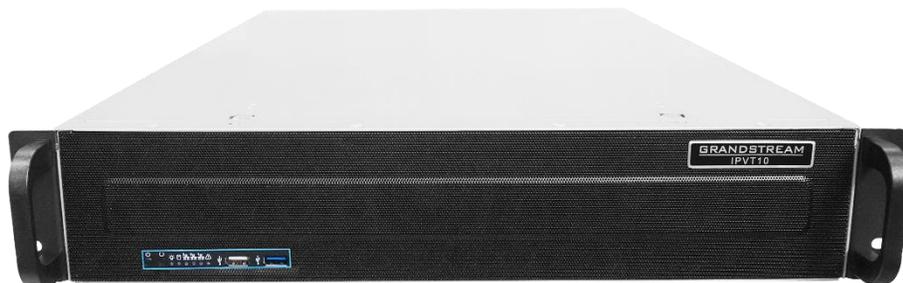


Grandstream Networks, Inc.

IPVT10

Video Conferencing Server

Administration Guide



COPYRIGHT

©2022 Grandstream Networks, Inc. <https://www.grandstream.com>

All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

The latest electronic version of this guide is available for download here:

<https://www.grandstream.com/support>

Grandstream is a registered trademark and the Grandstream logo is the trademark of Grandstream Networks, Inc. in the United States, Europe, and other countries.



CAUTIONS

To use the equipment correctly and safely, please read the safety cautions carefully before using it and strictly follow them when using it. "Equipment" refers to the equipment itself and its accessories by default in this document.

Basic Requirements

- Please keep the equipment dry and avoid violent collisions between the equipment and other objects during storage, transportation, and usage.
- Please do not disassemble the equipment. Please contact Grandstream support or designated distributor when users encounter problems.
- Any individual or enterprise may not change the structure, safety, or performance design of the equipment without Grandstream authorization.
- When using this equipment, users should follow the relevant laws and regulations, and respect the legal rights of others.

Environmental Requirements

- Before plugging or unplugging the cables of the equipment, users should stop using the equipment and disconnect the power supply.
- Please keep the equipment away from the heat source or fire such as an electric heater, candle, etc.
- Please keep the equipment away from the strong magnetic or strong electric appliances, such as microwave ovens, refrigerators, mobile phones, etc.
- Please place the equipment on the stable worktable.
- Please place the equipment in a ventilated, direct-light free environment. The recommended operating environment temperature of this equipment is 0°C to 45°C.
- Do not block the openings of the device with any object and leave more than 10cm of heat dissipation space around the equipment.
- Do not place any objects (such as candles or water containers) on the equipment. If foreign objects or liquids are in the equipment, stop using the equipment and disconnect the power supply immediately, unplug all the cables connected to the equipment, and contact Grandstream's designated service center.
- Do not place the equipment near water or a humid area.
- Please keep the equipment clean and away from the dust.
- Do not place the equipment near the objects which are easily combustible, such as foam materials and etc.



 **Note:** If the device keeps running for a long time, the shell of the device will be heat with a certain degree. Please do not worry about it, and the equipment can still be working normally.

Terms and Conditions

- Please keep the equipment away from children, in order to avoid dangers such as swallowing.
- Please use the accessories which are coming with the equipment or recommended by the manufacturer.
- Do not place the equipment near water or a humid area. If the liquid flows into the equipment accidentally, please disconnect the power supply immediately, and unplug all cables connected to the equipment, such as power cable. Then, please contact with Grandstream designated service center.
- The supplied voltage of the equipment has to meet the input voltage requirement of the equipment. Please use the lightning protection socket which matches the requirements.
- Before plugging or unplugging the cables from the equipment, please stop using the equipment and disconnect the power supply from the equipment.
- Please keep the hands dry when plugging and unplugging the cables from the equipment.
- Do not step on, pull, or bend the cables excessively of the equipment to avoid equipment failure.
- Do not use the damaged or aged cables with the equipment.
- Please keep the power plug clean and dry to avoid electric shock or other hazards.
- Please disconnect the power supply from the equipment in a thunderstorm, and remove all the cables connect to the equipment, such as power supply cable, in order to avoid lightning damage to the equipment.
- If users do not plan to use the equipment for a long time, please disconnect the power supply and remove all cables connect to the equipment.



- Do not look at the fiber interface on the equipment to avoid to impaired vision.
- If any abnormal issue occurs, such as equipment smoking, abnormal sound, abnormal odor, please stop using the equipment and disconnect the power supply from the equipment immediately. Please unplug all the cables connected to the equipment and contact with Grandstream designated support center.
- Please avoid the foreign objects (such as metal) enter the equipment from the heat dissipation hold.
- Before connecting other cables to the equipment, connect the ground cable to the host first; When users try to disconnect the cables from the equipment, please remove the ground cable at the end.
- Please ensure the protection ground cable of the three-phase socket is grounded effectively. The neutral wire and the live wire are not connected reversely.
- Do not scratch the shell of the equipment. Otherwise, the peeled paint may cause allergy, or equipment failure (falling into the equipment and causing failure).
- To ensure the safety, when the fuse in the equipment is blown, please replace the fuse with the same model and size.

Cleaning Instructions

- Before cleaning, please stop using the equipment and disconnect the power supply, and unplug all cables connected to the equipment.
- Do not clean the equipment shell with cleaning liquids or spray cleaner. Users could use a soft cloth to wipe the equipment shell.



Table of Content

DOCUMENT PURPOSE	13
CHANGE LOG	14
Firmware Version 1.0.6.13	14
Firmware Version 1.0.6.10	14
Firmware Version 1.0.6.9	14
Firmware Version 1.0.6.8	14
Firmware Version 1.0.6.5	14
Firmware Version 1.0.5.26	14
Firmware Version 1.0.5.20	15
Firmware Version 1.0.5.17	15
Firmware Version 1.0.5.12	15
Firmware Version 1.0.5.4	15
Firmware Version 1.0.4.12	15
Firmware Version 1.0.3.24	15
Firmware Version 1.0.3.17	15
Firmware Version 1.0.3.13	15
Firmware Version 1.0.2.8	16
Firmware Version 1.0.1.5	16
Firmware Version 1.0.0.15	16
WELCOME	17
PRODUCT OVERVIEW	18
Feature Highlights	18
IPVT10 Technical Specifications	19
INSTALLING IPVT10	21
Equipment Package Content	21



Installation Process	21
Equipment Inspection	22
<i>Equipment Appearance</i>	22
<i>Equipment Specifications</i>	25
Mounting IPVT10 Equipment to Cabinet	25
Connecting IPVT10 Server	27
<i>Connecting Network Cables</i>	27
<i>Connecting Power Supply cables</i>	27
Powering on IPVT10	28
CONFIGURING IPVT10	30
Descriptions of Meeting Capacity	30
Configuration Instructions	32
<i>First-time Configuration</i>	32
<i>Configuration Parameters Modification</i>	33
<i>Upgrading Service</i>	33
<i>Factory Reset</i>	33
Login the Configuration Page	34
<i>Accessing the Configuration Page directly via a Browser</i>	34
<i>Accessing the Configuration Page via IPVideoTalk Portal</i>	37
Update Login Password	37
Forgot Password	38
Setup Wizard	39
Server Status	42
System Information	45
Cluster Host Server Configuration	45
<i>Network Settings</i>	45
<i>Configure Service NAT Interfaces</i>	50
<i>Time Configuration</i>	52



<i>Configure SIP Trunk Service Address</i>	<i>53</i>
<i>Configure SMTP Mailbox</i>	<i>58</i>
<i>Configuring Conference Management Platform Information</i>	<i>59</i>
<i>Third Party Speech Recognition Service Configuration</i>	<i>62</i>
<i>Extended Disk</i>	<i>63</i>
<i>Cluster Settings</i>	<i>64</i>
<i>Slave Server Management</i>	<i>65</i>
<i>Configure IPVT10 Server Region</i>	<i>66</i>
<i>Region Management</i>	<i>67</i>
<i>Cluster Code</i>	<i>68</i>
<i>Configure Slave Server</i>	<i>68</i>
<i> Network Settings</i>	<i>68</i>
<i> Configure Service NAT Interfaces</i>	<i>70</i>
<i> Time Configuration</i>	<i>71</i>
<i> Cluster Settings</i>	<i>72</i>
<i>Advanced Settings</i>	<i>73</i>
<i> Alarm Email Setup</i>	<i>73</i>
<i> Enable/Disable SSH</i>	<i>73</i>
<i> Access Restrictions</i>	<i>74</i>
<i> Firewall Settings</i>	<i>75</i>
<i> Fail2Ban</i>	<i>76</i>
<i>License Management</i>	<i>77</i>
<i> View License Information</i>	<i>77</i>
<i> Update License</i>	<i>78</i>
<i>Maintenance</i>	<i>79</i>
<i> Upgrade</i>	<i>79</i>
<i> Factory Reset</i>	<i>80</i>
<i> Reboot</i>	<i>81</i>



<i>System Logs</i>	81
<i>Packet Capture</i>	81
<i>Traceroute</i>	82
<i>Ping</i>	83
<i>Operation Logs</i>	83
TYPICAL NETWORK SOLUTIONS.....	84
Scenario 1: Internal Network	84
Scenario 2: External Network	85
Scenario 3: External Users to Internal Server	86
Scenario 4: Internal Network and External Network.....	87
Scenario 5: Internal Network and some External Users.....	88
CONFIGURE GVC32XX CONFERENCE CLIENTS	90
Configure Service IP Address	90
START CONFERENCES	91
EXPERIENCING IPVT10 VIDEO CONFERENCING SERVER.....	93



Table of Tables

Table 1: IPVT10 Features in a Glance	18
Table 2: IPVT10 Technical Specifications	19
Table 3: IPVT10 Installation Process	21
Table 4: IPVT10 Front Panel Description	23
Table 5: IPVT10 Back Panel Description	24
Table 6: IPVT10 Equipment Specifications	25
Table 7: Checking the indicators after powering up IPVT10	29
Table 8: IPVT10 Server Meetings Performance	30
Table 9: Steps for First-time Configuration.....	32
Table 10: Modify Configuration Options	33
Table 11: Default Login Username and Password	34
Table 12: Parameters Descriptions	46
Table 13: Configure Network Routing Rules	49
Table 14: Service Port Configuration	51
Table 15: Configure SMTP Mailbox.....	58
Table 16: Configure Conference Management Platform.....	61
Table 17: Extended Disk (NFS) Parameters	63
Table 18: Parameters Descriptions	68
Table 19: Service Port Configuration	70



Table of Figures

Figure 1: IPVT10 Package Content	21
Figure 2: IPVT10 Front Panel	22
Figure 3: IPVT10 Back Panel.....	24
Figure 4: Connecting Ethernet Cables to Ethernet Interfaces	27
Figure 5: IPVT10 powered on	28
Figure 6: IPVT10 Web GUI - Login	35
Figure 7: IPVT10 Web GUI – Modify Password.....	35
Figure 8: Connect IPVT 10 with a PC Directly	36
Figure 9: Accessing the IPVT10 Configuration Page via IPVideoTalk Portal	37
Figure 10: Modify Password.....	37
Figure 11: Reset Password	38
Figure 12: Setup example	39
Figure 13: Server/Conference Status – Host Server	42
Figure 14: Server/Conference Status – Slave Server.....	44
Figure 15: System Information	45
Figure 16: Service IP Address Config – Internal Network Adapter	47
Figure 17: Service IP Address Config – External Network Adapter	49
Figure 18: Configure Network Routing Rules	49
Figure 19: Use Custom Certificate	50
Figure 20: Service Port Configuration	51
Figure 21: Time Settings	52
Figure 22: SIP Trunk Service Configuration - Access	53
Figure 23: SIP Trunk Service Configuration - Call	57
Figure 24: Configure SMTP Mailbox	58



Figure 25: Test Email	59
Figure 26: Configure Conference Management Platform	60
Figure 27: Configure Conference Management Platform – Speech Recognition Configuration	62
Figure 28: Activate/Inactivate NFS Storage Disk	63
Figure 29: Cluster Settings.....	64
Figure 30: Check Slave Server’s Information	65
Figure 31: IPVT10 Server Region	66
Figure 32: Move Scheduled Meetings Prompt.....	67
Figure 33: Region Management	67
Figure 34: Service IP Address Config – Network Adapter	69
Figure 35: Service Port Configuration	71
Figure 36: Time Settings	72
Figure 37: Cluster Settings.....	72
Figure 38: Alarm Email Setup	73
Figure 39: Access Restrictions.....	74
Figure 40 : IPVT10 Firewall settings	75
Figure 41 : IPVT10 Fail2Ban feature	76
Figure 42: View License Information.....	78
Figure 43: Upload License Key File	78
Figure 44: Upgrade Service	79
Figure 45: Clear Data.....	80
Figure 46: Download System Logs	81
Figure 47: Packet Capture	82
Figure 48: Traceroute.....	82
Figure 49: Ping	83
Figure 50 : Operation Logs	83



Figure 51: Network Deployment Diagram – Internal.....	84
Figure 52: Configure Internal Network Adapter.....	84
Figure 53: Network Deployment Diagram – External	85
Figure 54: Configure External Network Adapter	85
Figure 55: Network Deployment Diagram – External Users to Internal Server	86
Figure 56: Configure External Network Adapter and NAT	86
Figure 57: Network Deployment Diagram – Internal Network and External Network.....	87
Figure 58: Configure External Network Adapter and Internal Network Adapter	88
Figure 59: Network Deployment Diagram – Internal Network and Some External Users	89
Figure 60: Configure External Network Adapter and Internal Network Adapter - II	89
Figure 61: Configure Service IP Address	90
Figure 62: Service Configuration	91
Figure 63: Login Conference Management Platform.....	91
Figure 64: Manage Meeting Histories	92



DOCUMENT PURPOSE

This document covers the topics of device installation, configuration, and technical specifications, as well as IPVideoTalk Cloud service items, user's clients, service management and advanced features. To learn more information about IPVT10, please visit link www.ipvideotalk.com to get more information.

This guide covers following topics:

- [Product Overview](#)
- [Installing IPVT10](#)
- [Configuring IPVT10](#)
- [Typical Network Solutions](#)
- [Configure GVC32xx Conference Clients](#)
- [Start Conferences](#)
- [Experiencing IPVT10 Video Conferencing Server](#)



CHANGE LOG

This section documents significant changes from previous versions of Administration guide for IPVT10. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here. Users could log in to the product page to get more firmware update logs:

<https://www.grandstream.com/support/firmware/>

Firmware Version 1.0.6.13

- No Major Changes.

Firmware Version 1.0.6.10

- No Major Changes.

Firmware Version 1.0.6.9

- No Major Changes.

Firmware Version 1.0.6.8

- Added support for a new Video Mode option [Video Mode]
- Added support for a new Video Stream option [Video Stream]
- Support setting IVR to Russian Language [Configuring Conference Management Platform Information]

Firmware Version 1.0.6.5

- Supported Spanish IVR if the user changes the default language to Spanish on the management platform. [Configuring Conference Management Platform Information]
- Supported to allow users to configure the dynamic domain name in Network Settings. [Network Settings]

Firmware Version 1.0.5.26

- Supported to custom the host code length of the meeting to 4 – 32 digits. [Length of Host Code]
- Added access restriction feature. The user can add the IP addresses to the white list, and only the IP addresses on the white list can access the deployment management page and meeting management



page. [Access Restrictions]

- Add option to "Ignore certificate" that allows mailbox to send Mail if the SMTP server is a self-signed certificate. [Ignore certificate]

Firmware Version 1.0.5.20

- No Major Changes.

Firmware Version 1.0.5.17

- Added ability to configure video bit rate type and video bit rate.

Firmware Version 1.0.5.12

- No Major Changes.

Firmware Version 1.0.5.4

- No Major Changes.

Firmware Version 1.0.4.12

- Added support for Google Speech Recognition service. [Third Party Speech Recognition Service Configuration]

Firmware Version 1.0.3.24

- Added support for alarm notification email configuration. [Alarm Email Setup]
- Added support for static defense settings.
- Added support for operation logs viewing. [Operation Logs]
- Added support for Fail2Ban feature.

Firmware Version 1.0.3.17

- Added support for Ping and Traceroute troubleshooting tools.

Firmware Version 1.0.3.13

- Improve the meeting capacity: Support up to 50 meetings of two parties, or 10 meetings of three parties. Each meeting layout occupies 1 meeting resource. [PRODUCT OVERVIEW]



- Add support H.323. [IPVT10 Technical Specifications]
- Add multiple meeting layouts choices for each meeting, also add support meeting caption, sending pictures and files, and NFS extended disk. [IPVT10 Technical Specifications]
- Improve IPVT10 Web UI: Display NFS extended disk, display all sockets status, configure the meeting URL for public, add displaying system information, and add “Trial” tag on License.
- Add support to send test email for SMTP mailbox. [Configure SMTP Mailbox]
- Changing initial password is mandatory.
- Add support for Video display for terminals registered to UCM that is connected to IPVT10 server via trunk. [connect the IPVideoTalk Conference System with a 3rd party platform]

Firmware Version 1.0.2.8

- Add the region management function to the device. [Configure IPVT10 Server Region] [Region Management]

Firmware Version 1.0.1.5

- Added resetting the login password to the default password. [Forgot Password]
- Added Setup wizard for first time use. [Setup Wizard]
- Added Server status Dashboard. [Server Status]
- Added support for Cluster Host/Slave server. [Cluster Host Server Configuration] [Configure Slave Server] [Setup Wizard]
- Added support for “Debug” for any troubleshooting needs.

Firmware Version 1.0.0.15

- This is the initial version.



WELCOME

Thanks for purchasing Grandstream Network IPVT10 full-HD conferencing system.

This document introduces the IPVT10 installation process and usage instructions, including environment setup, start meetings and operations, scheduling meeting and etc.

For more information about IPVT10 and IPVideoTalk service, please visit the product page at:

<https://www.ipvideotalk.com>

This manual is applicable to IPVT10 equipment administrators.



Note:

Any change that is not authorized by Grandstream Networks Inc., or any operation that is not following this IPVT10 user guide will void the manufacturer's warranty of IPVT10.



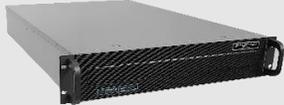
PRODUCT OVERVIEW

IPVT10 is an On-Premises Video Conferencing Server designed for enterprises seeking a powerful and secure video conferencing solution. It offers one easy-to-use platform that combines all aspects of an enterprise video conferencing applications, including room and web-based options and conferencing management. IPVT10 provides a centralized solution to manage an entire businesses' conferencing needs through one single server and interface. This On-Premises Video Conferencing Server is ideal for internal conferencing solutions among small and medium-sized enterprises, especially those with multiple locations, for example, communication between headquarters and multiple branch offices. It is also ideal for organizations who need to communicate with remote employees and those who perform remote training and/or education through video conferencing.

Feature Highlights

The following tables contain the major features of the IPVT10:

Table 1: IPVT10 Features in a Glance

 <p>IPVT10</p>	<ul style="list-style-type: none"> • Supports up to 300 participants and 50 meetings of two parties or 10 meetings of more than three parties conference simultaneously. • Audio, video, charts & reports recording capabilities with 500GB local storage. • 1080p H.264 for real-time video and screen sharing. • Up to 120 video feeds and 300 participants per single conference session. • Live broadcast using Facebook/YouTube Live features. • Advanced meeting control, flexible scheduling, customizable registration, invitation, follow-ups & reports. • Advanced anti-jitter algorithm to sustain smooth audio & video against up to 30% packet loss. • Access from PC/Mac, mobile devices, video conferencing systems, video phones, PSTN trunk, or SIP PBX. • HTTPS and WSS/DTLS SRTP encryption for WebRTC, TLS/SRTP encryption for SIP.
--	--

IPVT10 Technical Specifications

The following table resumes all the technical specifications including the protocols/standards supported, server module, audio/video features, MCU functional features, meeting, and device management for IPVT10.

Table 2: IPVT10 Technical Specifications

Application Functions	Built-in Video MCU, SIP Registrar Server, H.323 Gateway, NAT Traversal Server, Enterprise Collaboration Server, Contacts Manager, Recording/Storage Server, WebRTC Server.
Conference Capacity	<p>Up to 120-way 1080p H.264 video/audio MCU.</p> <p>Up to 300 participants (aggregate) with 2-way audio and 1-way 1080p H.264 video streaming.</p> <p>Up to 10 meetings of more than three parties or 50 meetings of two parties without WebRTC client.</p>
Video Support	H.264 BP/MP/HP with up to 1080p resolution and 6Mbps bit rate per stream.
Audio Support	Opus, G.722, G.711a/u, up to 48KHz wide-band audio mixing.
Network Jitter Resilience	<p>Advanced anti-jitter algorithms to sustain high quality audio/video against up to 30% packet loss.</p> <p>Smart adaptation to dynamically adjust bandwidth between 64Kbps and 6Mbps based on network condition.</p>
Security	Support HTTPS and WSS/DTLS-SRTP encryption for WebRTC, and TLS/SRTP encryption for SIP
Video Display	<p>Support 2x2/3x3/4x4/5x5/6x6/7x7 Tile Video Layout, or 1 Primary + N Secondary (up to 7 secondary) Video Layout.</p> <p>1 meeting supports up to 3 meeting layouts, also supports to assign the viewing permission for other participants.</p>
Active Speaker Highlight	Automated active speaker detection and highlight.



Meeting Management	<p>Support Immediate or Scheduled Meetings/Webinars, multiple hosts/panelists, audio/video ON/OFF control.</p> <p>Desktop/application sharing, group or private chat, Q&A, meeting banners/captions, sending pictures and files, forced attendee Mute/Camera-Off/Exit by host.</p> <p>Customizable content for meeting invitation/registration/reminder/post-meeting reports and follow-up.</p>
Live Streaming	Support live streaming with Facebook and YouTube, and other live streaming platforms via RTMP push.
Supported Devices	<p>Grandstream GVC series video conference systems, GXV series video phones, PC/Mac using WebRTC browsers, Android/iOS based mobile devices using Grandstream IPVideoTalk mobile APP.</p> <p>Audio calling from PSTN SIP trunk or SIP based IPPBX, 3rd party SIP based video conference systems and video phones.</p>
Meeting Records	<p>Support up to 500GB local storage of audio/video/chats recording, meeting reports, etc.</p> <p>Support remote mounting NFS extended disk.</p>
Deployment Scalability	Scalable architecture to support multi-server configuration with load-balancing and redundancy for large deployments.
Multi-language	English, German, French, Spanish, Chinese, Japanese, Arabic, etc.
Power Supply	Redundant 550W power supplies.
Network Interfaces	2x Gigabit network ports, 1x RJ45 IPMI network port.
Auxiliary Interfaces	3x USB 3.0 ports, 3x USB 2.0 ports, and 1x VGA port.
Physical Dimension	430mm (W) x 650mm (L) x 88mm (H), 2U rack design suitable for 19-inch cabinet and guide rail.
Temperature & Humidity	Operations 0°C to 45°C, Humidity 10% ~ 90% non-condensing.
Compliance	FCC, CE, RCM.



INSTALLING IPVT10

Equipment Package Content

Users need to open the package, check the equipment and parts to ensure the integrity and availability of the equipment.

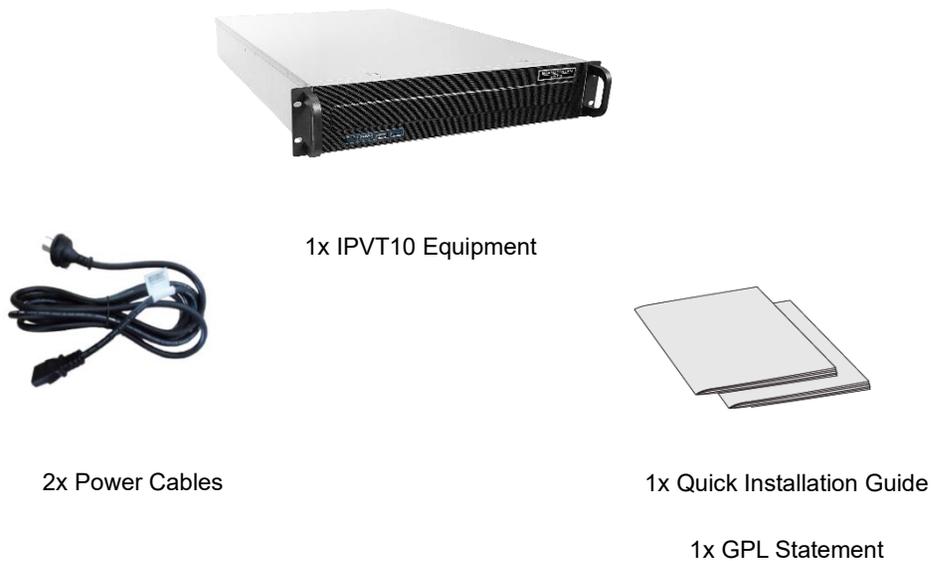


Figure 1: IPVT10 Package Content

Installation Process

Users need to follow the steps described in the table below in order to correctly complete the installation of the IPVT10:

Table 3: IPVT10 Installation Process

Index	Steps	Instructions
1	Equipment Inspection	Open the package, check the equipment and accessories, and inspect the hardware structure of the IPVT10.

2	Install to Cabinet (Optional)	Install IPVT10 to the cabinet
3	Connect to Network	Connect to the network with the Ethernet cable.
4	Connect to power supply	Connect to the power supply with the power adapter.
5	Power On	Inspect the running status of the equipment.

Equipment Inspection

Users need to open the package, check the equipment and parts to ensure the integrity and availability of the equipment.

Equipment Appearance

- **IPVT Front Panel**

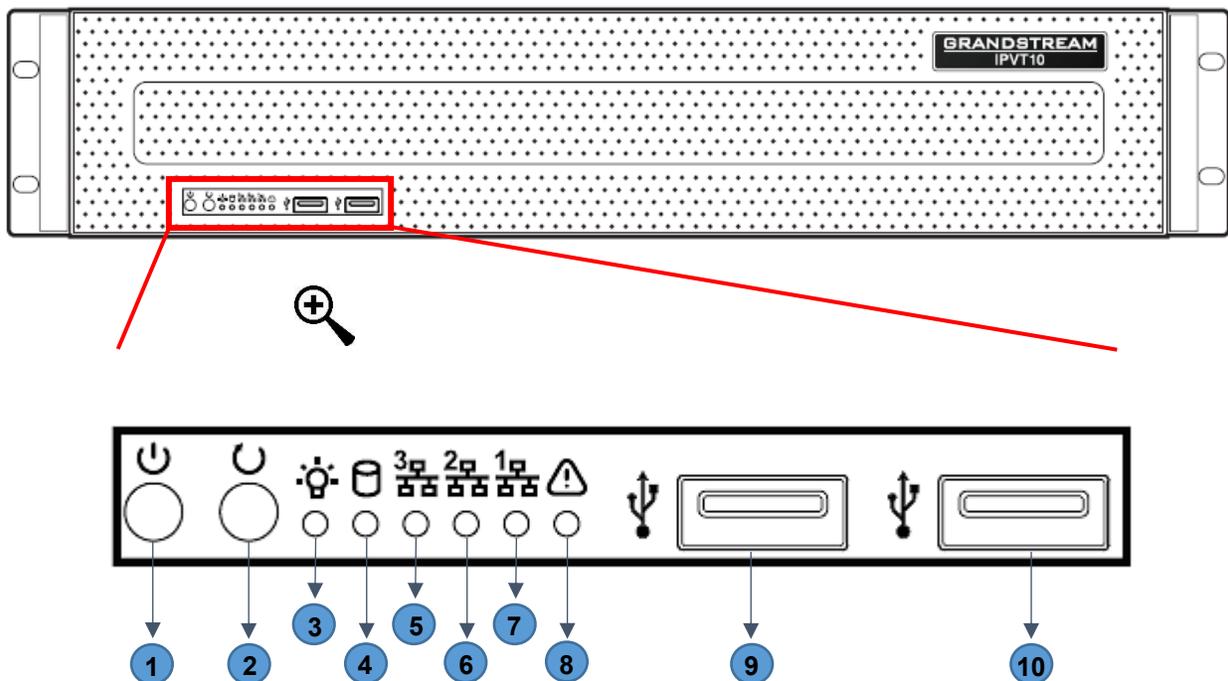


Figure 2: IPVT10 Front Panel

Table 4: IPVT10 Front Panel Description

NO.	Name	Description
1	Equipment Switch	When the equipment is not running, press the switch to turn on the equipment, and when the equipment is running normally, long press the switch (5 seconds) will turn off the equipment.
2	Reboot Switch	When the equipment is running normally, pressing this switch will reboot the equipment.
3	Power Indicator	<ul style="list-style-type: none"> • When the equipment is ON and connected to the power supply: the light is solid green. • When the equipment is OFF, and the power supply is not connected with the equipment: the light is off.
4	Hard Disk Indicator	<ul style="list-style-type: none"> • When the hard disk is running normally: the light is off. • When the hard disk is reading and writing: the light is solid blue.
5	Network Connection Indicator	<ul style="list-style-type: none"> • When the network connection is normal: the light is flashing yellow. • When the network connection is abnormal, or the network is not connected with the equipment: the light is off.
6	Ethernet Interface 1 Indicator	<ul style="list-style-type: none"> • When the network connection is normal: the light is flashing yellow. • When the network connection is abnormal, or the network is not connected with the equipment: the light is off.
7	Ethernet Interface 2 Indicator	<ul style="list-style-type: none"> • When the network connection is normal: the light is flashing yellow. • When the network connection is abnormal, or the network is not connected with the equipment: the light is off.
8	Failure Indicator	<ul style="list-style-type: none"> • Normal condition: the light is always off. • When the equipment is faulted: the light is flashing red.
9	USB Interface 1	USB 2.0. Users could connect with a mouse or keyboard.
10	USB Interface 2	USB 3.0. Users could connect with a mouse or keyboard.



- **IPVT Back Panel**

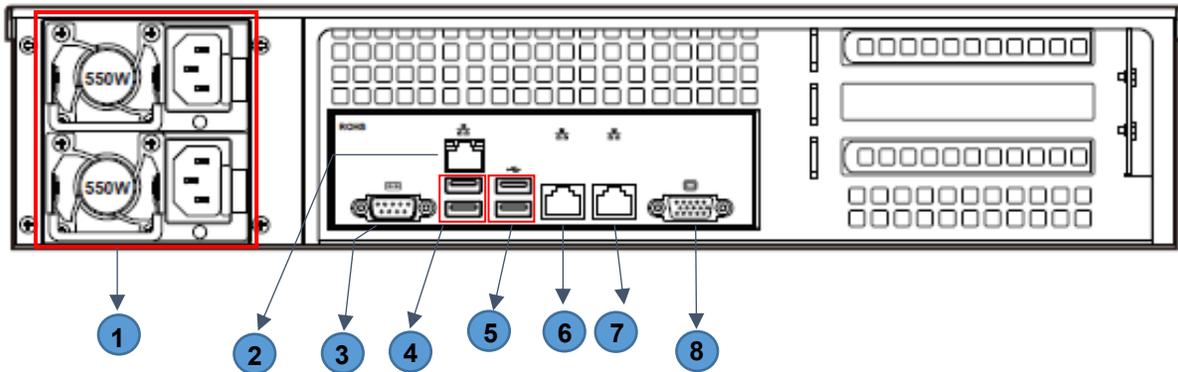


Figure 3: IPVT10 Back Panel

Table 5: IPVT10 Back Panel Description

NO.	Name	Description
1	Power Supply Interfaces	Two Power Supply Interfaces are available on the IPVT10, the users need to connect the power cables to the two interfaces to keep powering the device and to avoid shutting it down in case one of the power supply is defective.
2	IPMI Interface	Intelligent Platform Management Interface.
3	COM Interface	RS-232 serial communication interface
4	USB Interfaces 3 and 4	USB 2.0. Users could connect with a mouse or keyboard.
5	USB Interfaces 5 and 6	USB 3.0. Users could connect with a mouse or keyboard.
6	1000M Ethernet Interface 1	Connect to the network LAN port, connect with a PC to access the configuration page of the server
7	1000M Ethernet Interface 2	Connect to the network LAN port
8	VGA Interface	Connect to a VGA equipment

Equipment Specifications

Table 6: IPVT10 Equipment Specifications

Name	Description
Power Supply	550W. (Redundancy PSU)
Applicable Cabinet	2U Rackmount Design, and it supports 19" cabinets and rails.
Equipment Size	Base Equipment Size: Height 88mm * Width 430mm * Depth 650mm.
USB Interfaces	3x USB 3.0 (2 rear, 2 via header). 3x USB 2.0 (2 rear, 2 via header).
LAN Interfaces	2x RJ45 Gigabit Ethernet LAN ports. 1x RJ45 Dedicated IPMI LAN port.
Display Interfaces	1 x VGA port.
Operating Temperature	0°C to 45°C

Mounting IPVT10 Equipment to Cabinet

Users can install the IPVT10 in a 19-inch cabinet that conforms to the IEC (International Electro-Technical Commission) 60297 standards.

1. The IPVT10 server is heavy, and we suggest carrying it by two people at least.
2. If cabinet has been installed, then suggest a space of at least "2U" (1U=44.45mm) to be reserved.
3. Users can select the regular rail for installation, or optional installation.

Example:

Rail structure: It is composed of inner rail, outer rail, and rail holder. The inner rail and the outer rail are connected, and they cannot be split. They are mounted on the cabinet through the rail holder; the inner rail is installed on the server equipment (Rails and Rail Holders are not included within the package contents).

Steps:

1. Remove the rail holder and the rails by loosening the 4 screws first, and then removing the front and back rail holders.



2. Install the inner rail to the server case. Pull the inner rail out of the rail until it cannot be pulled.
3. Fix the inner rail with 2 screws to the server case. Fit the smooth surface of the inner rail to the side of the server case and match the screw holes on the inner rail with the screw holes on the server case. Hold the inner rail tightly against the server case and tighten with the screws.
4. Repeat steps 1 to 3 to install the other inner rail on the other side of the server case.
5. Install the rail holder to the cabinet. Make sure the installation position of the front rail holder on the cabinet, align the two fixing holes between the rail holder and the cabinet corner, tighten the screws. Then, according to the depth of the cabinet (the depth of the cabinet is 650mm), adjust the back-rail holder properly, and align the two fixing holes between the back-rail holder and the cabinet corner at the back of the cabinet, tighten the screws. (Note: Please make sure that the front and back rail holders are horizontal).
6. Repeat the above steps to install the other front and back rail holders to the cabinet. (Note: Please make sure that the left and right-side rails are horizontal).
7. Lift the server up and close to the cabinet so that the back of the server faces the front of the cabinet. Insert the inner rails on the two sides of the server into the front and back rail holders on the cabinet, align the fixing holes and tighten the screws.
8. When the installation is completed, push the server into the cabinet.



Connecting IPVT10 Server

Connecting Network Cables

To ensure to run IPVT10 Server properly, users need to connect the server to a Gigabit switch.

Please connect IPVT10 Server according to the following procedures:

1. Connect the RJ45 Ethernet cable with the Ethernet Interface 1.
2. Connect the RJ45 Ethernet cable with the Gigabit switch.
3. Repeat steps “1” and “2” to connect with Ethernet interface 2.



Note:

- Please do not use 100M or 10M switches.
- If only one network is used, only one network interface needs to be connected to the switch (Internal Network - Setup Ethernet Interface 1, External Network - Setup Ethernet Interface 2).

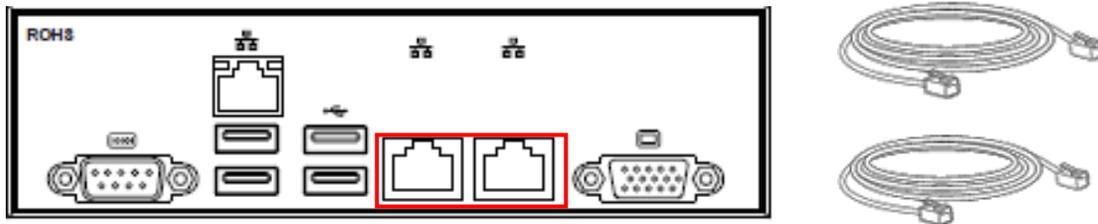


Figure 4: Connecting Ethernet Cables to Ethernet Interfaces

Connecting Power Supply cables

IPVT10 only supports AC power supply, users can connect the two power supply cables following the steps below:

1. Connect the standard power supply cable with the equipment.
2. Plug the power supply into the AC power supply.
3. Repeat steps “1” and “2” to connect the second power supply cable.



 **Notes:**

- Please use the standard three-phase power outlet.
- Please make sure that the output voltage is within the range of the power module (90~264VAC, 8.5~2.7A, 50/60Hz). If it is not within the working range, correct it and do not power on the equipment.

Powering on IPVT10

Before powering on the equipment, users need to ensure that the equipment meets the following conditions:

- If the equipment is installed in a cabinet, please ensure that the screws are fixed, and the equipment has enough space for heat dissipation.
- The connections of the cables on the equipment are normal.
- The input power and current are within the working range of the equipment.
- The distance between the power cable and the Ethernet cable outside the cabinet must be greater than 30 mm.

Once the previous conditions are checked, the users can power up the IPVT10 Server. In order to make the equipment run properly, users need to press the equipment switch in the front panel of the server to power on the equipment. The indicator will turn to solid green.

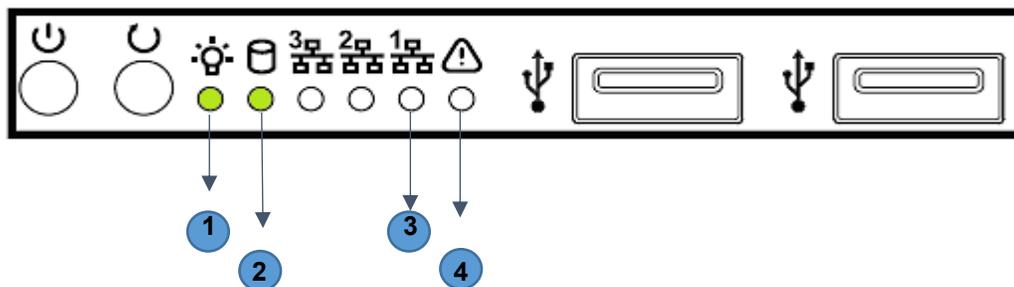


Figure 5: IPVT10 powered on

After the equipment is turned on, please check the following indicators to make sure the equipment is working properly.

Table 7: Checking the indicators after powering up IPVT10

NO.	Name	Description
1	Power Indicator	<ul style="list-style-type: none"> When the equipment is ON and connected to the power supply: the light is solid green When the equipment is OFF, and the power supply is not connected with the equipment: the light is off
2	Hard Disk Indicator	<ul style="list-style-type: none"> When the hard disk is running normally: the light is off. When the hard disk is reading and writing: the light is solid blue.
3	Network Connection Indicator	<ul style="list-style-type: none"> When the network connection is normal: the light is flashing yellow When the network connection is abnormal, or the network is not connected with the equipment: the light is off
4	Failure Indicator	<ul style="list-style-type: none"> Normal condition: the light is always off When the equipment is faulted: the light is flashing red.

Note: If you encounter any problem about the equipment, please contact with Grandstream support engineer.

CONFIGURING IPVT10

Descriptions of Meeting Capacity

Table 8: IPVT10 Server Meetings Performance

Current Meeting Number	Max Video Feeds	Max Participants	Descriptions
1	120	300 (Dual NICs) 200 (Single NIC)	<ul style="list-style-type: none"> If the participant only uses single NIC to join into the conference, it only supports 200 participants in the conference which is limited by the bandwidth. If the participants use dual NICs at the same time, the participants could use different IP addresses to join into the meeting, and the participant amount is up to 300. Supported H.264 The meeting allows users to enable all specified meeting layouts.
2	120	200	<ul style="list-style-type: none"> Supported H.264 Both 2 current meetings could enable all specified meeting layouts.
4	120	160	<ul style="list-style-type: none"> With more conferences at the same time for the server loading, the maximum number of participants in the conference will be less. Supported H.264 The 4 meetings could enable up to 6 specified meetings layouts.
6	120	140	<ul style="list-style-type: none"> With more conferences at the same time for the server loading, the maximum number of participants in the conference will be less. Supported H.264 The 6 meetings could enable up to 4 specified meetings layouts.



8	120	130	<ul style="list-style-type: none"> • With more conferences at the same time for the server loading, the maximum number of participants in the conference will be less. • Supported H.264 • The 8 meetings could enable up to 2 specified meetings layouts.
10	120	120	<ul style="list-style-type: none"> • With more conferences at the same time for the server loading, the maximum number of participants in the conference will be less. • Supported H.264 • The 10 meetings cannot enable any specified meeting layout.
50	100	100	<ul style="list-style-type: none"> • The current meeting amount only allows users to start meetings of two parties, which means each meeting only has 2 participants, and allow the two participants to enable their cameras. • Supported H.264

Note:

- Under poor network condition, packets loss will cause the performance degradation.
- A minimum bandwidth of 5Mbps Download/Upload is required per participant for a 1080p resolution.



Configuration Instructions

Users could manage and configure the IPVT10 configuration information by logging in the Web UI of IPVT10 server via a browser of the computer.

First-time Configuration

Users need to properly follow the steps listed in the table below at the first login.

Table 9: Steps for First-time Configuration

Steps	Description
Configure Service IP Address	According to the configuration of the network solution, configure the service IP address. Support to configure dual network adapters, NAT, and routing rules.
Configure SMTP Mailbox	The SMTP mailbox is used as a sender to send the meetings invitation Emails, meetings notification Emails etc. Users could configure Enterprise email as SMTP Mailbox.
Configure Conference Management Platform Information	This is used to configure the login account, enterprise information, default language, default time-zone, and other information on the platform.

Note: Each one of the steps is described in the next sections. Please, refer to the following sections for more details about IPVT10 initial configuration.



Configuration Parameters Modification

After the deployment is completed, users can modify the configuration parameters.

Table 10: Modify Configuration Options

Parameters	Description
Update Service IP Address	Please configure this parameter carefully: <ul style="list-style-type: none"> If the IP address of the IPVT10 is updated during a meeting, the meeting will encounter abnormal issues. The URLs of the scheduled meetings will be inaccessible. When the IP address of the IPVT10 is updated, the service will be restarted automatically.
Update SMTP Mailbox	When the SMTP Mailbox is updated, it will take effect immediately, and does not affect other data.
Update Conference Management Platform Information	When the Conference Management Platform information is updated, it will take effect immediately, and does not affect other data.

Upgrading Service

If users need to upgrade the software system in the IPVT10, users can log into the Conference Management Platform and upgrade the service.

- Please download the system installation package from Grandstream Official Website.
- During the upgrading process, the system service will be suspended.
- The upgrading service will not affect the data in the database server and the original configuration.

Factory Reset

Users need to be careful about factory reset operation. When users start to factory reset the device, it will be restored to the factory default settings, and all the data will be erased, including user's data and meetings data.



Login the Configuration Page

IPVT10 has a built-in Web Configuration Management Platform, and users could log in the platform via a browser by entering the Web Management Platform IP Address or via IPVideoTalk Portal in order to manage the configuration of the IPVT10.

Accessing the Configuration Page directly via a Browser

Users need to have a computer that is at the same VLAN network as the server, in order to be able to log into the server's web management platform.

Table 11: Default Login Username and Password

Parameters	Description
Web Management Platform IP Address	192.168.88.88
Admin User Name	admin
Admin Default Password	<ul style="list-style-type: none"> If there is no sticker on the device with the random default password, the default password of the device is "change_me". If there is a sticker on the device with the random default password, please use the password on the sticker as the default login password.

Users need to follow the steps below to log in into IPVT10 Web UI:

1. Please make sure that the IP address of the computer is at the same network segment as the servers. If not, go to "Network" configuration page of the computer to setup the network segment to be the same as IPVT10 servers.
2. Enter the default IP address (<http://192.168.88.88>) of the equipment in the browser of the PC, and press "Enter" to access the configuration page, as the screenshot shows below:



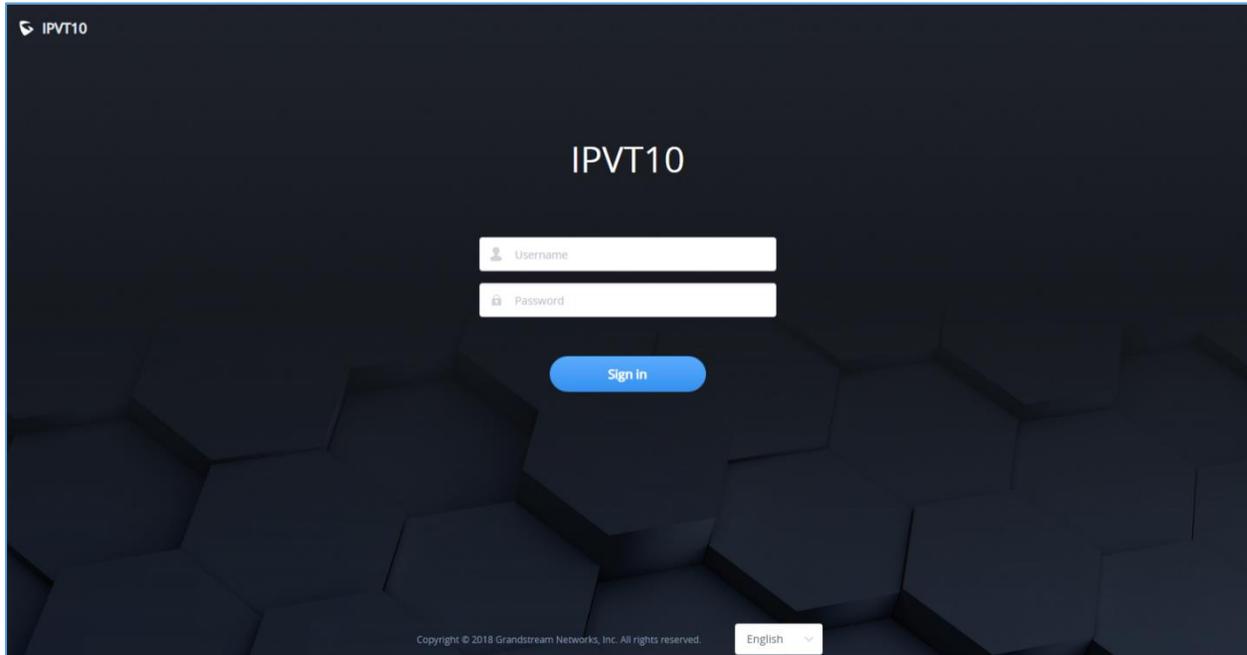


Figure 6: IPVT10 Web GUI - Login

3. Input login user name and password (If there is no sticker on the device with the random default password, the default password of the device is "change_me"; If there is a sticker on the device with the random default password, use the password on the sticker as the default login password)
4. For security reasons, Users will be asked to change the default password and choose another one before logging in.

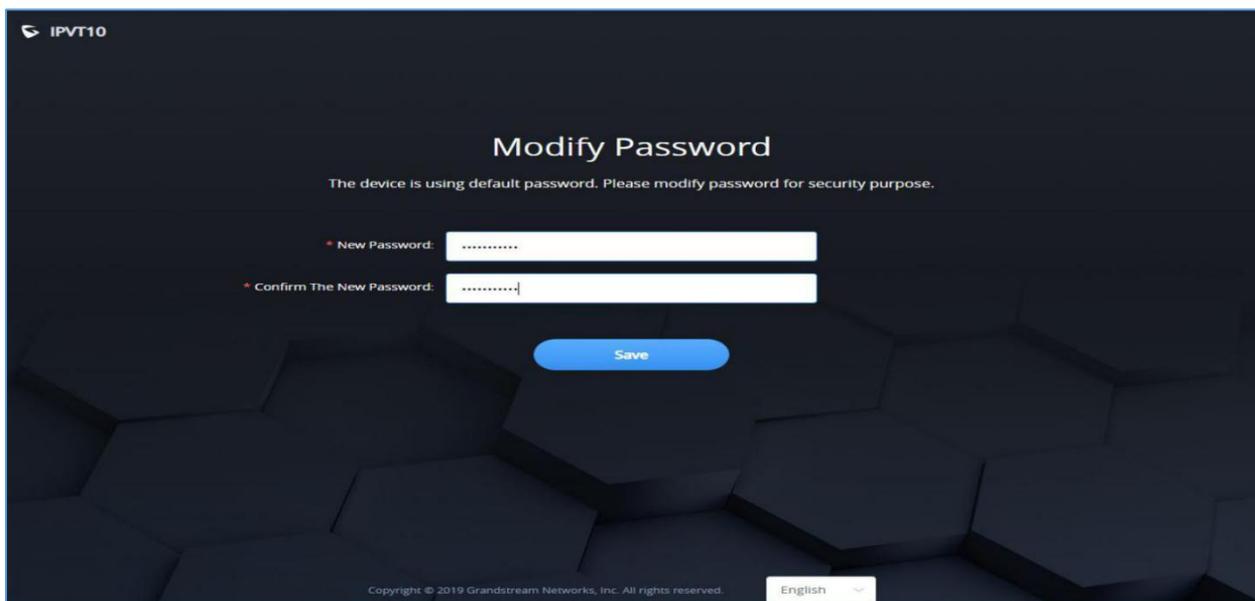


Figure 7: IPVT10 Web GUI – Modify Password



5. (Optional) Users could select the language on the list at the bottom of the configuration page.
6. Click to login the configuration page.

If there is an IP conflict, users can connect the PC directly to the server via an Ethernet cable for configuration purpose. Follow the steps below:

1. Unplug the Ethernet cable from the Ethernet Port 1 on the IPVT equipment (the first cable interface from left to right in the figure).
2. Then, connect the Ethernet Port 1 and a PC with an Ethernet cable as shown in the figure:

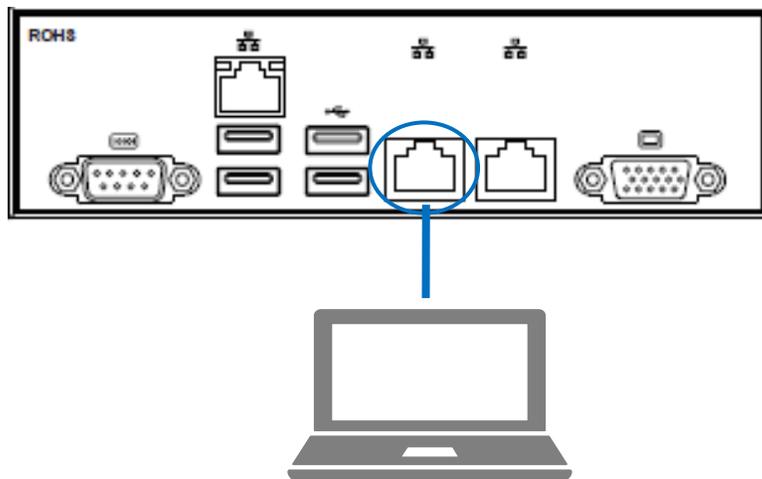


Figure 8: Connect IPVT 10 with a PC Directly

3. Enter the default IP address (<http://192.168.88.88>) of the IPVT10 equipment in the browser of the computer, and press “Enter” to access the configuration page.
4. Input login username and password
5. (Optional) Users could select the language on the list at the bottom of the configuration page.
6. Click to login the configuration page.



Note: After the configurations are complete, users must unplug the Ethernet cable from Ether Port 1 and reconnect the server to the Gigabit Ethernet switch to ensure that the two Ethernet ports of the equipment are connected to the Gigabit Ethernet.

Accessing the Configuration Page via IPVideoTalk Portal

Users could log into IPVT10 Web Interface via IPVideoTalk Portal by clicking on “Maintenance”, as per following figure:



Figure 9: Accessing the IPVT10 Configuration Page via IPVideoTalk Portal

Update Login Password

When users first-time log in to IPVT10 Web Deployment Platform, it is recommended to modify the password of the administrator account to ensure the security of the system. Refer to the following steps:

1. Login to the Web page of IPVT10.
2. Click on the option “Advanced Settings → Modify Password” to access the configuration.

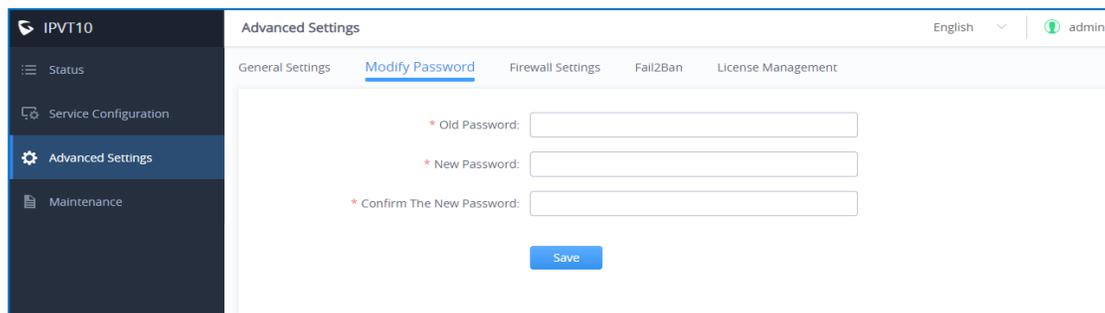


Figure 10: Modify Password

3. Input “Original Password”, “New Password”, and “Confirm New Password”.
4. Click to save the configuration, and the system will prompt to save successfully. If the original password is incorrect, or the new password format is incorrect, the corresponding error will be prompted.

Note: The password must contain two of the numbers, lowercase letters, uppercase letters, and special characters, and the length is limited to 8-16 characters.



Forgot Password

If users forgot the login password of IPVT10, users could reset the login password to the default password.

1. Connect your PC to the Ethernet port 1 of IPVT10 server directly or change the IP address of your PC to the same network segment as IPVT10 server (192.168.88.xx), users could access the IPVT10 Web UI directly.
2. Using the browser in your PC to access address "**192.168.88.88/iforget**" to open the login password reset page, as the screenshot shows below:

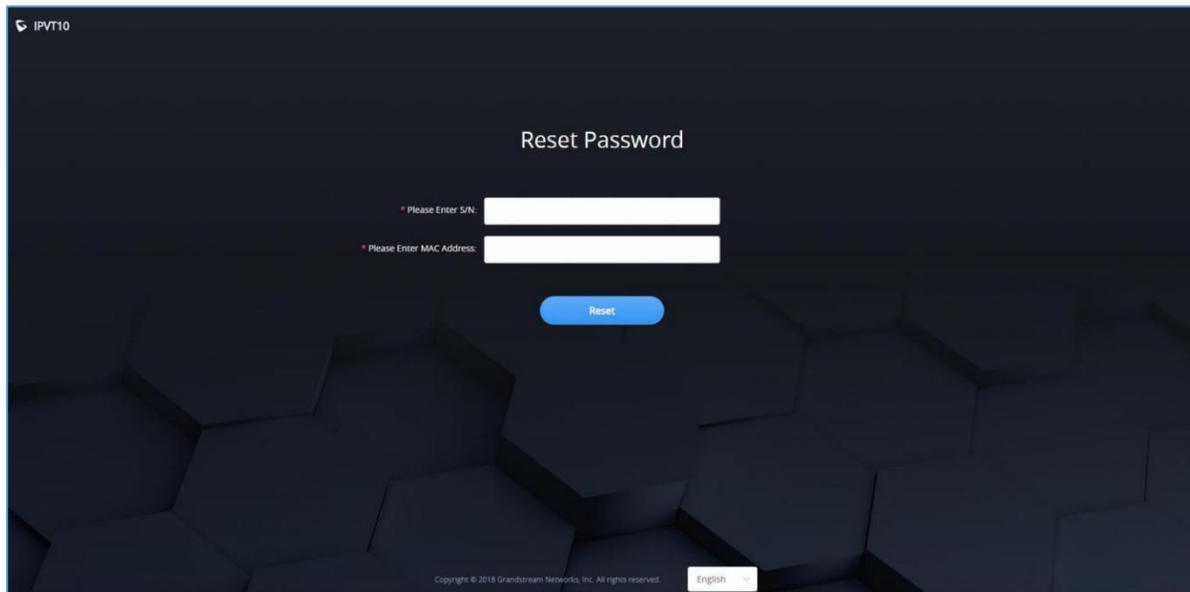


Figure 11: Reset Password

3. Users need to input the MAC address of IPVT10 server and serial number on the login password reset page.
4. Click on "Reset", and the login password will be reset to the default login password:
 - If there is no sticker on the device with the random default password, the default password of the device is "change_me".
 - If there is a sticker on the device with the random default password, please use the password on the sticker as the default login password.



Setup Wizard

When users try to login the IPVT10 Web UI for first time, users could follow the Setup Wizard to setup the IPVT10 server.

1. Users need to select if they want to use the IPVT10 as the host server or slave server:

- **Host Server:** IPVT10 is used alone or used as a host server in a cluster. There is only one host server in a cluster, users cannot set multiple hosts in a cluster.
- **Slave Server:** IPVT10 is used as the slave server in a cluster with another host server and other slave servers. IPVT10 is used to extend the MCU conferencing function for the host server. The slave server does not need to configure N°5 – N°7 in the following configuration steps.

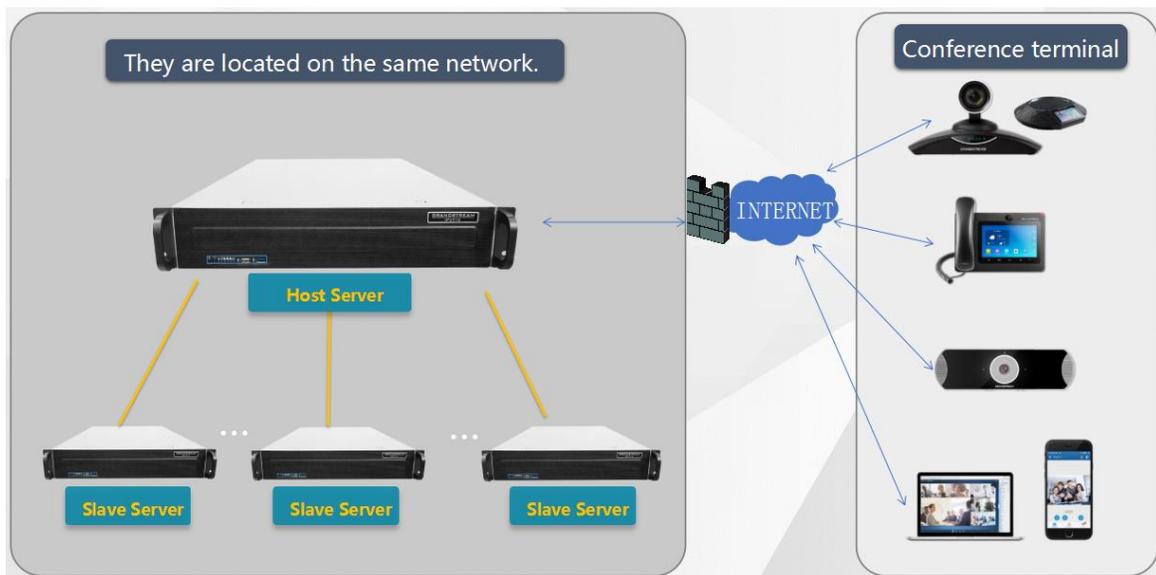


Figure 12: Setup example

2. **Network Settings:** Users could configure server IP address or domain name under this menu. *For more details, please refer to section [Network Settings].*

3. (Optional) **Configure Service NAT Interfaces:** Users could configure the custom server port under this menu. *For more details, please, refer to section [Configure Service NAT Interfaces]*

4. **Time Configuration:** The default setting is the server time is synchronized with the NTP server time. If the device is not connected to an external network, users need to set the time manually. *For more details, please, refer to section [Time Configuration].*

5. (Optional) **Configure SIP Trunk Service Address:** If users need to connect IPVT10 to an external SIP Trunk server, users need to setup the SIP Trunk Service under this menu. *For more details, please, refer to section [Configure SIP Trunk Service Address].*

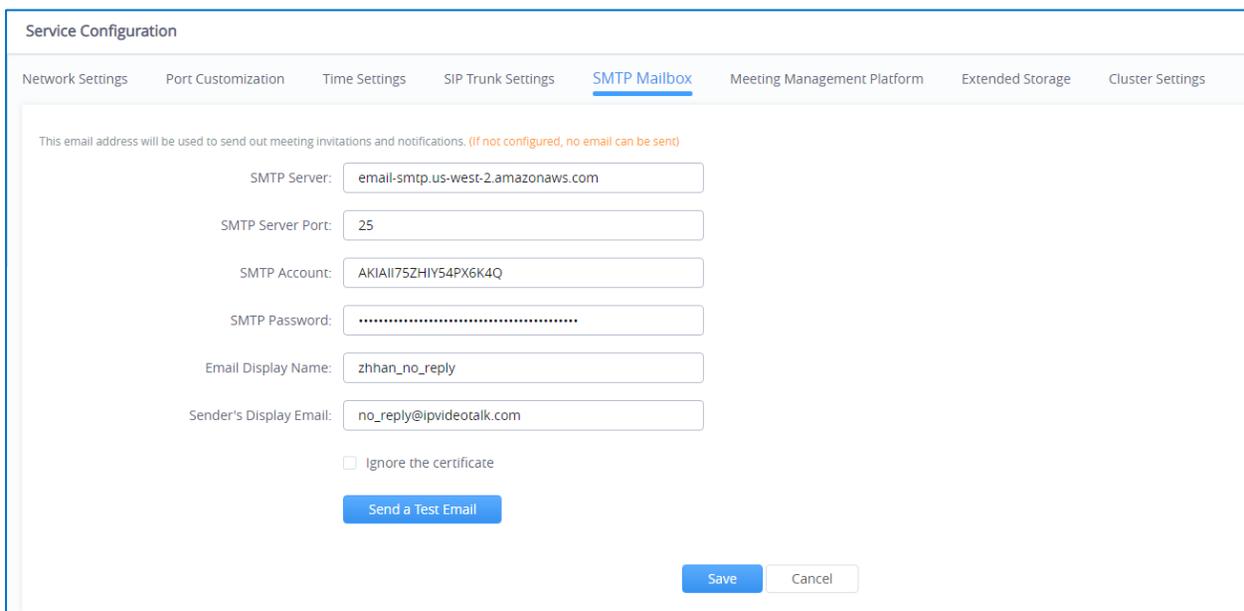
6. (Optional) **Configure SMTP Mailbox:** It is recommended to fill in the SMTP Mailbox address. This is used to send invitation Emails to other meeting participants. *For more details, please, refer to section [Configure SMTP Mailbox].*

7. **Configure Conference Management Platform Information:** This page is used to set the login account information of the conference management platform. This platform is used to manage the devices and conferences. The Conference Management Platform is an independent platform compares with Setup Wizard. *Please refer to section [Configure SMTP Mailbox]*

This Email box is used to send the meeting invitation Emails, meeting reminder, and other notifications as the Email sender. If users do not configure this Email box, the system cannot send the Emails to inform the meeting participants.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Service Configuration” and configure “SMTP Mailbox” options, as shown below:



The screenshot shows the 'Service Configuration' page with the 'SMTP Mailbox' tab selected. The page contains the following fields and controls:

- SMTP Server:** email-smtp.us-west-2.amazonaws.com
- SMTP Server Port:** 25
- SMTP Account:** AKIAII75ZHIY54PX6K4Q
- SMTP Password:** (masked with dots)
- Email Display Name:** zhhan_no_reply
- Sender's Display Email:** no_reply@ipvideotalk.com
- Ignore the certificate
- Send a Test Email** (button)
- Save** (button) and **Cancel** (button)

Figure 24: Configure SMTP Mailbox

- Input the mailbox and configure the options below:

Table 15: Configure SMTP Mailbox

Parameters	Example
SMTP Server	smtp.gmail.com
SMTP Port	465
SMTP Username	test@gmail.com
SMTP Password	***
Mailbox Display Name	User's enterprise name

- If the SMTP server is a self-signed certificate, you need to check "**Ignore certificate**". Otherwise, the SMTP mailbox cannot send mail.
- Before saving the SMTP mailbox configuration, users could click on "Send a Test Email" button, and input the test email address in the pop out window to receive the test email, then click on "Send" button to send out the test email. Then, users could go to the test email box to check the test email. If the user could receive the test email, the SMTP mailbox has been configured correctly. Otherwise, the user needs to check the SMTP mailbox configuration on the Web UI.

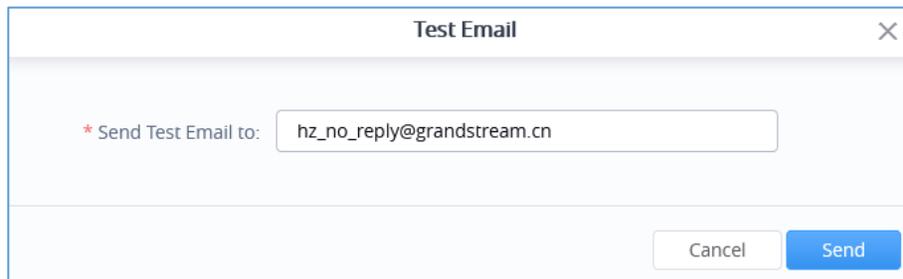


Figure 25: Test Email

- Users could click to save the configuration and click on "Apply Now" to apply the entire configurations of this page to the server. When the deployment is complete, it will take effect immediately.



Note:

If the mailbox configuration is incorrect, or not configured, the Conference Management Platform will not be able to send the meeting invitation Emails, meeting reminder, notification Emails, and etc.

Configuring Conference Management Platform Information].

8. Cluster Settings: If users only use one IPVT10 server alone, users could ignore this setup step. If users use the IPVT10 in a cluster, this setup step is a necessary step. *Please, refer to section [Cluster Settings]*

Server Status

Users could login IPVT10 and check the server/conference status for the cluster host server like the screenshot shown below:

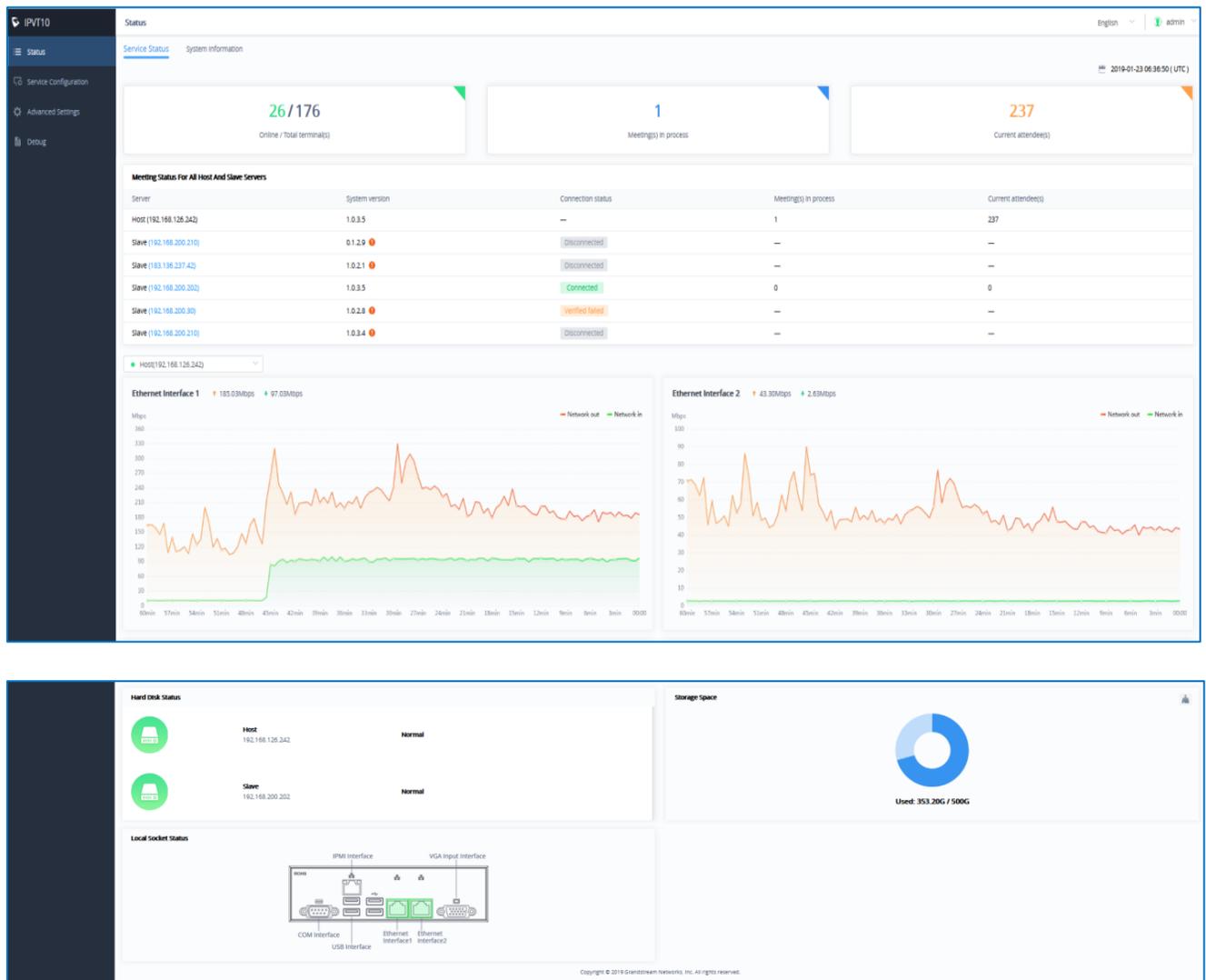


Figure 13: Server/Conference Status – Host Server

- **Online / Total terminal(s):** This information shows the number of the devices online currently, and the total number of devices.
- **Meeting(s) in process:** This information shows the total number of meetings in progress currently. If the IPVT10 is a cluster host server, it will show the total number of ongoing meetings for all servers in the cluster.
- **Current attendee(s):** The information shows the total number of current participants attending the meeting. If the IPVT10 is a cluster host server, it shows the total number of current participants for all servers.
- **Meeting status for all host and slave servers:** The information shows the connection status of each slave server in the cluster, the number of conferences in progress, and the number of total meeting participants.
- **Hard disk status:** If an error occurs in the hard disk of IPVT10 server, there will be a prompt indicating users the error. It also displays the hard disk status of each slave server in the cluster.
- **Storage Space:** It shows the current used storage space and remaining storage space. Users could click on the button  at the upper right corner to erase all files quickly in the storage space, including the recording files in the storage. If the server mounts NFS storage disk, it will show the storage space of the NFS disk. Users could click on Clear button to clean up all data in the NFS disk.
- **Network Status:** This information shows the network speed of the two Ethernet ports on IPVT10 server.
- **Interface Status:** This information shows the current server's socket usage status. If the socket usage status is detected as "In use", it will display solid green.

Users could check the server/conference status for the cluster slave server as the screenshot shows below:



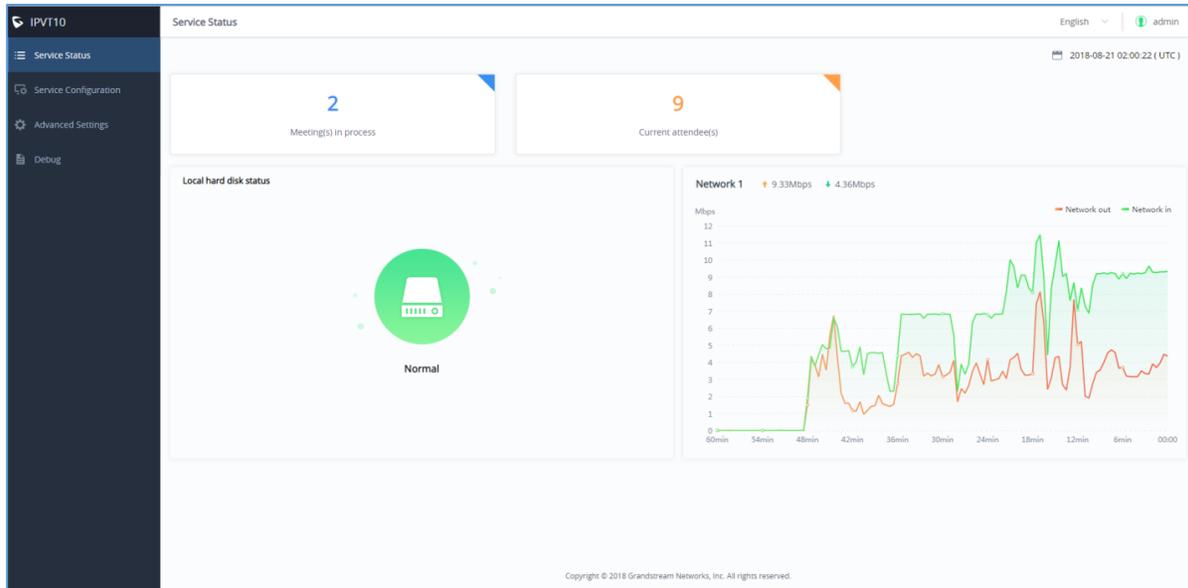


Figure 14: Server/Conference Status – Slave Server

- **Meeting(s) in process:** This information shows the total number of meetings in progress currently. If the IPVT10 is a cluster host server, it will show the total number of ongoing meetings for all servers in the cluster.
- **Current attendee(s):** The information shows the total number of current participants attending the meeting. If the IPVT10 is a cluster host server, it shows the total number of current participants for all servers.
- **Hard disk status:** If an error occurs in the hard disk of IPVT10 server, there will be a prompt indicating users the error. It also displays the hard disk status of each slave server in the cluster.
- **Network Status:** This information shows the network speed of the Ethernet ports on IPVT10 server. For slave server, users only need to connect the Ethernet port 2 with the Internet.
- **Interface Status:** This information shows the current server's socket usage status. If the socket usage status is detected as "In use", it will display solid green.

Below the explanations of each Hard Disk status icons:



This icon represents the normal status of the Hard disk.



This icon means that the Hard disk status is abnormal, and the specific disk symbol will be displayed.



This icon means that the drive letter is rebuilt, and the specific disk symbol is displayed. After the reconstruction is successful, it will return to normal.

System Information

Users could view the system information of the server, such as MAC address, System version number, IP address, etc., as shown in figure below:

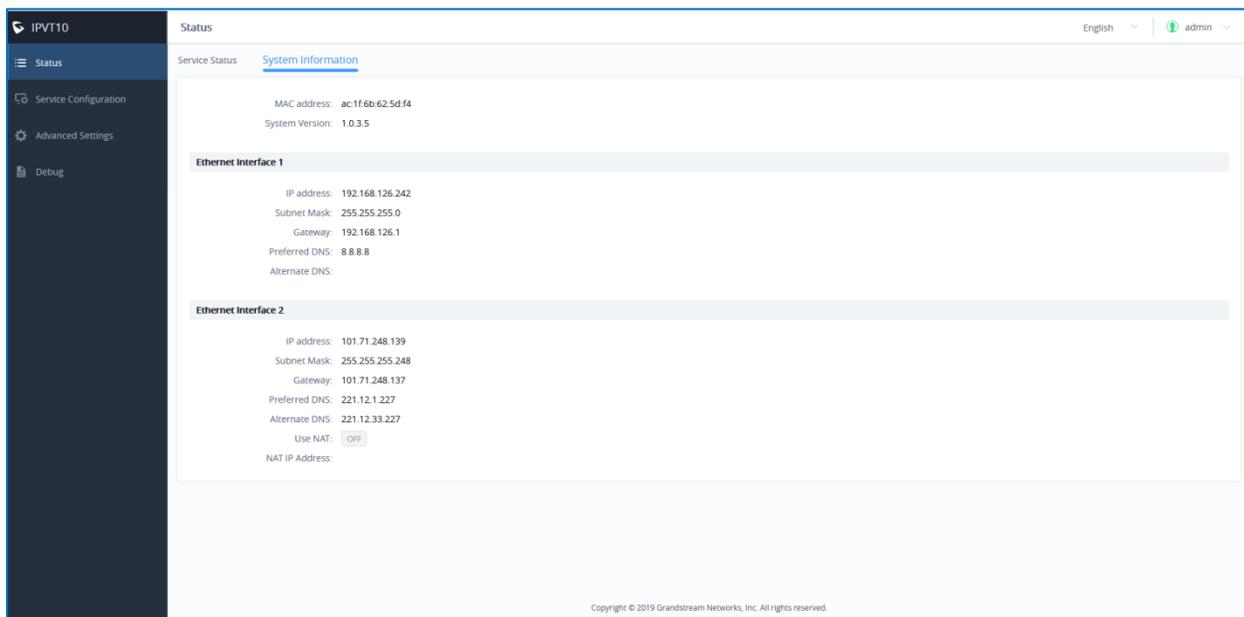


Figure 15: System Information

Cluster Host Server Configuration

Network Settings

The IPVT10 server supports two network adapters that can be configured based on the actual requirements.

There are 5 typical network deployment Scenarios:



- **Scenario 1:** The server is deployed on the internal network. The end users use the service only within the internal network. Users could only configure the internal network IP address.
- **Scenario 2:** The server is deployed on the external network. The end users use the service via the public network. Users need to configure the external IP address.
- **Scenario 3:** The server is deployed on the internal network. The end users use the service via the public network. In this case, users need to configure the internal IP address and NAT in the server.
- **Scenario 4:** The server is deployed on the internal network. The end users can use the service via both internal and external network. In this case, users need to configure the server with both internal network and external network, and routing rules.
- **Scenario 5:** The server is deployed on the internal network. The end users can use the service via the internal network and limit certain external IP address to access the service. In this case, users need to configure internal network, external network, NAT, and routing rules in the server.

Options Descriptions

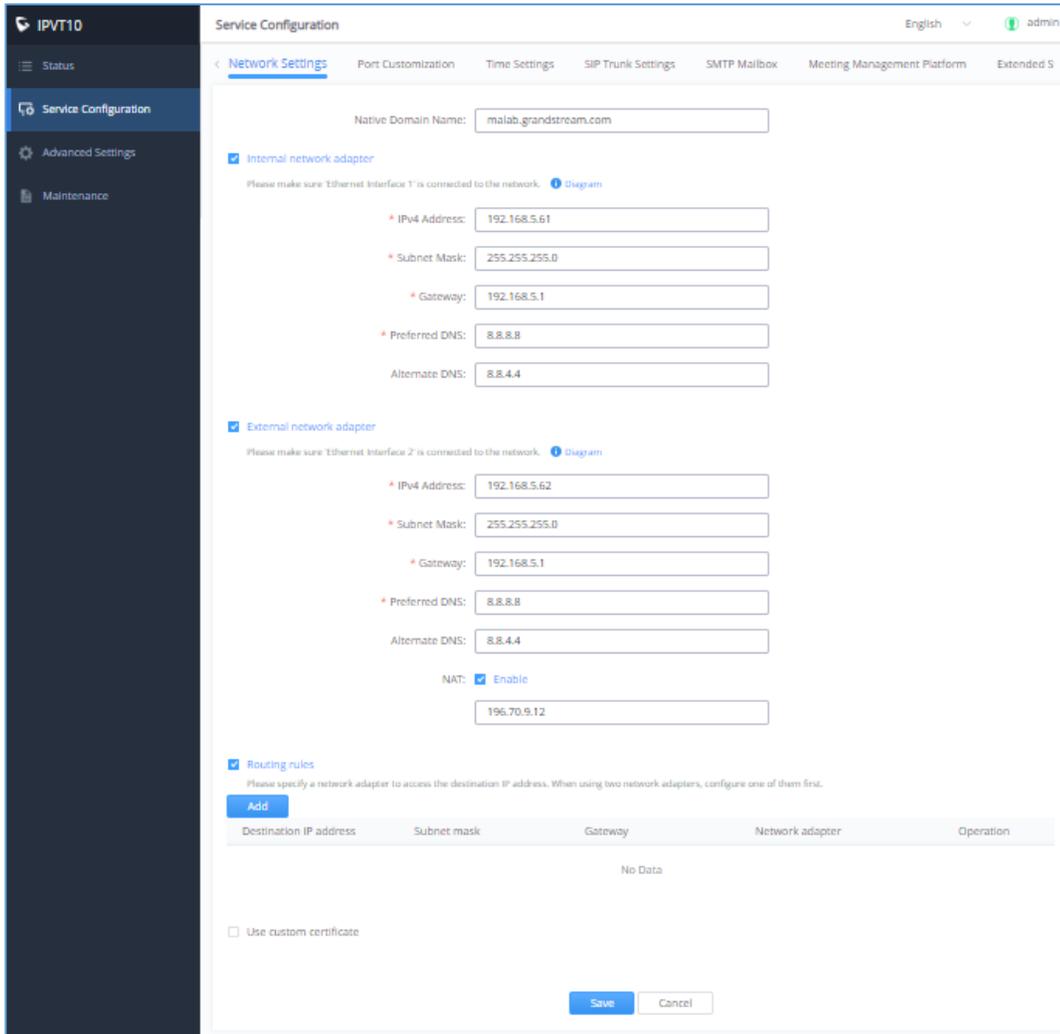
Table 12: Parameters Descriptions

Parameters	Description
Native Domain Name	Configures the domain name of IPVT10 server.
Internal Network Adapter	Configures Internal Network Adapter's parameters.
External Network Adapter	Configures External Network Adapter's parameters.
IPv4 Address	Configures the IP Address for IPVideoTalk Portal.
Subnet Mask	Configures the Subnet Mask.
Gateway	Configures the default Gateway.
Preferred DNS	Set the Preferred DNS.
Alternative DNS	Set the Alternative DNS.
NAT	Enable/Disable NAT. It allows users to set the IP address of NAT, or the dynamic domain name of NAT.
Routing Rules	Set the advanced configuration Routing Rules to ensure accessing the destination IP address when using two Network Adapters.
Use Custom Certificate	Configures the key of the custom certificate.



Please refer to the following steps:

1. Login IPVT10 Web UI.
2. Go to “Service Configuration” → “Network Settings”, as the figure shown below:



The screenshot displays the 'Service Configuration' page for 'IPVT10'. The 'Network Settings' tab is active. The 'Native Domain Name' is set to 'malab.grandstream.com'. Under 'Internal network adapter', the IP address is 192.168.5.61, subnet mask is 255.255.255.0, gateway is 192.168.5.1, preferred DNS is 8.8.8.8, and alternate DNS is 8.8.4.4. Under 'External network adapter', the IP address is 192.168.5.62, subnet mask is 255.255.255.0, gateway is 192.168.5.1, preferred DNS is 8.8.8.8, and alternate DNS is 8.8.4.4. The NAT setting is 'Enable' with an IP address of 196.70.9.12. A routing rules table is shown with columns for Destination IP address, Subnet mask, Gateway, Network adapter, and Operation, and it currently contains no data. There is also a checkbox for 'Use custom certificate' which is unchecked. 'Save' and 'Cancel' buttons are at the bottom.

Figure 16: Service IP Address Config – Internal Network Adapter

3. (Optional) Users could configure the domain name of the IPVT10 server, and users have to own the permission of this domain name. Users also need to point this domain name to the IP address of the IPVT10 configured address.

Note: If users configure the internal IP address and external IP address for the IPVT10 server, users need to point the internal network of the domain name to the internal IP address of the IPVT10 server, and point the external network of the domain name to the external IP address of the IPVT10 server.



4. According to the actual requirements, users could configure the 1 or 2 network adapters. Users could configure Internal Network Adapter only, External Network Adapter only, or both.
5. Users need to configure “IPv4 Address”, “Subnet Mask”, “Gateway”, “Preferred DNS”, “Alternative DNS” (optional) for the network adapter.

Note: Please make sure that there should be no conflict in the IP address. Otherwise, the service will be unavailable.

6. (Optional) If the selected adapter is external network adapter, users could configure static NAT or dynamic NAT for the IPVT10. If the user configures a dynamic domain name, the user needs to configure the interval (count by minutes) to resolve the IP address of the domain name. The default setting is 1 minute.

NOTES:

- NAT could translate the private IP address of the internal network into a public IP address, so that an external conference client can access the server of the internal network through the public network.
- If dynamic NAT used, once the IP address of the domain name changed, the system will be restarted the service automatically, which will cause the current ongoing meeting to be temperately disrupted. (dynamic NAT is not recommended unless no choice available)



External network adapter

Please make sure 'Ethernet Interface 2' is connected to the network. [Diagram](#)

* IPv4 Address:

* Subnet Mask:

* Gateway:

* Preferred DNS:

Alternate DNS:

NAT: Enable

Dynamic DNS:

Parsing polling (in minutes)

Figure 17: Service IP Address Config – External Network Adapter

7. When two network adapters are configured, users must configure the routing rules based on the actual requirements by clicking icon . Multiple routing rules can be configured in the IPVT10 server. Users can also edit and delete a certain routing rule.

Note: Routing rules must be specified for the external network and all network segments in the enterprise network environment.

Routing rules

Please specify a network adapter to access the destination IP address. When using two network adapters, configure one of them first.

Destination IP address	Subnet mask	Gateway	Network adapter	Operation
0.0.0.0	0.0.0.0	192.168.126.1	Internal network adapter	 

Figure 18: Configure Network Routing Rules

Table 13: Configure Network Routing Rules

Parameters	Description
Destination IP Address	This is used to configure the destination IP address for the network. This option must be configured with the Subnet Mask option.
Subnet Mask	This is used to configure the subnet mask.
Gateway	This is used to configure the gateway of the destination network.
Network Adapter	This is used to select the server network adapter for destination network.

8. (Optional) If users set the domain name as the in the IPVT10, users could also set “Use Custom Certificate” like the screenshot shown below:

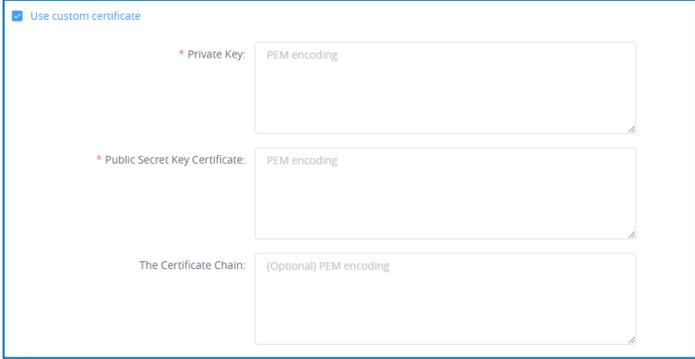


Figure 19: Use Custom Certificate

Note: This certificate is the server signaling certificate and Web access certificate for the server.

9. Continue to fill in the other configuration options. For the first deployment, users must fill in all required fields.
10. User could click to save the configuration and click on “Apply Now” to apply the entire configurations of this page to the server. When the deployment is complete, it will take effect immediately.

 **Notes:**

- When the deployment is complete, users need to check whether all network interfaces of the server are all connected. For a single network, only one network interface needs to be connected to the network (Internal Network – Network Interface 1, External Network – Network Interface 2).
- If users modify the IP address of the server during the conferences, it may cause the abnormal issues for the ongoing conferences, and the scheduled conferences will be inaccessible.
- When users modify the parameters of the server, the server will restart the service automatically.

Configure Service NAT Interfaces

In order to use IPVT10 service at the enterprise’s private network, users could customize the service port.



The default service ports are shown as following below:

Table 14: Service Port Configuration

Server Components	Protocol	Default Port	Descriptions
Web Server	HTTP	80	Conference Web UI, Requests Management, API Server
Web Server	HTTPS/WSS	443	Conference Web UI, Requests Management, API Server, Connect to Web socket
SIP Server	TCP/UDP	5060	SIP signaling access for different devices, Trunk/PSTN Connection
SIP Server	TLS	5061	SIP signaling access for different devices, Trunk/PSTN Connection
SIP Server	UDP	1719	H323 RAS Registered Access
SIP Server	TCP	1720	H323 Q93 Call Access
Media Server	TCP/UDP	5062	External control port
Media Server	UDP	60000-65000	Port range of media streams: Requirements: Port starting should not be lower than 1024, the range is not less than 3000.

Please refer to the following steps:

1. Login IPVT10 Web Management UI.
2. Click on the “Service Configuration” on the left side of the UI and select “Service Port Configuration”, as shown below:

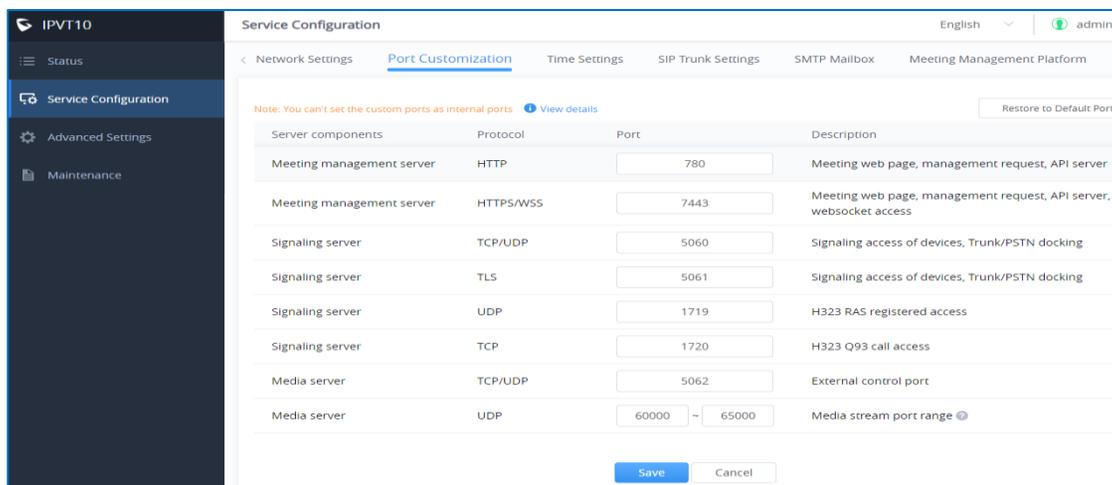


Figure 20: Service Port Configuration

3. Click to open the menu “Service Port Configuration” to customize the service ports based on the requirements.
4. When finished updating the ports, click on “Save” button to save the configuration, and click on the button “Apply Now” to confirm the customized service ports. The server will reboot to apply the changes.

 **Notes:**

- The customized service ports cannot be duplicated.
 - The ports below cannot be set as customized service ports: “21, 25, 1718, 3000, 3306, 5070, 5071, 5072, 5073, 5074, 5080, 6379, 6380, 6381, 8006, 8008, 8010, 8012, 8080, 8081, 8083, 8090, 9080, 80000, 111, 2049, 3002, 3003, 3004”.
 - If the service ports are set incorrectly, users cannot use the corresponding services normally.
-

Time Configuration

Users could check the current time and time-zone of the server and correct it at any time to avoid the meeting time inaccurate or cannot be launched issues.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Service Configuration”, and configure “Time Settings” options, as the figure shown below:

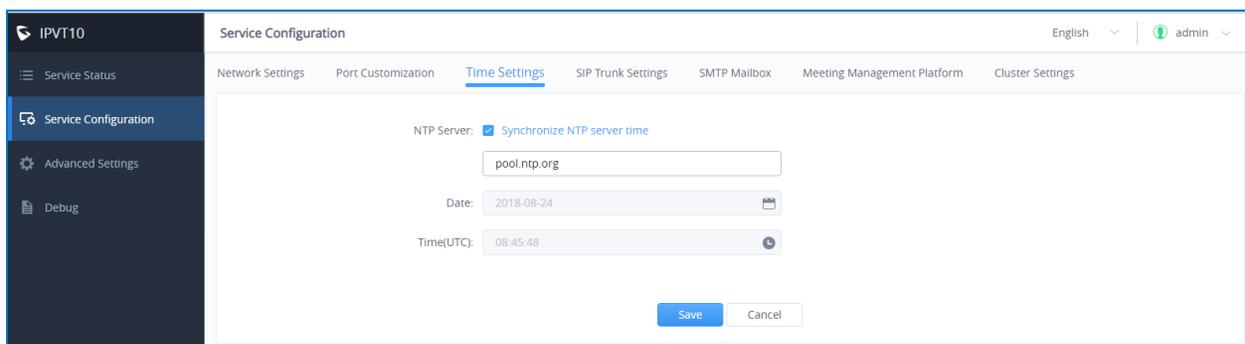


Figure 21: Time Settings



3. It shows the current time of the server by default.
4. Users could set whether to synchronize the SNTP server time. If there is no available SNTP server, users could adjust the date and time manually.
5. Users could click on “Save” to update the server time immediately.

Configure SIP Trunk Service Address

(Optional) Users could configure the SIP Trunk server address based on the actual requirements. If users configure this service, users could use PBX platform or PSTN Trunk server to connect via IPVideoTalk conference system, user also could set Dialplan to dial out the 3rd party PBX platform.

- **Connecting to the IPVideoTalk Conference System with 3rd Party Platform (PBX or PSTN)**

In order to connect the IPVideoTalk Conference System with a 3rd party platform, please refer to the following steps:

1. Login IPVT10 Web Management UI.
2. Go to “Service Configuration→SIP Trunk Settings”, users will see the page below:

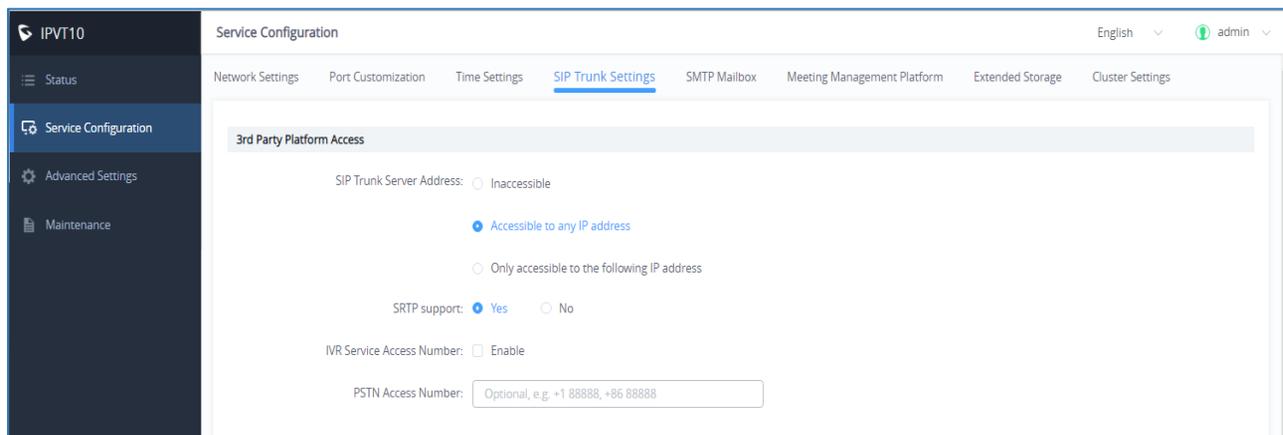


Figure 22: SIP Trunk Service Configuration - Access

3. Configure the SIP Trunk server address. If the option “Accessible to any IP address” is checked, all the IP addresses can connect to the IPVT10 server. If the option “Only accessible to the following IP address” is checked, users need to input the certain IP addresses which can access the IPVT10 server. Users could configure up to 10 IP addresses, and only the candidates can access the IPVT10 conference system.

4. Check and choose whether 3rd party supporting SRTP. If supported, then use SRTP otherwise use RTP instead.
5. (Optional) Configure the IVR voice access number. If the configured Trunk server connects to the conference via IVR voice access number, users need to configure the IVR voice access number before using the service. If the Trunk server supports to recognize the IPVideoTalk conference ID, and dials to the IPVT10 server via the conference ID, then users do not need to configure the IVR voice access number.
6. (Optional) Configure the PSTN access number, this is only used for displaying. If users want to show the PSTN access number in the conference invitation Emails, or the meeting details, users could configure this option. If there are multiple PSTN access numbers, please separate the numbers by comma (e.g., +861234567, +8687654321).



Typical Scenarios

Scenario 1

There are one or more SIP Trunk servers in the enterprise, and the administrator wants the users to dial to the meeting by IPVT10 meeting ID directly.

Prerequisites:

SIP Trunk server needs to be able to recognize the conference ID of IPVT10. When users dial this conference ID, users will be connected to IPVT10 server.

Configuration:

Users need to configure one or more SIP Trunk server addresses.

Scenario 2

There are one or more SIP Trunk servers in the enterprise, and the administrator wants the users to dial the unique access number and follows the IVR to input the conference ID to join into the meeting.

Prerequisites:

SIP Trunk server needs to be able to recognize the IVR access number. When users dial this IVR access number, users will be connected to the IPVT10 server.

Configuration:

- One or more SIP Trunk server addresses
- IVR voice access number

Scenario 3

There are one or more PSTN Trunk servers in the enterprise, and the administrator wants the PSTN users to access to the IPVT10 conference.

Prerequisites:

Users need to configure the unique accessible PSTN numbers for the PSTN Trunk servers. When users dial the PSTN numbers, users can connect to IPVT10 server.

Configuration:

- One or more SIP Trunk server addresses
- (Optional) IVR voice access number
- If users want to show the PSTN access number in the invitation Emails, users could configure the PSTN access number option.



Scenario 4

There is one SIP Trunk server and one PSTN Trunk server in the enterprise, and the administrator wants the PSTN users and SIP users both could join into the IPVT10 conference.

Prerequisites:

- If users connect to the SIP Trunk server via IVR, the IVR access number should be recognized (refer to scenario 2). Otherwise, please kindly refer to scenario 1.
- Users need to configure the unique accessible PSTN numbers for the PSTN Trunk servers. When users dial the PSTN numbers, users can connect to IPVT10 server.

Configuration:

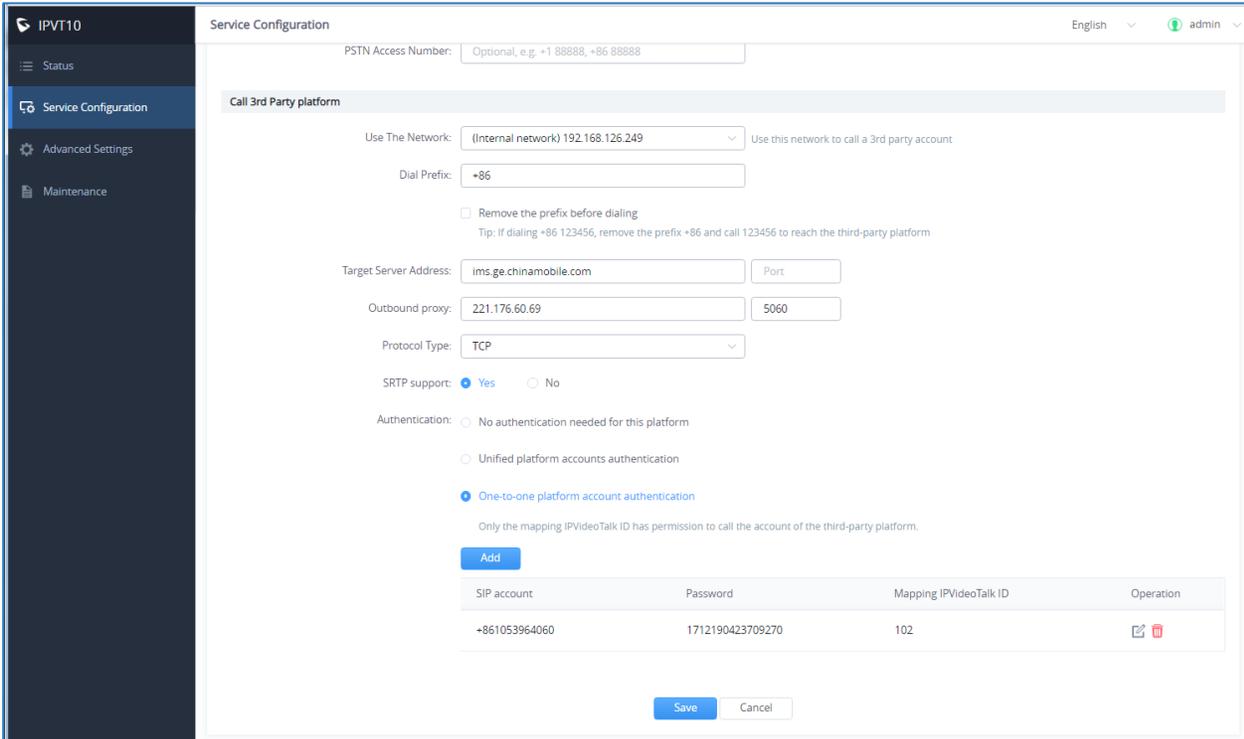
- One or more SIP Trunk server addresses
 - (Optional) IVR voice access number
 - If users want to show the PSTN access number in the invitation Emails, users could configure the PSTN access number option.
-
- **Dial out to the Accounts on the 3rd Party Platform**

If users need to join into the IPVT conference with the 3rd party platform accounts, users need to configure the 3rd party platform accounts rules and server address in the IPVT10. Please, refer to the following steps:

1. Login IPVT10 Web Management UI.
2. Click on the “Service Configuration” on the left side of the UI, check the figure below:
3. Users could select using which IP address of the IPVT10 server (internal network/external network) to call the third-party platform.
4. Input the dialing prefix, and it is used to recognize the accounts in the 3rd party platform. The special characters (e.g., + * #) are necessary. For example, the account in the 3rd party platform is +86 88888, and the +86 is the dialing prefix. The call will be made to the target server including the prefix.

Note: Users could check the option “Remove the prefix before dialing”, in order to remove the prefix when dialing to the third-party platform account.





The screenshot shows the 'Service Configuration' page for 'Call 3rd Party platform'. The page includes a sidebar with 'Status', 'Service Configuration', 'Advanced Settings', and 'Maintenance'. The main content area has the following fields and options:

- PSRN Access Number:** Optional, e.g. +1 88888, +86 88888
- Use The Network:** (Internal network) 192.168.126.249. Use this network to call a 3rd party account.
- Dial Prefix:** +86
- Remove the prefix before dialing. Tip: If dialing +86 123456, remove the prefix +86 and call 123456 to reach the third-party platform.
- Target Server Address:** ims.ge.chinamobile.com (Port: 5060)
- Outbound proxy:** 221.176.60.69 (Port: 5060)
- Protocol Type:** TCP
- SRTP support:** Yes No
- Authentication:**
 - No authentication needed for this platform
 - Unified platform accounts authentication
 - One-to-one platform account authentication

Only the mapping IPVideoTalk ID has permission to call the account of the third-party platform.

An **Add** button is located below the authentication options. Below it is a table with the following data:

SIP account	Password	Mapping IPVideoTalk ID	Operation
+861053964060	1712190423709270	102	 

At the bottom of the form are **Save** and **Cancel** buttons.

Figure 23: SIP Trunk Service Configuration - Call

5. Configure the server address and port for the target server, which is the server IP address or domain name of the 3rd party platform, and the port number of the target server.
6. Select the “Protocol Type” for the 3rd party platform (TCP/TLS/UDP).
7. Check and choose whether 3rd party supporting SRTP. If support, then use SRTP otherwise use RTP instead.
 - **Unified platform accounts authentication:** Users only need to configure 1 SIP account and password on the 3rd party platform, the IPVT10 will always use this SIP account and password authentication to access the 3rd party platform.
 - **One-to-one platform account authentication:** Users need to configure multiple SIP accounts, passwords and mapped IPVT ID on the 3rd party platform. Only the authenticated IPVT IDs can access to the 3rd party platform. Users could add multiple accounts or edit/delete the accounts.

Note: The mapped IPVT IDs have to be the existing accounts in the IPVT10 server.

8. When the configurations are done, users click to save the configuration and click on “Deploy to server” button to apply the changes. The server will reboot to apply the changes.

Note: Video display is supported for UCM meeting attendees.

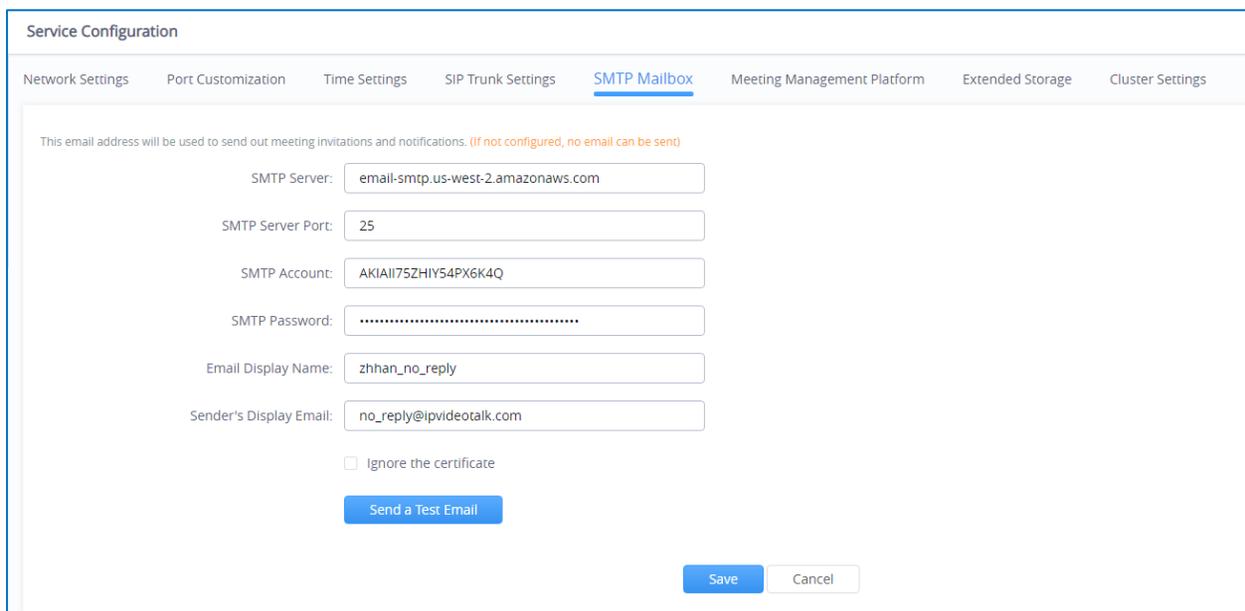


Configure SMTP Mailbox

This Email box is used to send the meeting invitation Emails, meeting reminder, and other notifications as the Email sender. If users do not configure this Email box, the system cannot send the Emails to inform the meeting participants.

Please, refer to the following steps:

7. Login IPVT10 Web UI.
8. Click on “Service Configuration” and configure “SMTP Mailbox” options, as shown below:



Service Configuration

Network Settings Port Customization Time Settings SIP Trunk Settings **SMTP Mailbox** Meeting Management Platform Extended Storage Cluster Settings

This email address will be used to send out meeting invitations and notifications. (If not configured, no email can be sent)

SMTP Server:

SMTP Server Port:

SMTP Account:

SMTP Password:

Email Display Name:

Sender's Display Email:

Ignore the certificate

Figure 24: Configure SMTP Mailbox

9. Input the mailbox and configure the options below:

Table 15: Configure SMTP Mailbox

Parameters	Example
SMTP Server	smtp.gmail.com
SMTP Port	465
SMTP Username	test@gmail.com
SMTP Password	***
Mailbox Display Name	User's enterprise name



10. If the SMTP server is a self-signed certificate, you need to check "**Ignore certificate**". Otherwise, the SMTP mailbox cannot send mail.
11. Before saving the SMTP mailbox configuration, users could click on "Send a Test Email" button, and input the test email address in the pop out window to receive the test email, then click on "Send" button to send out the test email. Then, users could go to the test email box to check the test email. If the user could receive the test email, the SMTP mailbox has been configured correctly. Otherwise, the user needs to check the SMTP mailbox configuration on the Web UI.

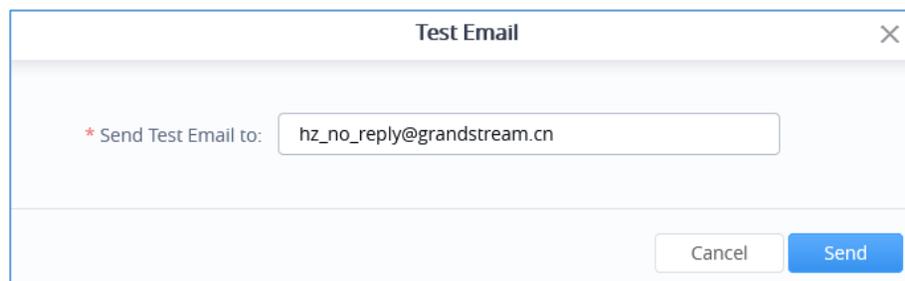


Figure 25: Test Email

12. Users could click to save the configuration and click on "Apply Now" to apply the entire configurations of this page to the server. When the deployment is complete, it will take effect immediately.



Note:

If the mailbox configuration is incorrect, or not configured, the Conference Management Platform will not be able to send the meeting invitation Emails, meeting reminder, notification Emails, and etc.

Configuring Conference Management Platform Information

The Conference Management Platform provides the following features:

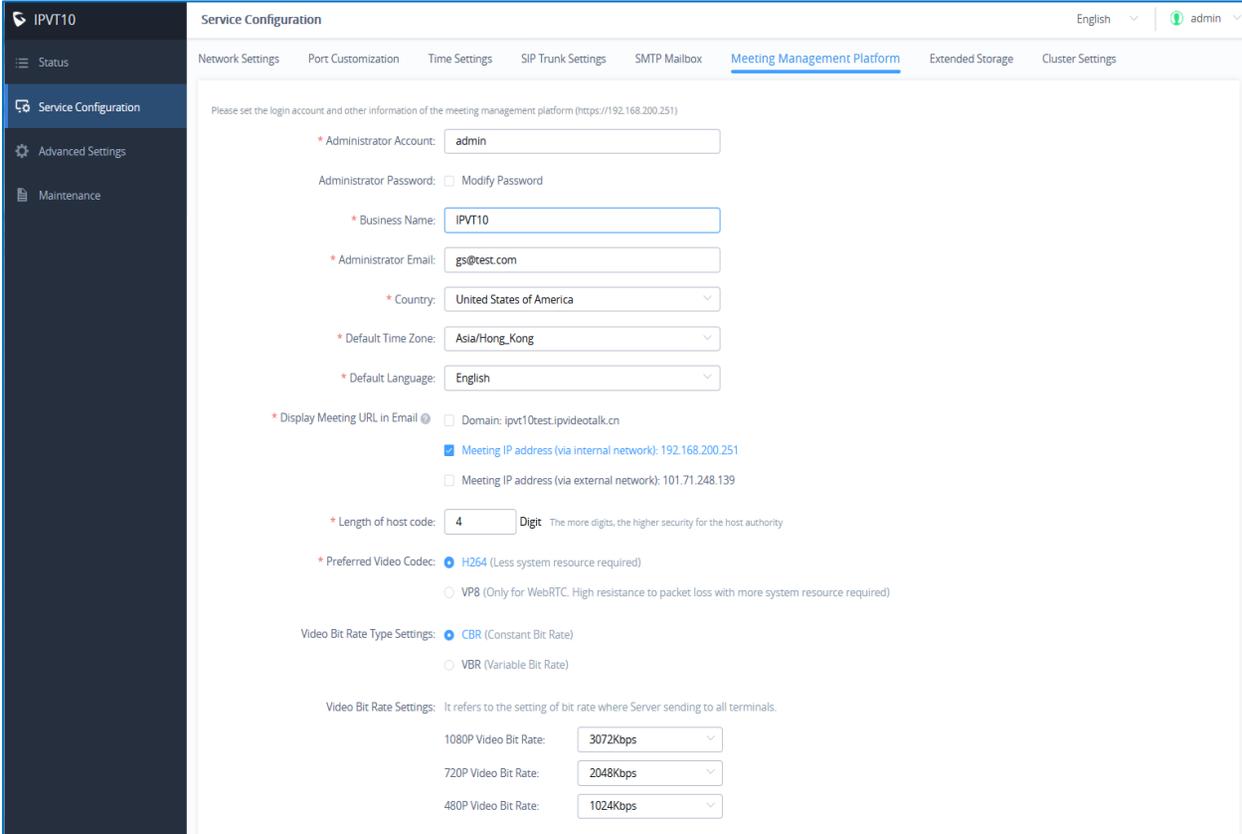
- **Instant Meeting:** Create a temporary meeting for a certain conference client.
- **Schedule Meeting:** Remote schedule a meeting for a certain conference client.
- **Join Meeting:** Join a meeting with browser WebRTC client.



- **Manage Meeting:** Start/Cancel scheduled meetings, check the meeting histories, check the meeting participants list after the meeting and other statics information.
- **Manage Recording Files:** Check/Download cloud recording files.
- **Manage Clients:** Manage all clients which are connected to the IPVT10 server, such as GVC32XX.
- **Add User:** Create user accounts for Conference Management Platform.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Service Configuration”, and configure “Meeting Management Platform” options, as the figure shown below:



The screenshot shows the 'Service Configuration' page for the 'Meeting Management Platform'. The page is titled 'Please set the login account and other information of the meeting management platform (https://192.168.200.251)'. The settings are as follows:

- Administrator Account:** admin
- Administrator Password:** [Empty field] Modify Password
- Business Name:** IPVT10
- Administrator Email:** gs@test.com
- Country:** United States of America
- Default Time Zone:** Asia/Hong_Kong
- Default Language:** English
- Display Meeting URL in Email:** Domain: ipvt10test.ipvideotalk.cn
- Meeting IP address (via internal network):** 192.168.200.251
- Meeting IP address (via external network):** 101.71.248.139
- Length of host code:** 4 **Digit** (The more digits, the higher security for the host authority)
- Preferred Video Codec:** H264 (Less system resource required)
 - VP8 (Only for WebRTC. High resistance to packet loss with more system resource required)
- Video Bit Rate Type Settings:** CBR (Constant Bit Rate)
 - VBR (Variable Bit Rate)
- Video Bit Rate Settings:** It refers to the setting of bit rate where Server sending to all terminals.
 - 1080P Video Bit Rate: 3072Kbps
 - 720P Video Bit Rate: 2048Kbps
 - 480P Video Bit Rate: 1024Kbps

Figure 26: Configure Conference Management Platform

3. Input the parameters as follows:

Table 16: Configure Conference Management Platform

Parameters	Description	Example
Admin Username	Conference Management Platform administrator's username.	The default value is "admin".
Admin Password	Conference Management Platform administrator's password.	The default value is "admin".
Enterprise Name	Conference Management Platform enterprise display name	User's enterprise name
Admin Email	This is used to retrieve the passwords or receive system notification Emails.	Administrator's Email box
Country	Enterprise Location	The default value is "US".
Language	Conference Management Platform language	The default value is "English". Note: If language changed to Spanish or Russian, the conference IVR will also be switched to Spanish or Russian. While for all other languages the IVR will still be English.
Displaying Meeting Address in Email	Select the meeting address that needs to be release in public, which is the meeting address displayed in the invitation email. Users could select the domain name, internal IP address, external IP address which has been configured in the server.	If the domain name could be resolved automatically to the internal IP address or external IP address according to the local network, users only need to release the domain name in public.
Length of Host Code	Set the host code length of the meeting. Supports [4 – 32] digits. Note: The host code is used to obtain the permission of the host in the meeting.	The default setting is 4 digits. If the user needs to improve the security, he can increase up to 32 digits.
Video Mode	Force to use MCU Mode	The default setting is Disabled



Video Stream	Force to send 1080p video to 3 rd -party Endpoint	The default setting is Disabled
Video Bit Rate Type Settings	Select the type of video bit rate for media server, dynamic bit rate or static bit rate.	The default setting is static bit rate.
Video Bit Rate Settings	Select the video bit rate sent to each client by media server, including the bit rate corresponding to various resolutions.	The default setting is the maximum supported performance of the server, which is based on the local network conditions.

4. Click on “Apply Now” to apply the entire configurations of this page to the server. When the deployment is complete, it will take effect immediately.

Third Party Speech Recognition Service Configuration

Users can configure the Speech Recognition Service in Google account for IPVT10 in order to benefit from Google Speech Recognition Services to convert meeting speech to text as meeting records.

Prerequisite: The user needs to have a Google account which has speech-to-text service enabled, and the user needs to download the relevant certificates. (Users may need to check Google official website to learn more details about this service.)

1. Login IPVT10 Web UI.
2. Click on “Service Configuration”, and configure “Meeting Management Platform” options, as the figure shown below:

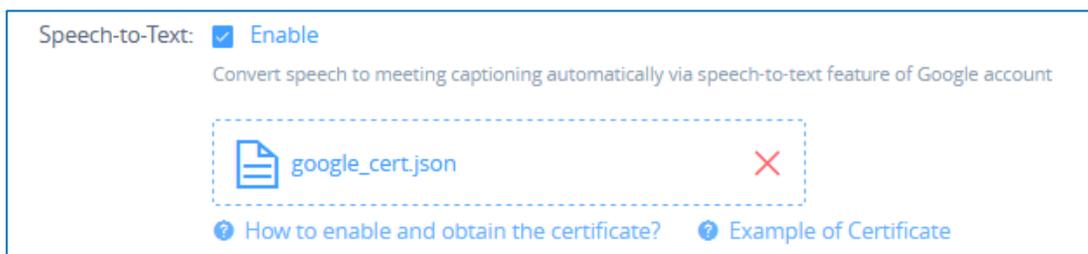


Figure 27: Configure Conference Management Platform – Speech Recognition Configuration

3. Check “Enable” option and upload the service certificate of Google Speech Recognition.

- Click “Save” button to apply the changes, the Google Speech Recognition service will be enabled during the meeting (WebRTC client). The meeting speech will be converted to live meeting captioning during the meeting.

Note: Currently, only English is supported for this service, other languages are not supported.

Extended Disk

If the user needs more storage disks or prefers to store meeting files on other extended disks, the user could follow the steps below to setup the extended disks:

- Login IPVT10 Web UI.
- Go to “Service configuration” and configure “Extended Storage” options.
- Select to activate or inactivate “NFS Storage Disk”, as the figure shows below:

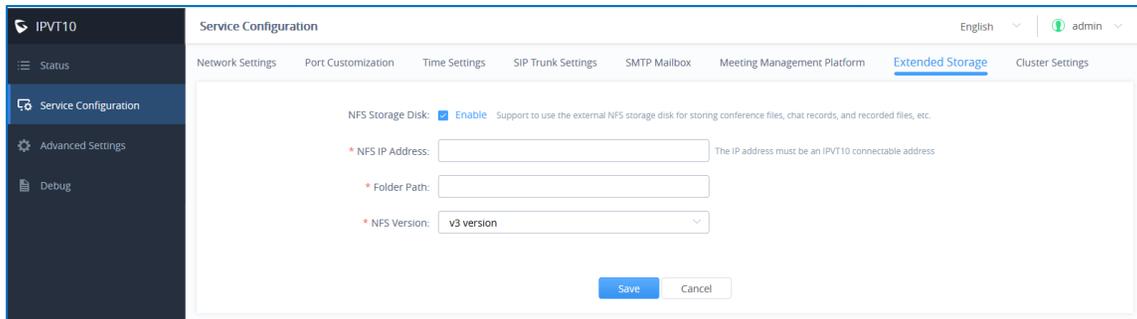


Figure 28: Activate/Inactivate NFS Storage Disk

- Fill in the following information as required:

Table 17: Extended Disk (NFS) Parameters

Parameters	Description	Example
NFS Extended Disk IP Address	Fill in the IP address of the NFS extended disk. This IP address must be reachable for IPVT10 server. Otherwise, the setup will be failed.	
Storage Address	Fill in the file path which will be stored in the NFS extended disk, and the root directory is required.	e.g., <i>/folder1/folder2</i>
NFS Version	The current installed system version of NFS is V3 or V4, users need to select the actual version of NFS. Otherwise, the negotiation between IPVT10 and NFS will be failed.	



- Click on “Apply Now” to apply the entire configurations of this page to the server. When the deployment is complete, it will take effect immediately.

Notes:

- The current extended disk only supports NFS.
- When the extended disk is efficient, all recorded documents and meeting documents will be saved into the NFS extended disk. If the disk is full, it will be prompted.
- If the network of the NFS extended disk is abnormal, or due to some unexpected reasons, the IPVT10 server cannot connect with the NFS, it will also cause non-recording/non-saving issue.
- If the NFS extended disk is disabled, the previous saving files in the NFS extended disk will not be able to be read and downloaded.

Cluster Settings

If users need multiple IPVT10 servers to create a cluster, users need to set one IPVT10 server as the cluster host server. Please, refer to the following steps:

- Login IPVT10 Web UI.
- Go to “Service configuration” and configure “Cluster Settings” options.
- Select to check the option “Active cluster service” to activate the server cluster service, and use the IPVT10 as the cluster host server, as the figure shown below:

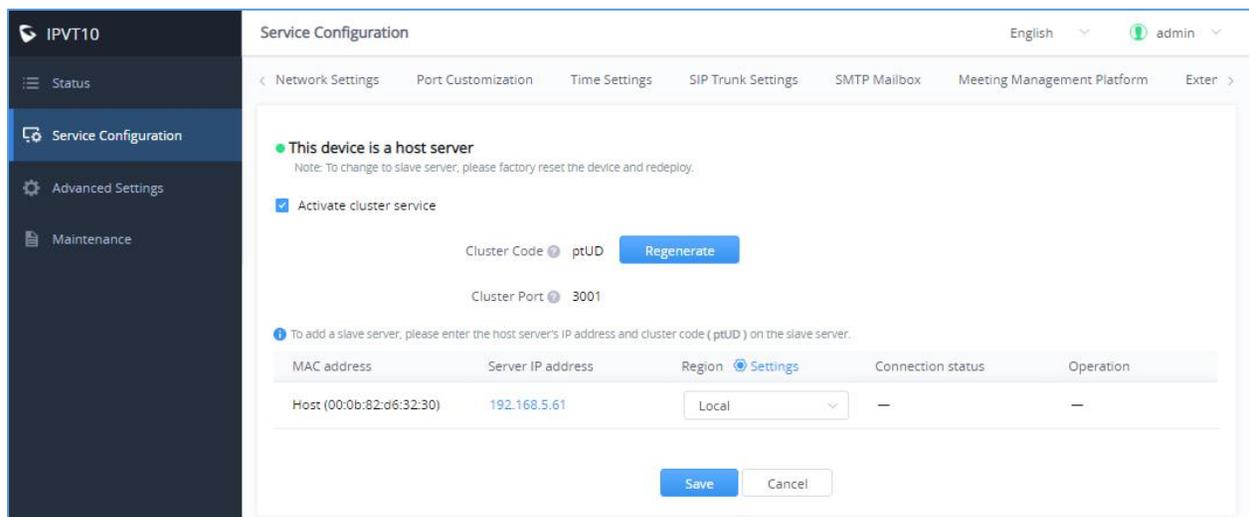


Figure 29: Cluster Settings

- Users need to click to save the configuration and click on “Apply Now” to setup the cluster host server. Then, the cluster host server IPVT10 will be activated.



- In the slave servers, users need to input the “Cluster Code” (e.g., “Cv1R” in the screenshot above, case sensitive). Then, the connection between the cluster host server and slave server will be established.

Notes:

- If the cluster service is enabled and NAT is used, the cluster port 3001 need to be configured for NAT.
 - If users want to change the cluster host server to a slave server, users need to factory reset the IPVT10 device and setup the device as a slave server.
 - It is recommended to connect up to 10 slave servers in order to maximize the performance of IPVT10 host server.
-

Slave Server Management

Users could login IPVT10 cluster host server to check the information of slave servers in the cluster, and block/delete the slave servers on the cluster host server IPVT10’s Web UI.

Please, refer to the following steps:

- Login IPVT10 Web UI.
- Go to “Service configuration” → “Cluster Settings”, users could check the information of the slave servers.

 To add a slave server, please enter the host server's IP address and cluster code (lqxG) on the slave server.

MAC address	Server IP address	Region	Connection status	Operation
50:9a:4c:77:37:61	192.168.200.198	Local	Connected	
ac:1f:6b:65:9e:5e	192.168.200.30	Local	Disconnected	 

Figure 30: Check Slave Server’s Information

- Users could click on the IP address of the slave server, and login the Web UI of the slave server with the credentials.
- Users could click on the icon  to block the connection of the slave server. When the connection is blocked, the slave server IPVT10 cannot establish the connection with the cluster host server, and the cluster host server IPVT10 cannot negotiate with this slave server. Users could also click on icon  to cancel blocking and recover the connection between the slave server and the host server.
- If the connection between the slave server and host server is lost, or the slave server is not available anymore, users could click on icon  to delete the slave server.

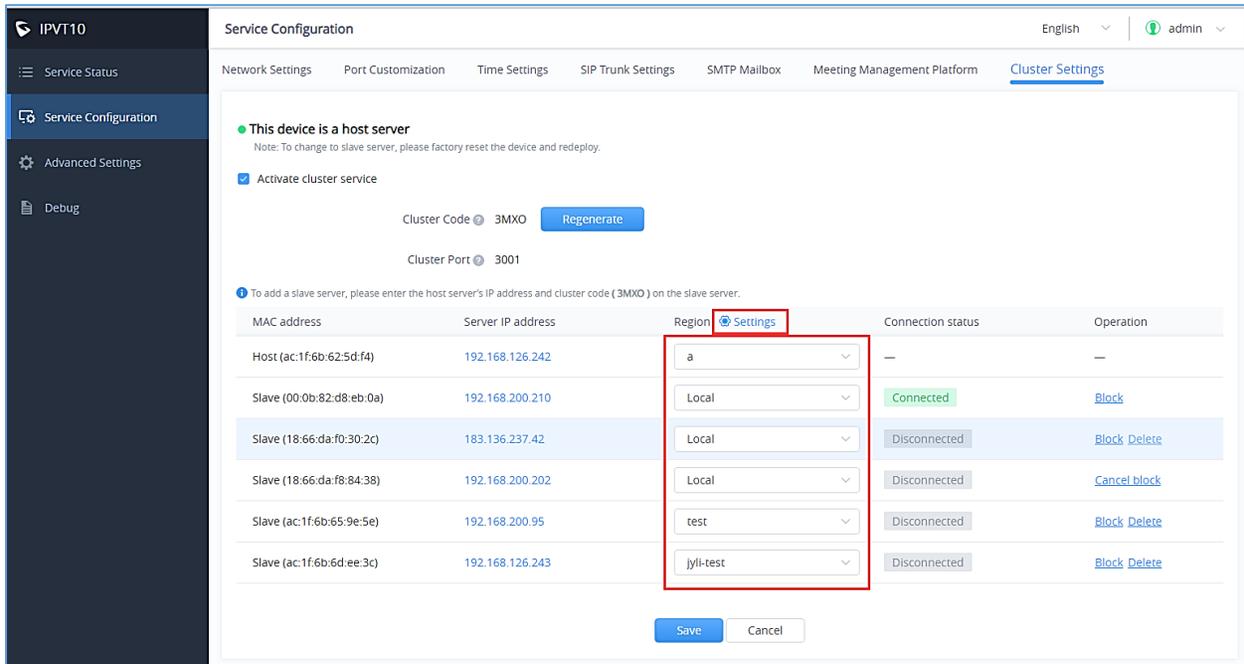


- Users need to click on “Save” button to save the configuration and click on “Apply Now” to effect on the device.

Configure IPVT10 Server Region

Users could manage the clustered IPVT10 servers by different regions. For example, if IPVT10 servers A, B, C are assigned to region 1, and IPVT10 servers D, E are assigned to region 2, for the GVC devices or IPVideoTalk IDs which are assigned to region 1 can only use the resources in the IPVT10 servers which belong to region 1, and they cannot access to use the resources in region 2.

- Login IPVT10 Web UI.
- Go to “Service configuration” → “Cluster Settings”, users could view the Host/Slave Servers List.
- Users could change the region of the IPVT10 server under “Region” menu by clicking the drop-down menu. The default setting is “Local”. If users want to add new region, please click on the “Settings” icon besides “Region” menu option, as the following figure shows.



The screenshot displays the 'Cluster Settings' page in the IPVT10 Web UI. It includes a sidebar with navigation options like 'Service Status', 'Service Configuration', 'Advanced Settings', and 'Debug'. The main content area shows configuration options for 'Cluster Code' (3MXO) and 'Cluster Port' (3001). Below this is a table of servers with columns for MAC address, Server IP address, Region, Connection status, and Operation. A red box highlights the 'Region' column and the 'Settings' icon next to it. The table contains one host and five slave servers with various regions and connection statuses.

MAC address	Server IP address	Region	Connection status	Operation
Host (ac:1f:6b:62:5d:f4)	192.168.126.242	a	—	—
Slave (00:0b:82:d8:eb:0a)	192.168.200.210	Local	Connected	Block
Slave (18:66:da:f0:30:2c)	183.136.237.42	Local	Disconnected	Block Delete
Slave (18:66:da:f8:84:38)	192.168.200.202	Local	Disconnected	Cancel block
Slave (ac:1f:6b:65:9e:5e)	192.168.200.95	test	Disconnected	Block Delete
Slave (ac:1f:6b:6d:ee:3c)	192.168.126.243	lyll-test	Disconnected	Block Delete

Figure 31: IPVT10 Server Region

- Users need to click on “Save” button to save the configuration and click on “Apply Now” to take effect on the device.

Note: If there is a region that does not include any IPVT10 server, all the scheduled meetings in this region cannot be started, and there will be a prompt to indicate the user that all scheduled meetings in this region will be moved to another region. As shown on the following figure:

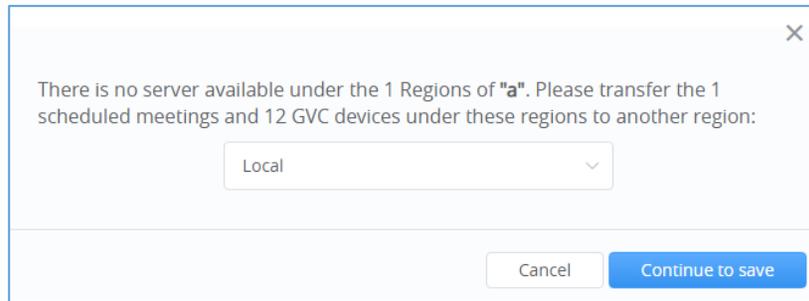


Figure 32: Move Scheduled Meetings Prompt

Region Management

Users could add multiple new regions and change the names of the regions.

1. Login IPVT10 Web UI.
2. Go to “Service configuration” → “Cluster Settings”, and click the icon  **Settings** besides the Host/Slave Servers List, users could see the prompt as the figure shows below:

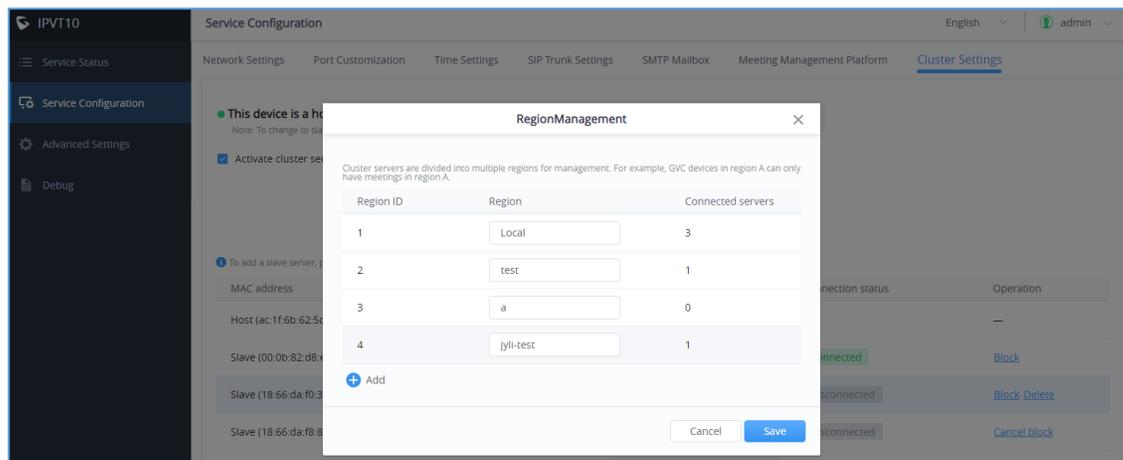


Figure 33: Region Management

Notes:

- The connected IPVT10 servers amount for each region in the list is indicating that the available IPVT10 servers amount, it does not include the blocked servers.
- Users could add new regions, input the region name, and click “Save” button to save the regions.
- Users could also update the region name for a certain region and click “Save” button to save the region name.

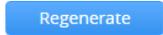


- Users need to click on “Apply Now” to effect on the device.

Cluster Code

Users could generate a new cluster code in the cluster, and all slave servers cannot connect with the cluster host server without the new cluster code.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Go to “Service configuration” → “Cluster Settings” and click on the button  to generate a new cluster code for the cluster service.
3. Users need to click on “Save” button to save the configuration and click on “Apply Now” to effect on the device.

Then, all slave servers cannot connect with the cluster host server without the new cluster code.

Users need to input the cluster code again in the slave servers to recover the connection with the cluster host server.

Configure Slave Server

Network Settings

Options Descriptions

Table 18: Parameters Descriptions

Parameters	Description
Network Adapter	Configures Network Adapter’s parameters, which requires to establish the connection with the host server.
IPv4 Address	Configures the IP Address for IPVideoTalk Portal.
Subnet Mask	Configures the Subnet Mask.
Gateway	Configures the default Gateway.
Preferred DNS	Set the Preferred DNS.
Alternative DNS	Set the Alternative DNS.
NAT	Enable/Disable NAT and set the NAT IP address.



Note:

Ethernet port 1 is used to connect user's PC with the IPVT10 server to login the configuration page of the device. Users need to connect the Internet with the **Ethernet port 2** on the IPVT10 server.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Go to “Service configuration” → “Network Settings”, as the figure shown below:

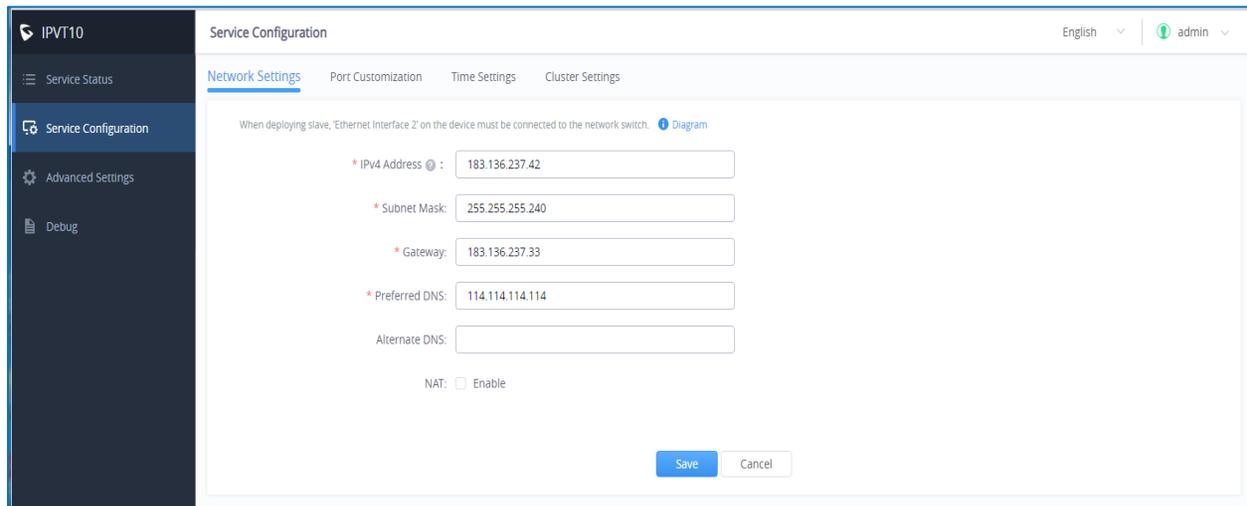


Figure 34: Service IP Address Config – Network Adapter

3. Users need to configure “IPv4 Address”, “Subnet Mask”, “Gateway”, “Preferred DNS”, “Alternative DNS” (optional) for the network adapter.

Notes:

- Please make sure that the IP address is available to reach the cluster host server. This IP address could be an internal IP address or an external IP address.
 - Please make sure that there should be no conflict in the IP address. Otherwise, the service will be unavailable.
-

4. (Optional) If the selected adapter is external network adapter, users could configure static NAT for the IPVT10.



Note: NAT could translate the private IP address of the internal network into a public IP address, so that an external conference client can access the server of the internal network through the public network.

5. Continue to fill in the other configuration options. For the first deployment, users must fill in all required fields.
6. Users need to click to save the configuration and click on “Apply Now” to apply the entire configurations of this page to the server. When the deployment is complete, it will take effect immediately.



Notes:

- When the deployment is complete, users need to check whether all network interfaces of the server are all connected.
- Users need to connect the Internet with the Ethernet port 2 on the IPVT10 slave server so that the connection could be established with the cluster host server.
- If users modify the IP address of the server during the conferences, it may cause the abnormal issues for the ongoing conferences, and the scheduled conferences will be inaccessible.
- When users modify the parameters of the server, the server will restart the service automatically.

Configure Service NAT Interfaces

(Optional) users could customize the service port. Our default service ports are shown as following below:

Table 19: Service Port Configuration

Server Components	Protocol	Default Port	Descriptions
Media Server	TCP/UDP	5062	External control port
Media Server	UDP	60000-65000	Port range of media streams: Requirements: Port starting should not be lower than 1024, the range is not less than 3000.

Please, refer to the following steps:



1. Login IPVT10 Web Management UI.
2. Click on the “Service Configuration” on the left side of the UI and select “Port Customization”, users will see the page below:

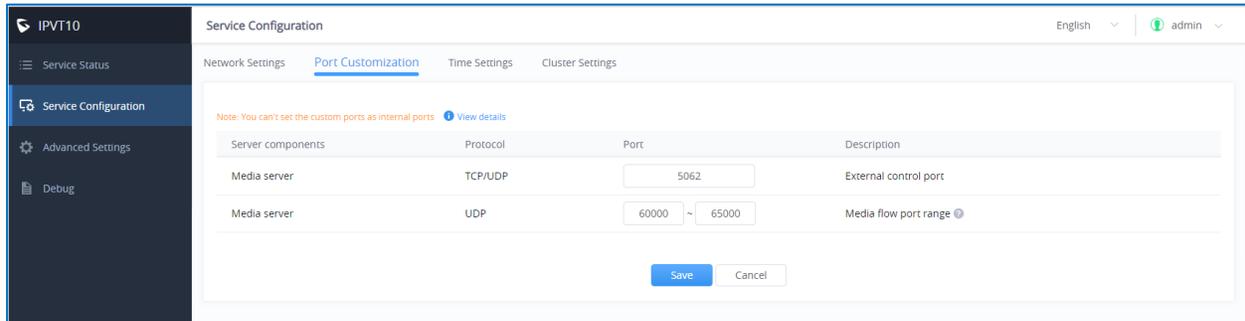


Figure 35: Service Port Configuration

3. Users could customize the service ports based on the requirements.
4. When users finish updating the ports, users need to click to save the configuration, and click on the button “**Deploy Now**” to confirm the customized service ports. The server will reboot to apply the changes.

Notes:

- The customized service ports cannot be duplicated.
- The ports below cannot be set as customized service ports: "25,80,443, 3000, 3306, 5060,5061, 5070, 5071,5072, 5080, 6379, 6380, 6381, 8006, 8008, 8010, 8012, 8080, 8081, 8083, 9080, 80000, 26222".
- If the service ports are set incorrectly, users cannot use the corresponding services normally.

Time Configuration

Users could check the current time and time-zone of the server and correct it at any time to avoid the meeting time inaccurate or cannot be launched issues.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Service Configuration”, and configure “Time Settings” options, as the figure shown below:



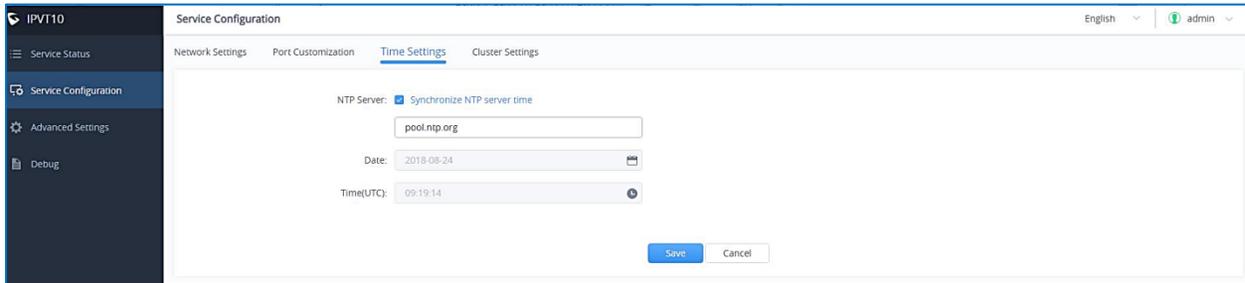


Figure 36: Time Settings

3. It will show the current time of the server by default.
4. Users could set whether to synchronize the SNTP server time. If there is no available SNTP server, users could adjust the date and time manually.
5. Users need to click to save the configuration and click on “Apply Now” to update the server time immediately.

Cluster Settings

Users need to input the IP address of the cluster host server and the cluster code in the slave server to finish configuration.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Service Configuration” → “Cluster Settings”, as the figure shown below:

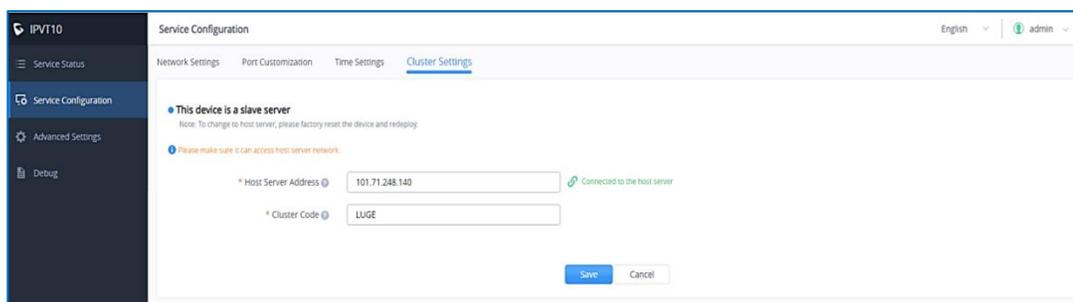


Figure 37: Cluster Settings

3. Input the IP address of the cluster host server. This IP address must be a reachable address for the slave server.
4. Input the Cluster Code in slave server (case sensitive).
5. Users need to click to save the configuration and click on “Apply Now” to update the server time immediately.



Advanced Settings

Alarm Email Setup

Users can configure and enable Alarm Email. The alarm email includes high CPU usage, HDD abnormal, slave machine connection abnormal, system reboot, system upgrade, admin log in failed continuously, password changed, etc.

1. Login IPVT10 Web UI.
2. Click on “Advanced Settings” and go to “General Settings”.
3. Click to enable “Send Alarm Email” and input the receiver email addresses, multiple email addresses allowed.
4. Click “Save” to save the setting. Alarm Email would be sent to the subscriber’s email addresses once alarm events happened

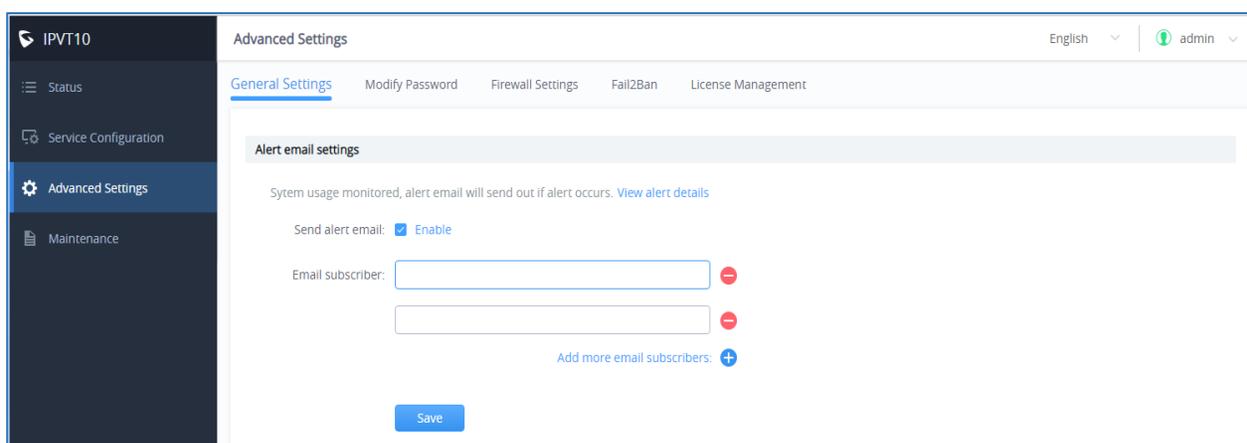


Figure 38: Alarm Email Setup

Enable/Disable SSH

If your IPVT10 server encounters any failure, you may need to contact with Grandstream technical support to troubleshoot the problem. You can enable SSH service on IPVT10 server’s Web UI, in order to allow our technical support to access the IPVT10 server remotely for troubleshooting purpose.

Note: To ensure IPVT10 server security, users currently do not have permission to access IPVT10 server through SSH.



Please refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Advanced Settings” and go to “General Settings”.
3. The default SSH port is 26222, and users could change the SSH port by editing the port number directly.
4. Click on “Enable SSH”.
5. If users want to disable the SSH service, please click on button “Disable SSH”.

Access Restrictions

Users can set a white list to only allow specific IP addresses to access the deployment management page and the meeting management platform. Please refer to the following steps to enable this feature.:

1. Login IPVT10 Web UI.
2. Click on “**Advanced Settings**” and go to “**Access Restriction**”.
3. Enable this option.
4. Then, enter multiple IP addresses and IP segments on the white list, such as 192.168.1.1/24.
This is a mandatory option.
5. Click “**Save**” button to complete the setup.

Note: When this feature is enabled, only the IP addresses on the white list can access the deployment page and meeting management page. While other IP addresses cannot access both those pages. But any given IP will have access the meeting URL normally.

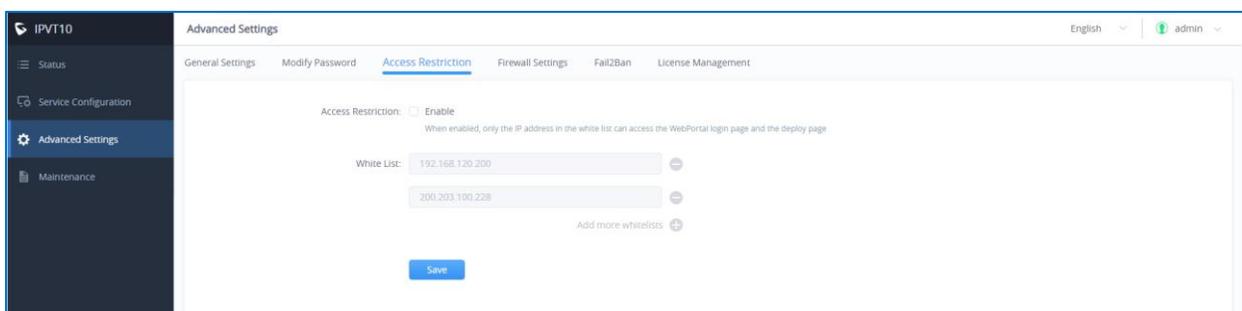


Figure 39: Access Restrictions



Firewall Settings

Firewall configuration is provided to protect the device and system from malicious attacks by processing different data passing through the system properly and ensuring the bandwidth and security.

In “Advanced Settings”, go to “Firewall” web GUI, user can see the Firewall Config page to setup and adjust the related parameters accordingly.

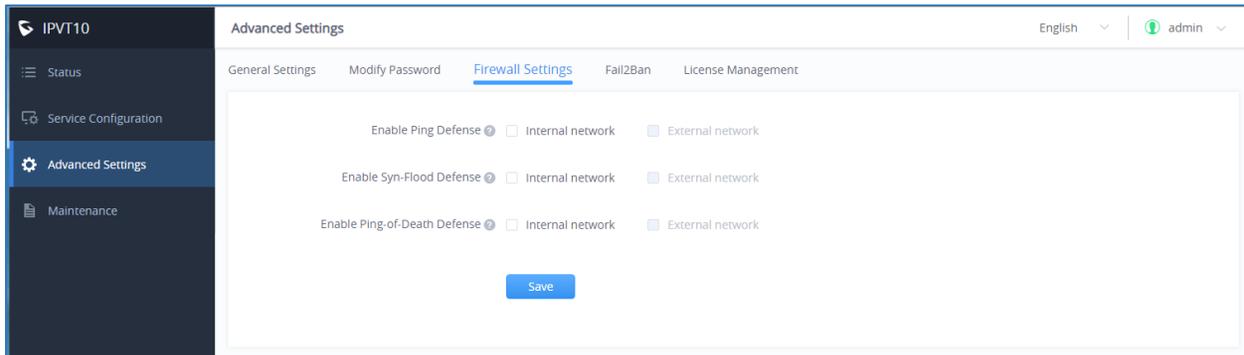


Figure 40 : IPVT10 Firewall settings

Table 20: IPVT10 Firewall settings

Parameters	Description
Enable Ping Defense	If enabled, no echo response to “PING” ICMP message. Default disabled. If IPVT10 has internal and external two IP addresses, this can be configured separately and independently.
Enable Syn-Flood Defense	Enable to protect device from flood attacking or DDoS attack. Default disabled. If IPVT10 has internal and external two IP addresses, this can be configured separately and independently.
Enable Ping-Of-Death Defense	Enabled to protect device from Ping of Death (PoD) flood DDoS attack. Default disabled. If IPVT10 has internal and external two IP addresses, this can be configured separately and independently.

Fail2Ban

Fail2Ban feature will discover and block authentication errors that occur during SIP registration, authentication, and access connections. If a host fails and exceeds the maximum allowed value (named as matching threshold) within the specified time span, IPVT10 will mark out and block the host for a period. This feature helps to detect and prevent violent attacks to the IPVT conferencing system in a timely manner.

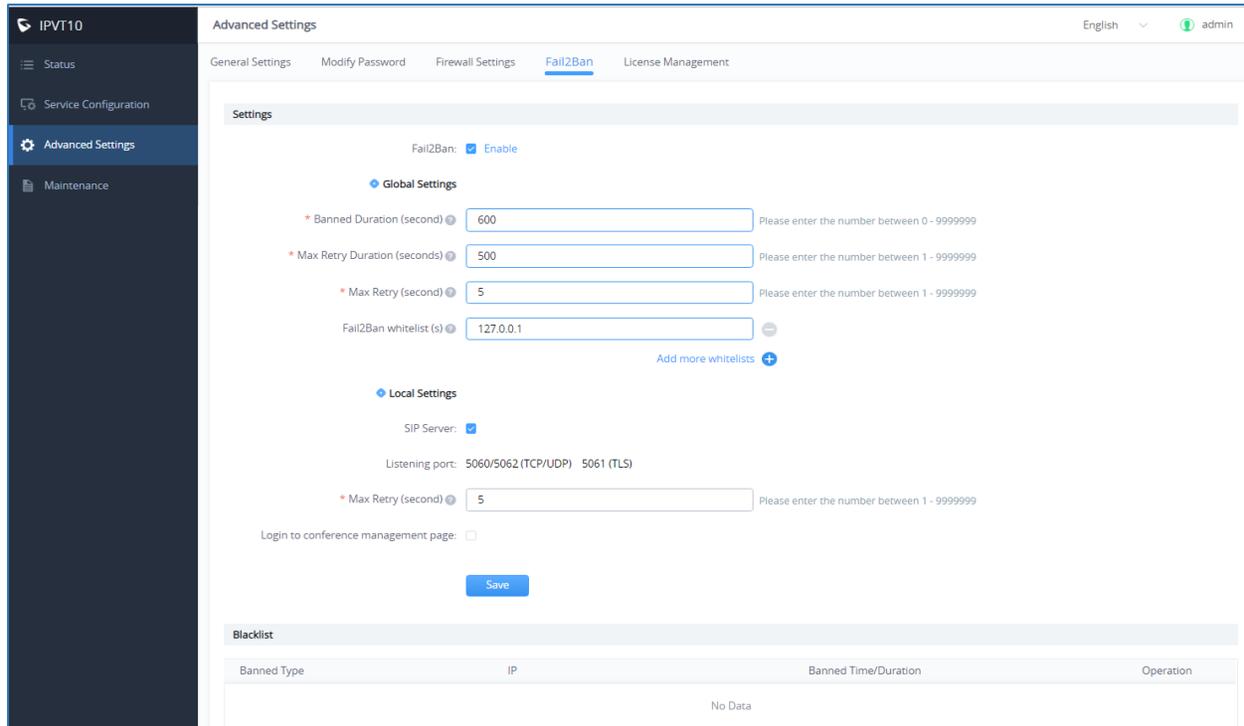


Figure 41 : IPVT10 Fail2Ban feature

Table 21: Fail2Ban settings

Parameters	Description
Settings	
Enable	Click to enable Fail2Ban. Default settings is disabled. If enabled, it will be effective to SIP Server and the login to Conference Management Platform.
Global Settings	
Banned Duration (seconds)	Configure host forbidden timespan by firewall, in seconds. Default value 300 seconds (5 minutes). the host will be always banned.

Max Retry Duration (seconds)	Within this duration (in seconds), if a host exceeds the max times of retry as defined in "Max Retry", the host will be banned. The default setting is 600.
Max retry	Configure the number of authentication failures during "Max Retry Duration" before the host is banned. The default setting is 5.
Fail2Ban Whitelist	Set the Whitelist via IP address or a DNS domain name. Fail2Ban will not block hosts in the Whitelist. Maximum 20 hosts allowed in the Whitelist.
Local Settings	
SIP Server	Enable to setup individual matching threshold for the "SIP Server". Default is disabled. Note: <i>Listening Port is Not configurable.</i> <i>Current supported ports: 780 (HTTP) 7443 (HTTPS/WSS)</i>
Login to conference management page	Allows login to Conference management page. Default is disabled. Note: <i>Listening Port is Not configurable.</i> <i>Current supported ports: 5060/5062 (TCP/UDP) and 5061 (TLS)</i>
Max retry	When the number of failed logins attempts from an IP address exceeds the Max retry number, that IP address will be banned from accessing the Web GUI.
Settings	
Blacklist	Users will be able to view the IPs that have been blocked by IPVT10.

License Management

View License Information

Users could view the license information of the IPVT10 on its Web UI.

Please refer to the following steps:

1. Login IPVT10 Web UI.



2. Click on “Advanced Settings”, and go to “License Management”, users could check the current license information details as the screenshot shows below:

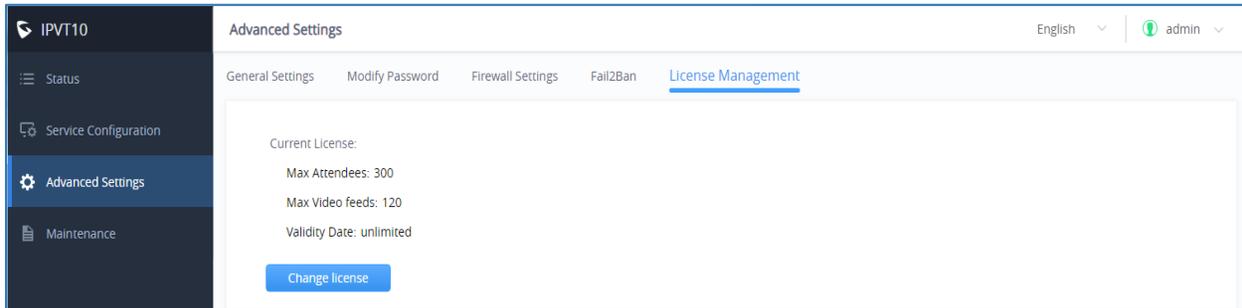


Figure 42: View License Information

Note:

If the current license is on trial, the “Trial” tag will be displayed.

Update License

Users could update license of the IPVT10 server on its Web UI.

Please refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Advanced Settings” and go to “License management” menu.
3. Click on “Change License” option.
4. Upload the new license file into the IPVT10 server.

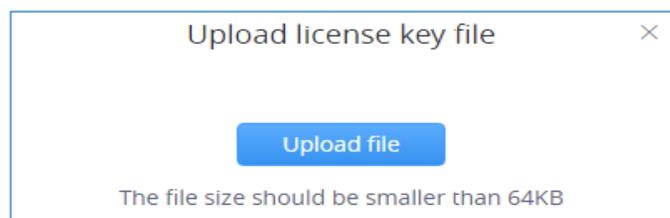


Figure 43: Upload License Key File

5. When finish uploading, users need to click on “Active Now” to apply the new license in the IPVT10 server.

Note: If the current license has not expired, and the user wants to upload a license, the current license will be expired. Users cannot use the previous license to activate any IPVT10 device even though the license is not expired.



Maintenance

Upgrade

Users need to take in consideration the following notes when upgrading IPVT10:

- During the upgrading service, the IPVT10 service will be suspended, and users cannot login the Conference Management Platform or start meetings.
- It is suggested to upgrade the device when there is no scheduled or activated meetings during the period.
- It is suggested to download the upgrading firmware from Grandstream official website or using the firmware from Grandstream designated technical support.

Please refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Maintenance”→ “Upgrade”.
3. Click on “Upgrade”.

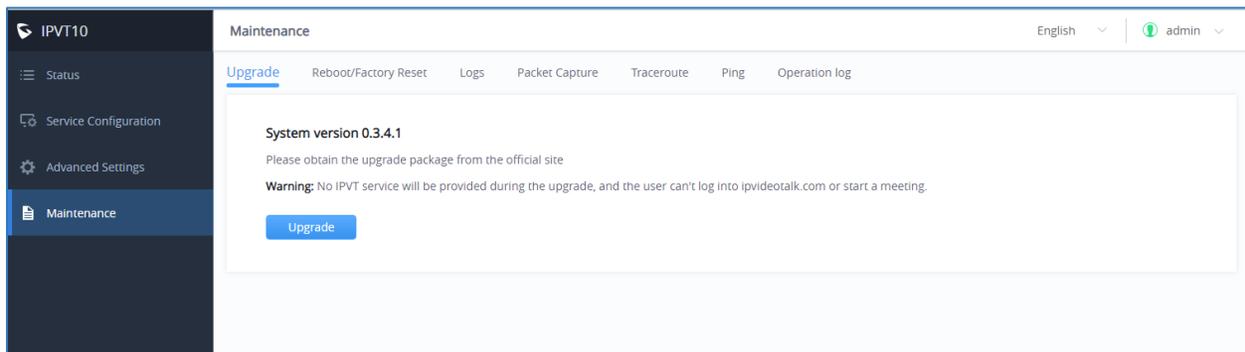


Figure 44: Upgrade Service

4. Select the upgrading firmware from the local PC and upload the firmware to the device.
5. When users click to confirm upgrading, the device will process to upgrade the firmware. This process may take several minutes.
6. When the upgrading is complete, the server will restart the service automatically.



Factory Reset

When users restore the device to factory reset, all the data in the database server will be erased, including the meetings data and user's data, as for all the configurations in the server will be erased, and restore to the factory default configuration.

Please, refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on "Maintenance" → "Reboot/Factory Reset".
3. Click on "Factory Reset".
4. The system will pop up a prompt to ask the users to confirm "Are you sure to factory reset the device?", and users could click on "Yes" to start to factory reset the device. All the data will be erased, and the service will be restarted. Users could also select to clear all user's data or remain the data.
 - If users only clear the configurations in the IPVT10, and remain the user's data, all of the settings will be recovered to default settings, and all of the logcat will be deleted, the user's data such as account information, scheduled meetings, meeting histories, and recording files will be remained.
 - If the user selects to clear all user's data, all the configurations and user data will be erased from the IPVT10 server.

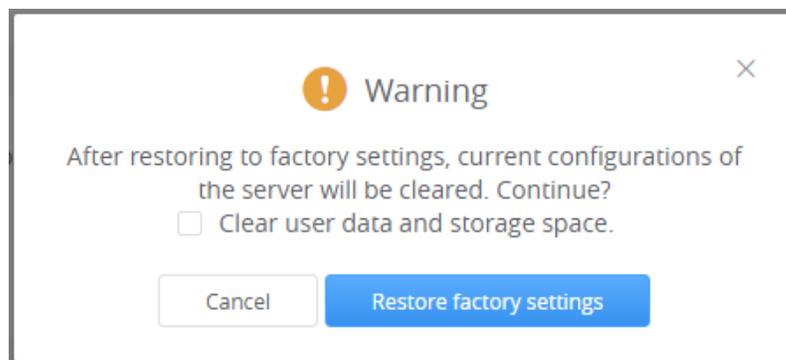


Figure 45: Clear Data

Reboot

Users could reboot the IPVT10 server on its Web UI. Please refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Maintenance” → “Reboot/Factory Reset”.
3. Click on “Reboot” to reboot the IPVT10 server, and the current meetings which are in progress will be terminated.

System Logs

Users could check and download the logs of each component from IPVT10 server (e.g., MCU/SIP server/WebRTC/Conference Management Platform).

Please refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Maintenance” → “Logs” menu, as the figure shows below:

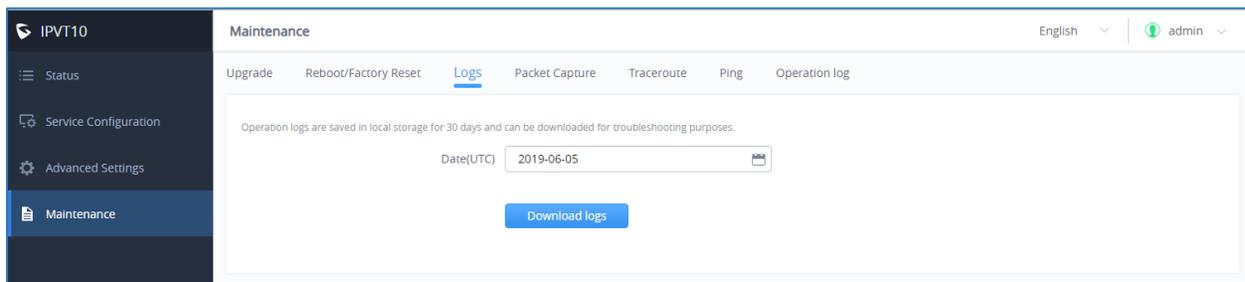


Figure 46: Download System Logs

3. Select the date of generating the logs. Users could select the date up to past 30 days.
4. Click on “Download logs”, and the logs which is generating on that date will be downloaded into the user’s PC.

Packet Capture

Users could capture the traces in IPVT10 server to troubleshoot the problems.

Please refer to the following steps:

1. Login IPVT10 Web UI.
2. Click on “Maintenance” → “Packet capture”, as the figure shows:



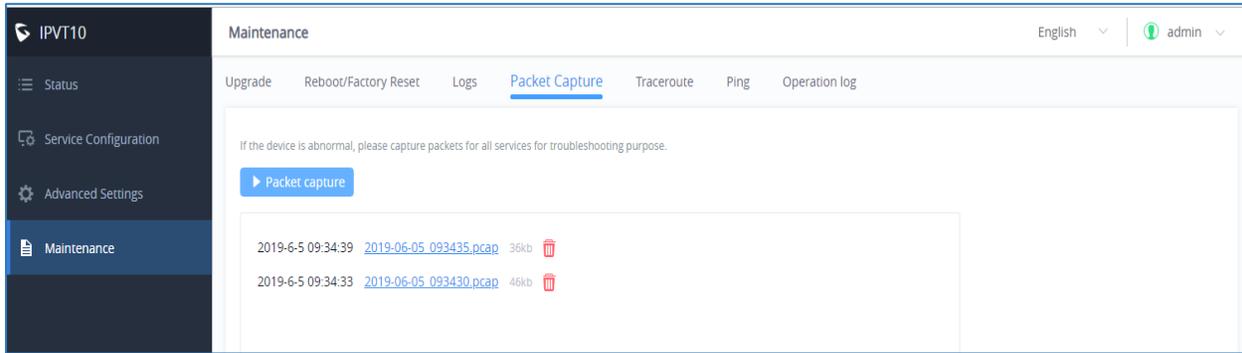


Figure 47: Packet Capture

3. Click on “Packet capture” option to start capturing in IPVT10 server.
4. Click on icon  to stop capturing the trace, and the trace file will be shown up on the menu below.
5. Click on the file name, such as [2018-08-22_100130.pcap](#) to download the trace into the user’s PC. If the traces are too many items in the IPVT10 server, the user could click on icon  to delete the certain trace file.

Traceroute

Users could perform a traceroute by entering the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below:

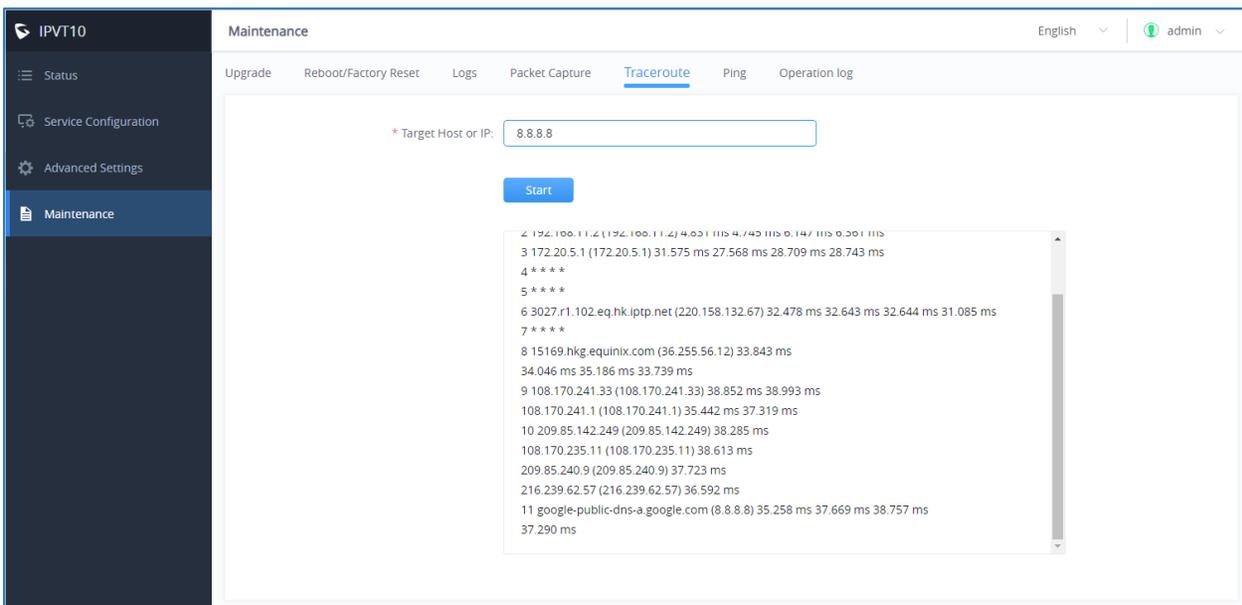
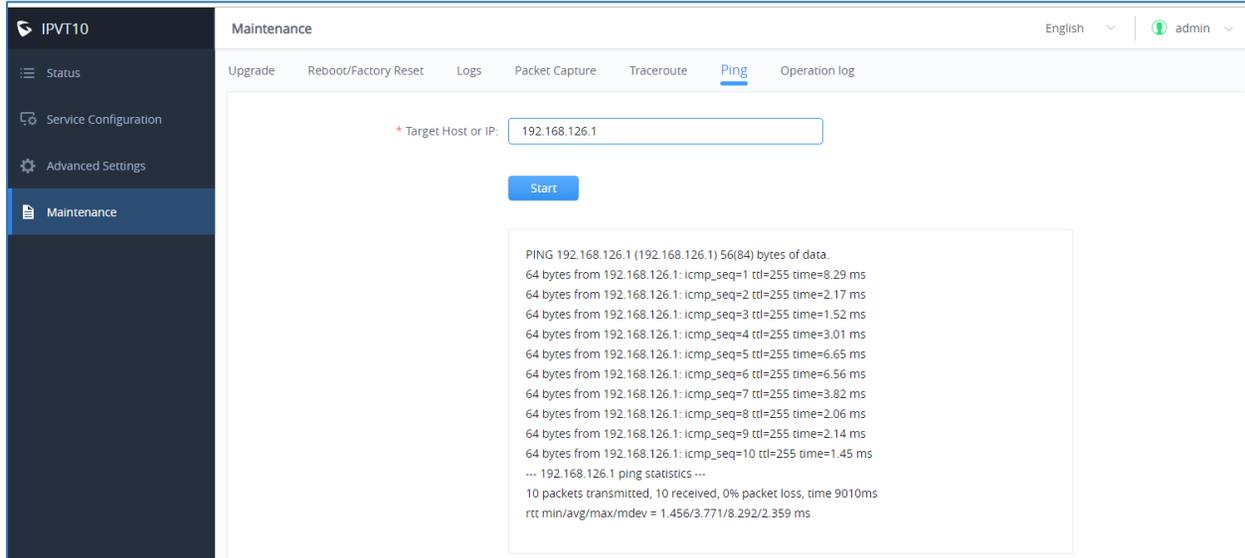


Figure 48: Traceroute



Ping

Enter the target host in host name or IP address. Then press "Start" button. The output result will dynamically display in the window below.



The screenshot shows the IPVT10 Maintenance page with the 'Ping' tab selected. The target host is set to 192.168.126.1. The output displays the following ping statistics:

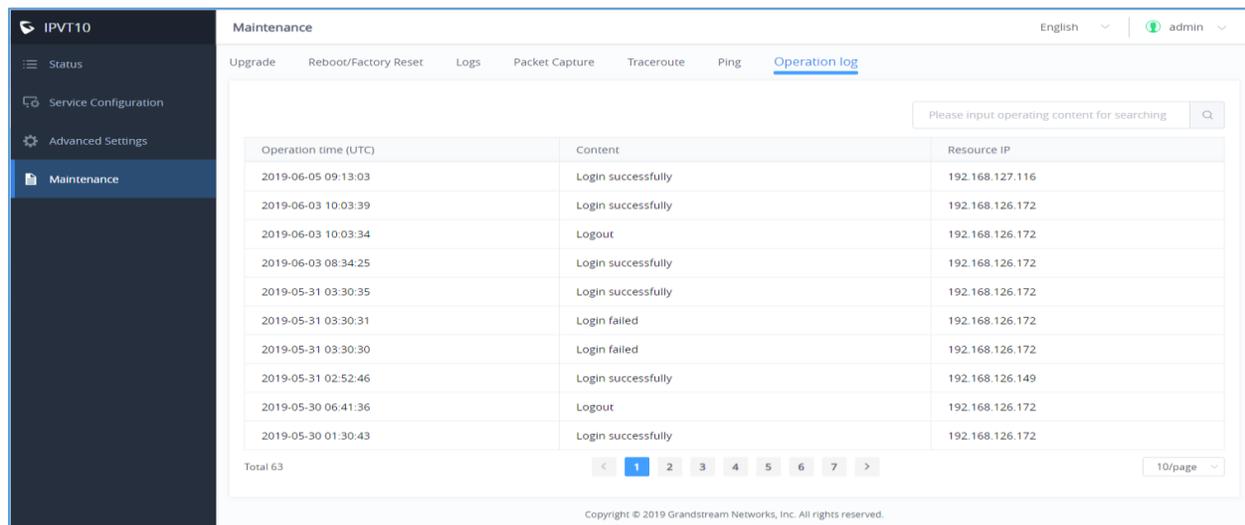
```

PING 192.168.126.1 (192.168.126.1) 56(84) bytes of data:
64 bytes from 192.168.126.1: icmp_seq=1 ttl=255 time=8.29 ms
64 bytes from 192.168.126.1: icmp_seq=2 ttl=255 time=2.17 ms
64 bytes from 192.168.126.1: icmp_seq=3 ttl=255 time=1.52 ms
64 bytes from 192.168.126.1: icmp_seq=4 ttl=255 time=3.01 ms
64 bytes from 192.168.126.1: icmp_seq=5 ttl=255 time=6.65 ms
64 bytes from 192.168.126.1: icmp_seq=6 ttl=255 time=6.56 ms
64 bytes from 192.168.126.1: icmp_seq=7 ttl=255 time=3.82 ms
64 bytes from 192.168.126.1: icmp_seq=8 ttl=255 time=2.06 ms
64 bytes from 192.168.126.1: icmp_seq=9 ttl=255 time=2.14 ms
64 bytes from 192.168.126.1: icmp_seq=10 ttl=255 time=1.45 ms
--- 192.168.126.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9010ms
rtt min/avg/max/mdev = 1.456/3.771/8.292/2.359 ms
  
```

Figure 49: Ping

Operation Logs

Users can view all the operation logs in the "Maintenance" page. All the operations on the service platform displayed here, such as login, deployment service, restart service, factory reset, firmware upgrade, license modification, and packet capture, etc.



The screenshot shows the IPVT10 Maintenance page with the 'Operation log' tab selected. The table below displays the operation logs:

Operation time (UTC)	Content	Resource IP
2019-06-05 09:13:03	Login successfully	192.168.127.116
2019-06-03 10:03:39	Login successfully	192.168.126.172
2019-06-03 10:03:34	Logout	192.168.126.172
2019-06-03 08:34:25	Login successfully	192.168.126.172
2019-05-31 03:30:35	Login successfully	192.168.126.172
2019-05-31 03:30:31	Login failed	192.168.126.172
2019-05-31 03:30:30	Login failed	192.168.126.172
2019-05-31 02:52:46	Login successfully	192.168.126.149
2019-05-30 06:41:36	Logout	192.168.126.172
2019-05-30 01:30:43	Login successfully	192.168.126.172

Total 63

Figure 50 : Operation Logs



TYPICAL NETWORK SOLUTIONS

Users could select the network solutions based on the actual requirements. There are several scenarios:

Scenario 1: Internal Network

The server is deployed on the internal network. The users use the service via internal network. Users need to configure the internal network IP address for the server. If users register accounts and start conferences on the internal network, and other participants are all on the internal network, users could only deploy the server on the internal network, and only configure the internal network adapter. For example, users could configure this server in the private networks.



Figure 51: Network Deployment Diagram – Internal

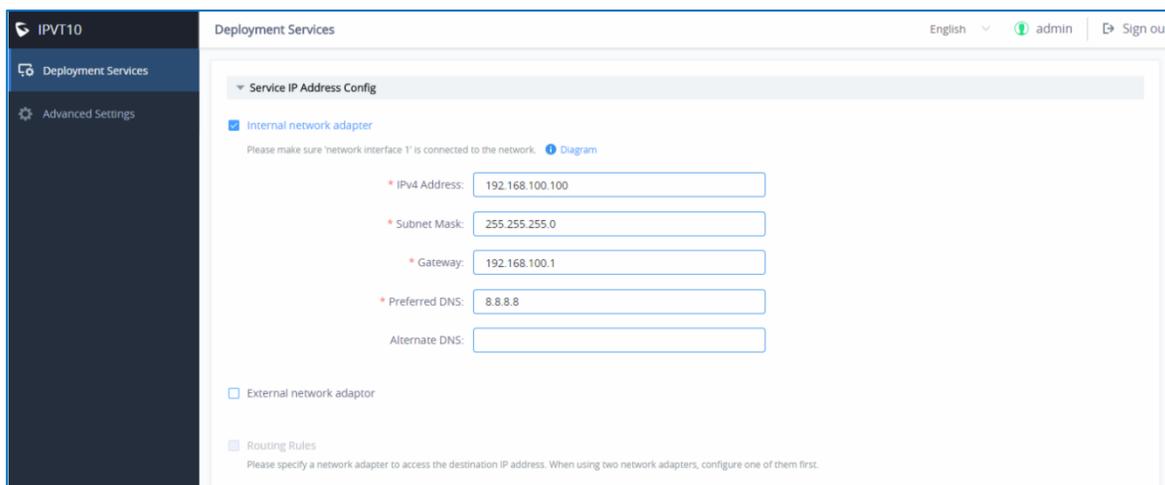


Figure 52: Configure Internal Network Adapter

Scenario 2: External Network

The server is deployed on the external network. Users could access the server via the public network. Users need to configure the external network IP address in the server. If users register accounts and start conferences on the public network, and other participants are all on the public network, users could only deploy the server on the public network and configure the public network adapter.

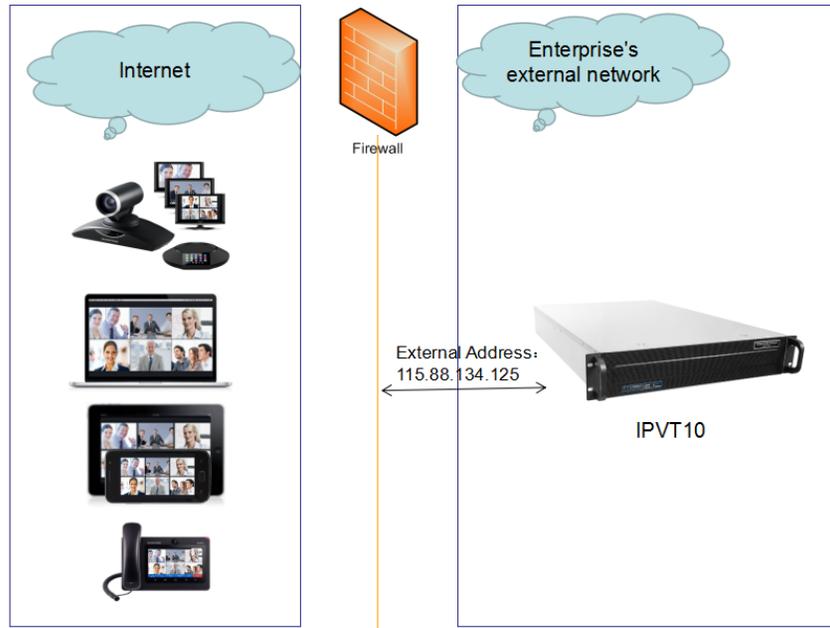


Figure 53: Network Deployment Diagram – External

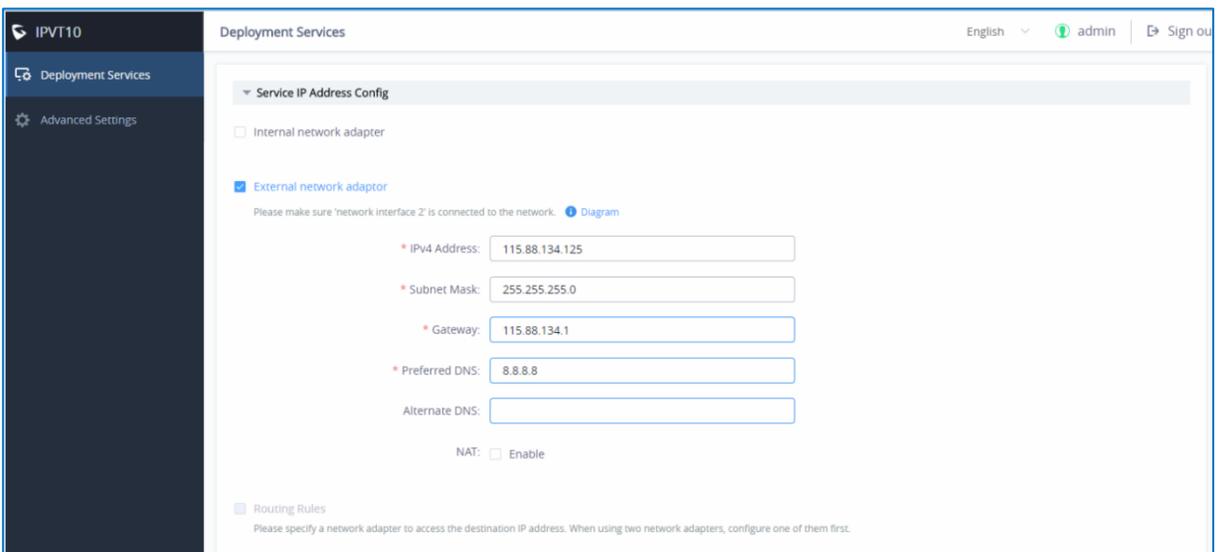


Figure 54: Configure External Network Adapter

Scenario 3: External Users to Internal Server

The server is deployed on the internal network for external users. The users need to use the service via the public network. In this case, users need to configure the external network IP address and static NAT in the server. If the server is deployed on the internal network, and all participants need to use the service via public network, users need to configure the static NAT to ensure the certain public networks can access the server. Users could configure the External Network Adapter and NAT to complete the configuration. This deployment does not support users to access the server directly via the internal network. Otherwise, it may cause the abnormal issues for the conferences.

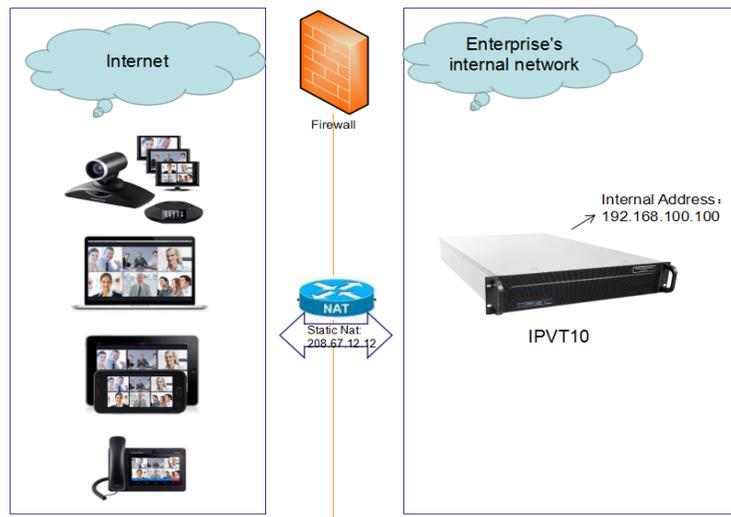


Figure 55: Network Deployment Diagram – External Users to Internal Server

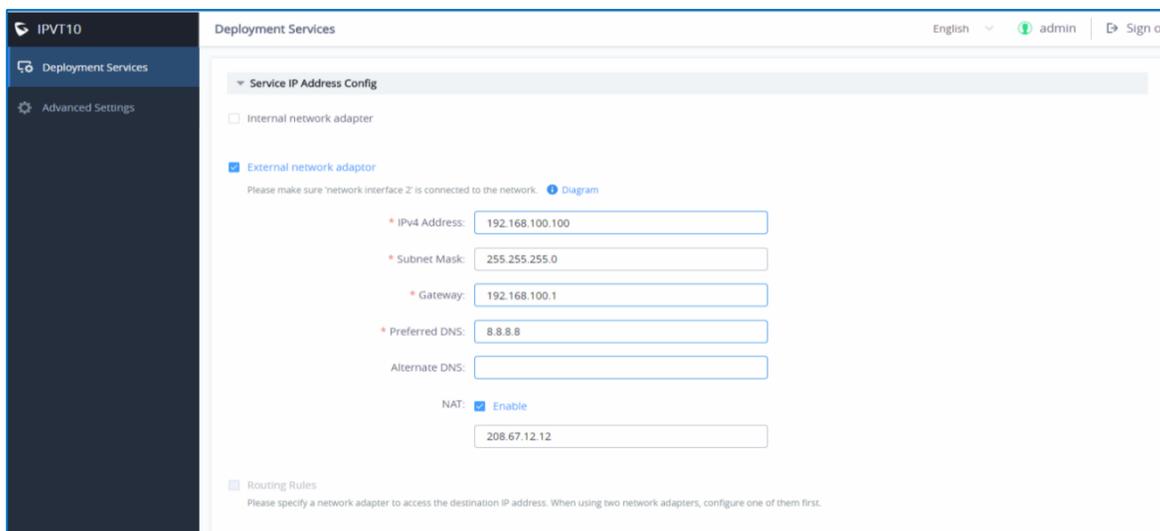


Figure 56: Configure External Network Adapter and NAT

Scenario 4: Internal Network and External Network

The server is deployed on the internal network. The users could access and use the service via either internal network or external network. In this case, users need to configure both internal network and external network in the server, and routing rules. Users need to configure both Internal Network Adapter and External Network Adapter.

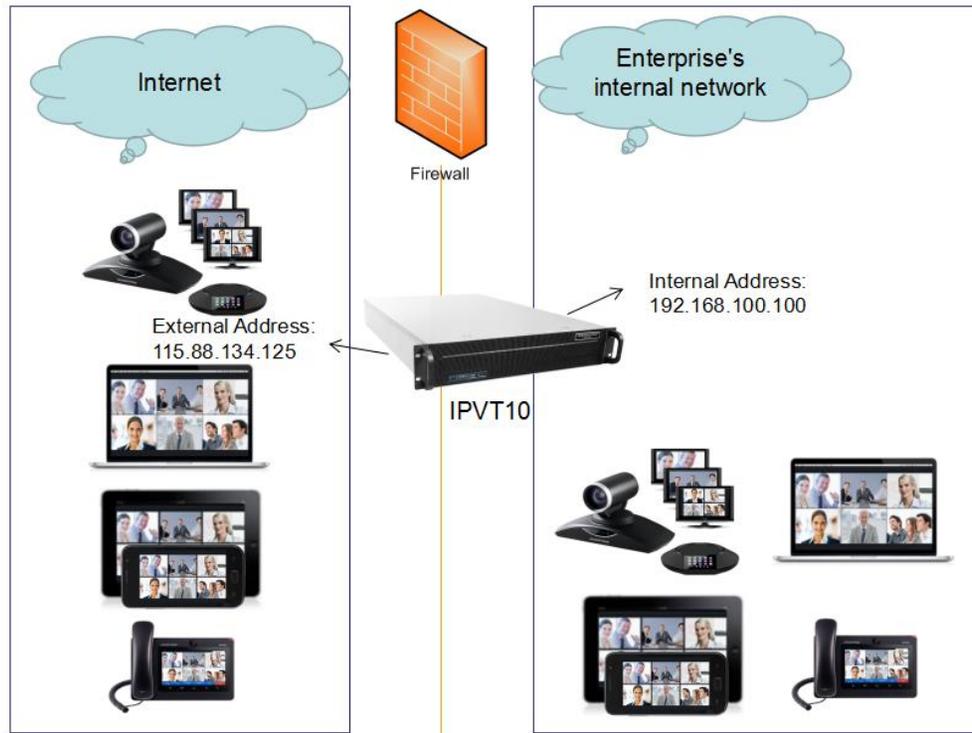


Figure 57: Network Deployment Diagram – Internal Network and External Network

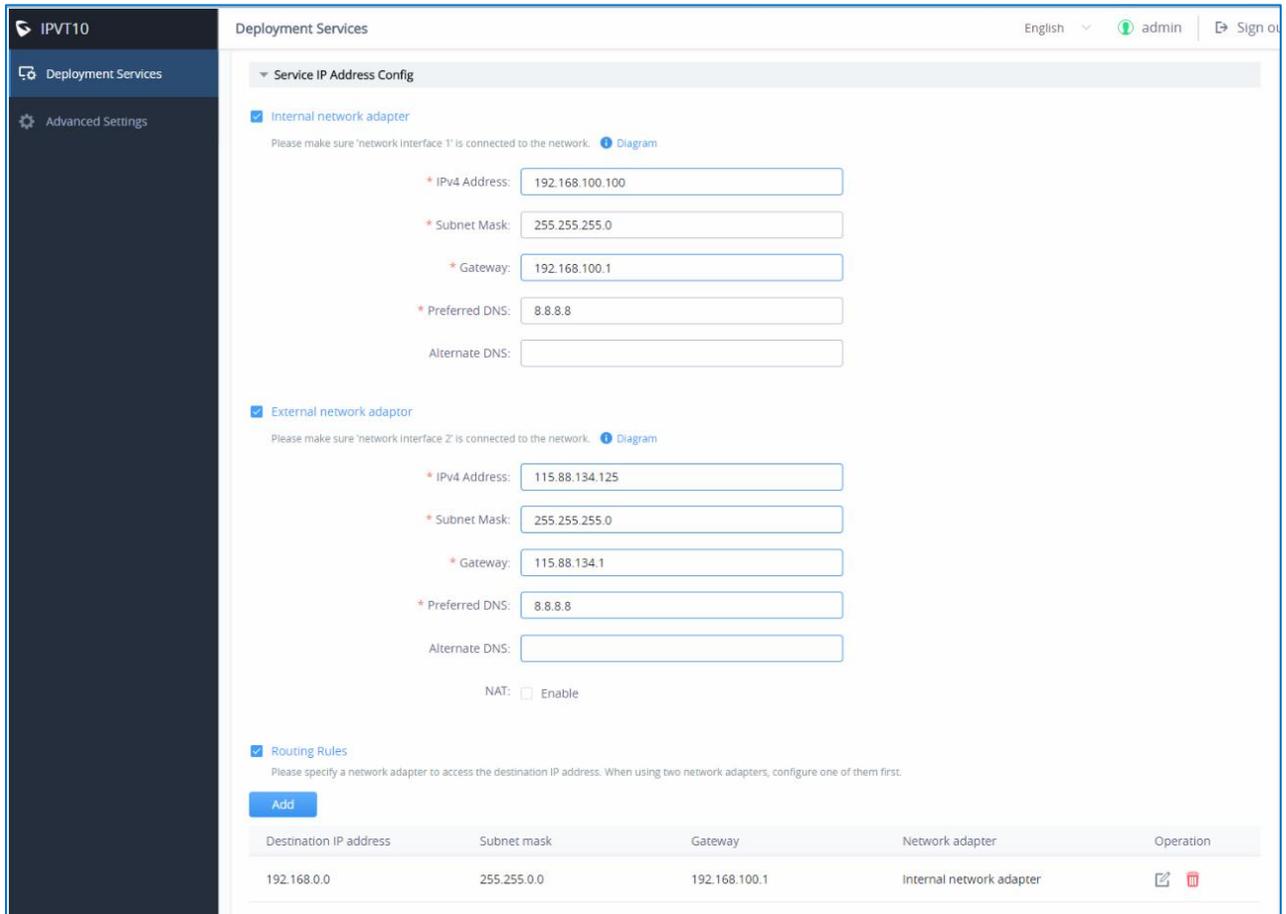


Figure 58: Configure External Network Adapter and Internal Network Adapter

Scenario 5: Internal Network and some External Users

The server is deployed on the internal network. Users could access and use the service via internal network and limit some certain public IP address to be able to access the server. In this case, users must configure 2 networks (Internal network and external network with NAT), and the routing rules. The server's private network address can be configured via static NAT to allow certain external users to access the server.

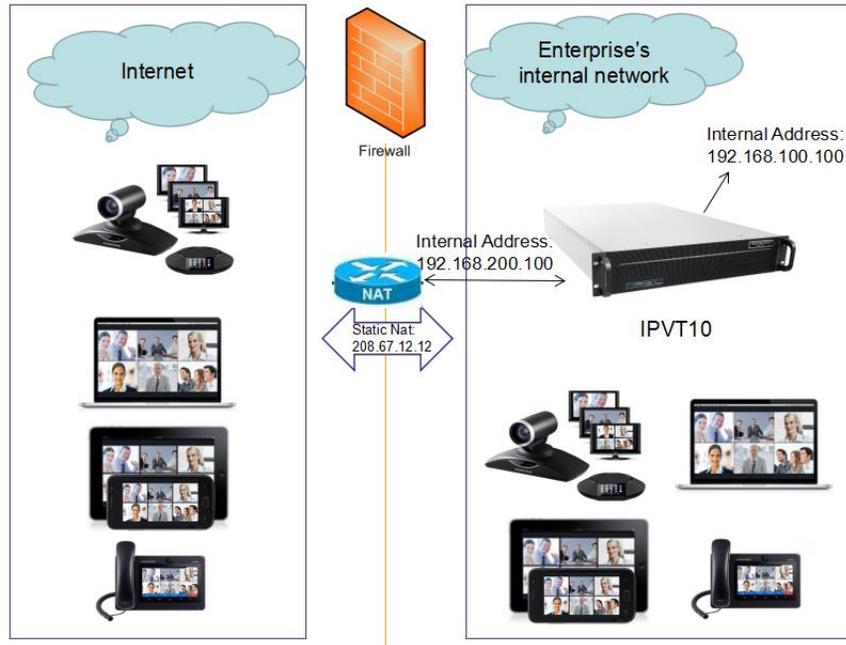


Figure 59: Network Deployment Diagram – Internal Network and Some External Users

IPVT10 Deployment Services

English admin Sign out

Internal network adaptor
Please make sure 'network interface 1' is connected to the network. [Diagram](#)

* IPv4 Address: 192.168.100.100
* Subnet Mask: 255.255.255.0
* Gateway: 192.168.100.1
* Preferred DNS: 8.8.8.8
Alternate DNS:

External network adaptor
Please make sure 'network interface 2' is connected to the network. [Diagram](#)

* IPv4 Address: 192.168.200.100
* Subnet Mask: 255.255.255.0
* Gateway: 192.168.200.1
* Preferred DNS: 8.8.8.8
Alternate DNS:

NAT: **Enable**
208.67.12.12

Routing Rules
Please specify a network adaptor to access the destination IP address. When using two network adaptors, configure one of them first.

[Add](#)

Destination IP address	Subnet mask	Gateway	Network adaptor	Operation
192.168.0.0	255.255.0.0	192.168.100.1	Internal network adaptor	Edit Delete

Figure 60: Configure External Network Adaptor and Internal Network Adaptor - II



CONFIGURE GVC32XX CONFERENCE CLIENTS

Configure Service IP Address

Before a conference starts on the GVC32xx client, the user must configure the IP address of the IPVideoTalk server. Please, refer to the following steps the IP address of IPVideoTalk.

1. Start GVC32xx device, and ensure to connect the GVC32xx client to the network correctly
2. Click on IPVideoTalk application 
3. Select “Settings” icon , and go to the configuration as shown below:
4. Input “IPVideoTalk Server” address which is the IP address of IPVT10 server.

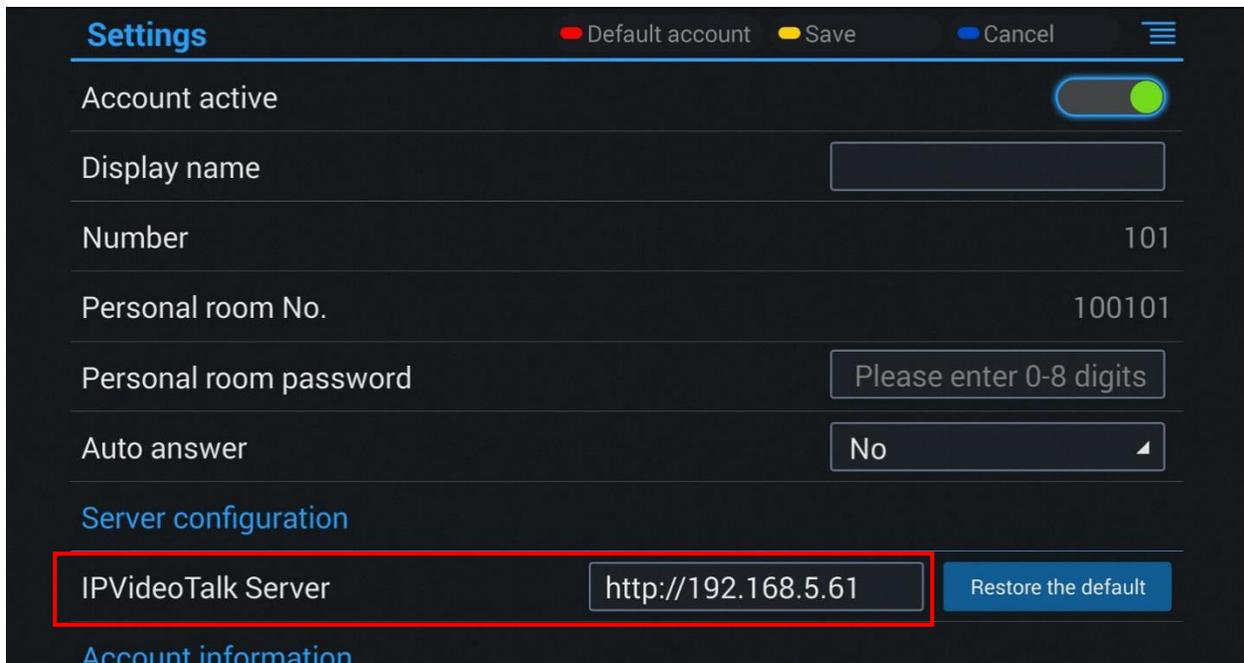


Figure 61: Configure Service IP Address

5. Click to save the configuration, and the device will connect to the IPVideoTalk server automatically. The device will be automatically assigned an IPVideoTalk ID, starting from “100”. If the IPVideoTalk ID status icon turns green, that means the account could be used normally.

START CONFERENCES

When the server is configured, users could use the conference client to start conferences.

1. Input the domain name or IP address of the IPVT10 server in the browser.

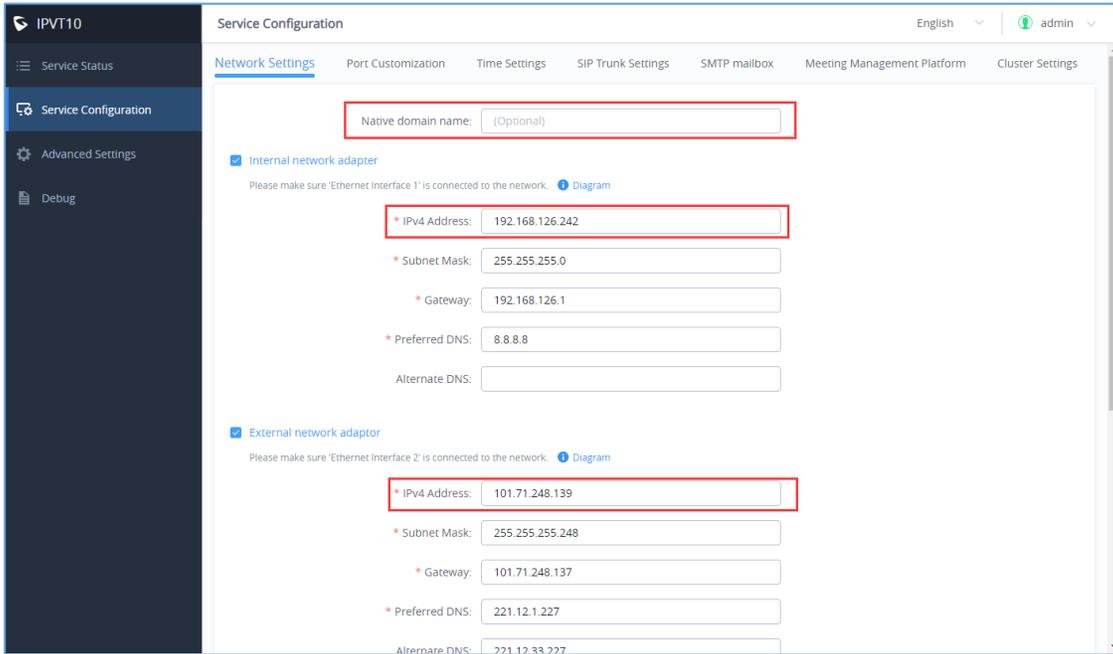


Figure 62: Service Configuration

2. Login the Conference Management Platform with the credentials (The default username and password are admin/admin, and users could configure the new username/password on IPVT10's Web UI).

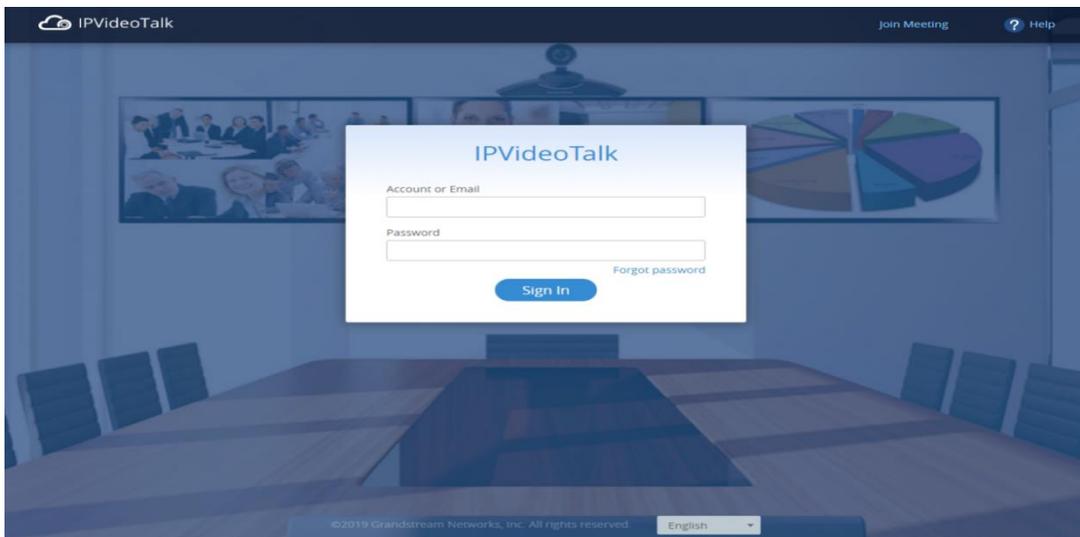


Figure 63: Login Conference Management Platform



3. Users could schedule meetings and check the meeting histories on the Meeting Management Platform, as the screenshot shows below:

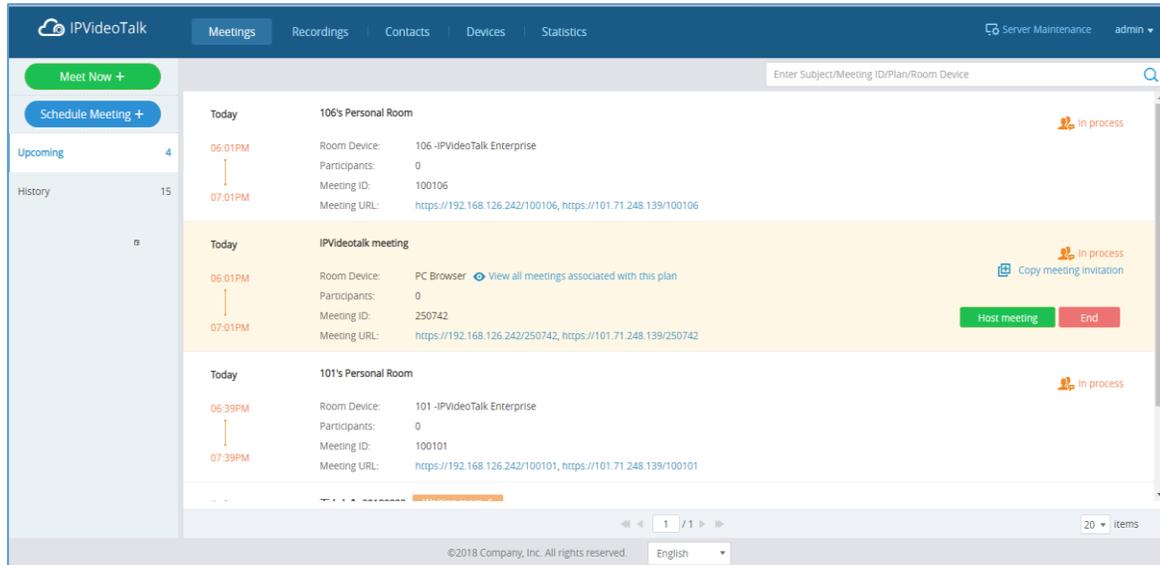


Figure 64: Manage Meeting Histories

For more information, users could go to Grandstream official website <https://www.grandstream.com/support> and download the User Guide of IPVT10 to get more details.

EXPERIENCING IPVT10 VIDEO CONFERENCING SERVER

Please visit our product website at <https://www.ipvideotalk.com> for the latest release, features instructions, FAQs, latest documentations, and latest products information.

We encourage you to browse our [product related documentation](#), [FAQs](#) and [User and Developer Forum](#) for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all your questions. Contact a technical support member or [submit a trouble ticket online](#) to receive in-depth support.

Thank you again for using Grandstream IPVT10 Conferencing Server, it will be sure to bring convenience to both your business and personal life.

