

Cisco Airespace VSAs on Cisco Secure ACS Server Configuration Example

Document ID: 97849

Introduction

Prerequisites

Requirements

Components Used

Conventions

Background Information

Before Using RADIUS Attributes on Cisco Secure ACS

Import the Cisco Airespace VSAs to Cisco Secure ACS

Define the Cisco Airespace VSAs in a RADIUS Vendor/VSA Import File

Airespace Dictionary File

Add the Cisco Airespace VSAs to the Cisco Secure ACS

Verify

Troubleshoot

Related Information

Introduction

Cisco Secure Access Control Server (ACS) release 4.0 and later supports the Cisco Airespace Vendor Specific Attributes (VSA) by default. For ACS versions before release 4.0, the Cisco Airespace dictionary file must be imported to the Cisco Secure ACS. This document explains how to import the Cisco Airespace dictionary file to the Cisco Secure ACS for versions before 4.0. The vendor code for Cisco Airespace VSAs is 14179.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of how to configure a Cisco Secure server to authenticate wireless clients
- Knowledge of Cisco Unified Wireless Security Solutions

Components Used

The information in this document is based on Cisco Secure ACS server version 3.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

With Cisco Secure ACS release 4.0 and later, the ACS supports these Cisco Airespace VSAs by default:

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

For more information on these attributes, refer to the RADIUS Attributes Used in Identity Networking section of *Cisco Wireless LAN Controller Configuration Guide, Release 4.1*.

For ACS versions before release 4.0, the Cisco Airespace dictionary file must be imported to the Cisco Secure ACS. The next section explains how to import the Cisco Airespace dictionary file to the Cisco Secure ACS.

Before Using RADIUS Attributes on Cisco Secure ACS

In order to configure a specific attribute to be sent for a user, you must ensure that:

- In the **Network Configuration** section, you must configure the AAA client entry that corresponds to the access device. This access device grants network access to the user to use a variety of RADIUS that supports the attribute you want sent to the AAA client.
- In the **Interface Configuration** section, you must enable the attribute so it appears on user or user group profile pages. You can enable attributes on the page that corresponds to the RADIUS variety that supports the attribute. For example, IETF RADIUS Session-Timeout attribute (27) appears on the RADIUS (IETF) page.

Note: By default, per-user RADIUS attributes are not enabled because they do not appear in the Interface Configuration page. Before you can enable attributes on a per-user basis, you must enable the per-user TACACS+/RADIUS Attributes option on the **Advanced Options** page in the **Interface Configuration** section. After you enable per-user attributes, a user column will appear as disabled in the **Interface Configuration** page for that attribute.

- In the profile you use to control authorizations for the user, which is in the user or group edit pages or Shared RADIUS Authorization Component page, you must enable the attribute. When this attribute is enabled, the ACS sends the attribute to the AAA client in the access-accept message. In the options that are associated with the attribute, you can determine the value of the attribute that is sent to the AAA client.

Note: The settings in a user profile override settings in a group profile. For example, if you configure Session-Timeout in the user profile and also in the group to which the user is assigned, the ACS sends the AAA client the Session-Timeout value that is specified in the user profile.

Import the Cisco Airespace VSAs to Cisco Secure ACS

In order to import the Cisco Airespace VSAs to the Cisco Secure ACS, you must complete these steps:

1. Define the Cisco Airespace VSAs in a RADIUS vendor/VSA import file.
2. Determine the RADIUS vendor slot to which you want to add the new RADIUS vendor and VSAs.
3. Add the Cisco Airespace VSAs to the Cisco Secure ACS.

Note: Make sure that the application **regedit** is not running. If regedit is running on the Cisco Secure ACS Windows server, it can prevent Registry updates required to add a custom RADIUS vendor and VSA set.

Define the Cisco Airespace VSAs in a RADIUS Vendor/VSA Import File

In order to import Cisco Airespace VSAs set into the Cisco Secure ACS, you must define the RADIUS vendor and VSA set in an import file. This section details the format and content of RADIUS VSA import files.

RADIUS vendor/VSA import files use a Windows **.ini** file format. Each RADIUS vendor/VSA import file comprises three types of sections. These sections are detailed in this table. Each section comprises a section header and a set of keys and values. The order of the sections in the RADIUS vendor/VSA import file is irrelevant.

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.

Vendor and VSA Set Definition

Each RADIUS vendor/VSA import file must have one vendor and VSA set section. The section header must be [User Defined Vendor].

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 <i>n</i> (where <i>n</i> 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.

For example, this vendor and VSA set section defines the vendor Cisco Airespace, whose IETF–assigned vendor number is 14179.

```
[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
```

Attribute Definition

Each RADIUS vendor/VSA import file must have one attribute definition section for each attribute defined in the vendor and VSA set section. The section header of each attribute definition section must match the attribute name defined for that attribute in the vendor and VSA set section. This table lists the valid keys for an attribute definition section:

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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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)	Enumerations section name	The name of the enumeration section. Note Several attributes can reference the same enumeration section.

For example, this attribute definition section defines the **Airespace-Interface-Name VSA**, which is a string used to specify the interface name.

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

Enumeration Definition

Enumeration definitions enable you to associate a text-based name for each valid numeric value of an integer-type attribute. In the Group Setup and User Setup sections of the Cisco Secure ACS HTML interface, the text values you define appear in lists associated with the attributes that use the enumerations. Enumeration definition sections are required only if an attribute definition section references them. Only attributes that are integer-type attributes can reference an enumeration definition section.

The section header of each enumeration definition section must match the value of an Enums key that references it. An enumeration definition section can be referenced by more than one Enums key, thus allowing for re-use of common enumeration definitions. An enumeration definition section can have up to 1000 keys. This table lists the valid keys for an enumeration definition section:

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

For example, this enumerations definition section defines the **QOS-VALUES** enumeration, which associates the string value silver with the integer 0, the string value Gold with the integer 1 and so on.

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

Airespace Dictionary File

You need to consider all these parameters needed to create the AirespaceVSA.ini file. Here is an example:

```
[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

```

Save this file as **Airespace.ini** and store it on the hard drive, preferably in the **C:\Cisco Secure ACS 3.2\Utils** directory. The next step is to add the VSAs to the Cisco Secure ACS.

Add the Cisco Airespace VSAs to the Cisco Secure ACS

You can use the **CSUtil.exe –addUDV** command available under the Utils directory (C:\Cisco Secure ACS 3.2\Utils directory) to add up to ten custom RADIUS vendors and VSA sets to the Cisco Secure ACS. Each RADIUS vendor and VSA set is added to one of ten possible user-defined RADIUS vendor slots.

The **CSUtil.exe –listUDV** command lists each user-defined RADIUS vendor slot in slot number order. The **CSUtil.exe** command lists slots that do not contain a custom RADIUS vendor as Unassigned. An unassigned slot is empty. You can add a custom RADIUS vendor to any slot listed as Unassigned. Here is an example:

```

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

```

While the **CSUtil.exe** command adds a custom RADIUS vendor and VSA set to the Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated during this process.

Complete these steps in order to add the Cisco Airespace VSAs to the Cisco Secure ACS:

1. On the computer that runs Cisco Secure ACS, open an MS DOS command prompt and change directories to the directory that contains CSUtil.exe. For example, if Cisco Secure ACS is installed in the C:\Cisco Secure ACS 3.2 directory, the Utils directory will be available under this directory. From the DOS prompt, enter this:

```
C:\Cisco Secure ACS 3.2\cd Utils
```

```
C:\Cisco Secure ACS 3.2\Utils
```

2. Now, enter this command:

```
CSUtil.exe -addUDV slot-number filename
```

where **slot-number** is an unused Cisco Secure ACS RADIUS vendor slot and **filename** is the name of a RADIUS vendor/VSA import file. The filename can include a relative or absolute path to the RADIUS vendor/VSA import file. Press **Enter**.

For example, to add the Cisco Airespace VSAs defined in **C:\Cisco Secure ACS 3.2\Utils\Airespace.ini** to slot 5, the command is:

```
CSUtil.exe -addUDV 5 Airespace.ini
```

CSUtil.exe displays a confirmation prompt.

3. In order to confirm that you want to add the VSAs and halt all Cisco Secure ACS services during the process, type **Y** and press **Enter**.

CSUtil.exe halts Cisco Secure ACS services, parses the vendor/VSA input file, and adds the new RADIUS vendor and VSAs to Cisco Secure ACS. This process can take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.

Here is an example:

```
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
```

Verify

Once the Cisco Airespace VSAs are added to the Cisco Secure ACS, you can verify the same from the Cisco Secure ACS GUI. Complete these steps in order to verify:

1. Login to the Cisco Secure ACS GUI.
2. Click **Network Configuration** from the left side menu and navigate to the **Add a AAA client** page.

In the AAA Client window, you will find the RADIUS (Airespace) option under the Authenticate Using pull down menu.

Here is an example:

AAA Client Setup For Test

AAA Client IP Address: 172.16.1.100

Key: [Empty]

Network Device Group: (Not Assigned)

Authenticate Using: **RADIUS (Airespace)**

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Buttons: Submit, Submit + Restart, Delete, Delete + Restart, Cancel, Back to Help

Help

- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Deleting a AAA Client](#)
- [Renaming a AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

AAA Client IP Address

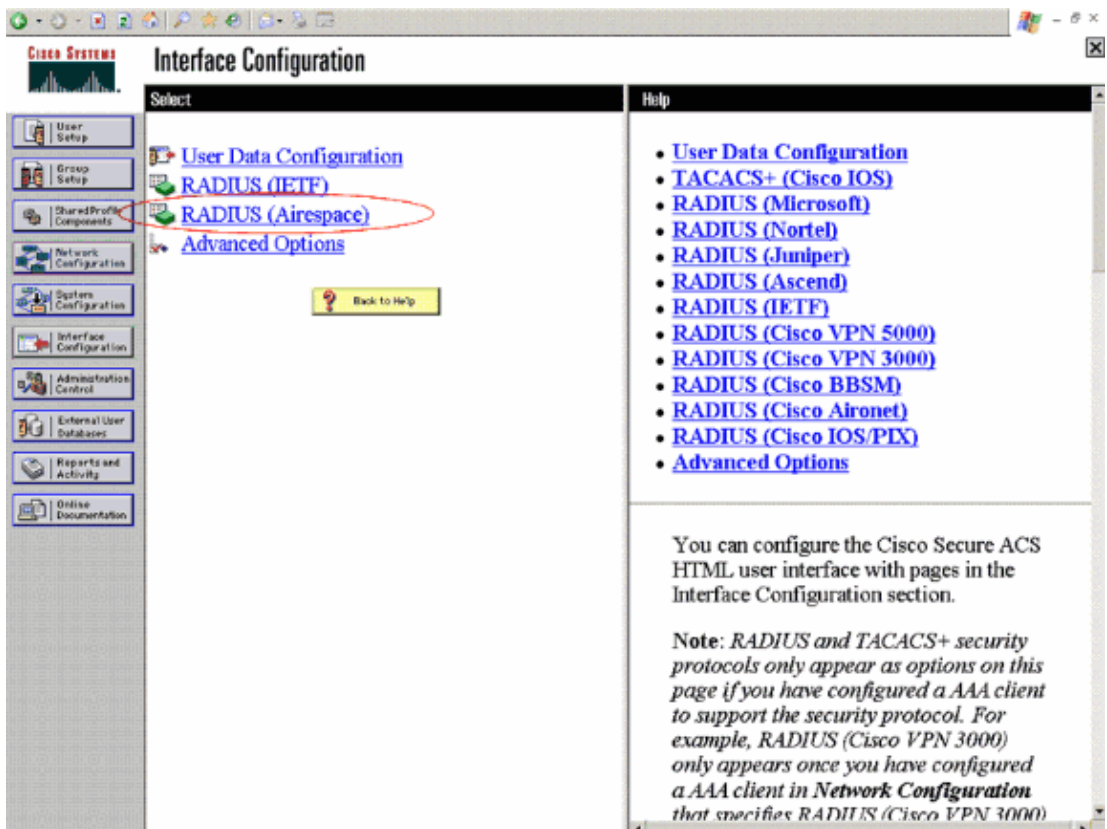
Type the IP address information for this AAA client.

If you want to designate more than one AAA client with a single AAA client entry in Cisco Secure ACS, you can specify the IP address for each AAA client to be represented by this AAA client entry. To separate each IP address, press **Enter**.

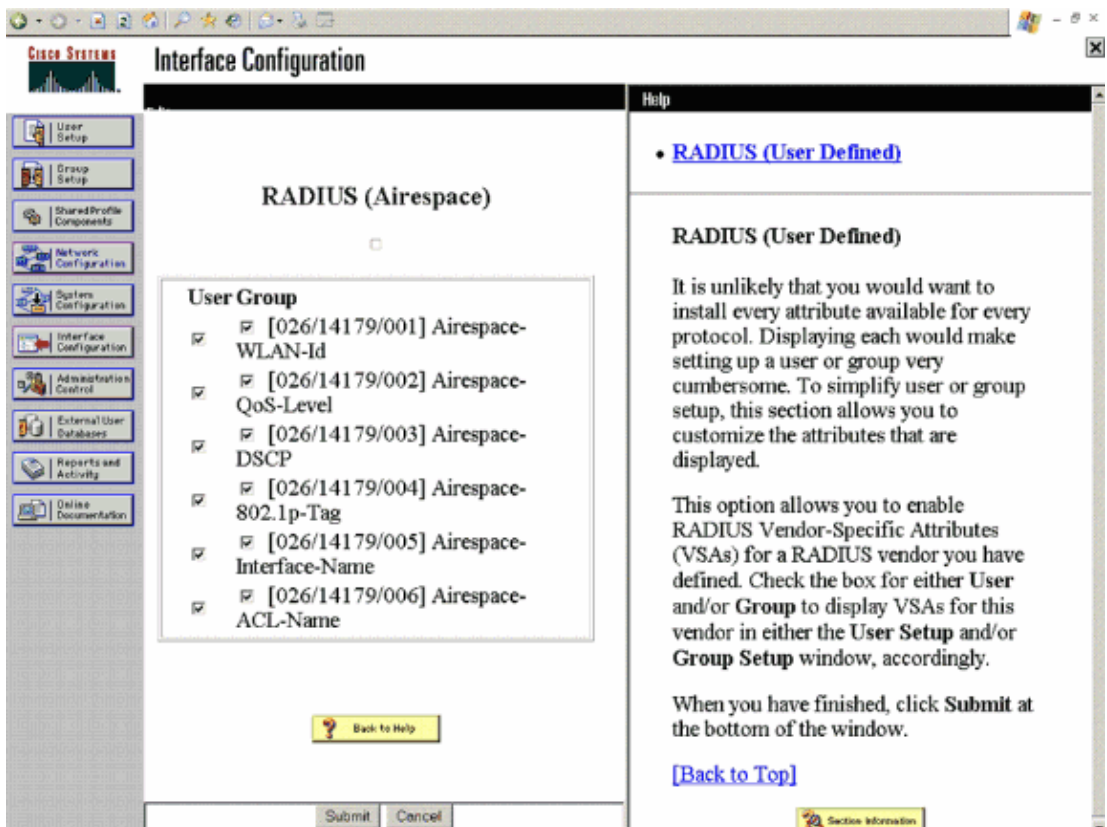
You can use the wildcard asterisk (*) for

On the Interface Configuration page, you will find the RADIUS (Airespace) attributes listed.

Note: In the **Network Configuration** section, you must configure the AAA client entry that corresponds to the access device that grants network access to the user to use the RADIUS (Airespace) attributes that you want sent to the AAA client. Then the corresponding RADIUS attributes will be listed on the Interface Configuration page.



3. When you click the **RADIUS (Airespace)** link on this page, you can view and select the attributes.



Troubleshoot

If the Airespace dictionary file is not imported to the Cisco Secure ACS, check these:

- Ensure that you are importing a properly formatted **.ini (VSA import file)** file. If the format of the file is not correct, you will see this error message:

```
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
```

- Ensure that the vendor slot where you are trying to import the dictionary is free and is not assigned to a different vendor dictionary. If you try to install the VSA to a slot which is already assigned, you will receive this error:

```
Vendor Slot already configured, specify alternate value
```

You can use the **CSUtil.exe -listUDV** command in order to view the list of slots that are empty.

Related Information

- [Supported RADIUS Attributes on the Wireless LAN Controller](#)
- [Cisco Airespace VSAs on MS IAS Radius Server Configuration Example](#)
- [RADIUS Server Authentication of Management Users on the Controller Configuration Example](#)
- [User Guide for Cisco Secure ACS for Windows Server 3.2](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Apr 14, 2009

Document ID: 97849
