隔離されたゲスト ネットワークの静的リダイレクトによる ISE の設定例

目次

概要

このドキュメントでは、冗長性を維持するために、隔離されたゲスト ネットワークへの静的リダイレクトを使用して Cisco Identity Services Engine（ISE）を設定する方法を説明します。 また、証明書を検証できないという警告がクライアントに出されないようにポリシー ノードを設定する方法についても説明します。

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。

- Cisco ISE Central Web Authentication（CWA）および関連するすべてのコンポーネント
- ブラウザによる証明書の有効性確認
- Cisco ISE バージョン 1.2.0.899 以降
- Cisco Wireless LAN Controller（WLC）バージョン 7.2.110.0 以降（バージョン 7.4.100.0 以降を推奨）

注: CWA については、記事「WLC および ISE での中央 Web 認証の設定例」を参照してください。

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 ISE バージョン 1.2.0.899
- Cisco Virtual WLC（vWLC）バージョン 7.4.110.0
- Cisco 適応型セキュリティ アプライアンス（ASA）バージョン 8.2.5

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。

背景説明

多くの Bring Your Own Device（BYOD）環境では、緩衝地帯（DMZ）の内部ネットワークから完全にゲスト ネットワークが分離されます。 ゲスト ユーザに提供されるサービスはインターネット アクセスだけなので、ほとんどの場合、ゲスト DMZ の DHCP はゲスト ユーザに対して公開ドメイン ネーム システム（DNS）サーバを提供します。

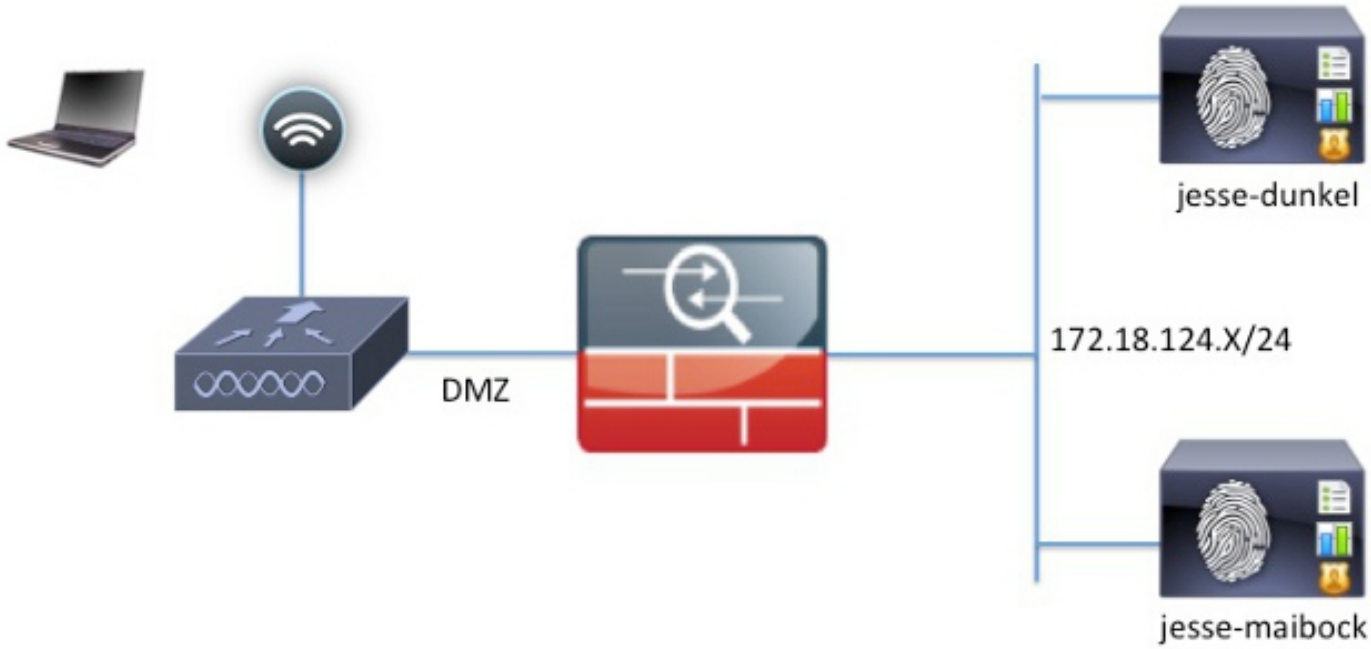
バージョン 1.2 より前の ISE では Web 認証のためにクライアントを完全修飾ドメイン名（FQDN）にリダイレクトするため、これらの ISE でゲストをリダイレクトするのは困難です。 ただし、ISE バージョン 1.2 以降では、管理者がゲスト ユーザを静的 IP アドレスまたはホスト名にリダイレクトできるようになっています。

設定

ネットワーク図

論理図は次のとおりです。

> **注:** 物理的には、内部ネットワークにワイヤレス コントローラがあり、アクセス ポイント（AP）は内部ネットワークで稼働します。サービス セット識別子（SSID）は DMZ コントローラに固定されます。 詳細については、Cisco WLC のマニュアルを参照してください。



設定

WLC 上の設定は、通常の CWA 設定と変わりません。 SSID は、RADIUS 認証で MAC フィルタリングを行えるように設定され、RADIUS アカウンティングは 2 つ以上の ISE ポリシー ノードを指しています。

このドキュメントでは、ISE の設定を重点的に取り上げています。

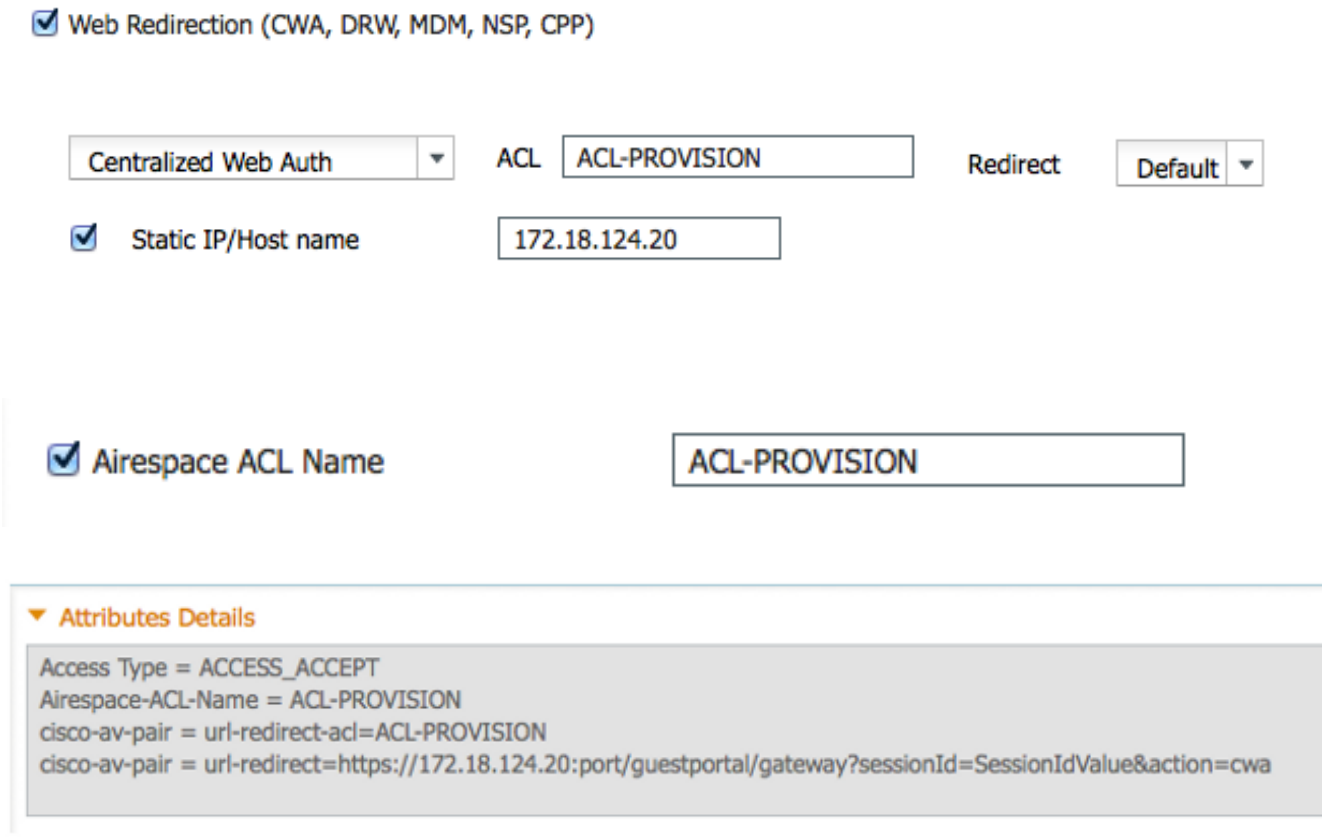
> **注:** この設定例でのポリシー ノードは **jesse-dunkel**（172.18.124.20）と **jesse-maibock**（172.18.124.21）です。

CWA フローは、WLC が RADIUS MAC 認証バイパス（MAB）要求を ISE に送信した時点で始まります。 ISE は HTTP トラフィックを ISE にリダイレクトするために、コントローラにリダイレクト URL を返して応答します。 セッションは単一のポリシー サービス ノード（PSN）で維持されるため、RADIUS および HTTP トラフィックが同じ PSN に送信されることが重要です。 これは一般に単一のルールで対処され、PSN は独自のホスト名を CWA URL に挿入します。 ただし、静的リダイレクトの場合は、RADIUS および HTTP トラフィックが同じ PSN に送信されるようにするために、PSN ごとにルールを作成する必要があります。

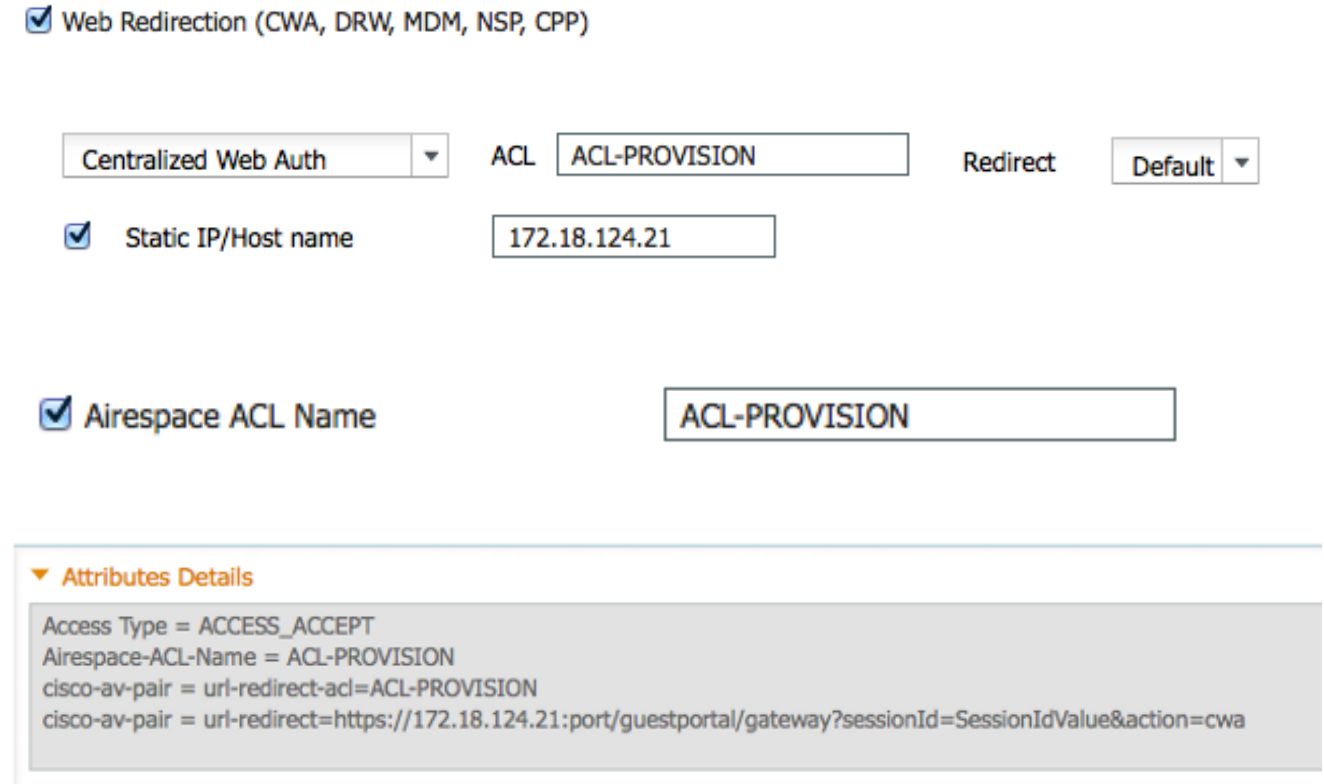
ISE を設定するには、次の手順を実行します。

1. クライアントを PSN の IP アドレスにリダイレクトするために、2 つのルールを設定します。 [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。

   次の図に、プロファイル名 **DunkelGuestWireless** の情報を示します。

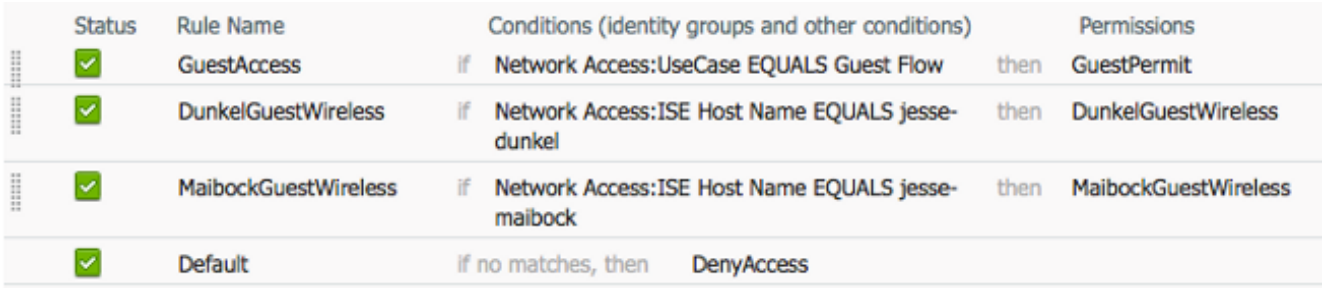


次の図に、プロファイル名 **MaibockGuestWireless** の情報を示します。



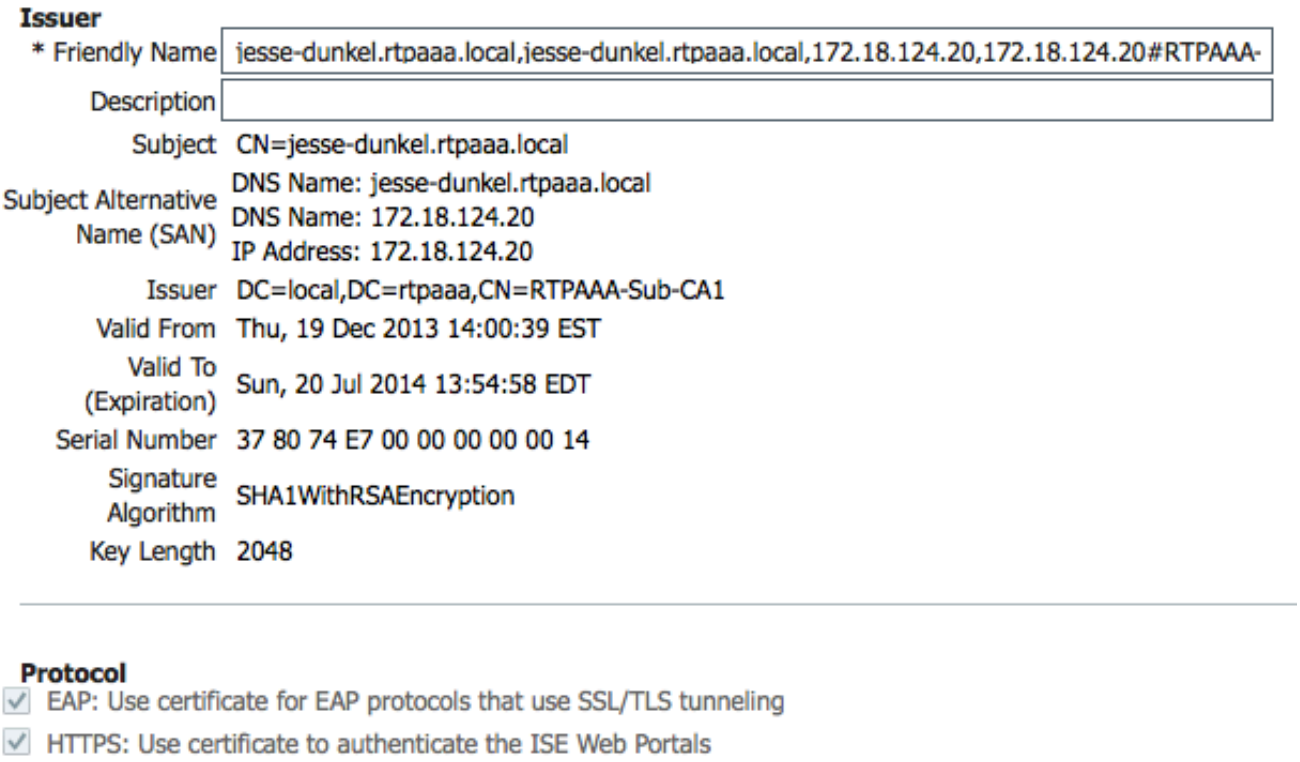
注: ACL-PROVISION は、認証の際にクライアントが ISE と通信できるようにするために、WLC 上に設定されるローカル アクセス コントロール リスト（ACL）です。 詳細については、シスコの記事「WLC および ISE での中央 Web 認証の設定例」を参照してください。

2. [Network Access: ISE Host Name] 属性と一致して、適切な認証プロファイルを提供するように認証ポリシーを設定します。



Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	GuestAccess	if Network Access:UseCase EQUALS Guest Flow	then	GuestPermit
✓	DunkelGuestWireless	if Network Access:ISE Host Name EQUALS jesse-dunkel	then	DunkelGuestWireless
✓	MaibockGuestWireless	if Network Access:ISE Host Name EQUALS jesse-maibock	then	MaibockGuestWireless
✓	Default	if no matches, then DenyAccess		

これで、クライアントは IP アドレスにリダイレクトされますが、URL が証明書内の情報と一致しないため、ユーザには証明書に関する警告が表示されます。 たとえば、証明書内の FQDN は jesse-dunkel.rtpaaa.local ですが、URL は 172.18.124.20 です。 ブラウザが IP アドレスで証明書の有効性を確認できるようにするための証明書の例は、次のとおりです。



Issuer

* Friendly Name	jesse-dunkel.rtpaaa.local,jesse-dunkel.rtpaaa.local,172.18.124.20,172.18.124.20#RTPAAA-
Description	
Subject	CN=jesse-dunkel.rtpaaa.local
Subject Alternative Name (SAN)	DNS Name: jesse-dunkel.rtpaaa.local DNS Name: 172.18.124.20 IP Address: 172.18.124.20
Issuer	DC=local,DC=rtpaaa,CN=RTPAAA-Sub-CA1
Valid From	Thu, 19 Dec 2013 14:00:39 EST
Valid To (Expiration)	Sun, 20 Jul 2014 13:54:58 EDT
Serial Number	37 80 74 E7 00 00 00 00 00 14
Signature Algorithm	SHA1WithRSAEncryption
Key Length	2048

Protocol

- ☑ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling
- ☑ HTTPS: Use certificate to authenticate the ISE Web Portals

サブジェクト代替名（SAN）エントリを使用することにより、ブラウザは IP アドレス 172.18.124.20 を含む URL の有効性を確認できます。. さまざまなクライアントの非互換性に対処するには、3 つの SAN エントリを作成する必要があります。

3. DNS 名の SAN エントリを作成し、[Subject] フィールドの [CN=] エントリと一致することを確認します。

4. クライアントが IP アドレスの有効性を確認できるようにするためのエントリを 2 つ作成します。 この 2 つのエントリは、IP アドレスの DNS 名と [IP Address] 属性に示される IP アドレスに対応するものです。 一部のクライアントは DNS 名のみを参照します。 その他のクライアントは [DNS Name] 属性に指定された IP アドレスを受け入れませんが、代わりに [IP Address] 属性を参照します。

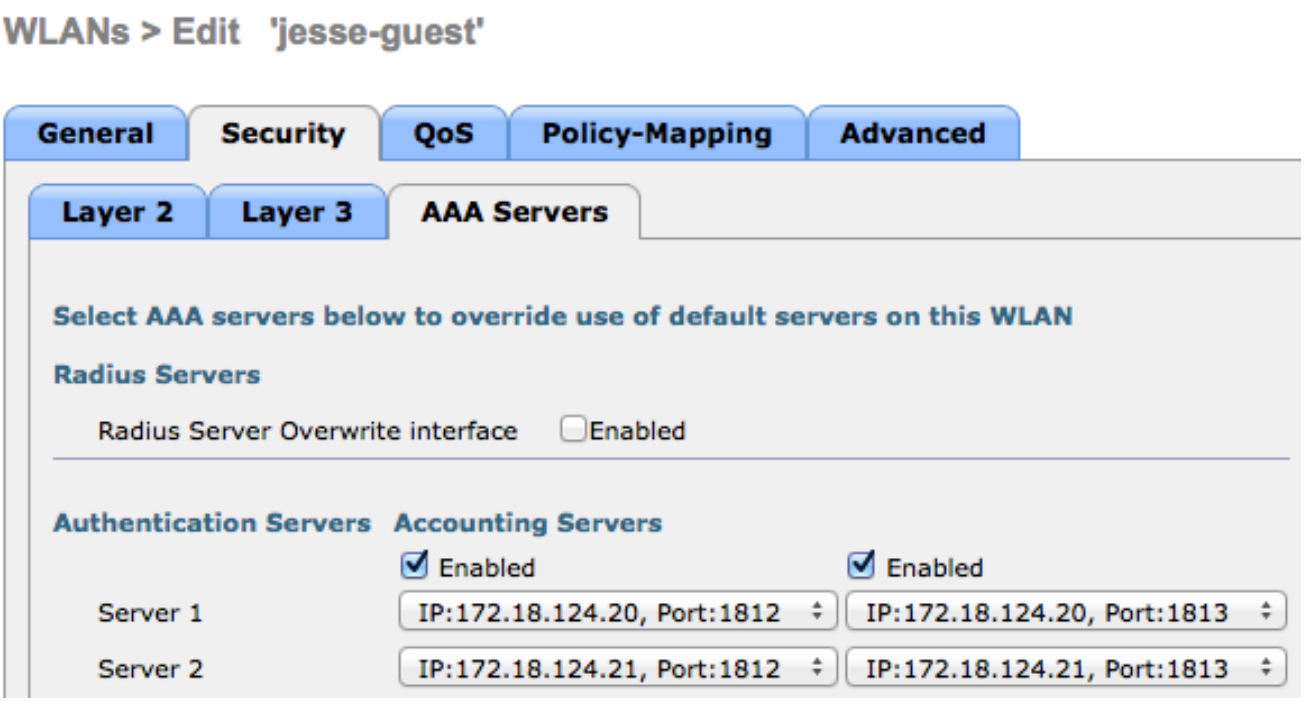
注: 証明書の生成について詳しくは、『Cisco Identity Services Engine Hardware Installation

Guide, Release 1.2』を参照してください。

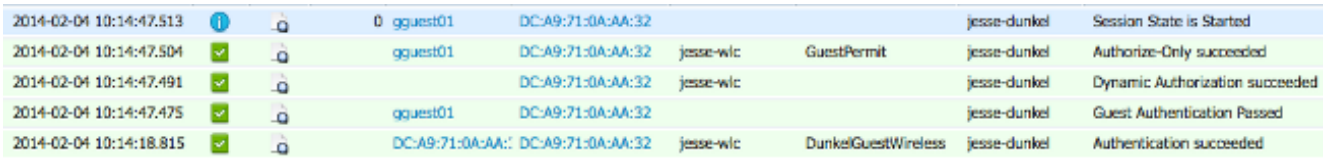
確認

設定が適切に機能していることを確認するには、次の手順に従います。

1. 両方のルールが機能していることを確認するために、WLAN 上に設定されている ISE PSN の順序を手動で設定します。



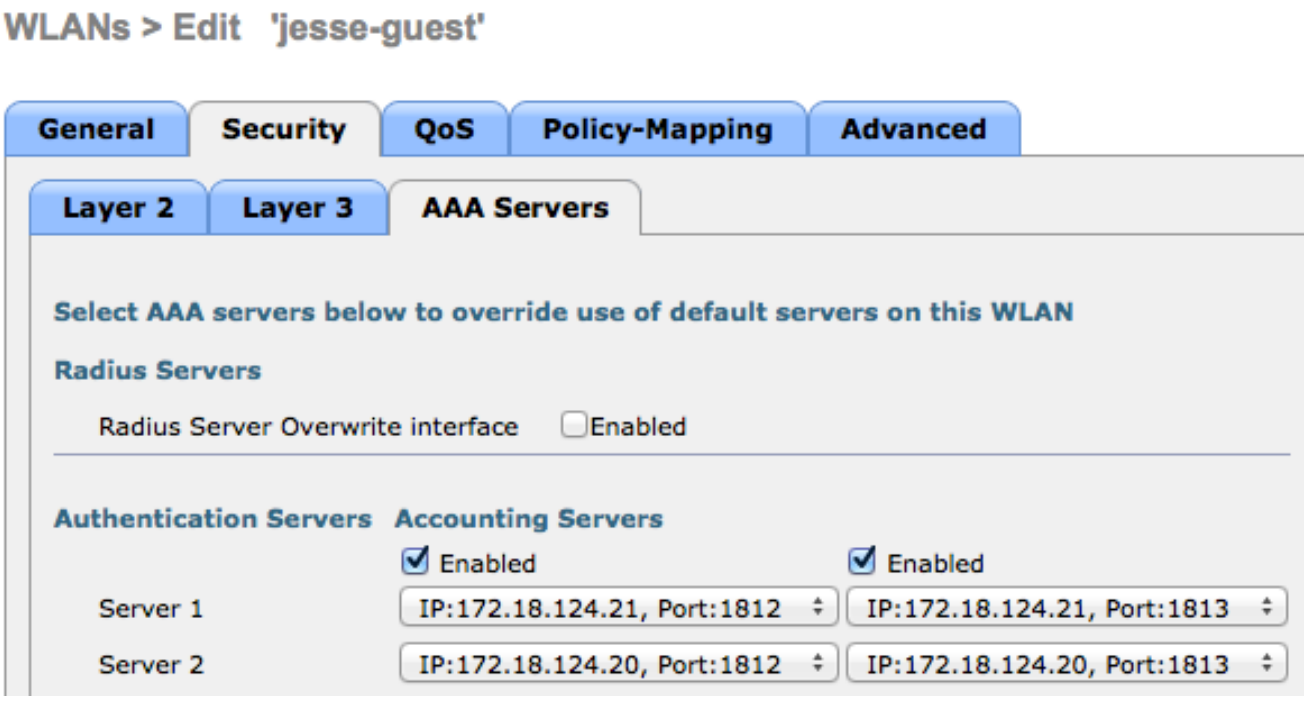
2. ゲスト SSID にログインし、ISE の [Operation] > [Authentications] に移動して、正しい認証ルールにヒットすることを確認します。



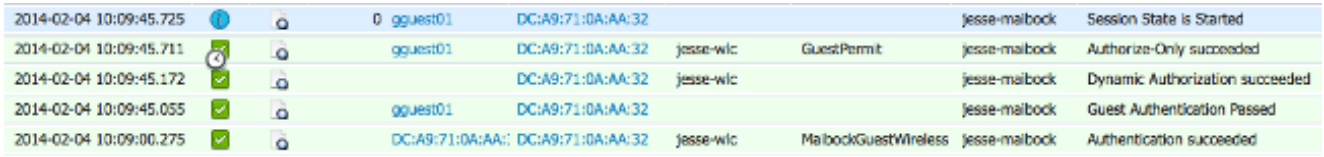
最初の MAB 認証は、**DunkelGuestWireless** 認証プロファイルに対して行われます。 このルールが、最初の ISE ノードである **jesse-dunkel** に明示的にリダイレクトします。 **gguest01** ユーザがログインすると、適切かつ最終的な **GuestPermit** の許可が付与されます。

3. WLC からの認証セッションをクリアするために、クライアント デバイスをワイヤレス ネットワークから切断し、WLC で [Monitor] > [Clients] に移動して出力からセッションを削除します。 デフォルトでは、WLC はアイドル セッションを 5 分間保持します。したがって、有効なテストを実行するには、新しいセッションを開始する必要があります。

4. ゲスト WLAN 設定での ISE PSN の順序を逆にします。



5. ゲスト SSID にログインし、ISE の [Operation] > [Authentications] に移動して、正しい認証ルールにヒットすることを確認します。



2 回目の試行では、最初の MAB 認証で正しく **MaibockGuestWireless** 認証プロファイルにヒットします。 **jesse-dunkel** に対する 1 回目の試行（ステップ 2）と同様に、**jesse-maibock** に対する認証では最終的な許可として **GuestPermit** にヒットします。 **GuestPermit** 認証プロファイルに PSN 固有の情報は含まれていないため、任意の PSN に対する認証に単一のルールを使用できます。

トラブルシューティング

[Authentication Details] ウィンドウは、認証/許可プロセスのすべてのステップを表示する強力なビューです。 このウィンドウにアクセスするには、[Operations] > [Authentications] に移動して、[Details] 列にある虫めがねアイコンをクリックします。 このウィンドウを使用して、認証/許可ルールの条件が正しく設定されていることを確認します。

その場合に第一の焦点となるのは、[Policy Server] フィールドです。 このフィールドに、認証を処理する ISE PSN のホスト名が設定されます。

Overview

Event	5200 Authentication succeeded
Username	DC:A9:71:0A:AA:32
Endpoint Id	DC:A9:71:0A:AA:32
Endpoint Profile	
Authorization Profile	DunkelGuestWireless
AuthorizationPolicyMatchedRule	DunkelGuestWireless
ISEPolicySetName	GuestWireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-02-04 10:14:18.79
Received Timestamp	2014-02-04 10:14:18.815
Policy Server	jesse-dunkel
Event	5200 Authentication succeeded

[Policy Server] のエントリをルール条件と比較して、この 2 つが一致することを確認します（この値では大文字小文字が区別されます）。

DunkelGuestWireless	if	Network Access:ISE Host Name EQUALS jesse-dunkel

注: 重要な点として、テストが終わって次のテストを開始する前に、必ず SSID から切断して、WLC からクライアント エントリをクリアしてください。