

スイッチおよび Identity Services Engine を使用した中央 Web 認証の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[概要](#)

[ダウンロード可能な ACL の作成](#)

[認可プロファイルの作成](#)

[認証ルールの作成](#)

[認可ルールの作成](#)

[IP 更新の有効化 \(オプション \)](#)

[スイッチの設定 \(抜粋 \)](#)

[スイッチの設定 \(すべての設定 \)](#)

[HTTP プロキシ設定](#)

[SVI スイッチに関する重要な注意事項](#)

[HTTPS リダイレクションに関する重要な注意事項](#)

[最終結果](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、スイッチに接続された有線クライアントと Identity Services Engine (ISE) を使用して、中央 Web 認証を設定する方法について説明しています。

中央 Web 認証とは、通常の Web 認証で使用される、スイッチ自体でのローカル Web 認証に対するものです。dot1x/mab 障害の発生時に、スイッチが webauth プロファイルにフェールオーバーし、クライアントのトラフィックがスイッチ上の Web ページにリダイレクトされます。

中央 Web 認証はウェブ ポータルとして機能する中央デバイスがあるために可能性を提供します (Th で例は、ISE あります)。通常のローカル Web 認証との主な相違点は、mac/dot1x 認証に伴ってレイヤ 2 にシフトされることです。また、RADIUS サーバ (この例では ISE) が、スイッチに対して Web リダイレクションの必要性を指示する特別な属性を返す点も異なります。このソリューションには、Web 認証の開始に必要なであった遅延を解消するという利点があります。全体の流れとしては、RADIUS サーバでクライアント ステーションの MAC アドレスが不明であるが、他の基準も使用できる場合に、サーバはリダイレクション属性を返します。スイッチは (MAC 認証バイパス (MAB) 経由で) 当該ステーションを許可しますが、同時にアクセス リストを適用して Web トラフィックをポータルにリダイレクトします。ユーザがゲスト ポータルにログインした後、CoA (認可変更) によってスイッチ ポートを復帰させて、新しいレイヤ 2 MAB 認証を開始できます。この後、ISE はそれが webauth ユーザであることを記憶し、そのユーザに

レイヤ 2 属性 (ダイナミック VLAN 割り当てなど) を適用できます。 ActiveX コンポーネントを使用して、クライアント PC で IP アドレスを強制的に更新することもできます。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Identity Services Engine (ISE)
- Cisco IOS[®] スイッチ設定

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。

- Cisco Identity Services Engine (ISE)、リリース 1.1.1
- ソフトウェアバージョン 12.2.55SE3 が稼働する Cisco Catalyst 3560 シリーズ スイッチ

注: プロシージャは他の Catalyst スイッチ モデルのために類似したまたは同一です。 Catalyst のためにすべての Cisco IOS ソフトウェア リリースのこれらのステップを特に明記しない限り使用できます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

概要

ISE の設定は、次の 5 段階の手順で実行します。

1. [ダウンロード可能なアクセス コントロール リスト \(ACL \) を作成します。](#)
2. [許可プロファイルを作成します。](#)
3. [認証ルールを作成します。](#)
4. [許可ルールを作成します。](#)
5. [IP 更新を有効化します \(オプション \) 。](#)

ダウンロード可能な ACL の作成

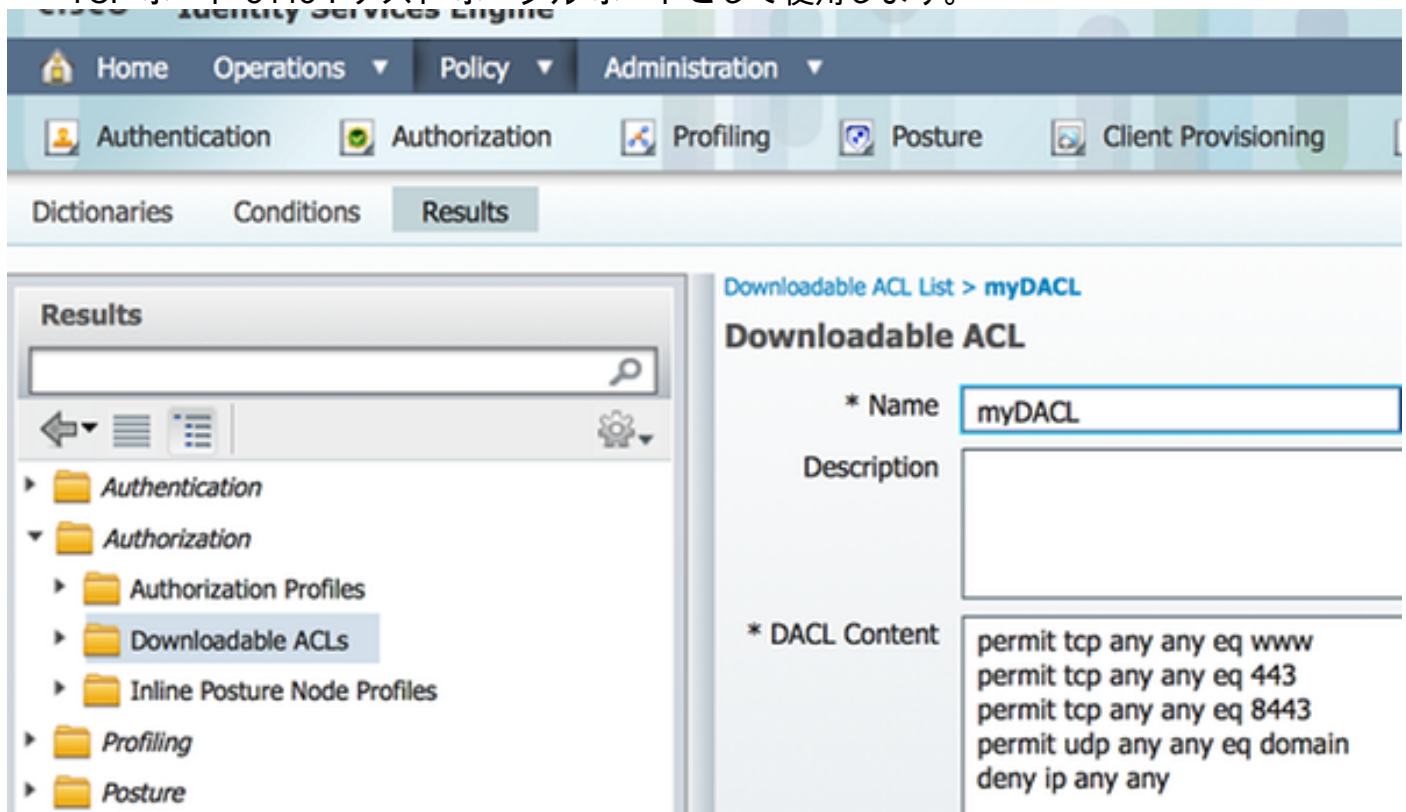
この手順は必須ではありません。 どのトラフィックを (HTTP か HTTPS) ISE にリダイレクトされるか中央 webauth プロファイルと送信されるリダイレクト ACL は判別します。 ダウンロード可能な ACL を作成することで、許可するトラフィックを定義できます。 通常は、DNS、HTTP (S)、および 8443 を許可し、それ以外を拒否します。 そうでない場合、スイッチは HTTP トラフィックをリダイレクトしますが、それ以外のプロトコルは許可されます。

ダウンロード可能な ACL (DACL) を作成するには、次の手順を実行します。

1. [Policy] をクリックし、[Policy Elements] をクリックします。
2. [Results] をクリックします。
3. [Authorization] を展開し、[Downloadable ACLs] をクリックします。
4. [Add] ボタンをクリックして、新しいダウンロード可能な ACL を作成します。
5. [Name] フィールドに、DACL の名前を入力します。この例は *myDACL* を使用します。

次の図は、一般的な DACL の内容を示しています。許可されているプロトコルは次のとおりです。

- DNS : ISE ポータル ホスト名を解決します。
- HTTP および HTTPS : リダイレクションを許可します。
- TCP ポート 8443 : ゲスト ポータル ポートとして使用します。



許可プロファイルの作成

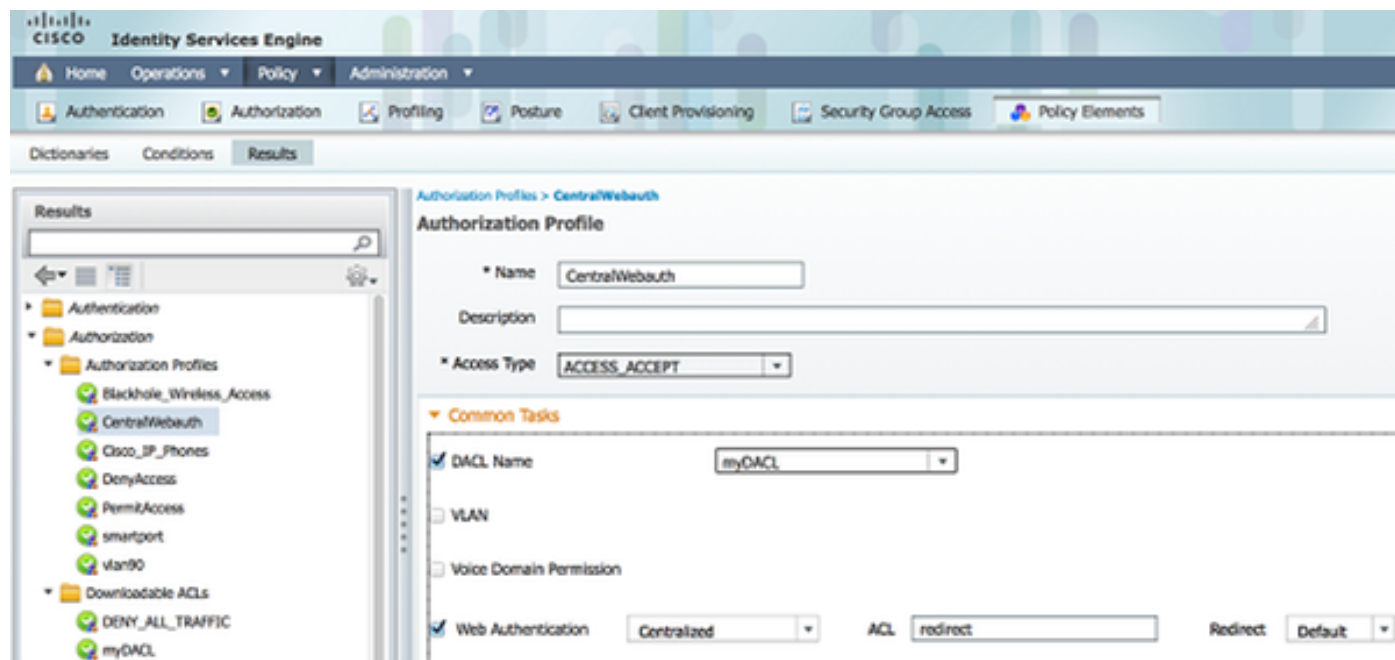
許可プロファイルを作成するには、次の手順を実行します。

1. [Policy] をクリックし、[Policy Elements] をクリックします。
2. [Results] をクリックします。
3. [Authorization] を展開して、[Authorization profile] をクリックします。
4. [Add] ボタンをクリックして、中央 webauth の新しい許可プロファイルを作成します。
5. [Name] フィールドに、プロファイルの名前を入力します。この例では「*CentralWebauth*」という名前を使用します。
6. [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。
7. [Web Authentication] チェックボックスをオンにし、ドロップダウン リストで [Centralized] を選択します。
8. [ACL] フィールドに、リダイレクトされるトラフィックを定義するスイッチ上の ACL の名前を入力します。この例は *リダイレクト* を使用します。

9. [Redirect] ドロップダウン リストで [Default] を選択します。

10. スwitchの静的ポート ACL の代わりに DACL を使用することにする場合 DACL 名前チェックボックスをチェックし、ドロップダウン list から myDACL を選択して下さい。

[Redirect] 属性は、ISE がデフォルトの Web ポータルと ISE 管理者が作成したカスタム Web ポータルのいずれを参照するかを定義します。たとえば、この例で使用されている *redirect* という名前の ACL は、HTTP または HTTPS トラフィックに対するクライアントから任意の場所へのリダイレクションをトリガーします。この ACL は、この設定で後ほど定義します。



認証ルールの作成

認証プロファイルを使用して認証ルールを作成するには、次の手順を実行します。

1. [Policy] メニューで [Authentication] をクリックします。

この図は、認証ポリシー ルールの設定方法の例を示します。この例では、MAB の検出時にルールがトリガーされるように設定されています。



2. 認証ルールの名前を入力します。この例では「MAB」という名前を使用します。

3. [If] 条件フィールドで、プラス ([+]) アイコンをクリックします。

4. [Compound condition] を選択し、[Wired_MAB] を選択します。

5. ルールをさらに展開するには [and ...] の横にある矢印をクリックします。

6. [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します

。

7. [If user not found] ドロップダウンリストで [Continue] を選択します。

このオプションにより、MAC アドレスが不明な場合でも、webauth によってデバイスが認証済みとなります。Dot1x クライアントはクレデンシャルを使用して認証できるので、この設定で考慮する必要はありません。

許可ルールの作成

ここでは、許可ポリシーでいくつかのルールを設定します。PC のプラグを接続すると、PC に対して MAB による認証が実行されます。この例では MAC アドレスを不明と想定しているため、webauth と ACL が返されます。この *MAC not known* ルールは下の図のように表示されます。このセクションでは、このルールを設定します。

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

許可ルールを作成するには、次の手順を実行します。

1. 新しいルールを作成し、名前を入力します。この例では、「*MAC not known*」という名前を使用します。
2. 条件フィールドでプラス ([+]) アイコンをクリックして、新しい条件を作成します。
3. [expression] ドロップダウン リストを展開します。
4. [Network Access] を選択し、展開します。
5. [AuthenticationStatus] をクリックし、[Equals] 演算子を選択します。
6. 右側のフィールドで [UnknownUser] を選択します。
7. [General Authorization] ページの [then] という単語の右側のフィールドで、[CentralWebauth] (許可プロファイル) を選択します。

この手順により、ユーザ (または MAC アドレス) が不明でも、ISE を続行することができます。

不明なユーザには、ここで [Login] ページが表示されます。しかし、ユーザがいったんクレ

デンシャルを入力しても、ISE の認証要求が再度表示されます。そのため、ゲスト ユーザの場合に満たされる条件を使用して、別のルールを設定する必要があります。この例では、[If UseridentityGroup equals Guest] を使用し、すべてのゲストがこのグループに属すると想定されています。

8. [MAC not known] ルールの末尾にあるアクション ボタンをクリックして、上で説明した新しいルールを挿入します。

注: この新しいルールは、[MAC not known] ルールの前に挿入することが重要です。

9. 新しいルールの名前を入力します この例では「IS-a-GUEST」という名前を使用します。
10. ゲスト ユーザに一致する条件を選択します。

この例では *InternalUser: IdentityGroup Equals Guest* を使用します。これは、すべてのゲスト ユーザが、このゲスト グループ (またはスポンサー設定に設定した別のグループ) にバインドされるためです。

11. [then] という単語の右側にある結果ボックスで、[PermitAccess] を選択します。

ユーザが [Login] ページでアクセスを許可されると、ISE によってスイッチ ポートでレイヤ 2 認証が再起動され、新しい MAB が開始されます。このシナリオでの違いは、ISE がそのユーザをゲスト認証済みとして記憶するための非表示のフラグが設定される点です。このルールは、[2nd AUTH] で、条件は [Network Access: UseCase Equals GuestFlow] になります。ユーザが webauth を介して認証され、スイッチ ポートに新しい MAB が再設定されると、この条件が満たされます。ここでは任意の属性を割り当てることができます。この例ではプロファイル *vlan90* を割り当てているので、ユーザはこの 2 番目の MAB 認証で VLAN 90 が割り当てられます。

12. IS-a-GUEST ルールの末尾の [Actions] をクリックし、[Insert new rule above] を選択します。
。
13. 名前フィールドに、「2nd AUTH」と入力します。
14. 条件フィールドでプラス (+) アイコンをクリックして、新しい条件を作成します。
15. [Network Access] を選択し、[UseCase] をクリックします。
16. 演算子として [Equals] を選択します。
17. 右のオペランドとして [GuestFlow] を選択します。
18. 許可ページで [then] の隣にあるプラス (+) アイコンをクリックし、ルールの結果を選択します。

この例では、事前設定されたプロファイル (vlan90) が割り当てられます。この設定はこのドキュメントには示されていません。

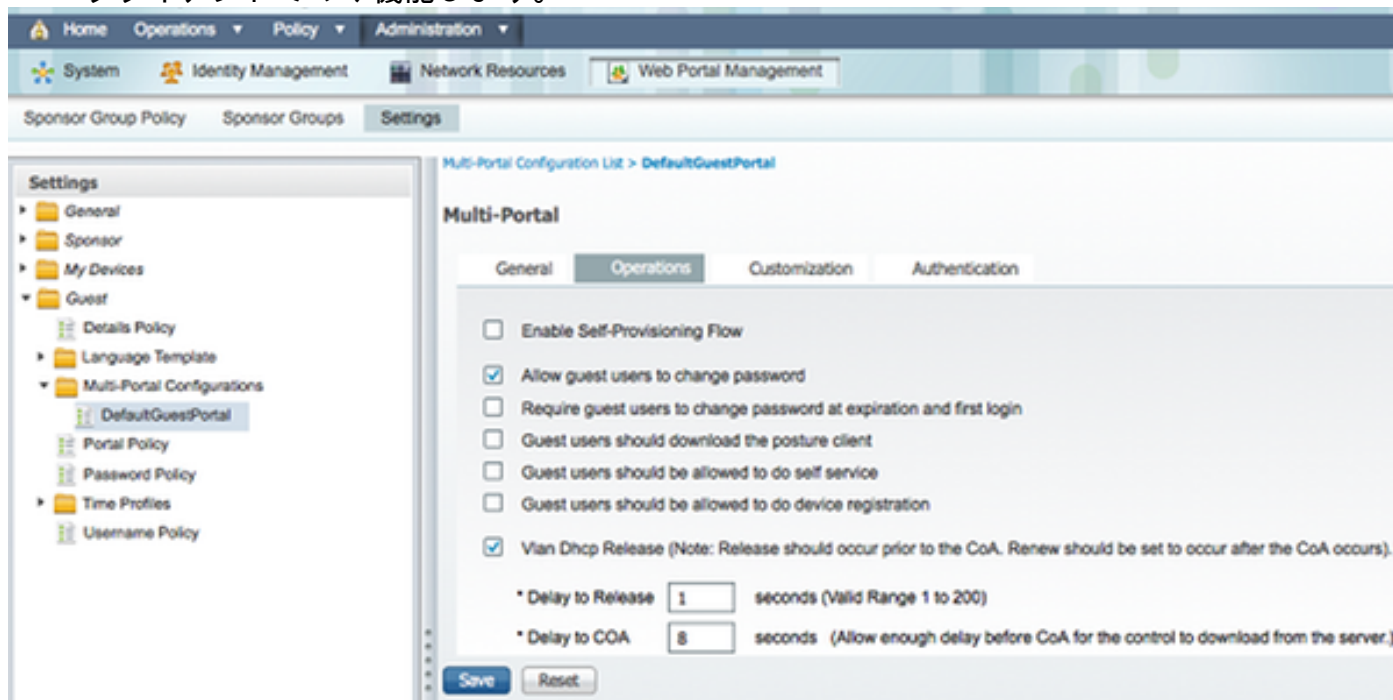
[Permit Access] オプションを選択するか、カスタム プロファイルを作成し、VLAN または任意の属性に戻ることができます。

IP 更新の有効化 (オプション)

VLAN を割り当てる場合、最後のステップとして、クライアント PC 用の IP アドレスを更新します。このステップは、Windows クライアント用のゲスト ポータルによって実行できます。前の手順で、2nd AUTH ルールに VLAN を設定していない場合は、このステップを省略できます。

VLAN を割り当てた場合は、次の手順を実行し、IP 更新を有効にします。

1. [Administration] をクリックし、[Guest Management] をクリックします。
2. [Setting] をクリックします。
3. [Guest] を展開し、[Multi-Portal Configuration] を展開します。
4. [DefaultGuestPortal] または作成したカスタム ポータルの名前をクリックします。
5. [Vlan DHCP Release] チェックボックスをオンにします。注: このオプションは Windows クライアントでのみ機能します。



スイッチの設定 (抜粋)

このセクションでは、スイッチの設定を一部抜粋して示します。すべての設定については、「[スイッチの設定 \(すべての設定 \)](#)」を参照してください。

次の例では、単純な MAB 設定を示します。

```
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 は完全なネットワーク接続を提供する VLAN です。次に示すように、*webauth* という名前のデフォルトのポート ACL が適用されて、定義されます。

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

この設定例では、ユーザが認証されない場合でも完全なネットワーク アクセスが提供されるため、未認証ユーザのアクセスを制限したいと考えるでしょう。

この設定では、ISE が *redirect* という名前のリダイレクト ACL を使用するよう設定されているため、HTTP および HTTPS によるブラウジングは、この別の ACL による認証なしには実行できません。次にスイッチの定義を示します。

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

スイッチがどのトラフィックに対してリダイレクションを実行するかを定義するには、スイッチ上にこのアクセスリストを定義する必要があります（*permit* でトラフィックを指定）この例では、クライアントが HTTP トラフィックまたは HTTPS トラフィックを送信するたびに、リダイレクションがトリガーされます。また、ISE IP アドレスが拒否されるので、ISE へのトラフィックは ISE に送られ、ループでのリダイレクトは行われません（このシナリオでは、拒否によってトラフィックがブロックされるのではなく、トラフィックは単にリダイレクトされません）。特別な HTTP ポートまたはプロキシを使用している場合は、別のポートを追加することができます。

または、一部の Web サイトへの HTTP アクセスを許可し、他の Web サイトについてはリダイレクトすることもできます。たとえば、ACL で内部 Web サーバについてのみ許可するように定義すると、クライアントは認証なしに Web を参照できますが、内部 Web サーバにアクセスしようとするとリダイレクトが発生します。

最後の手順として、スイッチの CoA を許可します。CoA を許可しない場合、ISE はスイッチに対してクライアントの再認証を強制できません。

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

次のコマンドは、スイッチが HTTP トラフィックに基づいてリダイレクトするために必要です。

```
ip http server
```

次のコマンドは、HTTPS トラフィックに基づいてリダイレクトするために必要です。

```
ip http secure-server
```

次のコマンドも重要です。

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

ユーザが未認証の場合、**show authentication session int <interface num>** コマンドは次の出力を返します。

```
01-SW3750-access#show auth sess int gil/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-myDAACL-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
```

注: ISE で MAC アドレスが不明なため、MAB 認証に成功した場合でも、リダイレクト ACL が適用されます。

スイッチの設定 (すべての設定)

このセクションではすべてのスイッチ設定を記載します。一部の不要なインターフェイスとコマンド行が省略されています。そのため、この設定例は参照用としてのみ使用し、コピーしないでください。

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

nmsp 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 プロキシ設定

クライアントに HTTP プロキシを使用すると、クライアントは次のように動作します。

- HTTP プロトコルに対して特殊なポートが使用されます。
- すべてのトラフィックがそのプロキシに送信されます。

特殊なポート (8080 など) でリッスンするためには、次のコマンドを使用します。

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

またすべてのクライアントが引き続きプロキシを使用するが、ISE IP アドレスにはプロキシを使用しないように設定する必要もあります。どのブラウザでも、プロキシを使用すべきでないホスト名または IP アドレスの入力が可能だからです。ISE の例外を追加しない場合、認証ページがループして表示されます。

さらに、プロキシ ポート (この例では、8080) で使用できるように、リダイレクション ACL を

変更する必要もあります。

SVI スイッチに関する重要な注意事項

現時点では、スイッチがクライアントに応答し、Web ポータル リダイレクションをクライアントに送信するためには、スイッチ仮想インターフェイス (SVI) が必要です。この SVI は、必ずしもクライアント サブネット/VLAN にある必要はありません。しかし、クライアント サブネット/VLAN に SVI が存在しなければ、スイッチは他の場所にある SVI を使用しなければならず、クライアント ルーティング テーブルの定義に従ったトラフィックの送信が必要になります。これは一般的には、トラフィックがネットワークの中心にある別のゲートウェイに送信された後で、クライアント サブネット内のアクセス スイッチに戻ることを意味します。

一般にファイアウォールは、このシナリオのような、スイッチから送信されて戻ってくるトラフィックをブロックするため、リダイレクションが正常に機能しない可能性があります。この問題を回避するには、ファイアウォールでこの動作を許可するか、クライアント サブネット内のアクセス スイッチに SVI を作成します。

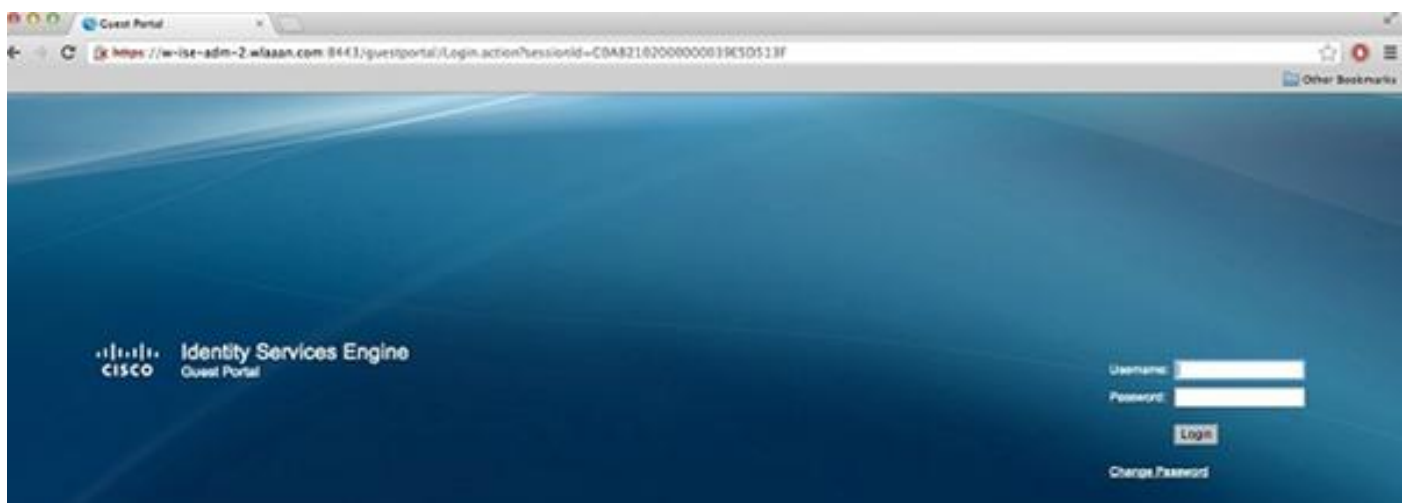
HTTPS リダイレクションに関する重要な注意事項

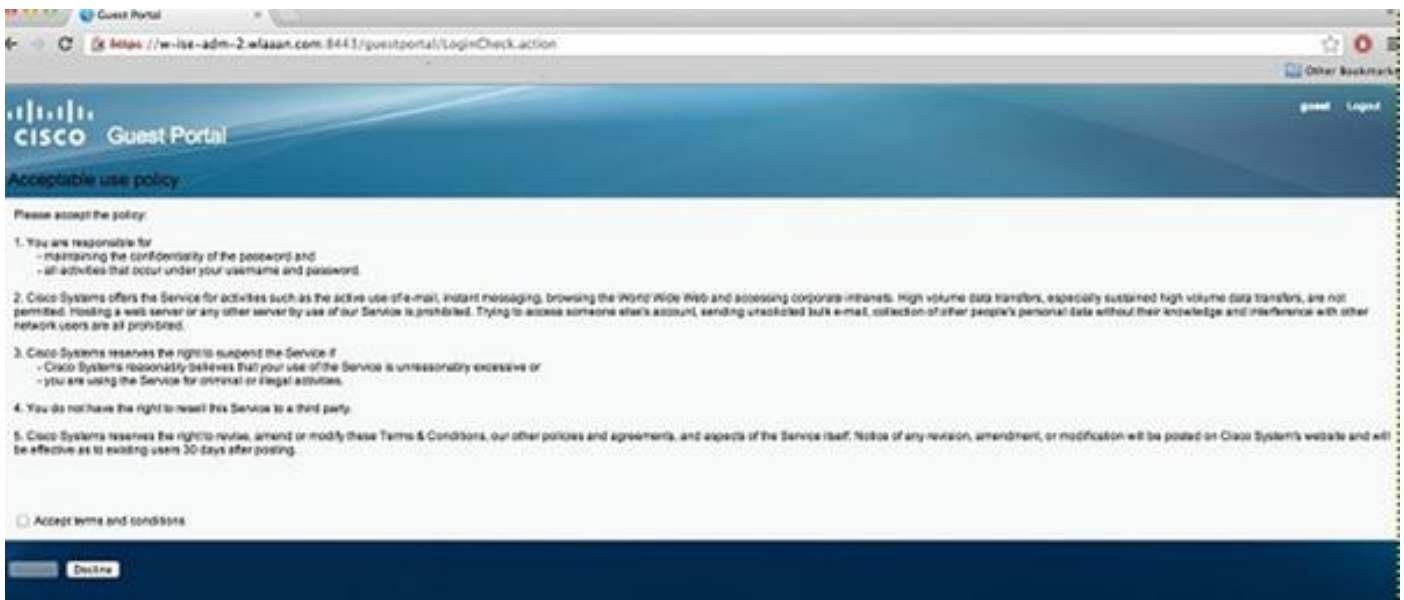
スイッチは HTTPS トラフィックをリダイレクトできます。そのため、ゲスト クライアントのホームページが HTTPS であれば、リダイレクションが適切に実行されます。

リダイレクションの概念そのものが、デバイス (この例ではスイッチ) は Web サイトの IP アドレスをスプーフィングするという事実に基づいています。しかし、スイッチはそれ自体の証明書を Transport Layer Security (TLS) のハンドシェイクでしか提示できないため、スイッチが HTTPS トラフィックを代行受信してリダイレクトすると重大な問題が発生します。またスイッチが提示する証明書は Web サイトが本来要求する証明書と異なるため、ほとんどのブラウザで重大なアラートが出されます。この場合、ブラウザによるリダイレクションも、別の証明書をセキュリティ上の問題として提示することも、ブラウザの処理として適切です。この問題の回避策は存在せず、スイッチが元の Web サイトの証明書をスプーフする方法はありません。

最終結果

クライアント PC のプラグを接続すると、MAB が実行されます。MAC アドレスが不明なので、ISE はリダイレクション属性をスイッチに返します。ユーザは Web サイトへの移動を試み、リダイレクトされます。





[Login] ページで認証に成功すると、ISE は認可変更によってスイッチポートを復帰させ、レイヤ 2 MAB 認証が再開します。

ただし、ISE はそのユーザが以前の webauth クライアントであることを ISE が認識し、(それがレイヤ 2 認証であるにもかかわらず) webauth クレデンシャルに基づいてクライアントを許可します。

ISE 認証ログでは、MAB 認証はログの最後に表示されます。不明な MAC アドレスであっても、その MAC アドレスは認証され、プロファイルされ、webauth 属性が返されます。次に、ユーザのユーザ名に対して認証が行われます (ユーザは [login] ページでこのクレデンシャルを入力します)。認証が完了すると、すぐにユーザ名をクレデンシャルとして新しいレイヤ 2 認証が実行され、この認証手順で、ダイナミック VLAN などの属性を返すことができます。

Mar 26,13 04:58:43.572 PM	🟢	🔒	Nico	00:0F:80:49:5C:48	Nicowitch	FastEthernet2/3	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 ...

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [Cisco Identity Services Engine](#)
- [Cisco Identity Services Engine CLI リファレンス ガイド](#)
- [ISE \(Identity Services Engine \) と Cisco WLC \(Wireless LAN Controller \) の統合](#)
- [Requests for Comments \(RFC \)](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)