# Microsoft IAS Radius サーバでの Cisco Airespace VSA の設定例

### 内容

概要前提条件要件使用するコンポーネント表記法背景説明Airespace VSA用のIASの設定IASでAAAクライアントとしてWLCを設定するIASでリモートアクセスポリシーを設定する設定例確認トラブルシュート関連情報

### <u>概要</u>

このドキュメントでは、Cisco Airespace Vendor Specific Attributes(VSA)をサポートするように Microsoft Internet Authentication Service(IAS)サーバを設定する方法について説明します。 Cisco Airespace VSA のベンダー コードは 14179 です。

# <u>前提条件</u>

#### <u>要件</u>

この設定を行う前に、次の要件が満たされていることを確認します。

- IASサーバの設定方法に関する知識
- Lightweight Access Point(LAP; Lightweight アクセス ポイント)および Cisco Wireless LAN Controller (WLC; ワイヤレス LAN コントローラ)の設定についての知識
- Cisco Unified Wireless Security ソリューションについての知識

#### <u>使用するコンポーネント</u>

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いています。

• IAS がインストールされた Microsoft Windows 2000 サーバ

- ・ソフトウェア バージョン 4.0.206.0 が稼動している Cisco 4400 WLC
- Cisco 1000 シリーズ LAP
- •ファームウェア 2.5 が稼働する 802.11 a/b/g ワイヤレス クライアント アダプタ
- Aironet Desktop Utility (ADU) バージョン 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ました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

注:このドキュメントは、Cisco Airespace VSAをサポートするためにIASサーバで必要な設定の 例を読者に示すことを目的としています。このドキュメントで示されているIASサーバの設定は 、ラボでテスト済みであり、期待どおりに動作します。IASサーバの設定に問題がある場合は、 Microsoftに問い合わせてください。Cisco TAC では、Microsoft Windows サーバの設定に関する サポートは行っていません。

このドキュメントでは、基本動作用に WLC が設定されており、WLC に LAP が登録されている ことを前提としています。WLC で LAP との基本動作を初めて設定する場合は、『<u>ワイヤレス</u> LAN コントローラ(WLC)への Lightweight AP(LAP)の登録』を参照してください。

#### <u>表記法</u>

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

#### <u>背景説明</u>

一般的な WLAN システムでは、Service Set Identifier(SSID)に関連付けられたすべてのクライ アントに適用されるスタティックなポリシーが各 WLAN に存在します。 この方法は強力ですが 、異なる QoS ポリシーやセキュリティ ポリシーを継承するために各クライアントを異なる SSID に関連付ける必要があるので、さまざまな制約があります。

ただし、Cisco Wireless LAN ソリューションでは、アイデンティティ ネットワーキングがサポー トされています。この場合、ネットワーク上で1つの SSID のみをアドバタイズすることによっ て、特定のユーザがそれぞれのポリシーに基づいた異なる QoS ポリシーまたはセキュリティ ポ リシーを継承できるようになります。特定のポリシーを制御するには、アイデンティティ ネット ワーキングの次の機能を使用します。

- Quality of Service: RADIUS Access Accept に含まれている場合、その QoS レベルの値によって、WLAN プロファイルに設定された QoS 値が上書きされます。
- ACL: RADIUS Access Accept に、アクセス コントロール リスト(ACL)属性が含まれてい る場合、システムによって、認証後にクライアント ステーションに ACL 名が適用されます 。これは、インターフェイスに割り当てられた ACL を上書きします。
- VLAN: RADIUS Access Accept に VLAN Interface-Name または VLAN-Tag が含まれている 場合、システムによって、クライアントが特定のインターフェイスに割り当てられます。
- WLAN ID: RADIUS Access Accept に WLAN ID が含まれている場合、システムによって、 認証後にクライアント ステーションに WLAN ID (SSID)が適用されます。WLAN ID は、 IPSec を除く、すべての認証のインスタンスの WLC によって送信されます。Web 認証では 、WLC が AAA サーバからの認証応答で WLAN ID を受信したときに、WLAN の ID と一致し なかった場合には、認証は拒否されます。他のタイプのセキュリティ方式では、これは実行 されません。

- **DSCP 値**: RADIUS Access Accept に含まれる場合、WLAN プロファイルに設定された DSCP 値が上書きされます。
- 802.1p タグ: RADIUS Access Accept に含まれる場合、WLAN プロファイルに設定されたデ フォルト値が上書きされます。

注: VLAN機能は、MACフィルタリング、802.1X、およびWi-Fi Protected Access(WPA)のみをサ ポートします。Web 認証または IPSec はサポートされていません。インターフェイス名に対応 するために、オペレーティング システムのロカール MAC フィルタ データベースが拡張されてい ます。その結果、ローカル MAC フィルタでは、クライアントに割り当てる必要があるインター フェイスを指定できるようになりました。別個の RADIUS サーバも使用できますが、Security メ ニューを使用して、その RADIUS サーバを定義する必要があります。

アイデンティティ ネットワーキングの詳細は、「<u>ID ネットワーキングの設定</u>」を参照してくださ い。

## <u>Airespace VSA用のIASの設定</u>

Airespace VSAのIASを設定するには、次の手順を実行する必要があります。

- 1. IASでAAAクライアントとしてWLCを設定する
- 2. IASでリモートアクセスポリシーを設定する
- 注:VSAはリモートアクセスポリシーで設定されます。

IASでAAAクライアントとしてWLCを設定する

IASでAAAクライアントとしてWLCを設定するには、次の手順を実行します。

1. [Programs] > [Administrative Tools] > [Internet Authentication Service] の順に選択し、 Microsoft 2000 サーバ上で IAS を起動します。



- 2. [Clients] フォルダを右クリックし、[New Client] を選択して、新しい RADIUS クライアント を追加します。
- 3. [Add Client] ウィンドウで、クライアントの名前を入力し、プロトコルとして [RADIUS] を 選択します。次に、[Next] をクリックします。この例では、クライアントの名前は *WLC-1* です。**注:デフォルト**では、プロトコルはRADIUSに設定されています。

| Add Client  |                                      | × |
|---|--------------------------------------|---|
| Name and Protocol<br>Assign a name and protocol for the | e client.                            |   |
| Type a friendly name and protocol                       | l for the client.                    |   |
| Eriendly name:  | WLC-1                                |   |
| Protocol:   | RADIUS                               |   |
|   |                                      |   |
|   |                                      |   |
|   |                                      |   |
|   |                                      |   |
|   |                                      |   |
|   |                                      | _ |
|   | < <u>B</u> ack <u>N</u> ext > Cancel |   |

4. [Add RADIUS Client] ウィンドウで、クライアント IP アドレス、クライアントのベンダー、 および秘密共有鍵を入力します。クライアント情報を入力したら、[Finish] をクリックしま す。この例では、クライアントの名前は *WLC-1* であり、IP アドレスは *172.16.1.30*、クラ イアントのベンダーは *Cisco*、秘密共有鍵は *cisco123* と、それぞれ設定されています。

| Add RADIUS Client   |        |               | ×  |
|---|--------|---------------|----|
| Client Information<br>Specify information regarding the client. |        |               |    |
| Client address (IP or DNS):                                     |        | Marilia       |    |
| Client-Vendor:  |        | <u>v</u> eniy |    |
| Cisco   |        | •             |    |
| Client must always send the signature attribute in the re-      | quest  |               |    |
| Shared secret:  |        |               |    |
| Confirm shared secret:  |        |               |    |
|   |        |               |    |
|   |        |               |    |
| < <u>B</u> ack  | Finish | Cano          | el |

この情報によって、IAS サーバの AAA クライアントとして、WLC-1 と名付けられた WLC が 追加されます。

| 🐤 Internet Authentication Service  |               |             |          |               |
|--|---------------|-------------|----------|---------------|
| <u>A</u> ction View   ← →   🗈 📧 💼 🖽 [  | 3             |             |          |               |
| Tree   | Friendly Name | Address     | Protocol | Client-Vendor |
| Internet Authentication Service (Local)   Image: Clients   Remote Access Policies |               | 172.16.1.30 | RADIUS   | <u>Gisco</u>  |
|  | 4             |             |          | - I           |

次の手順では、リモート アクセス ポリシーを作成し、VSA を設定します。

IASでリモートアクセスポリシーを設定する

IASで新しいリモートアクセスポリシーを設定するには、次の手順を実行します。

- 1. [リモートアクセスポ**リシー]を右クリック**し、[新しいリモー**トアクセスポリシー]を選択しま** す。[Policy Name] ウィンドウが表示されます。
- 2. ポリシーの名前を入力し、[Next] をクリックします。

| Remote Access Policy   |      |
|--|------|
| Policy Name<br>Specify a friendly name for the policy.   |      |
| A Remote Access Policy is a set of actions which can be applied to a group of users<br>meeting certain conditions.   |      |
| Analogous to rules you can apply to incoming mail in an e-mail application, you can<br>specify a set of conditions that must be matched for the Remote Access Policy to app<br>You can then specify actions to be taken when the conditions are met. | ly.  |
| Policy friendly name:  |      |
| Airespace VSA  |      |
|  |      |
|  |      |
|  |      |
|  |      |
|  |      |
| < Back Next > C:   | ance |

3. 次のウィンドウで、リモート アクセス ポリシーが適用される条件を選択します。[Add] をク リックし、条件を選択します。

| Add Remote Access Policy                         | Select Attribute   |
|--|--|
| Conditions<br>Determine the conditions to match. | Select the type of attribute to add, and then click the Add button.<br>Attribute types:  |
| Specify the conditions to match.                 | Name         Description           Called-Station-Id         Fhome number dated by user           Caling-Station-Id         Phone number from which call originated           Clent-Friendly-Name         Friendly name for the RADIUS clent. (IAS only)           Clent-IP-Address         IP address of RADIUS clent. (IAS only)           Clent-Wendor         Manufacturer of RADIUS proxy or NAS. (IAS only)           Clent-Vendor         Manufacturer of RADIUS proxy or NAS. (IAS only)           Day-And-Time-Restric         Time periods and days of week during which use           FramedProtocol         The protocol to be used           NAS-Identifier         String identifying the NAS originating the request (IA           NAS-Port-Type         Type of physical port used by the NAS originatin           Service-Type         Type of service user has requested           Tunnel-Type         Tunneling protocols to be used           Windows-Groups         Windows groups that user belongs to |
| Add Eenove Epit                                  |  |
| < <u>B</u> ack <u>N</u> ext> Cancel              | Agd Cancel   |

4. [Attribute types] メニューから、次の属性を選択します。[Client-IP-Address]: AAA クライア ントの IP アドレスを入力します。この例では、WLC から送信されるパケットにポリシーが 適用されるように、WLC の IP アドレスが入力されています。

| Client-IP-Address                       |            | ? ×    | 1         |
|---|------------|--------|-----------|
| Type a word or a wild card (for example | e, abc.*): |        |           |
| 172.16.1.30                             |            |        |           |
|   |            |        |           |
|   |            |        |           |
|   | OK         | Cancel |           |
|   |            |        | _[Windows |

Groups] : ポリシーが適用される Windows グループ(ユーザグループ)を選択します。以下 が一例です。

| 📲 Groups  | ? ×    |
|---|--------|
| The following groups are currently in this condition. |        |
| Groups:   |        |
| Name  |        |
| CAT-TD-2K\Test-Clients                                |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
|   |        |
| Add <u>R</u> emove                                    |        |
|   |        |
| OK 1  | Canad  |
|   | Lancei |

| Add Remote Access Policy                         | ×   |
|--|-----|
| Conditions<br>Determine the conditions to match. |     |
| Specify the conditions to match.                 |     |
| Client-IP-Address matches "172.16.1.30" AND      | I   |
| Windows-Groups matches "CAT-TD-2K\Test-Clients"  |     |
|  |     |
|  |     |
|  |     |
|  |     |
| A <u>d</u> d <u>R</u> emove <u>E</u> dit         |     |
| < <u>B</u> ack <u>N</u> ext > Can                | cel |

この例では、2 つの条件が選択されています。さらに条件を増やすには、同じように条件を 追加し、[Next] をクリックします。[Permissions] ウィンドウが表示されます。

5. [Permissions] ウィンドウで、[Grant remote access permission] を選択します。このオプションを選択すると、(手順2で)指定された条件に一致するユーザには、アクセスが提供されます。

| mote Access Policy   |   |   |              |
|--|---|---|--------------|
| nissions<br>Determine whether to grant or d                        | eny remote access permissio                                     | n.                                      |              |
| You can use a Remote Access<br>group of users, or to act as a filt | Policy either to grant certain<br>er and deny access privilege: | access privileges<br>s to a group of us | to a<br>ers. |
| If a user matches the specified o                                  | onditions:  |   |              |
| <ul> <li>Grant remote access permis</li> </ul>                     | ion   |   |              |
| Deny remote access permiss   | ion   |   |              |
|  |   |   |              |
|  |   |   |              |
|  |   |   |              |
|  |   |   |              |
|  |   |   |              |
|  |   |   |              |
|  |   |   |              |
|  | < <u>B</u> ack  | <u>N</u> ext >                          | Car          |

- 6. [next] をクリックします。
- 7. 次の手順に従って、ユーザ プロファイルを設定します。条件に基づいて、アクセスを拒否 または許可するユーザを指定した場合であっても、ユーザ単位でポリシーの条件が上書きさ れる場合には、従来どおりプロファイルを使用する必要があります。

| Add Remote Access Policy   | ×  |
|--|--|
| User Profile<br>Specify the user profile.  |  |
| You can now specify the profile for users w specified.                                       | vho matched the conditions you have  |
| Note: Even though you may have specified<br>profile can still be used if this policy's condi | d that users should be denied access, the<br>tions are overridden on a per-user basis. |
| Edit <u>P</u> rofile   |  |
|  |  |
|  |  |
|  |  |
|  | < <u>B</u> ack Finish Cancel   |

ユーザ プロファイルを設定するには、[User Profile] ウィンドウで、[Edit Profile] をクリック します。[Edit Dial-in Profile] ウィンドウが表示されます。

| : Dial-in Profile                      |                   |        | ?         | × |
|--|-------------------|--------|-----------|---|
| Authentication                         | Encryption        |        | Advanced  |   |
| Dial-in Constraints                    | IP                |        | Multilink |   |
| Disconnect if idle for:                |                   | 1      | 👘 min.    |   |
| Restrict <u>m</u> aximum session       | to:               | 1      | 🗾 min.    |   |
| Restrict access to the follo           | wing days and tir | nes: — |           |   |
|  |                   |        |           |   |
|  |                   |        |           |   |
|  |                   |        |           |   |
|  | <u>E</u> dit      |        |           |   |
| E Restrict <u>D</u> ial-in to this num | ber only:         |        |           | 1 |
| 🔲 <u>R</u> estrict Dial-in media: —    |                   |        |           |   |
| FDDI                                   |                   |        | <b>_</b>  |   |
| Token Ring                             |                   |        |           |   |
| Wireless - IEEE 802.11                 |                   |        |           |   |
|  |                   |        | -         |   |
| 1                                      |                   |        |           |   |
|  |                   |        |           |   |
|  | OK                | Cancel | Apply     |   |
|  |                   |        |           |   |

タブをクリックし、WLAN に使用する認証方式を選択します。この例では、[Unencrypted Authentication (PAP,SPAP)] が選択されています。

| it Dial-in Profile  |   |                                 | ? ×           |
|---|---|---------------------------------|---------------|
| Dial-in Constraints   | IP  | Multilink                       | t             |
| Authentication  | Encryption  | Advanced                        | <u>i</u>      |
| Check the authentication m<br>Extensible Authentica<br>Select the EAP type whic<br>Protected EAP (PEAP) | nethods which are allowe<br>ition Protocol<br>ih is acceptable for this p | d for this connection<br>olicy. | ι.<br>]       |
| Microsoft Encrypted A   | Authentication version <u>2</u> (   | MS-CHAP v2)                     |               |
| Microsoft Encrypted A   | Authentication (MS-CHAP   | ງ                               |               |
| Encrypted Authentica  | ition (CHAP)  |                                 |               |
| 🔽 Unencrypted Authent   | ication (PAP, SPAP)   |                                 |               |
| Unauthenticated Access<br>Allow remote <u>P</u> PP clie<br>any authentication me                        | ents to connect without n   | egotiating                      |               |
|   |   |                                 |               |
|   | OK Ca   | incel <u>A</u> pply             | y             |
| クリックします。デフォル  | ーーーーーー<br>・トのパラメータをす^   | <br>べて削除し、[Add]                 | ーーー」[<br>をクリッ |

| e                            |  |   |  | ?  | ×   |   |
|------------------------------|--|---|--|--|---|---|
| netrainte                    | ) ie   | 1   | M  | ultiliek   | -т İ  |   |
| tion                         | Encryption   |   | Adv  | anced  | -`1   |   |
| ial connection               | attributes to be i   | returned to   | the Rei  | note   |   |   |
|                              | Vendor   | Valu  | е  |  |   |   |
| <u>R</u> emove               | Edit   |   |  |  |   |   |
| [                            | ОК   | Cance   |  | Apply  |   |   |
| Service-Typ                  | <br>e] を選択し、》  | 欠のウィン   | ィドウマ   | د<br>[Login] ۵   | [<br>D値を  | Add Attributes]<br>と選択します。  |
| elect the attribute and clic | k Add  |   | Enumerable   | Attribute Inform   | ation   | 2   |
|                              | E Instraints tion Inal connection Inal Connect | E istraints IP tion Encryption al connection attributes to be r Vendor Remove Edit OK [Service-Type] を選択し、〉 | e<br>hstraints IP<br>tion Encryption<br>Hal connection attributes to be returned to<br>Vendor Valu<br>Remove Edit<br>OK Cance<br>[Service-Type] を選択し、次のウィン | Patraints IP Mution Encryption Adv<br>al connection attributes to be returned to the Ren<br>Vendor Value<br>Remove Edit<br>OK Cancel<br>[Service-Type] を選択し、次のウィンドウマ | a IP Multilink<br>tion Encryption Advanced<br>al connection attributes to be returned to the Remote<br>Vendor Value<br>Vendor Value<br>Edit<br>OK Cancel Apply<br>[Service-Type]を選択し、次のウィンドウで [Login] O | straints IP Multilink<br>tion Encryption Advanced<br>al connection attributes to be returned to the Remote<br>Vendor Value<br>Vendor Value<br>Edit<br>OK Cancel Apply<br>[Service-Type] を選択し、次のウィンドウで [Login] の値を |

次に、RADIUS の属性リストから、[Vendor-Specific] を選択します。

| Add Attributes   |  | Multivalued Attribute Information   | ? X                                    |
|--|--|---|--|
| Add Attributes To add an attribute to the Profile, select th RADIUS attributes:           Name         Vendor           Reply-Message         RADIUS S           Service-Type         RADIUS S           Turnel-Assignment-ID         RADIUS S           Turnel-ClerkEndpt         RADIUS S           Turnel-ClerkEndpt         RADIUS S           Turnel-Medium-Type         RADIUS S           Turnel-Persence         RADIUS S           Turnel-Persence         RADIUS S | e attribute and click Add  | Image: Multivalued Attribute Information       Attribute name:       Vendor-Specific       Attribute number:       26       Attribute format:       OctetString       Attribute values: |  |
| Tunnel-Pxt-Group-ID RADIUS S<br>Tunnel-Server-Auth-ID RADIUS S<br>Tunnel-Server-Auth-ID RADIUS S<br>Tunnel-Type RADIUS S<br>Vendor-Specific RADIUS S<br>Cisco-AV-Pai Cisco<br>Ignore-User-Diain-Properties Microsoft<br>USR-AT-Cal-Input-Filter U.S. Robo<br>USR-AT-Cal-Input-Filter U.S. Robo<br>USR-AT-Cal-Input-Filter U.S. Robo<br>USR-AT-Cal-Input-Filter U.S. Robo   | <ul> <li>Broup ID for a particular tunneled session</li> <li>Iandard Name used by the tunnel terminator during the autilitandard IP address of the server end of the tunnel</li> <li>Iandard Tunneling protocols to be used</li> <li>Iandard Used to support proprietary NAS features</li> <li>Cisco AV Pair VSA</li> <li>Ignore the user's dial-in properties</li> <li>tics, L Description not available</li> </ul> | Vendor Value  | Move Up<br>Move Down<br>Estrove<br>Est |
| <u> </u>   | AddCoose   |   | 0K Cancel                              |

次のウィンドウで、[Add] をクリックして、新しい VSA を追加します。[Vendor-Specific Attribute Information] ウィンドウが表示されます。[Specify network access server vendor] の 下で、[Enter Vendor Code] を選択します。Airespace VSA のベンダー コードを入力します 。Cisco Airespace VSA のベンダー コードは **14179** です。この属性は、RADIUS RFC の VSA 仕様に準拠しているため、[Yes. **It conforms.]** を選択します。

| Vendor-Specific Attribute   | Information                                  |      |
|---|--|------|
| Attribute name:<br>Vendor-Specific  |  |      |
| Specify network access servers<br>Select from list:<br>Enter Vendor Code:         | ver vendor. RADIUS Standard 14179            |      |
| Specify whether the attribute<br>vendor specific attributes.<br>Yes. It conforms. | conforms to the RADIUS RFC specification for |      |
| <ul> <li>No. It does not conform.</li> <li>Configure <u>Attribute</u></li> </ul>  |  |      |
|   | OK Cancel                                    | Conf |

[Configure Attribute]

をクリックします。[Configure VSA (RFC compliant)] ウィンドウで、ベンダーに割り当てら れる属性番号、属性の形式、および属性値を入力します。実際の値は、使用する VSA によ って異なります。ユーザごとに、次のように WLAN-ID を設定します。**属性名**: Airespace-WLAN-Id**ベンダーに割り当てられる属性番号**: 1**属性の形式**: Integer/Decimal (整数/10 進

#### 数) 值: WLAN-ID例 1

| Configure VSA (RFC compliant)     |    |       | ? × |
|-----------------------------------|----|-------|-----|
| Vendor-assigned attribute number: |    |       |     |
| 1                                 |    |       |     |
| Attribute format:                 |    |       |     |
| Decimal                           |    |       | •   |
| Attri <u>b</u> ute value:         |    |       |     |
| 2                                 |    |       |     |
|                                   |    |       |     |
|                                   |    | _     |     |
|                                   | OK | Cance |     |
|                                   |    |       |     |

ように QoS を設定します。属性名: Airespace-QoS-Levelベンダーに割り当てられる属性番号: 2属性の形式: Integer/Decimal (整数/10 進数) 値: 0 - Silver、1 - Gold、2 - Platinum、

| Configure VSA (RFC compliant)     | ? ×    |
|-----------------------------------|--------|
| Vendor-assigned attribute number: |        |
| 2                                 |        |
| <u>A</u> ttribute format:         |        |
| Decimal                           | •      |
| Attri <u>b</u> ute value:         |        |
| 3                                 |        |
|                                   |        |
|                                   |        |
| 01                                | Cancel |

3 - Bronze例 2

ザごとに、次のように DSCP を設定します。**属性名**:Airespace-DSCP**ベンダーに割り当て** られる属性番号:3属性の形式:Integer/Decimal(整数/10 進数)値:DSCP 値例 3

| complaite rom (in e compliant)   |  |  |
|--|--|--|
| Vendor-assigned attribute number:  |  |  |
| 3  |  |  |
| Attribute format:  |  |  |
| Decimal  | •  |  |
| Attri <u>b</u> ute value:  |  |  |
| 46   |  |  |
|  |  |  |
|  |  |  |
|  | OK Cancel  |  |
|  |  |  |
| のように 802.1n タグを設定します。  | ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■  | ■ユーザごとに、次<br>ッダーに割り当てら                               |
| のように 802.1p タグを設定します。<br><b>れる属性番号</b> :4 <b>属性の形式</b> :Intege   | <b>属性名</b> :Airespace-802.1p-Tag <b>べ</b> ン<br>er/Decimal(整数/10 進数) <b>値</b> :802                          | ■ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>_1p-Tag <b>例 4</b> |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br><mark>Configure V5A (RFC compliant)</mark>  | ■ <b>属性名</b> :Airespace-802.1p-Tagべこ<br>er/Decimal(整数/10 進数)値:802<br>・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ | ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b>  |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br><mark>Configure VSA (RFC compliant)</mark><br>Vendor-assigned attribute number:   | ■ <b>属性名</b> :Airespace-802.1p-Tag <b>べン</b><br>er/Decimal(整数/10 進数)値:802<br>? ➤                           | ■ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b> |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure ¥5A (RFC compliant)<br>⊻endor-assigned attribute number:<br>4   | 「 <b>属性名</b> :Airespace-802.1p-Tag <b>べン</b><br>er/Decimal(整数/10 進数)値:802<br><b>? </b> ▼                   | ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b>  |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure ¥SA (RFC compliant)<br>⊻endor-assigned attribute number:<br>4<br>Attribute format:  | , <b>属性名</b> :Airespace-802.1p-Tag <b>べ</b> ン<br>er/Decimal(整数/10 進数)値:802<br>? ➤                          | ■ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b> |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure VSA (RFC compliant)<br>Vendor-assigned attribute number:<br>4<br>Attribute format:<br>Decimal                                   | 「属性名:Airespace-802.1p-Tagべン<br>er/Decimal(整数/10 進数)値:802<br>? ➤  | ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b>  |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure VSA (RFC compliant)<br>⊻endor-assigned attribute number:<br>4<br>Attribute format:<br>Decimal<br>Attribute value:               | 「属性名:Airespace-802.1p-Tagべン<br>er/Decimal(整数/10 進数)値:802<br>? ▼  | ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b>  |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure VSA (RFC compliant)<br>⊻endor-assigned attribute number:<br>4<br>Attribute format:<br>Decimal<br>Attri <u>b</u> ute value:<br>5 | 「属性名:Airespace-802.1p-Tagべン<br>er/Decimal(整数/10 進数)値:802<br>? 文  | ■ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b> |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure VSA (RFC compliant)<br>Vendor-assigned attribute number:<br>4<br>Attribute format:<br>Decimal<br>Attri <u>b</u> ute value:<br>5 | 「属性名:Airespace-802.1p-Tagべン<br>er/Decimal(整数/10 進数)値:802<br>? ➤  | ■ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b> |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure VSA (RFC compliant)<br>⊻endor-assigned attribute number:<br>4<br>Attribute format:<br>Decimal<br>Attri <u>b</u> ute value:<br>5 | 属性名:Airespace-802.1p-Tagべ<br>er/Decimal(整数/10 進数)値:802<br>? ▼  | ■ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b> |
| のように 802.1p タグを設定します。<br>れる属性番号:4属性の形式:Intege<br>Configure VSA (RFC compliant)<br>⊻endor-assigned attribute number:<br>4<br>Attribute format:<br>Decimal<br>Attri <u>b</u> ute value:<br>5 | ■ 属性名:Airespace-802.1p-Tagペン<br>er/Decimal(整数/10 進数)値:802<br>?<br>▼  | ■ユーザごとに、次<br>ン <b>ダーに割り当てら</b><br>.1p-Tag <b>例 4</b> |

ように VLAN を設定します。属性名:Airespace-Interface-Nameベンダーに割り当てられる 属性番号:5属性の形式:String(文字列)値:インターフェイス名例 5

| Configure VSA (RFC compliant)     |    | ? ×    |                       |
|-----------------------------------|----|--------|-----------------------|
| Vendor-assigned attribute number: |    |        |                       |
| 5                                 |    |        |                       |
| Attribute format:                 |    |        |                       |
| String                            |    | •      |                       |
| Attribute value:                  |    |        |                       |
| vlan10                            |    |        |                       |
|                                   |    |        |                       |
|                                   |    |        |                       |
|                                   | OK | Canaal |                       |
|                                   |    | Cancer | <br> っ゙ <i>゚</i> ヸゔとに |

ように ACL を設定します。属性名: Airespace-ACL-Nameペンダーに割り当てられる属性番号: 6属性の形式: String (文字列) 値: ACL 名例 6

| Configure VSA (RFC compliant)     | ? ×       |
|-----------------------------------|-----------|
| Vendor-assigned attribute number: |           |
| 6                                 |           |
| <u>A</u> ttribute format:         |           |
| String                            |           |
| Attri <u>b</u> ute value:         |           |
| ACL1                              |           |
|                                   |           |
|                                   |           |
|                                   | OK Cancel |

- 8. VSA の設定が完了したら、[OK] をクリックします。やがて、ユーザ プロファイル ウィンド ウが表示されます。
- 9. [Finish] をクリックして、設定を完了します。リモート アクセス ポリシーの下に新しいポリ シーが表示されています。

| 🐤 Internet Authentication Service   |              |       |
|---|--------------|-------|
| Action View 🖉 🖚 🔁 🔢 🚱 😭   |              |       |
| Tree  | Name         | Order |
| Internet Authentication Service (Local)  Clients  Remote Access Logging  Remote Access Policies | Arespace VSA | 1     |
|   |              |       |

### <u>設定例</u>

この例では、WLAN は Web 認証用に設定されています。ユーザはIAS RADIUSサーバによって認証され、RADIUSサーバはユーザごとにQoSポリシーを割り当てるように設定されます。

| and the second s | MONITOR WLANS CO         | NTROLLER WIRELESS SECURITY MANAG             | SEMENT COMMANDS                              | HELP  |
|--|--------------------------|--|--|---|
| <b>NNS</b>   | WLANs > Edit             |  |  | < Back Apply                                |
| INS  | WLAN ID                  | 1  |  |   |
| ANs  | WLAN SSID                | SSID-WLC2                                    |  |   |
| Groups VLAN  | General Policies         |  | Security Policies                            |   |
|  | Radio Policy             | All 🗸  |  |   |
|  | Admin Status             | Enabled                                      | Layer 2 Security                             | None  |
|  | Session Timeout (secs)   | 0  |  | MAC Filtering                               |
|  | Quality of Service (QoS) | Silver (best effort)                         | Laver 3 Security                             | None  |
|  | WMM Policy               | Disabled w                                   |  | Web Policy *                                |
|  | 7920 Phone Support       | Client CAC Limit CAP CAC Limit               |  | Authentication O Passthro                   |
|  | Broadcast SSID           | Enabled                                      | Preauthenticatio                             | none 🖌                                      |
|  | Aironet IE               | Fnabled                                      | AC   |   |
|  | Allow AAA Override       | ✓ Enabled                                    | * Web Policy cannot<br>and L2TP.             | t be used in combination with IPs           |
|  | Client Exclusion         | Enabled ** 60                                | ** When client excl                          | usion is enabled, a timeout value           |
|  | DUCK Comme               | Timeout Value (secs)                         | zero means infinity(<br>to reset excluded of | will require administrative overri<br>ents) |
|  | DHCP Server              | Overnide                                     | *** CKIP is not sup                          | ported by 10xx APs                          |
|  | DHCP Addr. Assignment    | Required                                     |  |   |
|  | Interface Name           | internal M                                   |  |   |
|  | MFP Version Required     | 1  |  |   |
|  | Generation               | (Global MFP Disabled)                        |  |   |
|  | H-REAP Local Switching   | ant connected with 1955 C 1979, SOTE CRANITS |  |   |
|  | and FORTRESS authentice  | tions.                                       |  |   |
|  | Radius Servers           |  |  |   |
|  |                          | Authentication Servers Accounting Servers    |  |   |
|  | Server 1                 | IP:172.16.1.1. Port:1812 V none V            | $\geq$                                       |   |

ウィンドウに表示されているように、Web 認証がイネーブルにされています。認証サーバは 172.16.1.1 で、WLAN では、AAA Override もイネーブルにされています。この WLAN のデフォ ルトの QoS は、Silver に設定されています。

IAS RADIUS サーバでは、RADIUS Access Accept 要求に Bronze の QoS 属性を返すように、リ モート アクセス ポリシーが設定されています。これは、QoS 属性専用に VSA を設定するときに 実施されます。

| Configure VSA (RFC compliant)          | ? ×       |
|--|-----------|
| ⊻endor-assigned attribute number:<br>2 |           |
| <u>A</u> ttribute format:<br>Decimal   | <b>•</b>  |
| Attri <u>b</u> ute value:<br>3         |           |
| ·                                      |           |
|  | OK Cancel |

IASサーバでリモートアクセスポリシーを設定する方法の詳細については、このドキュメントの 「<u>IASのリモートアクセスポリシーの設定</u>」セクションを参照してください。

IASサーバ、WLC、およびLAPがこのセットアップ用に設定されると、ワイヤレスクライアント はWeb認証を使用して接続できます。

#### 確認

ここでは、設定が正常に機能しているかどうかを確認します。

ユーザがユーザIDとパスワードを使用してWLANに接続すると、WLCはクレデンシャルをIAS RADIUSサーバに渡し、IAS RADIUSサーバはリモートアクセスポリシーで設定された条件とユー ザプロファイルに対してユーザを認証します。ユーザ認証に成功した場合には、RADIUS サーバ は、AAA Override 値も含む RADIUS Accept 要求を返します。この場合には、ユーザの QoS ポ リシーが返されます。

認証中に発生するイベントのシーケンスを参照するために、debug aaa all enable コマンドを発行 できます。次に出力例を示します。

| (Ci | sco ( | Cont | croller) > | > debug | g aaa all enable  |
|-----|-------|------|------------|---------|---|
| Wed | Apr   | 18   | 18:14:24   | 2007:   | User admin authenticated                                |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for |
|     |       |      |            |         | mobile 28:1f:00:00:00:00                                |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | AuthorizationResponse: 0xbadff97c                       |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | structureSize70   |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | resultCode0   |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | protocolUsed0x0000008                                   |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | proxyState  |
|     |       |      |            |         | 28:1F:00:00:00:00-00:00                                 |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | Packet contains 2 AVPs:                                 |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | AVP[01] Service-Type                                    |
|     |       |      |            |         | 0x0000006 (6) (4 bytes)                                 |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | AVP[02] Airespace / WLAN-Identifier                     |
|     |       |      |            |         | 0x00000000 (0) (4 bytes)                                |
| Wed | Apr   | 18   | 18:14:24   | 2007:   | User admin authenticated                                |

Wed Apr 18 18:14:24 2007: 29:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile 29:1f:00:00:00:00 Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c 29:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007: Packet contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-Type..... 0x00000006 (6) (4 bytes) AVP[02] Airespace / WLAN-Identifier..... Wed Apr 18 18:14:24 2007: 0x00000000 (0) (4 bytes) Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-VLAN10 Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc Wed Apr 18 18:15:08 2007: Callback......0x8250c40 protocolType.....0x0000001 proxyState..... Wed Apr 18 18:15:08 2007: Wed Apr 18 18:15:08 2007: 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007: Packet contains 8 AVPs (not shown) Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful transmission of Authentication Packet (id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-96:ac Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00 00 00 00 00 00 00 00 00 ...h..... Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73 65 72 2d 56 4c 41 4e 31 .....User-VLAN1 Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a ba 57 38 11 bc 9a 5d 59 0...2W.\*.W8...]Y Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 00 01 04 06 ac 10 01 1e 20 ........ Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00 00 37 63 01 06 00 00 00 .WLC2....7c.... Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e 30 2e 30 2e 31 1e 0d 31 37 32 ...20.0.0.1..172 Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e 31 2e 33 30 .16.1.30 Wed Apr 18 18:15:08 2007: 00000000: 02 1a 00 46 3f cf 1b cc e4 ea 41 3e 28 7e cc bc ....F?.....A>(~... Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00 37 63 02 06 00 00 03 ..a....7c..... Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20 37 d0 03 e6 00 00 01 37 Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01 c7 7a 8b 35 20 31 80 00 00 ....z.5.1... Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 1b . . . . . . Wed Apr 18 18:15:08 2007: \*\*\*\*Enter processIncomingMessages: response code=2 Wed Apr 18 18:15:08 2007: \*\*\*\*Enter processRadiusResponse: response code=2 Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Access-Accept received from RADIUS server 172.16.1.1 for mobile 00:40:96:ac:e6:57 receiveId = 0 Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520 Wed Apr 18 18:15:08 2007: structureSize.....114 resultCode.....0 protocolUsed.....0x0000001 Wed Apr 18 18:15:08 2007: Wed Apr 18 18:15:08 2007: Wed Apr 18 18:15:08 2007: proxyState..... 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007: Packet contains 3 AVPs: Wed Apr 18 18:15:08 2007: AVP[01] Airespace / QOS-Level..... 0x0000003 (3) (4 bytes) Wed Apr 18 18:15:08 2007: AVP[02] Service-Type..... 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:08 2007: AVP[03] Class..... DATA (30 bytes) Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57

source: 48, valid bits: 0x3 qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1 dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: ' Wed Apr 18 18:15:12 2007: AccountingMessage Accounting Start: 0xa64c8bc Wed Apr 18 18:15:12 2007: Packet contains 13 AVPs: AVP[01] User-Name..... Wed Apr 18 18:15:12 2007: User-VLAN10 (11 bytes) Wed Apr 18 18:15:12 2007: AVP[02] Nas-Port..... 0x0000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[03] Nas-Ip-Address..... 0xac10011e (-1408237282) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[04] NAS-Identifier.... 0x574c4332 (1464615730) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[05] Airespace / WLAN-Identifier..... 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[06] Acct-Session-Id..... 4626602c/00:40:96:ac:e6:57/16 (29 bytes) AVP[07] Acct-Authentic..... Wed Apr 18 18:15:12 2007: 0x00000001 (1) (4 bytes) AVP[08] Tunnel-Type..... Wed Apr 18 18:15:12 2007: 0x000000d (13) (4 bytes) AVP[09] Tunnel-Medium-Type..... Wed Apr 18 18:15:12 2007: 0x0000006 (6) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[10] Tunnel-Group-Id..... 0x3230 (12848) (2 bytes) AVP[11] Acct-Status-Type..... Wed Apr 18 18:15:12 2007: 0x00000001 (1) (4 bytes) AVP[12] Calling-Station-Id..... Wed Apr 18 18:15:12 2007: 20.0.0.1 (8 bytes) Wed Apr 18 18:15:12 2007: AVP[13] Called-Station-Id..... 172.16.1.30 (11 bytes)

出力結果から、ユーザが認証されていることが確認できます。また、RADIUS の Accept メッセ ージとともに、AAA Override 値が返されています。この例では、ユーザには Bronze の QoS ポ リシーが与えられています。

これは、WLC GUI でも同じように確認できます。以下が一例です。

|   | MONITOR WLANS CONTR           | OLLER WIRELESS SECU | JRITY MANAGEMENT COMM   | IANDS HELP             |
|---|-------------------------------|---------------------|-------------------------|------------------------|
| nitor   | Clients > Detail              |                     |                         | < Back Link Test Remov |
| nmary   | Client Properties             |                     | AP Properties           |                        |
| tistics<br>entroller  | MAC Address                   | 00:40:96:ac:e6:57   | AP Address              | 00:0b:85:5b:fb:d0      |
| Ports<br>Wireless<br>Rogue APs<br>Known Rogue APs<br>Rogue Clients<br>Adhoc Rogues<br>802.11a Radios<br>002.11b/g Radios<br>Clients<br>RADIUS Servers | IP Address                    | 20.0.0.1            | AP Name                 | ap:5b:fb:d0            |
|   | User Name                     | User-VLAN10         | AP Type                 | 802.11a                |
|   | Port Number                   | 1                   | WLAN SSID               | SSID-WLC2              |
|   | Interface                     | internal            | Status                  | Associated             |
|   | VLAN ID                       | 20                  | Association ID          | 1                      |
|   | CCX Version                   | CCXv3               | 802.11 Authentication   | Open System            |
|   | E2E Version                   | Not Supported       | Reason Code             | 0                      |
|   | Mobility Role                 | Local               | Status Code             | 0                      |
|   | Mobility Peer IP Address      | N/A                 | CF Pollable             | Not Implemented        |
|   | Policy Manager State          | RUN                 | CF Poll Request         | Not Implemented        |
|   | Security Information          |                     | Short Preamble          | Not Implemented        |
|   | Security Policy Completed     | Yes                 | PBCC<br>Channel Agility | Not Implemented        |
|   | Policy Type                   | N/A                 |                         | Not Implemented        |
|   | Encryption Cipher             | None                | Timeout                 | 0                      |
|   | EAP Type                      | N/A                 | WEP State               | WEP Disable            |
|   | Quality of Service Properties |                     |                         |                        |
|   | WMM State                     | Disabled            |                         |                        |
|   | QoS Level                     | Bronze              |                         |                        |
|   | Diff Serv Code Point (DSCP)   | disabled            |                         |                        |
|   | 802.1p Tag                    | disabled            |                         |                        |
|   | Average Data Rate             | disabled            |                         |                        |

**注:この**SSIDのデフォルトQoSプロファイルはSilverです。ただし、AAA Overrideが選択され、 ユーザはIASサーバでBronzeのQoSプロファイルを使用して設定されているため、デフォルトの QoSプロファイルは上書きされます。

# <u>トラブルシュート</u>

WLC で debug aaa all enable コマンドを使用すると、設定のトラブルシューティングを行うこと ができます。稼動中のネットワークにおけるこのデバッグの出力例は、このドキュメントの「<u>確</u> 認」セクションで参照できます。

注: debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

## 関連情報

- <u>Cisco ワイヤレス LAN コントローラ コンフィギュレーション ガイド、リリース 4.0</u>
- WLC と Cisco Secure ACS を使用した SSID に基づく WLAN アクセス制限の設定例
- •<u>ワイヤレス製品に関するサポート</u>
- ・ <u>テクニカル サポートとドキュメント Cisco Systems</u>