Encrypted Vendor-Specific Attributes

Last Updated: January 15, 2012

The Encrypted Vendor-Specific Attributes feature provides users with a way to centrally manage filters at a RADIUS server and supports the following types of string vendor-specific attributes (VSAs):

- Tagged String VSA, page 2 (similar to Cisco VSA type 1 (Cisco:AVPair (1)) except that this new VSA is tagged)
- Encrypted String VSA, page 2 (similar to Cisco VSA type 1 except that this new VSA is encrypted)
- Tagged and Encrypted String VSA, page 3 (similar to Cisco VSA type 1 except that this new VSA is tagged and encrypted)

Cisco:AVPairs specify additional authentication and authorization information in the form an Attribute-Value Pair (AVPair) string. When Internet Engineering Task Force (IETF) RADIUS attribute 26 (Vendor-Specific) is transmitted with a vendor-Id number of “9” and a vendor-type value of “1” (which means that it is a Cisco AVPair), the RADIUS user profile format for a Cisco AVPair looks as follows: Cisco:AVPair = “protocol:attribute=value”.

- Finding Feature Information, page 1
- Prerequisites for Encrypted Vendor-Specific Attributes, page 2
- Information About Encrypted Vendor-Specific Attributes, page 2
- How to Verify Encrypted Vendor-Specific Attributes, page 3
- Configuration Examples for Encrypted Vendor-Specific Attributes, page 3
- Additional References, page 4
- Feature Information for Encrypted Vendor-Specific Attributes, page 5

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Encrypted Vendor-Specific Attributes

Before the RADIUS server can accept tagged and encrypted VSAs, you must configure your server for AAA authentication and authorization and to accept PPP calls.

For information on performing these tasks, refer to the chapter “PPP Configuration ” in the Cisco IOS Dial Technologies Configuration Guide, Release 12.4 and the chapters “Configuring Authentication” and “Configuring Authorization ” in th e Cisco IOS Security Configuration Guide, Release 12.4.

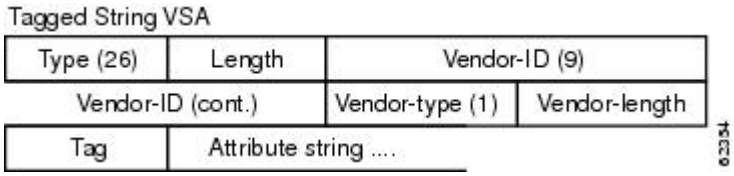
Information About Encrypted Vendor-Specific Attributes

- Tagged String VSA, page 2
- Encrypted String VSA, page 2
- Tagged and Encrypted String VSA, page 3

Tagged String VSA

The figure below displays the packet format for the Tagged String VSA:

Figure 1 Tagged String VSA Format

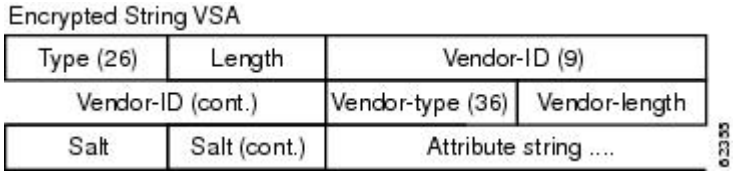


To retrieve the correct value, the Tag field must be parsed correctly. The value for this field can range only from 0x01 through 0x1F. If the value is not within the specified range, the RADIUS server ignores the value and considers the Tag field to be a part of the Attribute String field.

Encrypted String VSA

The figure below displays the packet format for the Encrypted String VSA:

Figure 2 Encrypted String VSA Format



The Salt field ensures the uniqueness of the encryption key that is used to encrypt each instance of the VSA. The first and most significant bit of the Salt field must be set to 1.

Note Vendor-type (36) indicates that the attribute is an encrypted string VSA.

Tagged and Encrypted String VSA

The figure below displays the packet formats for each of the newly supported VSAs:

Figure 3 Tagged and Encrypted String VSA Format

Tagged and Encrypted String VSA

Type (26)	Length	Vendor-ID (9)	
Vendor-ID (cont.)		Vendor-type (36)	Vendor-length
*Tag	Salt	Salt (cont.)	Attribute string ....

This VSA is similar to encrypted string VSAs except this VSA has an additional Tag field. If the Tag field is not within the valid range (0x01 through 0x1F), it is considered to be part of the Salt field.

How to Verify Encrypted Vendor-Specific Attributes

The Encrypted Vendor-Specific Attributes feature requires no configuration. To verify that RADIUS-tagged and encrypted VSAs are being sent from the RADIUS server, use the following command in privileged EXEC mode:

Command	Purpose
`Router#` **debug radius**	Displays information associated with RADIUS. The output of this command shows whether tagged and encrypted VSAs are being sent from the RADIUS server.

Configuration Examples for Encrypted Vendor-Specific Attributes

- NAS Configuration Example, page 3
- RADIUS User Profile with a Tagged and Encrypted VSA Example, page 4

NAS Configuration Example

The following example shows how to configure a network access server (NAS) with a basic configuration using tagged and encrypted VSAs. (This example assumes that the configuration required to make PPP calls is already enabled.)

```
aaa new-model
aaa authentication ppp default group radius
```

```
aaa authorization network default group radius
!
radius-server host 10.2.2.2 auth-port 1645 acct-port 1646
radius-server key cisco
```

RADIUS User Profile with a Tagged and Encrypted VSA Example

The following is an example of user profile on a RADIUS server that supports tagged and encrypted string VSAs:

```
mascot   Password = "password1"
         Service-Type = NAS-Prompt,
         Framed-Protocol = PPP,
         Cisco:Cisco-Enc = "ip:route=10.0.0.0 255.0.0.0"
         Cisco.attr Cisco-Enc 36 tag-encstr(*,*)
```

Additional References

The following sections provide references related to the Encrypted Vendor-Specific Attributes.

Related Documents

Related Topic	Document Title
RADIUS Attributes	*Cisco IOS Security Configuration Guide: Securing User Services* , Release 12.4T

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2865	Remote Authentication Dial In User Service (RADIUS)
RFC 2868	RADIUS Attributes for Tunnel Protocol Support

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

Feature Information for Encrypted Vendor-Specific Attributes

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Encrypted Vendor-Specific Attributes

Feature Name	Releases	Feature Information
Encrypted Vendor-Specific Attributes	12.2(8)T 12.2(28)SB 12.2(33)SRC Cisco IOS XE Release 2.3	The Encrypted Vendor-Specific Attributes feature provides users with a way to centrally manage filters at a RADIUS server and supports the Tagged String, Encrypted String, and Tagged and Encrypted String vendor-specific attributes (VSAs). This feature was introduced in Cisco IOS Release 12.2(8)T. This feature was integrated into Cisco IOS Release 12.2(28)SB. This feature was integrated into Cisco IOS Release 12.2(33)SRC. In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 series routers.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.