

Multi-Service Business Routers

Enterprise Session Border Controllers

VoIP Media Gateways

Configuration Note

RADIUS for Secure Device Access



December 2012

Document # LTRT-34201

Table of Contents

1	Introduction	1
2	Setting Up a Third-Party RADIUS Server	3
3	Configuring RADIUS for the Device.....	5
3.1	Configuring General RADIUS Settings	5
3.2	Securing RADIUS Communication	7
4	Authenticating RADIUS in the URL.....	9

List of Figures

Figure 1-1: Device Implementing RADIUS Application	1
Figure 3-1: RADIUS Settings Page	5
Figure 3-2: Enabling HTTPS for Securing Web Access.....	7

List of Tables

Table 2-1: Web User Access Levels / Privileges and RADIUS Server Representation.....	3
--	---

Notice

This document describes how to set up a RADIUS server and how to configure the device to support it.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2012 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: December-06-2012

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used,



Note: Throughout this document, unless otherwise specified, the term *device* refers to AudioCodes' VoIP Media Gateways, the Mediant MSBR Series and the Mediant E-SBC Series.

Reader's Notes

1 Introduction

You can enhance security for your AudioCodes device by implementing Remote Authentication Dial-In User Service (RADIUS - RFC 2865) for authenticating multiple login user accounts of the device's embedded Web and Telnet servers. Thus, RADIUS also prevents unauthorized access to your device.

When RADIUS authentication is not used, the login user name and password are locally authenticated by the device with the Web interface's local user names and passwords (defined in the 'Web User Accounts' page) or with the Telnet server's user names and passwords.

When RADIUS authentication is used, the RADIUS server stores the device's login user names, passwords, and access (authorization) levels (Web only). When a management client tries to access the device, the device sends the RADIUS server the client's username and password for authentication. The RADIUS server replies with an acceptance or a rejection notification. While RADIUS authentication is performed, the device's Web interface is blocked until an acceptance response is received from the RADIUS server.

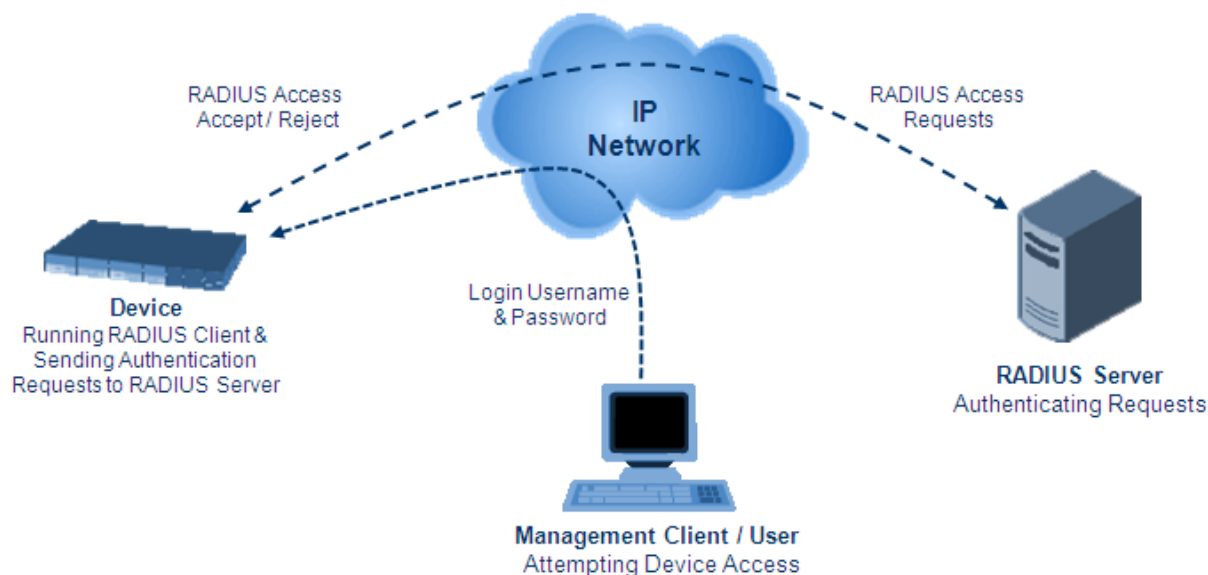
The local Web and Telnet user names and passwords can be used as a fallback mechanism in case the RADIUS server doesn't respond.

Note that communication between the device and the RADIUS server is done by using a Shared Secret, which is not transmitted over the network.

For setting up RADIUS support, the following needs to be done:

- Set up a RADIUS server (third-party) to communicate with the device.
- Configure the device as a RADIUS client for communication with the RADIUS server.

Figure 1-1: Device Implementing RADIUS Application



Reader's Notes

2 Setting Up a Third-Party RADIUS Server

This section provides an example for setting up the third-party RADIUS sever, *FreeRADIUS*, which can be downloaded from www.freeradius.org. Follow the directions at this Web site for installing and configuring the server. If you use a RADIUS server from a different vendor, refer to its appropriate documentation.

➤ **To set up a third-party RADIUS server (e.g., *FreeRADIUS*):**

1. Define the AudioCodes device as an authorized client of the RADIUS server, with the following:
 - Predefined *shared secret* (password used to secure communication between the device and the RADIUS server)
 - Vendor ID

Below is an example of the *clients.conf* file (FreeRADIUS client configuration):

```
#
# clients.conf - client configuration directives
#
client 10.31.4.47 {
    secret          = FutureRADIUS
    shortname       = audc_device
}
```

2. If access levels are required, set up a Vendor-Specific Attributes (VSA) dictionary for the RADIUS server and select an attribute ID that represents each user's access level. The example below shows a dictionary file for FreeRADIUS that defines the attribute "ACL-Auth-Level" with "ID=35". For the device's user access levels and their corresponding numeric representation in RADIUS servers, see [Table 2-1](#).

```
#
# AudioCodes VSA dictionary
#
VENDOR AudioCodes 5003
ATTRIBUTE ACL-Auth-Level 35 integer AudioCodes
VALUE ACL-Auth-Level ACL-Auth-UserLevel 50
VALUE ACL-Auth-Level ACL-Auth-AdminLevel 100
VALUE ACL-Auth-Level ACL-Auth-SecurityAdminLevel 200
```

Table 2-1: Web User Access Levels / Privileges and RADIUS Server Representation

Device Access Levels	Numeric Representation in RADIUS Server	Privileges
Security Administrator	200	Read-write privileges for all pages.
Administrator	100	Read-write privileges for all pages except security-related pages, which are read-only.
User Monitor	50	No access to security-related and file-loading pages; read-only access to the other pages. This read-only access level is typically applied to the secondary Web user account
No Access	0	No access to any page.

3. Define the list of users authorized to use the device, using one of the password authentication methods supported by the server implementation. The example below shows a user configuration file for FreeRADIUS using a plain-text password:

```
# users - local user configuration database

john    Auth-Type := Local, User-Password == "qwerty"
        Service-Type = Login-User,
        ACL-Auth-Level = ACL-Auth-SecurityAdminLevel

sue     Auth-Type := Local, User-Password == "123456"
        Service-Type = Login-User,
        ACL-Auth-Level = ACL-Auth-UserLevel
```

4. Record and retain the IP address, port number, shared secret code, vendor ID, and VSA access level identifier (if access levels are implemented) used by the RADIUS server.

3 Configuring RADIUS for the Device

This section describes how to configure the device for RADIUS support, using the device's embedded Web server interface.

3.1 Configuring General RADIUS Settings

The procedure below describes the general configurations for RADIUS support.

➤ **To configure the device's RADIUS support:**

1. Access the device's Web interface.
2. Open the RADIUS Settings page (**Configuration** tab > **System** menu > **Management** > **RADIUS Settings**).

Figure 3-1: RADIUS Settings Page

General RADIUS Setting	
3	Enable RADIUS Access Control: Enable
4	Use RADIUS for Web/Telnet Login: Enable
5	RADIUS Authentication Server IP Address: 90.11.4.46
	RADIUS Authentication Server Port: 1645
	RADIUS Shared Secret:
General RADIUS Authentication	
7	Default Access Level: 200
8	Device Behavior Upon RADIUS Timeout: Verify Access Locally
	Local RADIUS Password Cache Mode: Reset Timer Upon Access
6	Local RADIUS Password Cache Timeout [sec]: 300
	RADIUS VSA Vendor ID: 5003
	RADIUS VSA Access Level Attribute: 35

3. From the 'Enable RADIUS Access Control' drop-down list, select **Enable** to enable the RADIUS application.
4. From the 'Use RADIUS for Web/Telnet Login' drop-down list, select **Enable** to enable RADIUS authentication for Web and Telnet login.
5. Define the RADIUS server with which the device communicates:
 - a. In the 'RADIUS Authentication Server IP Address' field, enter the RADIUS server's IP address.
 - b. In the 'RADIUS Authentication Server Port' field, enter the RADIUS server's port number.
 - c. In the 'RADIUS Shared Secret' field, enter the shared secret code used to authenticate the device to the RADIUS server.
6. In the 'RADIUS VSA Vendor ID' field, enter the device's vendor ID. This must be the same one as configured in the RADIUS server (see Section 2, Step 2).

7. When implementing Web user access levels, do one of the following:
 - **If the RADIUS server response includes the access level attribute:** In the 'RADIUS VSA Access Level Attribute' field, enter the code that indicates the access level attribute in the VSA section of the received RADIUS packet. For defining the RADIUS server with access levels, see Section 2, Step 3.
 - **If the RADIUS server responses exclude the access level attribute:** In the 'Default Access Level' field, enter the default access level that is applied to all users authenticated by the RADIUS server.
8. Define RADIUS timeout handling:
 - a. From the 'Device Behavior Upon RADIUS Timeout' drop-down list, select the option if the RADIUS server does not respond within five seconds:
 - ◆ **Deny Access:** the device denies access to the Web and Telnet interfaces.
 - ◆ **Verify Access Locally:** the device checks the user name and password defined locally for the device (in the Web User Accounts page) and if correct, it allows access.
 - b. In the 'Local RADIUS Password Cache Timeout' field, enter a time limit (in seconds) after which the user name and password verified by the RADIUS server becomes invalid and a user name and password must be re-validated with the RADIUS server.
 - c. From the 'Local RADIUS Password Cache Mode' drop-down list, select the option for the local RADIUS password cache timer:
 - ◆ **Reset Timer Upon Access:** upon each access to a Web page, the timer resets (reverts to the initial value configured in the previous step).
 - ◆ **Absolute Expiry Timer:** when you access a Web page, the timer doesn't reset, but continues its count down.
9. Click **Submit**.
10. Save your settings to flash memory with a device reset (refer to the device's *User's Manual*).

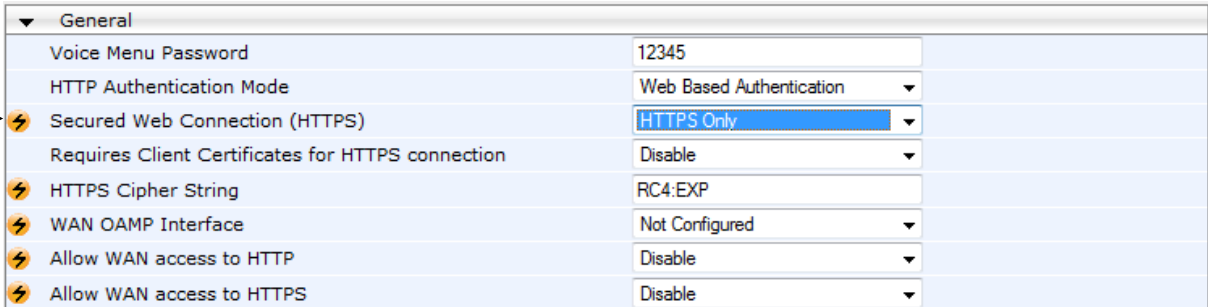
3.2 Securing RADIUS Communication

RADIUS authentication requires HTTP basic authentication (according to RFC 2617). However, this is insecure as the user names and passwords are transmitted in clear text over plain HTTP. Therefore, as digest authentication is not supported with RADIUS, it is highly recommended that the RADIUS implementation is used with HTTPS so that the user names and passwords are encrypted.

➤ **To configure HTTPS:**

1. Access the device's Web interface.
2. Open the WEB Security Settings page (**Configuration** tab > **System** menu > **Management** > **WEB Security Settings**).
3. From the 'Secured Web Connection (HTTPS)' drop-down list, select **HTTPS Only**.

Figure 3-2: Enabling HTTPS for Securing Web Access



The screenshot shows the 'General' tab of the WEB Security Settings page. The 'Secured Web Connection (HTTPS)' dropdown menu is highlighted in blue and set to 'HTTPS Only'. An arrow points to this dropdown menu. Other settings include: Voice Menu Password (12345), HTTP Authentication Mode (Web Based Authentication), Requires Client Certificates for HTTPS connection (Disable), HTTPS Cipher String (RC4:EXP), WAN OAMP Interface (Not Configured), Allow WAN access to HTTP (Disable), and Allow WAN access to HTTPS (Disable).

General	
Voice Menu Password	12345
HTTP Authentication Mode	Web Based Authentication
Secured Web Connection (HTTPS)	HTTPS Only
Requires Client Certificates for HTTPS connection	Disable
HTTPS Cipher String	RC4:EXP
WAN OAMP Interface	Not Configured
Allow WAN access to HTTP	Disable
Allow WAN access to HTTPS	Disable

4. Click **Submit**.
5. Save your settings to flash memory with a device reset.

Reader's Notes

4 Authenticating RADIUS in the URL

RADIUS authentication is typically done after the user accesses the Web interface by entering only the device's IP address in the Web browser's URL field (for example, <http://10.13.4.12/>) and then entering the user name and password credentials in the Web interface login screen.

Authentication with the RADIUS server can also be done immediately after the URL is entered if it includes the login credentials, for example:

<http://10.4.4.112/Forms/RadiusAuthentication?WSBackUserName=John&WSBackPassword=1234>



Note: This feature allows up to five simultaneous users only.

Configuration Note