Grandstream Networks, Inc.

HT8XX Series

GXW42XX Series

User Level Access Management

Table of Contents

OVERVIEW **4**

SETTING UP A RADIUS SERVER **5**

Create a RADIUS Client 5

Define Access Levels 5

Define Users Authorized to use the devices 6

CONFIGURE RADIUS SETTINGS ON HT8XX/GXW42XX **7**

SECURE AND USE RADIUS WEB ACCESS CONTROL AUTHENTICATION **8**

Securing RADIUS Communication 8

HT8XX Web Access Configuration *8*

GXW42XX Web Access Configuration *8*

RADIUS Authentication 9

Table of Figures

Figure 1: RADIUS Communication 4
Figure 2: RADIUS Configuration on HT8XX (under ADVANCED SETTINGS) 7
Figure 3: GXW42XX RADIUS Configuration (under Maintenance ➔ RADIUS) 7
Figure 4: HT8XX Web Access Configuration 8
Figure 5: GXW42XX Web Access Configuration 8
Figure 6: HT8XX Login Page 9
Figure 7: GXW42XX Login Page 9

OVERVIEW

This document describes basic configuration to enhance security for the HT8XX and GXW42XX using a Remote Radius Authentication. This would authenticate multiple users accounts to access the device.

If the Radius authentication is not used, the login username and password are locally authenticated by the device with the local available user accounts (Admin / User / Viewer).

In case the Radius authentication is used, the Radius server stores different login usernames, passwords and access level for each account. Those will be used to authenticate the entered credentials (Username and password) to access the device.

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.

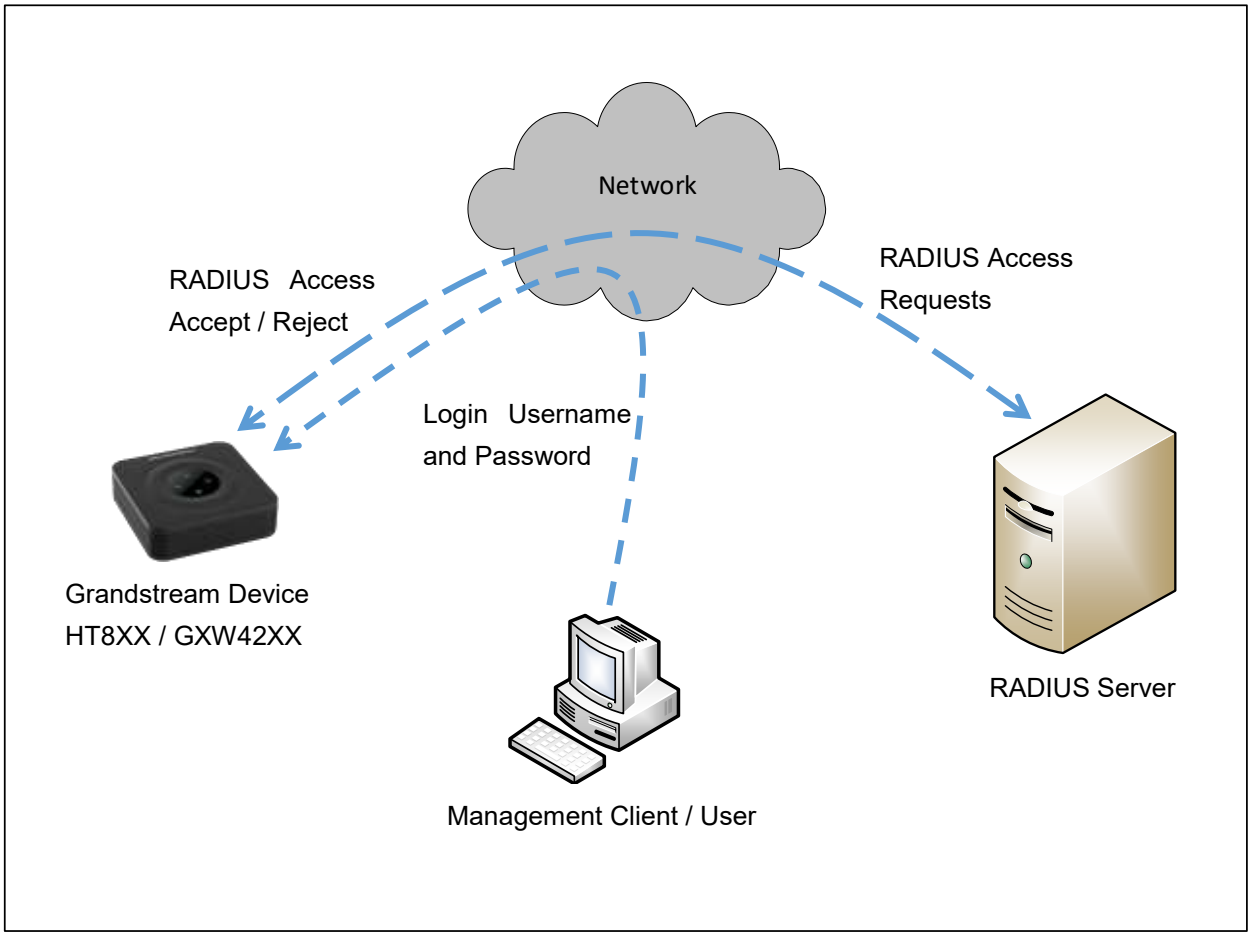

Figure 1: RADIUS Communication

SETTING UP A RADIUS SERVER

This is an example for setting up a RADIUS sever, *FreeRADIUS*. You can follow these instructions to install and configure the server. If you use a RADIUS server from a different vendor, refer to its appropriate documentation.

Create a RADIUS Client

Define the Grandstream devices as authorized clients of the RADIUS server, with the following:

- Predefined *shared secret* (password used to secure communication between the device and the RADIUS server)
- Vendor ID (***42397*** for Grandstream Networks Inc.)

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

```
client ht8xx {
       ipaddr = 192.168.5.204
       secret = Grandstream
}
client GXW {
       ipaddr = 192.168.5.195
       secret = Grandstream
}
```

Define Access Levels

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 below Table.

```
VENDOR Grandstream 42397
ATTRIBUTE ACL-Auth-Level 35 integer Grandstream
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 1: Web User Access Levels

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.

Define Users Authorized to use the devices

A list of the different users of the devices needs to be defined using a password authentication method.

The example below shows an example of ***users*** configuration file on FreeRADIUS:

```
John        Auth-Type := Accept, User-Password == "admin"
            Service-Type = Login-User,
            ACL-Auth-Level = ACL-Auth-SecurityAdminLevel

Jane        Auth-Type := Accept, User-Password == "user"
            Service-Type = Login-User,
            ACL-Auth-Level = ACL-Auth-AdminLevel

Doe         Auth-Type := Accept, User-Password == "viewer"
            Service-Type = Login-User,
            ACL-Auth-Level = ACL-Auth-UserLevel
```

CONFIGURE RADIUS SETTINGS ON HT8XX/GXW42XX

Access HT8XX/GXW42XX Web Interface and set the following:

1. Set “Enable RADIUS Web Access Control” to “Yes”
2. Set “Action upon Radius Auth Server Error” to “Authenticate Locally”
3. Enter in “RADIUS Auth Server Address” the IP address of the RADIUS server
4. Enter in “RADIUS Auth Server Port” the listening port if the RADIUS Server
5. Enter the “RADIUS Shared Secret” (e.g. ***Grandstream*** as set in the ***Clients.conf*** file of the RADIUS Server)
6. Enter the “RADIUS VSA Vendor ID” (e.g. ***42397*** as set in the ***dictionary*** file of the RADIUS Server)
7. Enter the “RADIUS VSA Access Level Attribute”
8. Press “Update” and “Apply”.

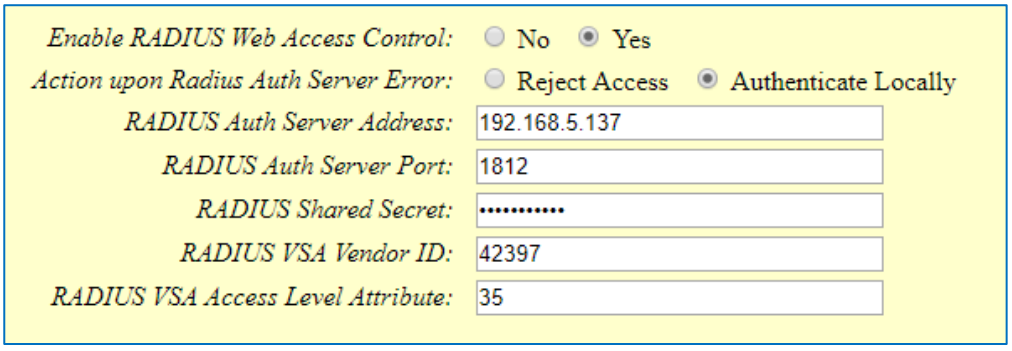

Figure 2: RADIUS Configuration on HT8XX (under ADVANCED SETTINGS)

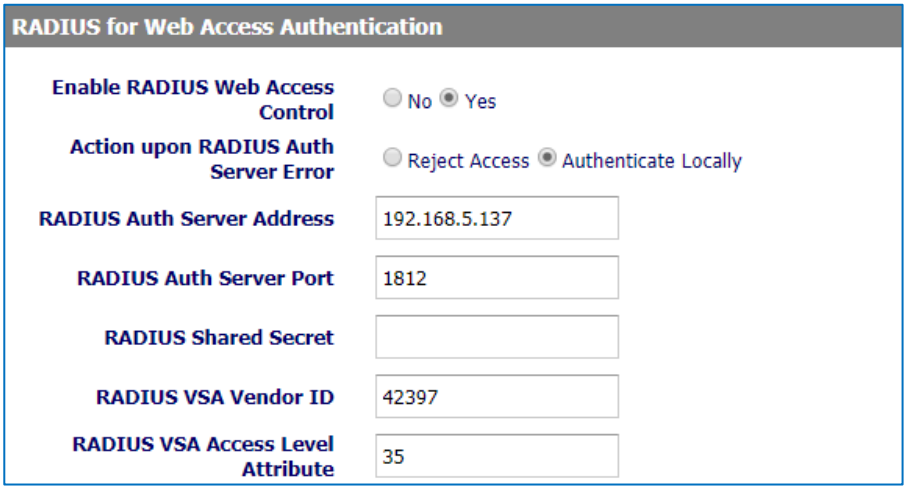

Figure 3: GXW42XX RADIUS Configuration (under Maintenance ➔ RADIUS)

SECURE AND USE RADIUS WEB ACCESS CONTROL AUTHENTICATION

Securing RADIUS Communication

To secure the RADIUS communication with HT8XX/GXW42XX, HTTPS web access needs to be enabled.

HT8XX Web Access Configuration

In the HT8XX web GUI under **BASIC SETTINGS**:

1. Set Web access mode to HTTPS.
2. Choose the HTTPS port to use.

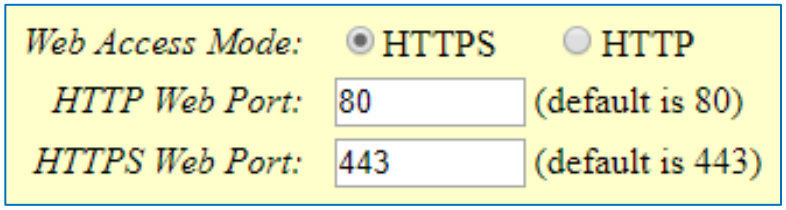

Figure 4: HT8XX Web Access Configuration

GXW42XX Web Access Configuration

In the GXW42XX Web GUI under **Maintenance ➔ Web/SSH Access:**

1. Set Web access mode to HTTPS.
2. Choose the HTTPS port to use.

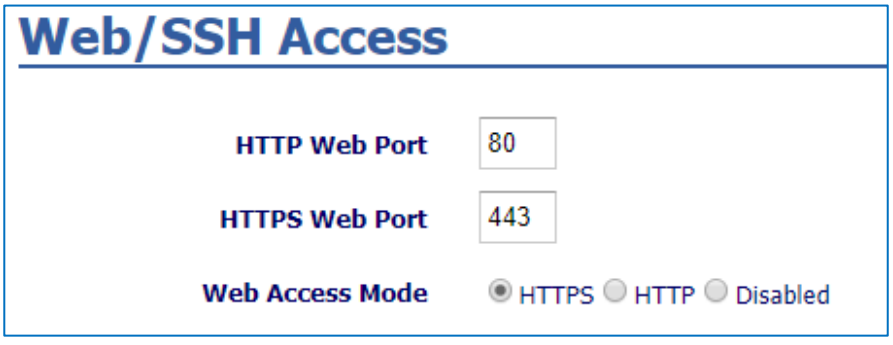

Figure 5: GXW42XX Web Access Configuration

RADIUS Authentication

In the unit's web interface: RADIUS authentication is done after the user accesses the Web interface by entering only the device's IP address in the Web browser's URL field (Example ***http://192.168.5.204/***) and then entering the username and password credentials in the Web interface login screen.

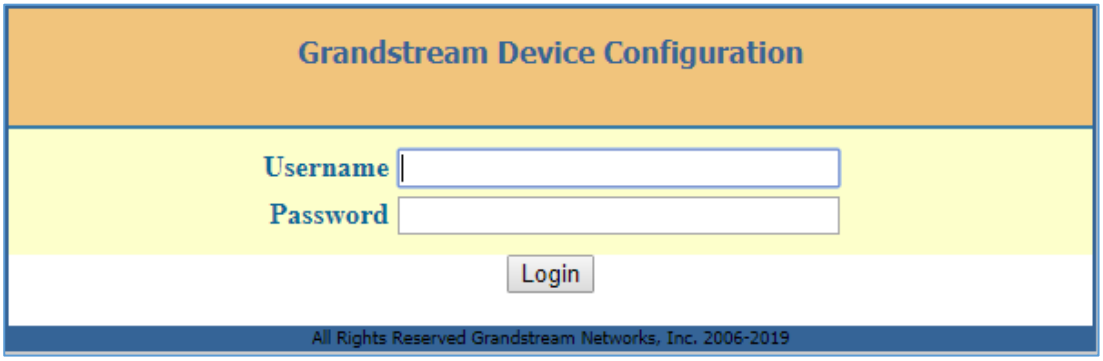

Figure 6: HT8XX Login Page

Figure 7: GXW42XX Login Page