



Cisco SCMS SM SCE-Sniffer RADIUS LEG Reference Guide

Release 3.1
May 2007

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-8234-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0501R)

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

Cisco SCMS SM SCE-Sniffer RADIUS LEG Reference Guide
© 2007 Cisco Systems, Inc. All rights reserved.



CONTENTS

Audience	v
Document Revision History	vi
Organization	vi
Document Conventions	vii
Related Documentation	viii
Obtaining Documentation, Obtaining Support, and Security Guidelines	viii

CHAPTER 1

About the SCE-Sniffer RADIUS LEG	1-1
Information About the SCE-Sniffer RADIUS LEG	1-1
RADIUS Integration Overview	1-2
Terms and Concepts	1-2
LEG (Login Event Generator)	1-3
RDR (Raw Data Record)	1-3
NAS (Network Access System)	1-3
RADIUS Authentication Transactions	1-3
RADIUS Accounting Transactions	1-3
Accounting-Start Packet	1-3
Accounting-Stop Packet	1-3
RADIUS Sniffer	1-3
Subscriber ID	1-4
Subscriber Mappings	1-4
Subscriber Domain	1-4
Subscriber Policy	1-4

CHAPTER 2

SCE-Sniffer RADIUS LEG Functionality	2-1
SCE-Sniffer RADIUS Functionality	2-1
Information About RADIUS Attributes	2-1
Subscriber ID Association	2-2
Domain Association	2-2
Policy Association	2-2
Subscriber IP Association	2-3
Information About RADIUS Packets	2-3
Accounting-Start Packet	2-4

Accounting-Interim-Update Packet 2-4
 Accounting-Stop Packet 2-4
 Access-Accept Packet 2-5

CHAPTER 3

Installing the SCE-Sniffer RADIUS LEG 3-1
 Installing the SCE-Sniffer RADIUS LEG Software 3-1
 Uninstalling the SCE-Sniffer RADIUS LEG 3-2
 Upgrading the SCE-Sniffer RADIUS LEG 3-3

CHAPTER 4

Configuring the SCE-Sniffer RADIUS LEG 4-1
 Configuring the General Settings 4-1
 Configuring the Subscriber ID 4-2
 Information About Configuring the Subscriber IP Address 4-3
 Subscriber IP Address Configuration Example 4-3
 Information About Configuring the Policy Settings 4-4
 Policy Configuration Example 4-5

CHAPTER 5

Using the SCE-Sniffer RADIUS LEG CLU 5-1
 Information About the SCE-Sniffer RADIUS LEG Utility 5-1
 Viewing the SCE-Sniffer RADIUS LEG Status 5-1
 Viewing the SCE-Sniffer RADIUS LEG Version 5-2
 Viewing the SCE-Sniffer RADIUS LEG Statistics 5-2



Preface

Revised: May 30, 2007, OL-8234-04

This guide describes the concept of a Remote Authentication Dial-In User Service (RADIUS) Login Event Generator (LEG) based on a RADIUS Sniffer, and explains how to install and configure it on the SCMS Subscriber Manager (SM) platform.



Note

This guide assumes a basic familiarity with telecommunications equipment and installation procedures, Cisco SCMS subscriber management, subscriber integration concepts, and the RADIUS protocol.

For complete information regarding Cisco's subscriber integration concept, see the *Cisco SCMS Subscriber Manager User Guide*.

This introduction provides information about the following topics:

- [Audience](#)
- [Document Revision History](#)
- [Organization](#)
- [Document Conventions](#)
- [Related Documentation](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines](#)

Audience

This document is intended for system administrators and system integrators who are familiar with the SCE-Sniffer RADIUS LEG concepts and with the Cisco SCMS Subscriber Management and Subscriber Integration concepts.

Document Revision History

Cisco Service Control Release	Part Number	Publication Date
Release 3.1.0	OL-8234-04	May, 2007

Description of Changes

- Updated for 3.1.0 release.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.5	OL-8234-03	November, 2006

Description of Changes

- Added new section describing subscriber IP association. See [Subscriber IP Association](#).
- Added new section describing configuring the subscriber IP address. See [Information About Configuring the Subscriber IP Address](#).
- Small changes to text throughout the guide.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0.3	OL-8234-02	May, 2006

Description of Changes

- Added new section describing the Accounting-Interim-Update packet. See [Accounting-Interim-Update Packet](#).
- Small changes to text throughout the guide.

Cisco Service Control Release	Part Number	Publication Date
Release 3.0	OL-8234-01	December, 2005

Description of Changes

- This is the first release of this document.

Organization

The major sections of this guide are as follows:

Table 1

Chapter	Title	Description
Chapter 1	About the SCE-Sniffer RADIUS LEG	Describes the SCE-Sniffer RADIUS LEG software module, and terms and concepts
Chapter 2	SCE-Sniffer RADIUS LEG Functionality	Provides a description of SCE-Sniffer RADIUS LEG transactions for login and logout operations

Table 1

Chapter	Title	Description
Chapter 3	Installing the SCE-Sniffer RADIUS LEG	Describes the installation process for installing the SM SCE-Sniffer RADIUS LEG
Chapter 4	Configuring the SCE-Sniffer RADIUS LEG	Provides the configuration instructions to configure the SCE-Sniffer RADIUS LEG
Chapter 5	Using the SCE-Sniffer RADIUS LEG CLU	Describes the Command-Line Utilities to retrieve information and statistics about the LEG

Document Conventions

This guide uses the following conventions:

- **Bold** is used for commands, keywords, and buttons.
- *Italics* are used for command input for which you supply values.
- Screen font is used for examples of information that are displayed on the screen.
- **Bold screen** font is used for examples of information that you enter.
- Vertical bars (|) indicate separate alternative, mutually exclusive elements.
- Square brackets ([]) indicate optional elements.
- Braces ({ }) indicate a required choice.
- Braces within square brackets ([{ }]) indicate a required choice within an optional element.



Note

Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the guide.



Timesaver

Means the *described action saves time*. You can save time by performing the action described in the paragraph.



Caution

Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.



Warning

Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. To see translated versions of warnings, refer to the *Regulatory Compliance and Safety Information* document that accompanied the device.

Related Documentation

Use this SCMS SM C/C++ API Programmer Guide in conjunction with all of the SCMS Subscriber Manager User, API, and Reference Guides.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>



CHAPTER 1

About the SCE-Sniffer RADIUS LEG

This module describes the SCE-Sniffer RADIUS LEG software module, and terms and concepts

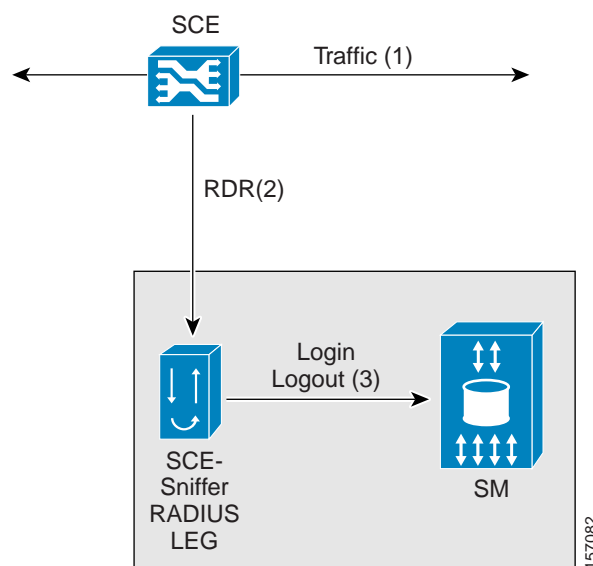
The SCMS SM SCE-Sniffer RADIUS LEG is a software module that receives RDR (Raw Data Record) messages containing RADIUS information from SCE devices configured with a RADIUS Sniffer service. The SCE-Sniffer RADIUS LEG is an extension of the Subscriber Manager (SM) software and runs as part of the SM process.

- [Information About the SCE-Sniffer RADIUS LEG](#)

Information About the SCE-Sniffer RADIUS LEG

The SCE device analyzes RADIUS traffic that traverses it (1), and reports the RADIUS transactions to the LEG using the RDR protocol (2). The LEG associates the RDR data to subscriber properties (name, subscriber IP, domain, and policies), and triggers a login or logout operation to the SM (3).

Figure 1-1 SCE-Sniffer RADIUS LEG Operation



- [RADIUS Integration Overview](#)
- [Terms and Concepts](#)

RADIUS Integration Overview

This implementation of the SCE-Sniffer RADIUS LEG supports RFC 2865 (RADIUS protocol) and RFC 2866 (RADIUS Accounting).

The LEG uses the following packet types:

- Accounting-Start—Initiates login operations (with subscriber IP, domain, and policies)
- Accounting-Interim-Update—Initiates login operations (with subscriber IP, domain, and policies)
- Accounting-Stop—Initiates logout operations
- Access-Request—Initiates domain and policies associations
- Access-Accept—Initiates login operations (with subscriber IP and policies)

The LEG uses the following attributes:

- User Name (Attribute #1)—Default attribute for subscriber ID
- NAS-IP-Address (Attribute #4)—Associates the NAS IP address as the subscriber's domain (optional)
- Framed-IP-Address (Attribute #8)—Associates an IP address to the subscriber
- Framed-IP-Netmask (Attribute #9)—Associates an IP netmask to the subscriber
- Framed-Route (Attribute #22)—Associates an IP/IP-range to the subscriber
- NAS-Identifier (Attribute #32)—Associates the NAS identifier as the subscriber's domain (optional)
- Acct-Status-Type (Attribute #40)—Distinguishes between the different accounting transactions.

To associate policies to the subscribers, configure the LEG with the attribute that contains the policy information. The Vendor Specific attribute (Attribute #26) can be used to associate policies to the subscribers in addition to all other RADIUS attributes of type string or integer.

To determine the subscriber ID, configure the LEG with the attribute that contains the subscriber ID information. The Vendor Specific attribute (Attribute #26) can be used to determine the subscriber ID in addition to all other RADIUS attributes of type string. By default, the User-Name (Attribute #1) is configured to hold the subscriber ID.

Terms and Concepts

The following list of terms and concepts are necessary to understand the SCE-Sniffer RADIUS LEG, configuration, and operation. Additional information regarding other various issues can be found in the *Cisco SCMS Subscriber Manager User Guide*.

- [LEG \(Login Event Generator\)](#)
- [RDR \(Raw Data Record\)](#)
- [NAS \(Network Access System\)](#)
- [RADIUS Authentication Transactions](#)
- [RADIUS Accounting Transactions](#)
- [Accounting-Start Packet](#)
- [Accounting-Stop Packet](#)
- [RADIUS Sniffer](#)
- [Subscriber ID](#)

- [Subscriber Mappings](#)
- [Subscriber Domain](#)
- [Subscriber Policy](#)

LEG (Login Event Generator)

A software component that performs subscriber login and logout operations on the SM, which is used to handle dynamic subscriber integration.

RDR (Raw Data Record)

A client/server data protocol that enables the SCE devices to export network transactions reports to external collectors. This is a Cisco proprietary protocol.

NAS (Network Access System)

A network device that serves as an access point for a remote user. It initiates RADIUS transactions to the RADIUS server to authenticate a remote user.

RADIUS Authentication Transactions

The RADIUS transactions are used for authenticating a remote user, and authorizing access to the network's resources. The LEG supports RADIUS authentication based on RFC 2865. The authentication RADIUS packets used by the LEG are ACCESS-REQUEST and ACCESS-ACCEPT.

RADIUS Accounting Transactions

The RADIUS accounting transactions are used to keep track of the services used by the user for administrative purposes. The LEG supports RADIUS accounting based on RFC 2866. The only RADIUS accounting packet the LEG uses is ACCOUNTING-REQUEST.

Accounting-Start Packet

An abbreviated term used in this document to describe an ACCOUNTING-REQUEST packet with the ACCT-STATUS-TYPE attribute set to start. The NAS sends this packet to the RADIUS server when the remote user starts using a network service. The LEG uses it to initiate a login operation on the SM.

Accounting-Stop Packet

An abbreviated term used in this document to describe an ACCOUNTING-REQUEST packet with the ACCT-STATUS-TYPE attribute set to stop. The NAS sends this packet to the RADIUS server when the remote user stops using a network service. The LEG uses it to initiate a logout operation on the SM.

RADIUS Sniffer

The software logic inside the SCE device that analyzes RADIUS traffic and sends the information to the SCE-Sniffer RADIUS LEG using the RDR protocol.

Subscriber ID

The Service Control solution requires a unique identifier for each subscriber. A subscriber ID represents a logical subscriber entity from the service provider perspective.

Subscriber Mappings

The SCE platform requires mappings between the network IDs (IP addresses) of the flows it encounters and the subscriber IDs. The SM database contains the network IDs that map to the subscriber IDs. The SCE network-ID-to-subscriber mappings are constantly updated from the SM database.

Subscriber Domain

The SM provides the option of partitioning SCE platforms and subscribers into subscriber domains. A subscriber domain is a group of SCE platforms that share a group of subscribers. Subscriber domains can be configured using the SM configuration file and can be viewed using the SM Command-Line Utility (CLU).

For additional information about domains and domain aliases, see the *Cisco SCMS Subscriber Manager User Guide*.

Subscriber Policy

A subscriber policy package usually defines the policy enforced by Cisco SCMS solutions on each subscriber. The SCE-Sniffer RADIUS LEG can handle the policy in any of the following ways:

- Set the policy according to configurable attributes of the RADIUS transactions
- Set the policy using a constant default value
- Leave the package ID unset

For additional information, see the *Cisco Service Control Application for Broadband User Guide*.



CHAPTER 2

SCE-Sniffer RADIUS LEG Functionality

This module describes the SCE-Sniffer RADIUS LEG transactions for login and logout operations. The SCE devices analyze the RADIUS transactions and send the information to the SCE-Sniffer RADIUS LEG that resides on the SM. The LEG performs login or logout operations to the SM using the information sent from the SCE devices.

- [SCE-Sniffer RADIUS Functionality](#)
- [Information About RADIUS Attributes](#)
- [Information About RADIUS Packets](#)

SCE-Sniffer RADIUS Functionality

The LEG supports the following integrations with the RADIUS transactions:

- Integrating with the RADIUS Accounting transactions
In this mode, the Accounting-Start and (optionally) Accounting-Interim-Update packets are used for login operations, and (optionally) the Accounting-Stop packets are used for logout operations. This integration mode is the simplest; therefore, if accounting transactions are used in your network it is advisable to use this integration mode.
- Integrating with the RADIUS Authentication transactions
In this mode, the Access-Request and Access-Accept packets are used for login operations. This mode does not support logout operations. Use this integration mode if RADIUS accounting is not used in your network.
- Integrating with the RADIUS Accounting and Authentication transactions
This mode combines the previous two modes. Login operations use Authentication transactions, and logout operations use Accounting transactions.

Information About RADIUS Attributes

This section describes how subscriber properties are extracted from the RADIUS attributes.

- [Subscriber ID Association](#)
- [Domain Association](#)
- [Policy Association](#)

- [Subscriber IP Association](#)

Subscriber ID Association

By default, the attribute used for the subscriber ID association is the User-Name attribute (#1), but it can be configured to any other attribute including the Vendor-Specific attribute (#26).

The only requirement is that the configured attribute must be of type **string**.

This attribute must exist in the RADIUS traffic for successful login operations, because a subscriber cannot be introduced to the SM without its ID.

For logout operations, which are triggered by Accounting-Stop packets only, this attribute is not mandatory, because logouts can be performed using the mapping information.

Domain Association



Note

Domain association is only relevant for login operations and is optional.

Domain association is based on the Network Access System (NAS) that initiated the RADIUS transaction. The RADIUS attributes that identify the NAS are NAS-Identifier (#32), and NAS-IP-Address (#4). If none of the attributes exist, the LEG tries to identify the NAS using the IP address of the NAS taken from the UDP packet.

Before a login operation occurs, the NAS properties, NAS-Identifier and NAS-IP-Address, are matched against the configured domains or domain aliases of the SM. The login operation uses the matched domain or domain alias as the subscriber domain.

The domain association is performed in stages, as follows:

1. If the NAS-Identifier attribute exists, and a domain name or alias is configured in the SM for the same NAS-Identifier, the domain name or alias is used as the subscriber domain.
2. If the previous step fails, the same test is performed on the NAS-IP-Address attribute.
3. If the NAS-IP-Address does not exist as well, the same test is performed on the IP address of the NAS.
4. If the NAS-Identifier and the NAS-IP-Address attributes are missing or does not match to an existing SM domain or alias, the default subscriber domain is used.

Policy Association



Note

Policy association is only relevant for login operations and is optional.

The user can configure policy association. You can use any RADIUS attribute for policy association, including the Vendor-Specific attribute.

The term policy association refers to the act of setting a subscriber property according to information extracted from the RADIUS packets. An example of policy association is setting the packageId property of the Service Control Application for Broadband (SCA BB) solution to control the network service level for which the subscriber is entitled.

To associate policy from a RADIUS attribute, the configured attribute must be of type **string** or **integer**. The subscriber property values are always integers. However, if the association is based on a string RADIUS attribute, it is mandatory to configure a mapping table. If the association is based on an integer RADIUS attribute, a mapping table is not needed, but can be used. See [Information About Configuring the Policy Settings](#) for more information on configuring a mapping table.

You can define a default value for the policy if the configured RADIUS attribute is missing from the packet. The default value is valid only if the policy has not been set before (for example by other LEGs, or the Subscriber Manager).

The [Information About Configuring the Policy Settings](#) section describes how to configure the policies.

Subscriber IP Association

The Subscriber IP Address is normally based on the Framed-IP-Address attribute, but can also be based on the RADIUS attribute. In different topologies, the subscriber IP address specification might be sent as a RADIUS attribute other than the Framed-IP-Address attribute.

The following algorithm extracts the IP addresses in this LEG:

1. If the user configured an attribute from which to extract the IP, the LEG will look for that attribute in the RDR. If the attribute exists, the LEG will use the attribute as the subscriber IP address.
2. If the attribute does not exist or is not configured, the LEG will look for the Framed-Route attributes; several Framed-Route attributes may exist. If any Framed-Route attributes exist, the LEG will use these attributes as the subscriber IP addresses.
3. If there are no Framed-Route attributes, the LEG will look for a Framed-IP-Address attribute and a Framed-IP-Netmask attribute. If a Framed-IP-Address attribute exists, the LEG will use this attribute as the subscriber IP address. If both the Framed-IP-Address and the Framed-IP-Netmask attributes exist, the operation is performed with the IP range represented by the IP address and the IP netmask.
4. Otherwise, the LEG will perform a login without the IP address.



Note

The configured attribute can be a regular RADIUS attribute or a VSA. It is possible to encode the attribute as an integer in which case it will be a single IP address. It can also be encoded as a string and will therefore be an IP-Address/IP-Range value: the value must be formatted as A.B.C.D/E or A.B.C.D



Note

The supported format of the Framed-Route attribute is as described in RFC-2865. It must start with a string that starts with the route itself in the format A.B.C.D/E followed by a space. Other values follow the space, but the LEG ignores these other values.

Information About RADIUS Packets

This section describes the RADIUS packets supported by the SCE-Sniffer RADIUS LEG and their impact on the SM.

- [Accounting-Start Packet](#)
- [Accounting-Interim-Update Packet](#)
- [Accounting-Stop Packet](#)

- [Access-Accept Packet](#)

Accounting-Start Packet

An Accounting-Start packet initiates a login operation with the following subscriber properties:

- Subscriber ID—See [Subscriber ID Association](#)
- Subscriber IP—See [Subscriber IP Association](#)
- Domain—See [Domain Association](#)
- Policy—See [Policy Association](#)

If the Accounting-Start packet does not hold the subscriber ID, the login operation is not performed and an error message is written to the user log. All other properties (subscriber IP, domain, and policy) are optional.



Note

The Accounting-Start and Accounting-Interim-Update packets are the only packets that hold all the subscriber properties. Use these packets whenever possible.

Accounting-Interim-Update Packet

An Accounting-Interim-Update packet initiates a login operation with exactly the same properties as the Accounting-Start packet.

If the Accounting-Interim-Update packet does not hold the subscriber ID, the login operation is not performed and an error message is written to the user log. All other properties (subscriber IP, domain, and policy) are optional.



Note

Use this packet when the subscribers are connected to the network for a long time in a single session.

Accounting-Stop Packet

An Accounting-Stop packet initiates a logout operation with the following subscriber properties:

- Subscriber ID—See [Subscriber ID Association](#)
- Subscriber IP—See [Subscriber IP Association](#)

Unlike the Accounting-Start packet, the subscriber ID is not mandatory in the Accounting-Stop packet. If it does not exist, the logout is based only on the mappings information. If the Accounting-Stop packet has a subscriber ID but does not have the mappings, all mappings of the subscriber are logged out. If both properties are missing, the logout operation is not performed and an error message is written to the user log.



Note

The Accounting-Stop packet is the only packet that initiates a logout operation. If you need to perform logouts, you must use this packet for integration.

Access-Accept Packet

An Access-Accept packet initiates a login operation with the following subscriber properties:

- Subscriber ID—See [Subscriber ID Association](#)
- Subscriber IP—See [Subscriber IP Association](#)
- Policy—See [Policy Association](#)

The subscriber ID is mandatory, subscriber IP and policy are not. If the subscriber ID is missing, the login operation is not performed and an error message is written to the user log.



Note

The Access-Accept packet does not hold any information needed for domain association. If you are using domains, consider using the accounting packets for domain integration.



CHAPTER 3

Installing the SCE-Sniffer RADIUS LEG

This module describes the procedures for installing and running the SCE-Sniffer RADIUS LEG. It also describes the procedure to uninstall the SCE-Sniffer RADIUS LEG.

The SCE-Sniffer RADIUS LEG is an external component (PQI file) of the SM software that should be installed separately using the SM command-line utilities. The SCE-Sniffer RADIUS LEG distribution is part of the SM LEG distribution.

The installation package of the LEG includes a set of configuration files and command-line utilities for the LEG.

- [Installing the SCE-Sniffer RADIUS LEG Software](#)
- [Uninstalling the SCE-Sniffer RADIUS LEG](#)
- [Upgrading the SCE-Sniffer RADIUS LEG](#)

Installing the SCE-Sniffer RADIUS LEG Software



Note

Before installation, verify that the Service Control Application for Broadband (SCA BB) is installed on all SM and SCE devices. If the application has not been installed, install the application as described in the *Cisco Service Control Application for Broadband User Guide*.



Note

After the installation of the PQI file, the SM will automatically restart.

SUMMARY STEPS

1. Install the PQI file of the SCE-Sniffer RADIUS LEG using the **p3instCLU**.
2. Edit the configuration file of the SCE-Sniffer RADIUS LEG
3. Load the configuration file to the SM using the **p3smCLU**
4. Configure the SCE to send RDRs to the LEG

DETAILED STEPS

-
- Step 1 Install the PQI file of the SCE-Sniffer RADIUS LEG using the **p3instCLU**.

Run the p3inst CLU from the SM CLU `<sm-inst-dir>/sm/server/bin` (`sm-inst-dir` refers to the SM installation directory):

```
>p3inst --install -f rad_snif.pqi
```

Step 2 Edit the configuration file of the SCE-Sniffer RADIUS LEG

The name of the configuration file is `rad_snif.cfg`, and it is located under the configuration folder of the SM (`<sm-inst-dir>/sm/server/root/config`).

It is recommended to familiarize yourself with this file immediately after the first installation, and edit it according to your specific needs. See [Configuring the SCE-Sniffer RADIUS LEG](#) for more information.

Step 3 Load the configuration file to the SM using the `p3sm` CLU

Run the p3sm command line utility from the SM CLU:

```
>p3sm --load-config
```

This command-line utility loads the new configuration to the SM and activates it.

Step 4 Configure the SCE to send RDRs to the LEG

Run the RDR-formatter Command-Line Interface (CLI) in the SCE to add the LEG as a category 3 RDR destination:

```
SCE2000>configureSCE2000(config)>RDR-formatterdestination SM-IPport portcategory number
3priority 100SCE2000(config)>exit
```

Use the same port number as defined by the RDR server in the SM. The default port number is 33001.



Note

To support SM cluster topology, set the cluster VIP as the SM-IP in the above CLI command.

Uninstalling the SCE-Sniffer RADIUS LEG

SUMMARY STEPS

1. Configure the SCE to stop sending RDRs to the LEG
2. Uninstall the SCE-Sniffer RADIUS LEG using the `p3inst` CLU

DETAILED STEPS

Step 1 Configure the SCE to stop sending RDRs to the LEG

Run the RDR-formatter CLI command in the SCE to remove the LEG as category 3 RDR destination:

```
SCE2000>configureSCE2000(config)>no RDR-formatterdestination SM-IPport
portSCE2000(config)>exit
```

Step 2 Uninstall the SCE-Sniffer RADIUS LEG using the `p3inst` CLU

Run the p3inst command line utility from the SM CLU:

```
>p3inst --uninstall -f rad_snif.pqi
```

**Note**

After the uninstall process has successfully completed, the SM will automatically restart.

Upgrading the SCE-Sniffer RADIUS LEG

The SCE-Sniffer RADIUS LEG must be upgraded when upgrading is performed between versions of the SM as part of the SM upgrade process. The upgrade for the SCE-Sniffer RADIUS LEG should be performed together with the upgrade process of the SM.

SUMMARY STEPS

1. Backup the configuration file of the SCE-Sniffer RADIUS LEG
2. Force the SCEs to store the RDRs during the upgrade
3. Uninstall the SCE-Sniffer RADIUS LEG using the **p3inst --uninstall**CLU of the SM
4. Perform the upgrade of the SM as described in the *Cisco SCMS Subscriber Manager User Guide*
5. Install the new version of the SCE-Sniffer RADIUS LEG using the **p3inst --install**CLU of the SM.
6. Restore the configuration files of the SCE-Sniffer RADIUS LEG
7. Make the SCEs send the RDRs that they stored during the upgrade
8. Load the new configuration by using the **p3sm --load-config**CLU of the SM.

DETAILED STEPS

-
- Step 1** Backup the configuration file of the SCE-Sniffer RADIUS LEG
- The original configuration file is deleted by the uninstall process in the next step.
- Step 2** Force the SCEs to store the RDRs during the upgrade
- To force the SCEs to store the RDRs, disable the RDR Server on the SM by setting the **start** parameter in the RDR Server section to **false** and loading the configuration by running the following CLU:
- ```
>p3sm --load-config
```
- Step 3** Uninstall the SCE-Sniffer RADIUS LEG using the **p3inst --uninstall**CLU of the SM
- Step 4** Perform the upgrade of the SM as described in the *Cisco SCMS Subscriber Manager User Guide*
- Step 5** Install the new version of the SCE-Sniffer RADIUS LEG using the **p3inst --install**CLU of the SM.
- Step 6** Restore the configuration files of the SCE-Sniffer RADIUS LEG
- Step 7** Make the SCEs send the RDRs that they stored during the upgrade
- To make the SCEs send the RDRs that they stored during the upgrade, enable the RDR Server on the SM by setting the **start** parameter in the RDR Server section to **true**.
- Step 8** Load the new configuration by using the **p3sm --load-config**CLU of the SM.
-





# CHAPTER 4

## Configuring the SCE-Sniffer RADIUS LEG

---

This module describes the configuration instructions to configure the SCE-Sniffer RADIUS LEG.

The SCE-Sniffer RADIUS LEG is configured using the configuration file **rad\_snif.cfg**, which resides in the **<sm-inst-dir>/sm/server/root/config** directory (**sm-inst-dir** refers to the SM installation directory).

The configuration file consists of sections headed by a bracketed section title; for example, **[SCE-Sniffer RADIUS LEG]**. Each section consists of several parameters with the format of **parameter=value**. The number sign (“#”) at the beginning of a line denotes that this is a remark line.

- [Configuring the General Settings](#)
- [Configuring the Subscriber ID](#)
- [Information About Configuring the Subscriber IP Address](#)
- [Information About Configuring the Policy Settings](#)

### Configuring the General Settings

The general configuration of the LEG appears under the section name **[SCE-Sniffer RADIUS LEG]**. The following list describes the general configuration parameters:

- **start**  
Defines whether the SM should run the LEG at startup.  
Possible values for this parameter are **yes** and **no**. The default value is **no**.  
To start using the LEG, change this setting to **yes**.
- **packet\_types**  
Defines the RADIUS packet types to analyze. You should set this parameter according to the integration mode you have chosen.  
Possible values are any combination of: **access-request**, **access-accept**, **accounting-start**, **accounting-interim**, and **accounting-stop** separated by commas.  
The default value is **accounting-start, accounting-interim, accounting-stop**.
- **log\_failures**  
Defines whether the LEG should add messages about failures to the user log.  
Possible values for this parameter are **true** and **false**. The default value is **true**.
- **log\_all**

Defines whether the LEG should add all messages, including successful logins and logouts, to the user log.

Possible values for this parameter are **true** and **false**. The default value is **false**.



Note

For this LEG to work correctly, use the configuration file to enable the RDR server in the SM.

## Configuring the Subscriber ID



Note

The Subscriber ID configuration is optional.

The subscriber ID is identified by the User-Name attribute by default. You can configure the LEG to use any other RADIUS attribute to identify the subscriber ID, including using the Vendor-Specific attribute.



Note

If you want to keep the default identification according to the User-Name attribute, you can skip this section.



Note

The configured attribute must be of data type **string**. When using the Vendor-Specific attribute, the configured vendor specific subtype must be of data type **string**.

The section used for subscriber ID configuration is called [**RADIUS.Subscriber ID**]. The following list describes the parameters:

- `radius_attribute`  
Defines the attribute number for the subscriber ID classification.  
The default value is 1 (User-Name attribute).
- `radius_attribute_vendor_id`  
This parameter is only relevant if **radius\_attribute** is configured to 26 (Vendor-Specific attribute).  
The parameter defines the vendor ID number for the subscriber ID classification.  
This parameter has no default value.
- `radius_sub_attribute`  
This parameter is only relevant if **radius\_attribute** is configured to 26 (Vendor-Specific attribute).  
The parameter defines the sub attribute within the vendor specific attribute that is used for subscriber ID classification.  
This parameter has no default value.
- `radius_attribute_type`  
Defines the attribute type. Possible values for this parameter are **integer** or **string**. The default value is **string**.



# Information About Configuring the Subscriber IP Address

**Note**

The Subscriber IP Address configuration is optional.

The subscriber IP Address is identified by the Framed-Route attributes, or the Framed-IP-Address attribute (Framed-IP-Netmask optional) by default. The LEG can be configured to use any other RADIUS attribute to identify the subscriber IP Address, including using the Vendor-Specific attribute as described in the [Subscriber IP Association](#) section .

To define which attribute to use for the subscriber IP address, configure the **[RADIUS.Subscriber IP Address]** section. In order to use the default values, leave the configuration remarked.

To define the attribute to be used, configure the following parameters:

- `radius_attribute`  
Configure the **radius\_attribute** parameter with the RADIUS attribute number. Enter the value of 26 for Vendor Specific Attributes (VSA).
- `radius_attribute_vendor_id`  
This parameter is only relevant if **radius\_attribute** is configured to 26 (Vendor-Specific attribute). The parameter defines the vendor ID number for the subscriber ID classification.  
This parameter has no default value.
- `radius_sub_attribute`  
This parameter is only relevant if **radius\_attribute** is configured to 26 (Vendor-Specific attribute). The parameter defines the sub attribute within the vendor specific attribute that is used for subscriber ID classification.  
This parameter has no default value.
- `radius_attribute_type`  
Configure the **radius\_attribute\_type** parameter according to the RADIUS attribute format.  
Possible values for this parameter are **integer** or **string**. If the type is **string**, you must supply a mapping table. The default value is string.
- [Subscriber IP Address Configuration Example](#)

## Subscriber IP Address Configuration Example

The following is an example of the configuration section to define which attribute to use for the subscriber IP address:

```
[RADIUS.Subscriber IP Address]
radius_attribute=26
radius_attribute_vendor_id=1000
radius_sub_attribute=3
radius_attribute_type=string
```

# Information About Configuring the Policy Settings



**Note** The policy configuration is optional.

Policy configuration assigns policy information such as package ID, according to the RADIUS packets. Configure the SCE-Sniffer RADIUS LEG using the policy section(s) to assign the policy information.



**Note** This section is optional. If you do not need to set policy information according to RADIUS packets, you can skip this section. The SCE-Sniffer RADIUS LEG will not include any policy information when it logs in subscribers. If the subscriber already has some policies set, the LEG will not affect it.

For each policy you want to define, you need to specify a different section named **[RADIUS.Policy.policyName]**. You can use any string you want for policyName if the policy name is unique inside the configuration file.

Each policy section has the following parameters:

- `radius_attribute`  
Defines the attribute number that holds the policy information.  
This parameter has no default value.
- `radius_attribute_vendor_id`  
This parameter is only relevant if `radius_attribute` is configured to 26 (Vendor-Specific attribute).  
The parameter defines the vendor ID number that holds the policy information.  
This parameter has no default value.
- `radius_sub_attribute`  
This parameter is only relevant if `radius_attribute` is configured to 26 (Vendor-Specific attribute).  
The parameter defines the sub attribute of the vendor specific attribute that holds the policy information.  
This parameter has no default value.
- `radius_attribute_type`  
Defines the type of the attribute.  
Possible values are **string** or **integer**.  
This parameter has no default value.
- `default_value`  
Defines the default value to set in case the attribute is not found in the traffic.  
The default value is set only if this policy has not been already set, for example by other LEG interfaces.  
This parameter is optional. If it does not exist, a default value will not be set for this policy.
- `policy_name`  
Defines the name of the subscriber property. For instance, the `packageId` property defines the policies of the SCA BB solution.  
This parameter has no default value.

- `mapping_table.<key>=<value>`  
A set of values (key, value) used to map the data retrieved from the RADIUS attribute to the policy index configured by the application.
- [Policy Configuration Example](#)

## Policy Configuration Example

The following configuration section associates the `packageId` property of the SCA BB solution with a Vendor Specific attribute of the RADIUS packet:

```
[RADIUS.policy.packageId]
radius_attribute=26
radius_attribute_vendor_id=1000
radius_sub_attribute=2
radius_attribute_type=string
default_value=1
policy_name=packageId
mapping_table.gold=11
mapping_table.silver=12
mapping_table.bronze=13
```

This configuration indicates that if the configured RADIUS attribute of data type string holds the value *gold*, the package ID that will be introduced to the SM will have the value of 11. If the configured vendor specific attribute does not appear in the traffic, the package ID that will be introduced to the SM will have the value 1.





# CHAPTER 5

## Using the SCE-Sniffer RADIUS LEG CLU

This module describes the Command-Line Utilities to retrieve information and statistics about the LEG

- [Information About the SCE-Sniffer RADIUS LEG Utility](#)

### Information About the SCE-Sniffer RADIUS LEG Utility

The SCE-Sniffer RADIUS LEG contains its own Command-Line Utility (CLU) commands, called **p3radiusniff**, for retrieving information and statistics about the LEG.

The **p3radiusniff** utility displays the LEG configuration and statistics. The command format is `p3radiusniff <operation>`.

The following table lists the **p3radiusniff** operations

**Table 5-1** *p3radiusniff Operations*

| Operation                      | Description                                                                                       |
|--------------------------------|---------------------------------------------------------------------------------------------------|
| <code>--show</code>            | Displays all of SCE-Sniffer RADIUS LEG configuration and status                                   |
| <code>--show-statistics</code> | Displays counters of RADIUS messages handled and number of login/logout operations performed      |
| <code>--show-version</code>    | Displays the SCE-Sniffer RADIUS LEG version number                                                |
| <code>--help</code>            | Displays a list of available operations and arguments with a short explanation of their meanings. |

- [Viewing the SCE-Sniffer RADIUS LEG Status](#)
- [Viewing the SCE-Sniffer RADIUS LEG Version](#)
- [Viewing the SCE-Sniffer RADIUS LEG Statistics](#)

### Viewing the SCE-Sniffer RADIUS LEG Status

The following example illustrates the **p3radiusniff** Command-Line Utility using the **show** operation:

```

>p3radiusniff --showSCE-Sniffer RADIUS LEG:
=====
Active: true
RADIUS packet types:
accounting_start
accounting_interim
accounting_stop
Subscriber ID Association
Attribute: 1
Policy Association:
attribute=26
vendorIdAttribute=1000
subAttribute=2
attributeType=string
defaultValue=1
policyName=packageName
Command terminated successfully
>

```

## Viewing the SCE-Sniffer RADIUS LEG Version

The following example displays the **p3radiusniff** Command-Line Utility using the **show-version** operation:

```

>p3radiusniff --show-versionSCE-Sniffer RADIUS LEG 3.1.0 Build 176
Command terminated successfully
>

```

## Viewing the SCE-Sniffer RADIUS LEG Statistics

The following example displays the **p3radiusniff** Command-Line Utility using the **show-statistics** operation:

```

>p3radiusniff --show-statisticsSCE-Sniffer RADIUS LEG statistics
=====
Total Received RDRs: 12
Accounting RDRs: 12
Accounting-Start RDRs: 6
Accounting-Interim RDRs: 0
Accounting-Stop RDRs: 6
Access RDRs: 0
Access-Request RDRs: 0
Access-Accept RDRs: 0
Invalid RDRs: 0
Successful logins: 6
Successful logouts: 6
Failed logins: 0
Failed logout: 0
Command terminated successfully
>

```