

Grandstream Device Configuration

STATUS **BASIC SETTINGS** **ADVANCED SETTINGS** **PROFILE 1** **PROFILE 2** **FXS PORTS**

New Admin Password: (purposely not displayed for security protection)

Confirm Admin Password:

802.1Q/VLAN Tag (0-4094)

Layer 2 QoS: SIP 802.1p (0-7)

RTP 802.1p (0-7)

Black List for WAN Side Port:

STUN server is: (URI or IP:port)

Keep-alive Interval: (in seconds, default 20 seconds)

Use STUN to detect network connectivity: ☒ No
☐ Yes, total STUN response misses to restart DHCP (minimum=3)

Use DNS to detect network connectivity: ☒ No ☐ Yes

Use ARP to detect network connectivity: ☐ No ☒ Yes

Verify host when using HTTPS: ☒ No ☐ Yes

Firmware Upgrade and Provisioning: Upgrade Via ☐ TFTP ☒ HTTP ☐ HTTPS ☐ FTP ☐ FTPS

Firmware Server Path:

Config Server Path:

XML Config File Password:

HTTP/HTTPS/FTP/FTPS User Name:

HTTP/HTTPS/FTP/FTPS Password:

Firmware File Prefix:

Firmware File Postfix:

Config File Prefix:

Config File Postfix:

Allow DHCP Option 66 or 160 to override server:

☐ No ☒ Yes

3CX Auto Provision:

☐ No ☒ Yes

Automatic Upgrade:

☒ No

☐ Yes, every minutes(30-5256000).

☐ Yes, daily at start hour (0-23), at end hour (0-23).

☐ Yes, weekly on day (0-6).

Randomized Automatic Upgrade: ☒ No ☐ Yes

☒ Always Check for New Firmware at Boot up

☐ Check New Firmware only when F/W pre/suffix changes

☐ Always Skip the Firmware Check

Disable SIP NOTIFY Authentication: ☒ No ☐ Yes (Device will not challenge NOTIFY with 401 when set to Yes)

Authenticate Conf File: ☒ No ☐ Yes (cfg file would be authenticated before acceptance if set to Yes)

Validate Server Certificates: ☒ No ☐ Yes (validate server certificates with our trusted list of TLS connections)

SIP TLS Certificate:

SIP TLS Private Key:

SIP TLS Private Key Password:

Custom Certificate:
(Private Key + Certificate)

Enable TR-069: ☐ No ☒ Yes

ACS URL:

ACS Username:

ACS Password:

Periodic Inform Enable: ☒ No ☐ Yes

Periodic Inform Interval: 300

Connection Request Username:

Connection Request Password:

CPE SSL Certificate:

CPE SSL Private Key:

Enable SNMP: ☒ No ☐ Yes

SNMP Version: Version 3 ▼

SNMP Port: 161 (161 or 1025-65535. Default 161)

| | |
|---------------------------------------|---|
| SNMP Trap IP Address: | <input type="text"/> |
| SNMP Trap Port: | <input type="text" value="162"/> (162 or 1025-65535. Default 162) |
| SNMP Trap Version: | <input type="text" value="Version 2c"/> |
| SNMP Trap Interval: | <input type="text" value="5"/> (1-1440. Default 5 minutes) |
| SNMPv1/v2c Community: | <input type="text"/> |
| SNMPv1/v2c Trap Community: | <input type="text"/> |
| SNMPv3 User Name: | <input type="text"/> |
| SNMPv3 Security Level: | <input type="text" value="noAuthUser"/> |
| SNMPv3 Authentication Protocol: | <input type="text" value="None"/> |
| SNMPv3 Privacy Protocol: | <input type="text" value="None"/> |
| SNMPv3 Authentication Key: | <input type="text"/> |
| SNMPv3 Privacy Key: | <input type="text"/> |
| SNMPv3 Trap User Name: | <input type="text"/> |
| SNMPv3 Trap Security Level: | <input type="text" value="noAuthUser"/> |
| SNMPv3 Trap Authentication Protocol: | <input type="text" value="None"/> |
| SNMPv3 Trap Privacy Protocol: | <input type="text" value="None"/> |
| SNMPv3 Trap Authentication Key: | <input type="text"/> |
| SNMPv3 Trap Privacy Key: | <input type="text"/> |
| Enable RADIUS Web Access Control: | <input checked="" type="radio"/> No <input type="radio"/> Yes |
| Action upon Radius Auth Server Error: | <input type="radio"/> Reject Access <input checked="" type="radio"/> Authenticate Locally |
| RADIUS Auth Server Address: | <input type="text"/> |
| RADIUS Auth Server Port: | <input type="text"/> |
| RADIUS Shared Secret: | <input type="text"/> |
| RADIUS VSA Vendor ID: | <input type="text" value="42397"/> |
| RADIUS VSA Access Level Attribute: | <input type="text"/> |
| Enable DDNS: | <input checked="" type="radio"/> No <input type="radio"/> Yes |
| DDNS Server: | <input type="text" value="dyndns.org"/> |
| DDNS Username: | <input type="text"/> |
| DDNS Password: | <input type="text"/> |
| DDNS Hostname: | <input type="text"/> |
| DDNS Hash: | <input type="text"/> |
| System Ring Cadence: | <input type="text" value="c=2000/4000;"/> |
| Call Progress Tones: | Dial Tone: |

f1=350@-17,f2=440@-17,c=0/0;

Ringback Tone:

f1=440@-17,f2=480@-17,c=2000/4000;

Busy Tone:

f1=480@-21,f2=620@-21,c=500/500;

Reorder Tone:

f1=480@-21,f2=620@-21,c=250/250;

Confirmation Tone:

f1=350@-11,f2=440@-11,c=100/100-100/100-100/100;

Call Waiting Tone:

f1=440@-13,c=300/10000;

Prompt Tone:

f1=350@-17,f2=440@-17,c=0/0;

Conference Party Hangup
Tone:

f1=425@-15,c=600/600;

Syntax: f1=val[, f2=val[, c=on1/off1[-on2/off2[-on3/off3]]]];

(Frequencies are in (300, 3400) Hz and cadence on and off are in (0, 64000) ms)

Prompt Tone Access Code:

 (Key pattern to get Prompt Tone. Maximum 20 digits. No default.)

Lock Keypad Update: ☒ No ☐ Yes (configuration update via keypad is disabled if set to Yes)

Disable Voice Prompt: ☒ No ☐ Yes (voice prompt is disabled if set to Yes)

Disable Direct IP Call: ☒ No ☐ Yes (direct IP call is disabled if set to Yes)

Blacklist For Incoming Calls:

NTP Server:

pool.ntp.org

(URI or IP address)

Allow DHCP Option 42 to override NTP
server:

☐ No ☒ Yes

DHCP Option 17 Enterprise Number:

3561

Syslog Server:

Syslog Level:

NONE ▼

Send SIP Log:

☒ No ☐ Yes

Automatic Reboot:

☒ No

☐ Yes, reboot every day at hour (0-23)

☐ Yes, reboot every week at day (0-6)

☐ Yes, reboot every month at day (0-30)

Download Device Configuration:

Download

Download Device XML Configuration:

Download

Upload Firmware:

Upload from local directory

Upload Configuration:

Upload from local directory

Export Backup Configuration:

Download

Restore From Backup Configuration:

Upload

Update

Apply

Cancel

Reboot

All Rights Reserved Grandstream Networks, Inc. 2006-2019