它們的代理，但不使用ISE IP地址的代理。所有瀏覽器都包含一項功能，允許您輸入不應使用代理的主機名或IP地址。如果沒有為ISE新增例外，則會遇到循環身份驗證頁面。

您還需要修改您的重新導向ACL，以便在代理連線埠（此範例中的是8080）上允許。

有關交換機SVI的重要說明

目前，交換器需要交換器虛擬介面(SVI)以回覆使用者端，並將網路入口重新導向傳送至使用者端。此SVI不必位於客戶端子網/VLAN上。但是，如果交換機在客戶端子網/VLAN中沒有SVI，則必須使用任何其他SVI並傳送客戶端路由表中定義的流量。這通常表示流量會傳送到網路核心中的另一個閘道；此流量返回客戶端子網內的接入交換機。

防火牆通常會封鎖進出同一交換器的流量（在此案例中），因此重新導向可能無法正常運作。解決方法是在防火牆上允許此行為，或在客戶端子網中的接入交換機上建立SVI。

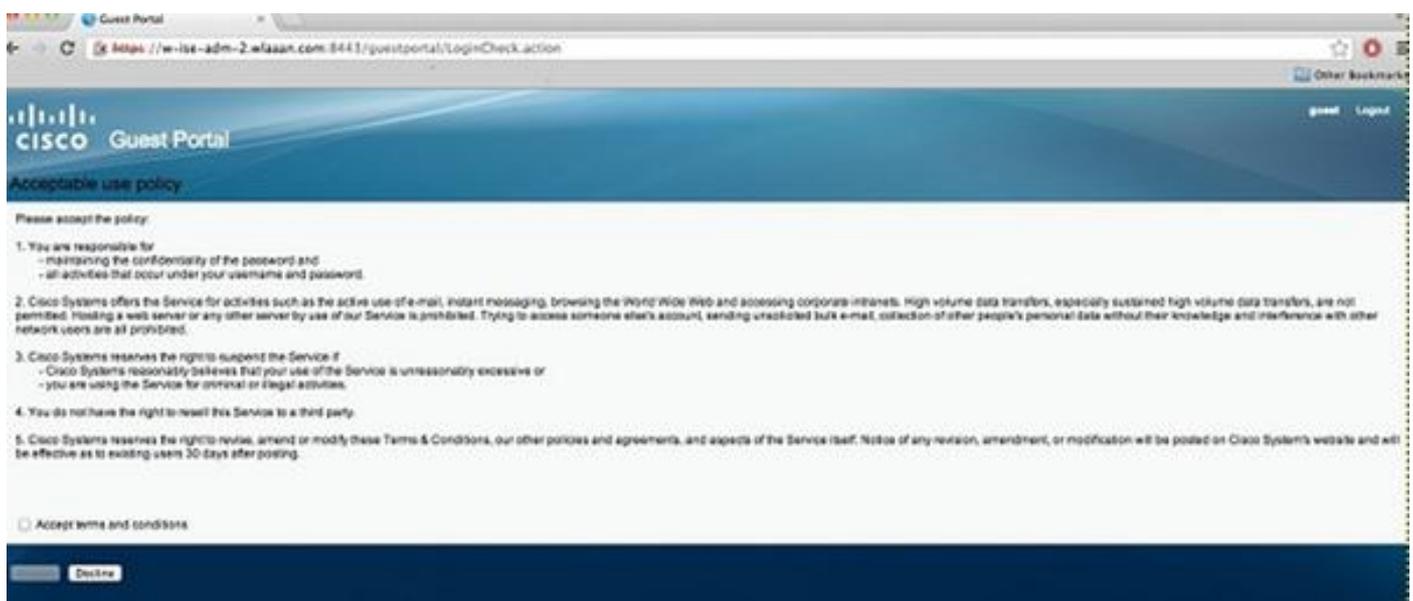
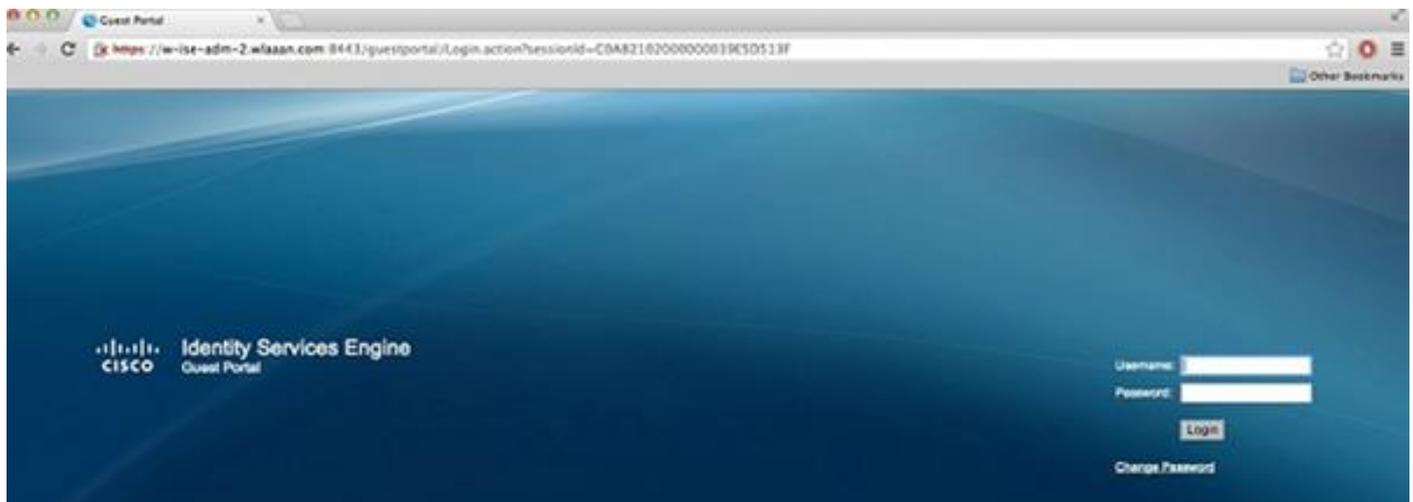
有關HTTPS重新導向的重要附註

交換器能夠重新導向HTTPS流量。因此，如果訪客使用者端有以HTTPS形式提供的首頁，則重新導向會正確執行。

重新導向的整個概念是基於一個裝置（在本例中為交換器）欺騙網站的IP地址。但是，當交換機攔截和重定向HTTPS流量時，將產生一個主要問題，因為交換機在傳輸層安全(TLS)握手中只能顯示自己的證書。由於此證書與最初請求的網站不同，大多數瀏覽器會發出重大警報。瀏覽器會出於安全考慮，正確處理另一個憑證的重新導向和呈現。沒有解決此問題的方法，交換機也無法偽裝您的原始網站證書。

最終結果

客戶端PC插入並執行MAB。MAC地址未知，因此ISE將重定向屬性推回交換機。使用者嘗試前往網站，且已重新導向。



當登入頁面的身份驗證成功時，ISE通過授權更改退回交換機埠，再次開始第2層MAB身份驗證。

但是，ISE知道它是以前的webauth客戶端，並根據webauth憑證授權客戶端（雖然這是第2層身份

驗證)。

在ISE身份驗證日誌中，MAB身份驗證顯示在日誌底部。雖然未知，但已對MAC地址進行身份驗證和效能分析，並返回webauth屬性。接下來，使用使用者的使用者名稱（即，使用者在登入頁面中鍵入其憑據）進行身份驗證。身份驗證後，立即進行新的第2層身份驗證，將使用者名稱用作憑據；在此驗證步驟中，您可以返回諸如動態VLAN之類的屬性。

Mar 26,13 04:58:43.572 PM	✔	🔒	Nico	00:0F:80:49:5C:48	Nicowitch	FastEthernet0/3	Vlan90	Guest	NotApplicable	
Mar 26,13 04:58:43.445 PM	✔	🔒			Nicowitch				Dynamic Author...	
Mar 26,13 04:58:43.438 PM	✔	🔒	Nico	00:0F:80:49:5C:48				Guest	Guest Authentic...	
Mar 26,13 04:58:37.900 PM	✔	🔒	#ACSACL#-3P-myDAC		celine				DACL Download...	
Mar 26,13 04:58:36.995 PM	✔	🔒		00:1A:6C:7B:56:0E	00:1A:6C:7B:56:0E	celine	GigabitEthernet2/0/10	CentralWebauth	Pending	Authentication ...

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [思科身分識別服務引擎](#)
- [思科身份服務引擎命令參考指南](#)
- [ISE \(身份服務引擎\) 與Cisco WLC \(無線LAN控制器\) 的整合](#)
- [要求建議 \(RFC\)](#)
- [技術支援與文件 - Cisco Systems](#)