Cisco Secure ACS サーバでの Cisco Airespace VSA の設定例

目次

概要

Cisco Secure Access Control Server (ACS) リリース 4.0 以降は、デフォルトで Cisco Airespace Vendor Specific Attributes (VSA) をサポートします。 リリース 4.0 よりも前の ACS バージョンでは、Cisco Airespace ディクショナリ ファイルを Cisco Secure ACS にインポートする必要があります。 このドキュメントでは、4.0 よりも前のバージョンで Cisco Secure ACS に Cisco Airespace ディクショナリ ファイルをインポート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。

前提条件

要件

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。

- Cisco Secure サーバでワイヤレス クライアントを認証するように設定する方法についての基本的な知識
- Cisco Unified Wireless Security ソリューションについての知識

使用するコンポーネント

このドキュメントの情報は、Cisco Secure ACS サーバ バージョン 3.2 に基づいています。

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。

表記法

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。

背景説明

Cisco Secure ACS リリース 4.0 以降 ACS は、デフォルトで次の Cisco Airespace VSA をサポートしています。

- Aire-WLAN-Id
- Aire-QoS-Level
- Aire-DSCP
- Aire-802.1P-Tag
- Aire-Interface-Name
- Aire-ACL-Name

これらの属性の詳細については、『*Cisco Wireless LAN Controller 設定ガイド、リリース 4.1*』の「アイデンティティ ネットワーキングで使用する RADIUS 属性」の項を参照してください。

リリース 4.0 よりも前の ACS バージョンでは、Cisco Airespace ディクショナリ ファイルを Cisco Secure ACS にインポートする必要があります。 次のセクションは、Cisco Airespace ディクショナリ ファイルを Cisco Secure ACS にインポートする方法について説明しています。

Cisco Secure ACS で RADIUS の属性を使用する前に

指定のユーザに特定の属性が送信されるように設定するには、次の項目を確認する必要があります。

- [Network Configuration] セクションで、アクセス デバイスに対応する AAA クライアント エントリを設定する必要があります。 このアクセス デバイスは、ユーザが AAA クライアントに送信する RADIUS 属性を使用できるように、ユーザにネットワークへのアクセスを許可します。
- [Interface Configuration] セクションで、属性を有効にしてユーザ プロファイルまたはユーザ グループ プロファイルのページに表示されるようにする必要があります。 各属性は、その属性をサポートする RADIUS に対応するページで有効にできます。 たとえば、IETF RADIUS Session-Timeout 属性（27）は [RADIUS (IETF)] ページに表示されます。**注:** ユーザごとの RADIUS 属性は、[Interface Configuration] ページには表示されないため、デフォルトでは有効になっていません。 ユーザごとに属性を有効にするには、[Advanced Options] ページの [Interface Configuration] セクションでユーザごとに [TACACS+/RADIUS Attributes] オプションを有効にする必要があります。 ユーザごとの属性を有効にすると、ユーザ列はその属性の [Interface Configuration] ページで無効として表示されます。
- ユーザに対する認証を制御するプロファイルは、ユーザまたはグループ編集ページ、または

[Shared RADIUS Authorization Component] ページにあり、ここで属性を有効にする必要があります。 この属性が有効の場合 ACS は、Access-Accept メッセージで AAA クライアントに属性を送信します。 属性に関連付けられたオプションで、AAA クライアントに送信する属性の値を決定できます。**注:** ユーザ プロファイル内の設定は、グループ プロファイル内の設定よりも優先されます。 たとえば、ユーザ プロファイルで Session-Timeout が設定されていて、ユーザが割り当てられているグループでも設定されている場合、ACS はユーザ プロファイルで指定された Session-Timeout 値を AAA クライアントに送信します。

Cisco Airespace VSA の Cisco Secure ACS へのインポート

Cisco Airespace VSA を Cisco Secure ACS にインポートするには、次の手順を完了する必要があります。

1. RADIUS ベンダー/VSA インポート ファイルで Cisco Airespace VSA を定義します。
2. 新しく RADIUS ベンダーと VSA を追加する RADIUS ベンダー スロットを決定します。
3. Cisco Airespace VSA を Cisco Secure ACS に追加します。

注: アプリケーション **regedit** が実行されていないことを確認します。 regedit が Cisco Secure ACS Windows サーバ上で実行されている場合、RADIUS ベンダーと VSA のカスタム セットを追加するために必要なレジストリの更新の妨げとなる場合があります。

RADIUS Vendor/VSA インポート ファイルでの Cisco Airespace VSA の定義

Cisco Secure ACS に Cisco Airespace VSA セットをインポートするには、RADIUS ベンダーと VSA のセットをインポート ファイルで定義する必要があります。 このセクションでは、RADIUS VSA インポート ファイルの形式と内容について詳しく説明します。

RADIUS ベンダー/VSA インポート ファイルでは、Windows の **.ini** ファイル形式を使用します。各 RADIUS ベンダー/VSA インポート ファイルは、3 つのタイプのセクションで構成されています。 次の表でこれらのセクションの詳細が示されています。 各セクションは、セクション ヘッダー、およびキーと値のセットで構成されています。 RADIUS ベンダー/VSA インポート ファイル内でのセクションの順序に意味はありません。

RADIUS VSA Import File Section Types			
Section	**Required**	**Number**	**Description**
Vendor and VSA set definition	Yes	1	Defines the RADIUS vendor and VSA set.
Attribute definition	Yes	1 to 255	Defines a single attribute of the VSA set.
Enumeration	No	0 to 255	Defines enumerations for attributes with integer data types.

ベンダーと VSA のセットの定義

各 RADIUS ベンダー/VSA インポート ファイルには、ベンダーと VSA のセットのセクションが 1 つ必要です。 セクション ヘッダーは、[User Defined Vendor] にする必要があります。

Vendor and VSA Set Keys			
Keys	**Required**	**Value Required**	**Description**
Name	Yes	Vendor name	The name of the RADIUS vendor.
IETF Code	Yes	An integer	The IETF-assigned vendor number for this vendor.
VSA *n* (where *n* is the VSA number)	Yes—you can define 1 to 255 VSAs	Attribute name	The name of a VSA. For each VSA named here, the file must contain a corresponding attribute definition section. **Note** Attribute names must be unique within the RADIUS vendor/VSA import file, and within the set of all RADIUS attributes in Cisco Secure ACS. To facilitate this, we recommend that you prefix the vendor name to each attribute name, such as "widget-encryption" for an encryption-related attribute for the vendor Widget. This also makes accounting logs easier to understand.

たとえば、このベンダーと VSA のセットのセクションでは、IETF 割り当てベンダー番号が 14179 のベンダー Cisco Airespace を定義します。

```
[User Defined Vendor]
Name=Airespace
IETF Code=14179
VSA 1=Airespace-WLAN-Id
VSA 2=Airespace-QoS-Level
VSA 3=Airespace-DSCP
VSA 4=Airespace-802.1p-Tag
VSA 5=Airespace-Interface-Name
VSA 6=Airespace-ACL-Name
```

属性定義

各 RADIUS ベンダー/VSA インポート ファイルには、ベンダーと VSA のセットのセクションで定義される属性ごとに 1 つの属性定義セクションが必要です。 各属性定義セクションのセクション ヘッダーは、ベンダーと VSA のセットのセクションにある属性に定義されている属性名と一致する必要があります。 次の表に、属性定義セクションで有効なキーの一覧を示します。

Attribute Definition Keys			
Keys	**Required**	**Value Required**	**Description**
Type	Yes	See Description	The data type of the attribute. It must be one of the following: • STRING • INTEGER • IPADDR If the attribute is an integer, Enums key is valid.

Profile	Yes	See Description	The attribute profile defines if the attribute is used for authorization or accounting (or both). At least one of the following two values must be present in the Profile key definition:
			▪ **IN**—The attribute is used for accounting. After you add the attribute to Cisco Secure ACS, you can configure your RADIUS accounting log to record the new attribute.
			▪ **OUT**—The attribute is used for authorization. In addition, you can use the value "MULTI" to allow several instances of the attribute per RADIUS message.
			Combinations are valid. For example:
			`Profile=MULTI OUT`
			or
			`Profile=IN OUT`

Enums	No (only valid when the TYPE value is INTEGER)	Enumera-tions section name	The name of the enumeration section. **Note** Several attributes can reference the same enumeration section.

たとえば、この属性定義セクションは、インターフェイス名を指定するために使用される Airespace-Interface-Name VSA を定義します。

```
[Airespace-Interface-Name]
Type=STRING
Profile=OUT
```

列挙型定義

列挙型定義を使用して、整数型属性の有効な数値ごとにテキストベースの名前を関連付けることができます。 Cisco Secure ACS HTML インターフェイスの [Group Setup] セクションと [User Setup] セクションでは、定義するテキスト値が、列挙型を使用する属性に関連付けられたリストに表示されます。 列挙型定義セクションは、属性定義セクションから参照される場合にだけ必要です。 列挙型定義セクションを参照できるのは、整数型の属性だけです。

各列挙型定義のセクション ヘッダーは、そのヘッダーを参照する Enums キーの値と一致している必要があります。 列挙型定義セクションは、1 つ以上の Enums キーで参照できるため、共通の列挙型定義を再利用できます。 列挙型定義セクションには、キーを 1000 個まで指定できます。 次の表に、列挙型定義セクションで有効なキーの一覧を示します。

Enumerations Definition Keys			
Keys	**Required**	**Value Required**	**Description**

n
 	
(See description.)
	Yes	String	For each valid integer value of the corresponding attribute, an enumerations section must have one key.
			
			Each key defines a string value associated with an integer value. Cisco Secure ACS uses these string values in the HTML interface.
			
			For example, if 0 through 4 are valid integer values for a given attribute, its enumeration definition would contain the following:
			
			`0=value0`
			`1=value1`
			`2=value2`
			`3=value3`
			`4=value4`

たとえば、この列挙型定義セクションでは、QOS-VALUES 列挙型を定義し、文字列値 silver を整数 0 と関連付け、文字列値 Gold を整数 1 と関連付けています。

```
[QOS-VALUES]
0=Silver
1=Gold
2=Platinum
3=Bronze
```

Airespace ディクショナリ ファイル

AirespaceVSA.ini ファイルを作成するために必要なこれらすべてのパラメータを考慮する必要があります。 次に例を示します。

```
[User Defined Vendor]
Name=Airespace
IETF Code=14179
VSA 1=Airespace-WLAN-Id
VSA 2=Airespace-QoS-Level
VSA 3=Airespace-DSCP
VSA 4=Airespace-802.1p-Tag
VSA 5=Airespace-Interface-Name
```

```
VSA 6=Airespace-ACL-Name

RadiusExtensionPoints=EAP

[Airespace-WLAN-Id]
Type=INTEGER
Profile=OUT

[Airespace-QoS-Level]
Type=INTEGER
Profile=OUT
Enums=QOS-VALUES

[QOS-VALUES]
0=Silver
1=Gold
2=Platinum
3=Bronze

[Airespace-DSCP]
Type=INTEGER
Profile=OUT

[Airespace-802.1p-Tag]
Type=INTEGER
Profile=OUT

[Airespace-Interface-Name]
Type=STRING
Profile=OUT

[Airespace-ACL-Name]
Type=STRING
Profile=OUT
```

このファイルを **Airespace.ini** としてハード ドライブに保存します。できれば **C:\Cisco Secure ACS 3.2\Utils** ディレクトリに保存します。 次に、VSA を Cisco Secure ACS に追加します。

Cisco Airespace VSA の Cisco Secure ACS への追加

Utils ディレクトリ (C:\Cisco Secure ACS 3.2\Utils ディレクトリ) で使用可能な **CSUtil.exe -addUDV** コマンドを使用して、RADIUS ベンダーと VSA のカスタム セットを、最大 10 セット Cisco Secure ACS に追加できます。 RADIUS ベンダーと VSA の各セットは、10 個あるユーザ定義 RADIUS ベンダー スロットのいずれかのスロットに追加されます。

CSUtil.exe -listUDV コマンドにより、ユーザ定義 RADIUS ベンダー スロットがスロットの番号順に一覧表示されます。 CSUtil.exe コマンドにより、カスタム RADIUS ベンダーを含んでいないスロットが [Unassigned] として一覧表示されます。 未割り当てスロットは空です。 [Unassigned] として一覧表示されたスロットにカスタム RADIUS ベンダーを追加できます。 次に例を示します。

```
C:\Program Files\CiscoSecure ACS v3.2\Utils>csutil -listUDV
CSUtil v3.2(1.20), Copyright 1997-2001, Cisco Systems Inc
UDV 0 - RADIUS (Airespace)
UDV 1 - Unassigned
UDV 2 - Unassigned
UDV 3 - Unassigned
UDV 4 - Unassigned
UDV 5 - Unassigned
UDV 6 - Unassigned
UDV 7 - Unassigned
```

```
UDV 8 - Unassigned
UDV 9 - Unassigned
```

CSUtil.exe コマンドで RADIUS ベンダーと VSA のカスタム セットを Cisco Secure ACS に追加すると、すべての Cisco Secure ACS サービスは自動的に停止し、再起動されます。 また、このプロセスの実行中にユーザ認証は行われません。

Cisco Airespace VSA を Cisco Secure ACS に追加するためにこれらの手順を繰り返します。

1. Cisco Secure ACS が稼働するコンピュータで、MS DOS コマンド プロンプトを開き、ディレクトリを CSUtil.exe があるディレクトリに変更します。 たとえば、Cisco Secure ACS が C:\Cisco Secure ACS 3.2 ディレクトリにインストールされている場合、Utils ディレクトリは、このディレクトリの下にあります。 DOS プロンプトから次を入力します。`C:\Cisco Secure ACS 3.2\cd Utils`

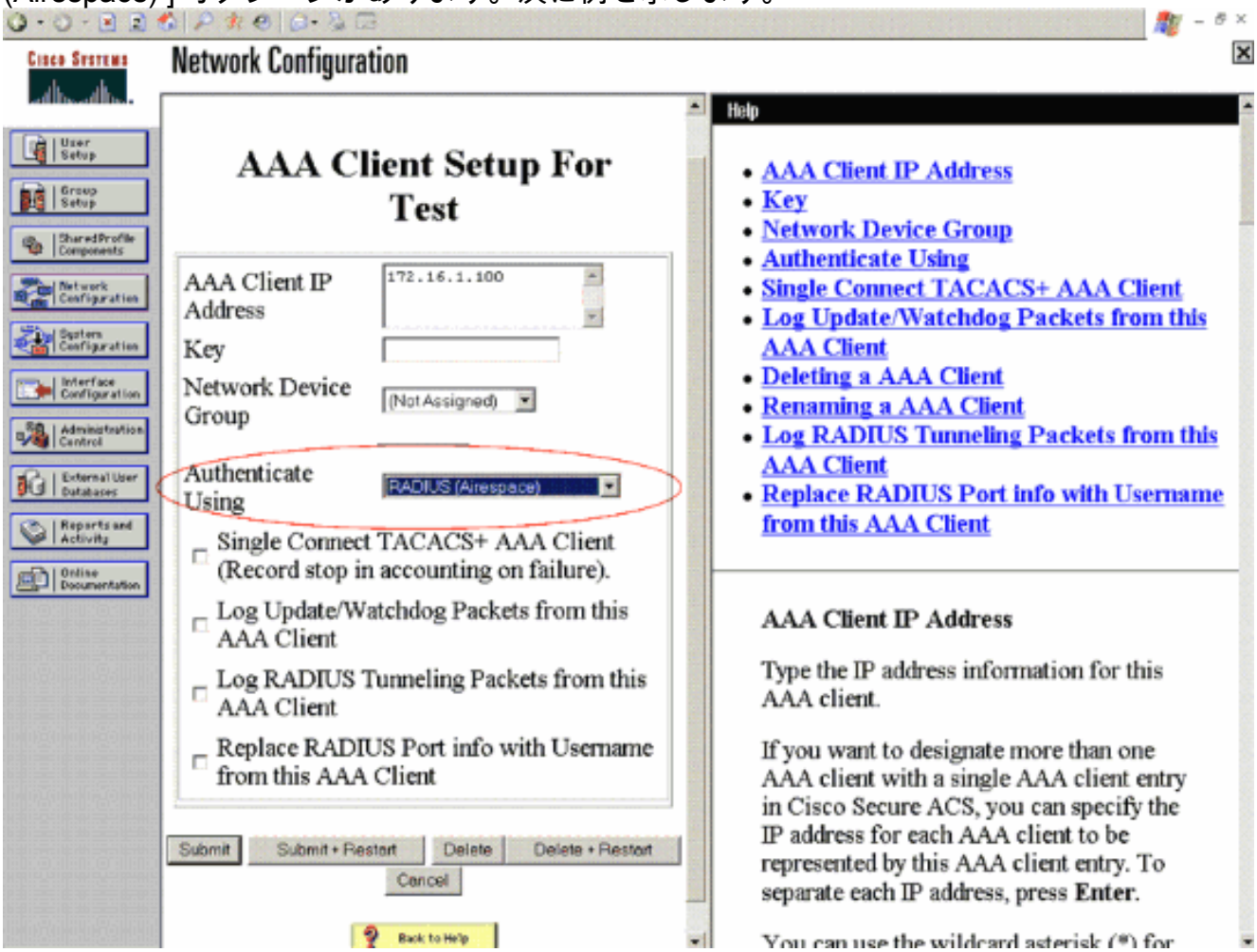
   ```
   C:\Cisco Secure ACS 3.2\Utils
   ```
2. 次のコマンドを入力します。`CSUtil.exe -addUDV slot-number filename`ここで、**slot-number** には未使用の Cisco Secure ACS RADIUS ベンダー スロットを、**filename** には RADIUS ベンダー/VSA インポート ファイルの名前を入力します。 filename には、RADIUS ベンダー/VSA インポート ファイルへの相対パスまたは絶対パスを含めることができます。 **Enter** キーを押します。たとえば、**C:\Cisco Secure ACS 3.2\Utils\Airespace.ini** で定義された Cisco Airespace VSA をスロット 5 に追加するには、コマンドは次のようになります。`CSUtil.exe -addUDV 5 Airespace.ini`CSUtil.exe により確認プロンプトが表示されます。
3. VSA を追加し、そのプロセスの実行中はすべての Cisco Secure ACS サービスを停止するには、**Y** と入力して Enter を押します。CSUtil.exe により Cisco Secure ACS サービスが停止され、ベンダー/VSA 入力ファイルが解析され、新しい RADIUS ベンダーと VSA が ACS に追加されます。 このプロセスには数分かかることがあります。 処理が完了すると、CSUtil.exe によって Cisco Secure ACS サービスが再起動されます。次に例を示します。

   ```
   C:\Program Files\CiscoSecure ACS v3.2\Utils>csutil -addUDV 0 Airespace.ini
   CSUtil v3.2(1.20), Copyright 1997-2001, Cisco Systems Inc

   Adding or removing vendors requires ACS services to be re-started.
   Please make sure regedit is not running as it can prevent registry
   backup/restore operations

   Are you sure you want to proceed? (Y or N)Y
   Parsing [.\Airespace.ini] for addition at UDV slot [0]
   Stopping any running services
   Creating backup of current config
   Adding Vendor [Airespace] added as [RADIUS (Airespace)]
   Adding VSA [Airespace-WLAN-Id]
   Adding VSA [Airespace-QoS-Level]
   Adding VSA [Airespace-DSCP]
   Adding VSA [Airespace-802.1p-Tag]
   Adding VSA [Airespace-Interface-Name]
   Adding VSA [Airespace-ACL-Name]
   Done
   Checking new configuration...
   New configuration OK
   Re-starting stopped services
   ```

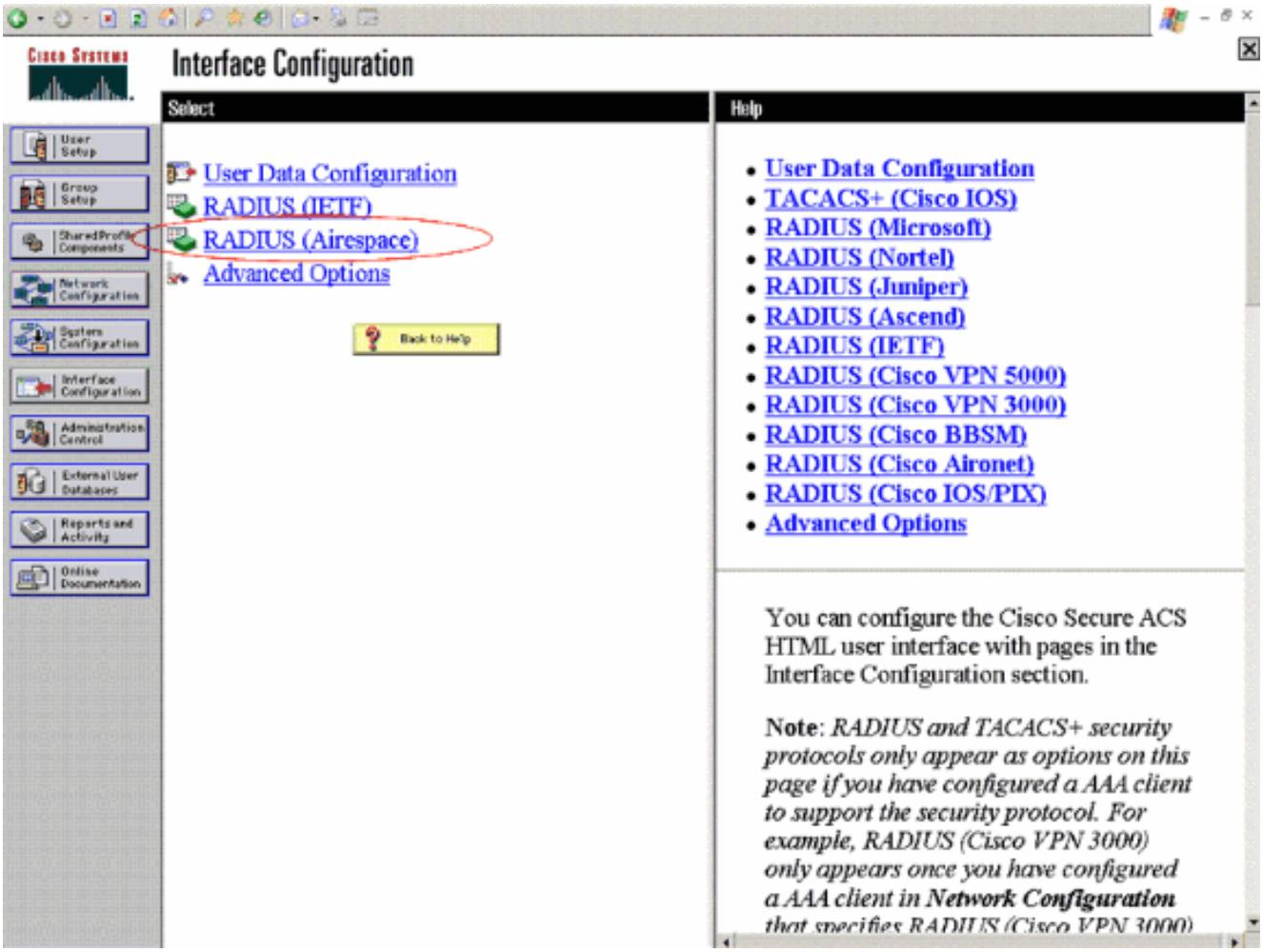
確認

Cisco Airespace VSA が Cisco Secure ACS に追加されたら、Cisco Secure ACS GUI からその結果を確認できます。 確認するには、次の手順を実行します。

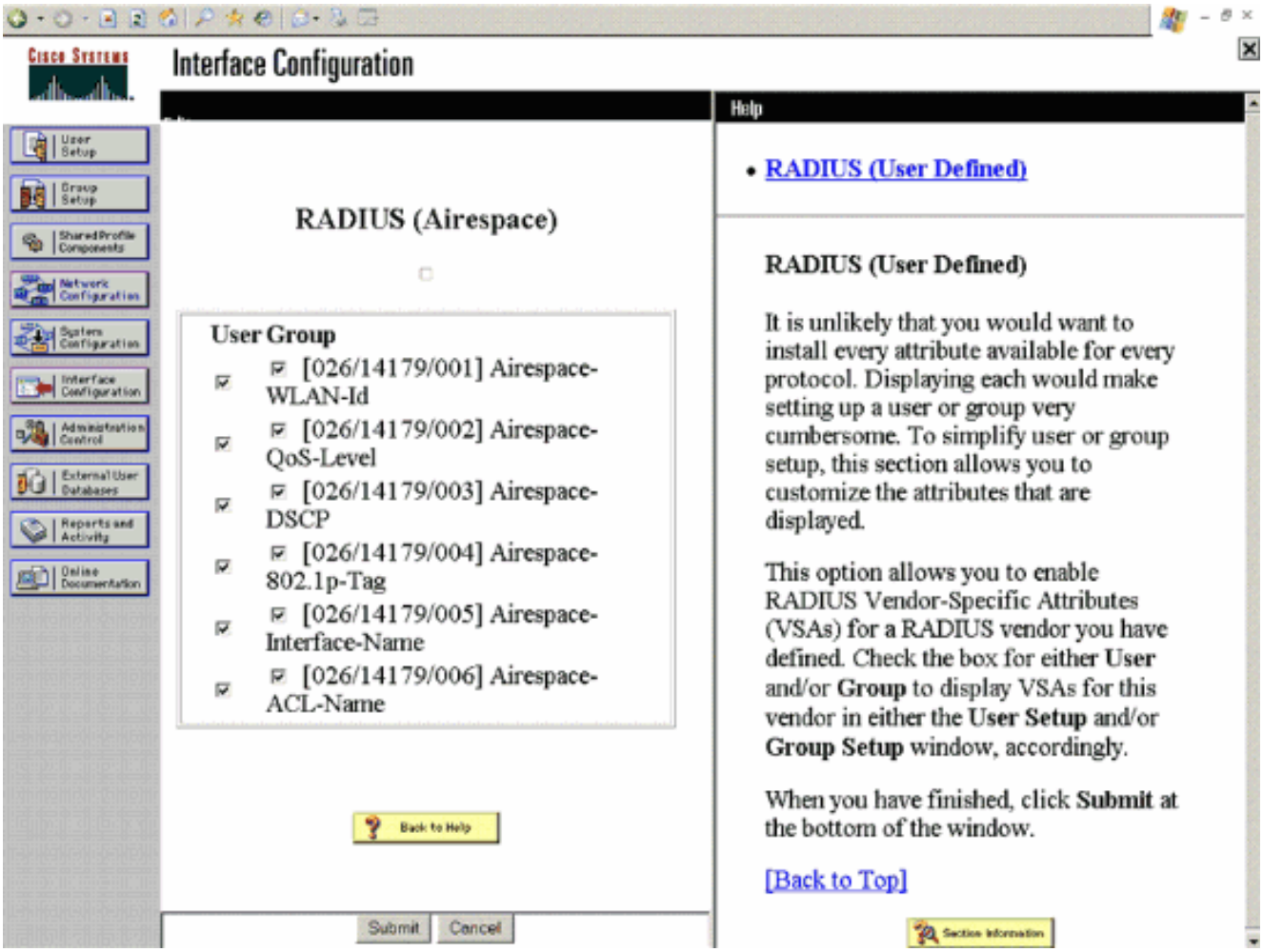
1. Cisco Secure ACS GUI にログインします。
2. 左側のメニューから [Network Configuration] をクリックし、[Add a AAA client] ページに移動します。[AAA Client] ウィンドウの [Authenticate Using] プルダウン メニューに [RADIUS (Airespace)] オプションがあります。次に例を示します。



[Interface Configuration] ページに RADIUS（Airespace）属性が一覧表示されています。**注**: [Network Configuration] セクションで、ユーザにネットワーク アクセスを許可するアクセス デバイスに対応した AAA クライアント エントリが、AAA クライアントに送信する RADIUS（Airespace）属性を使用するように設定する必要があります。 設定すると、対応する RADIUS 属性が [Interface Configuration] ページにリストされます。



3. このページで [RADIUS (Airespace)] リンクをクリックすると属性が表示され、選択することができます。



トラブルシューティング

Airespace ディクショナリ ファイルが Cisco Secure ACS にインポートされていない場合、次を確認してください。

- 適切な形式の .ini (VSA インポート ファイル) ファイルをインポートしていることを確認してください。 ファイルの形式が正しくない場合、次のエラー メッセージが表示されます。
  ```
  C:\Program Files\CiscoSecure ACS v3.2\Utils>csutil -addUDV 0 Airespace.dct CSUtil v3.2(1.20), Copyright 1997-2001, Cisco Systems Inc Adding or removing vendors requires ACS services to be re-started. Please make sure regedit is not running as it can prevent registry backup/restore operations Are you sure you want to proceed? (Y or N)Y Parsing [.\Airespace.ini] for addition at UDV slot [0] Cant find [Name] value
  ```
- ディクショナリをインポートしようとしているベンダーのスロットが空いていて、別のベンダーのディクショナリに割り当てられていないことを確認します。 すでに割り当てられているスロットに VSA をインストールしようとすると、このエラーが発生します。
  `Vendor Slot already configured, specify alternate value` 空のスロットのリストを表示するには、CSUtil.exe -listUDV コマンドを使用します。

関連情報

- ワイヤレス LAN コントローラでサポートされる RADIUS 属性
- MS IAS Radius サーバでの Cisco Airespace VSA の設定例
- コントローラ上で管理ユーザの RADIUS サーバ認証を行うための設定例
- 『Cisco Secure ACS ユーザ ガイド (Windows Server 3.2 用)』

- テクニカルサポートとドキュメント - Cisco Systems