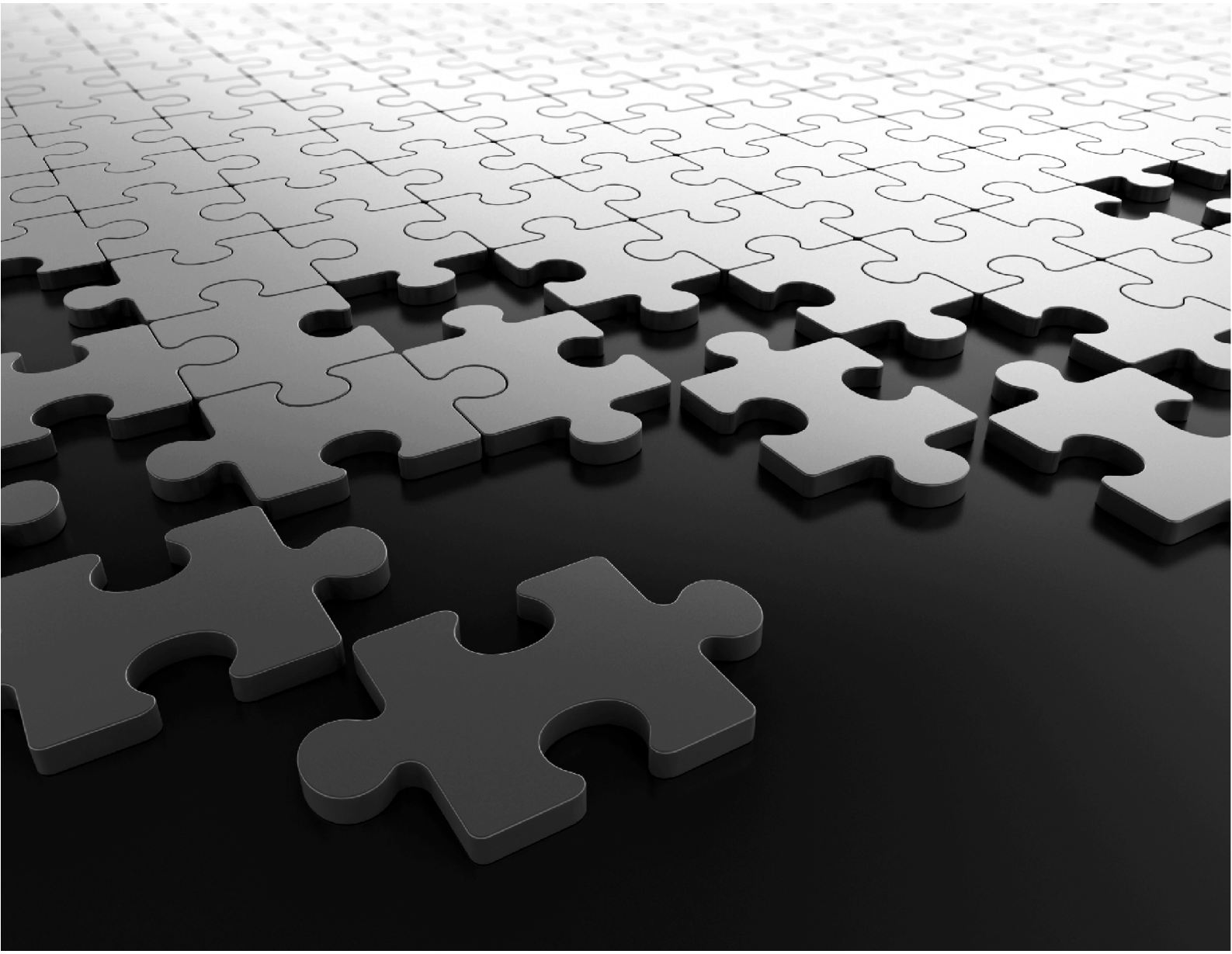
# SETU VG
# System Manual



MATRIX
TELECOM SOLUTIONS

MATRIX
TELECOM SOLUTIONS

# SETU VG

Multi-Port VoIP to GSM Gateway

## System Manual

# Documentation Disclaimer

Matrix Comsec reserves the right to make changes in the design or components of the product as engineering and manufacturing may warrant. Specifications are subject to change without notice.

This is a general documentation for all models of the product. The product may not support all the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this system manual, Matrix Comsec assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the purchaser of this product or third parties for damages, losses, costs or expenses incurred by the purchaser or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec's operating and maintenance instructions.

## Copyright



*Version 1*
*Release date: August 13, 2019*

CE RoHS COMPLIANT

# Contents

CHAPTER 1

# Introduction

## Welcome

Thank you for choosing SETU VG! We hope you will make optimum use of this intelligent, feature-packed VoIP-GSM Gateway. Please read this document carefully before installing your SETU VG.

## About this System Manual

This System Manual provides information about and instructions for installing, configuring and using the SETU VG.

You may also refer to the *SETU VG Quick Start* for quick installation. To view or download it, scan the QR Code printed on the Product Label/Packaging Label.

Both these documents—System Manual and Quick Start—are also available at: https://www.matrixtelesol.com/product-manuals.html

For product registration and warranty related details, please visit http://www.matrixcomsec.com/product-registration-form.html

SETU VG is available in two configurations—SETU VG8 and SETU VG4. This is a common System Manual for both the configurations. However, for the purpose of illustration SETU VG8 has been used throughout this System Manual, unless otherwise specified.

### Intended Audience

This System Manual is aimed primarily at **Network and System Engineers**, who will install, configure and maintain the SETU VG.

System Engineers are persons who customize the system configuration to meet the requirements of the organization/users. It is assumed that they have some experience in installing and configuring VoIP-GSM Gateways.

Part of this document containing description of features are aimed at **End Users**, who will actually use the SETU VG.

### Organization of this Document

This System Manual contains the following chapters:

**Introduction:** Gives an overview of this document, its purpose, intended audience, organization, terms and conventions used to present information and instructions.

**Know Your SETU VG:** Provides an overview of SETU VG.

**Installing SETU VG:** Contains information on how to install SETU VG and configure it using the web-based programming tool, Jeeves.

**Basic Settings:** Provides instructions for configuring the basic parameters of SETU VG, which are sufficient to get the system into operation.

**Advanced Settings:** Contains instructions for configuring the more advanced features and facilities of SETU VG.

**Features:** Describes the features of SETU VG for end users.

**Maintenance:** Provides instructions for back-up, generating reports and debugging.

**Status:** Describes the indicators of the System, Network, SIP Trunk and Mobile Ports status.

# How to Read this System Manual

This System Manual is organized in such a way that you will find all the information you need quickly and easily.

You may use the table of contents and the Index to navigate through this document to the relevant topic or information you want to look up.

Cross-references are provided in blue font with hyperlinks. You can look up the source by clicking the links.

## Conventions used in this System Manual

The following symbols have been used for notices to draw your attention to important things:

**Note:** *It indicates something that requires your special attention or it reminds you of something you need to do when you are using the SETU VG.*

**Tip:** *It indicates a helpful hint giving you an alternative way to operate the SETU VG or carry out a procedure more efficiently.*

**Caution:** *It indicates an action or condition that is likely to result in malfunction or damage to the SETU VG or your property.*

**Warning:** *It indicates a hazard or an action that will cause damage to the SETU VG and or cause bodily harm to the user.*

## Terminology used in this System Manual

In this system manual, the terms **SETU VG**, **System** and **Gateway** are used synonymously. Similarly, **SE Password**, **Login Password** and **Jeeves Password** are used synonymously.

Some of the terms specific to this document are defined below:

| Term | Usage in the document |
|---|---|
| **System Engineer (SE)** | The person who installs, configures and maintains SETU VG. |
| **User** | The person who uses SETU VG. |
| **Caller / Calling party** | The person who make calls using SETU VG. |
| **Callee / Called party** | The person to whom calls are made using SETU VG. |
| **Source / Originating Port** | A port from which a call originates. |
| **Destination / Terminating Port** | A port on which a call terminates. |

Using this System Manual, we hope, you will be able to install, operate and make optimum use of SETU VG. However, if you encounter any technical problems, please contact your dealer/reseller or Matrix Customer Care.

CHAPTER 2

# Know Your SETU VG

## Overview of SETU VG

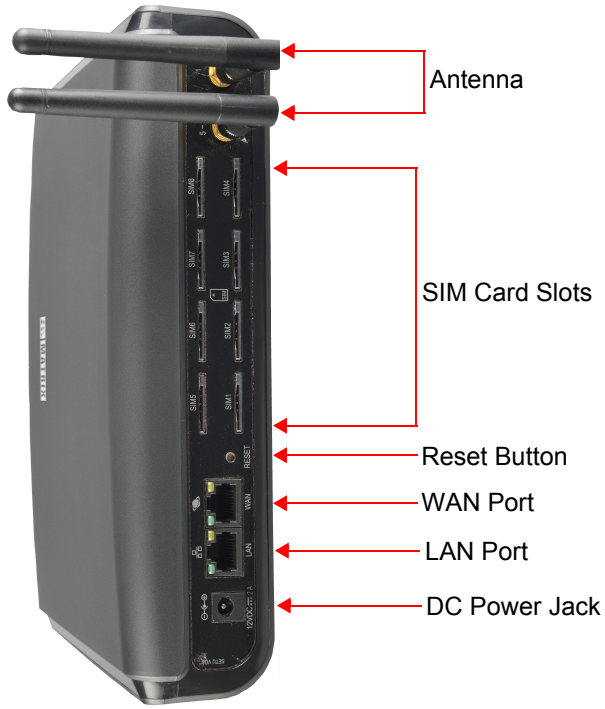
SETU VG is a gateway that provides voice services over IP network using SIP protocol. It is an effective and flexible solution for accessing internet-based telephone services and corporate intranet systems across established LAN. It is an innovative enterprise gateway that offers excellent functionality and sound quality. It supports two voice ports: Mobile and SIP.

SETU VG is available in two configurations:

- **SETU VG4** with 9 SIP Trunks and 4 Mobile Ports.
- **SETU VG8** with 9 SIP Trunks and 8 Mobile Ports.

For a complete list of Hardware and Software features, refer "Product Specifications" in the Appendix.

### Ports and Connectors



| Port | Connector | Description |
|---|---|---|
|  | SMA (Male) | To connect Antenna for the Mobile Ports. |
| SIM Card Slots (SIM1 to SIM8) | -- | To connect to GSM/UMTS[a] network. |
| Reset Button | -- | To restart the system or to restore the default LAN IP Address. |
| WAN Port | RJ45 | To connect to the IP network over a DSL Modem or Router or a LAN Switch. |
| LAN Port | RJ45 | To connect a computer or a LAN Switch. |
| 12VDC-2A | DC Jack | To connect 12VDC, 2A Power Adapter. |

*a.When the 3G module is installed in the system, you must disable Call Waiting on the SIM before inserting it into the system to prevent current calls from being disconnected.*

## LEDs

SETU VG has a **Power LED (PWR)**, a **Status LED (STS)** and eight **Port LEDs**. By default,

- In **SETU VG8**, the Port LEDs **M1 to M8** are assigned to Mobile Port 1 to Mobile Port 8 respectively.
- In **SETU VG4**, the Port LEDs **M1 to M4** are assigned to Mobile Port 1 to Mobile Port 4 respectively. The LEDs **M5** to **M8** cannot be assigned to any port.

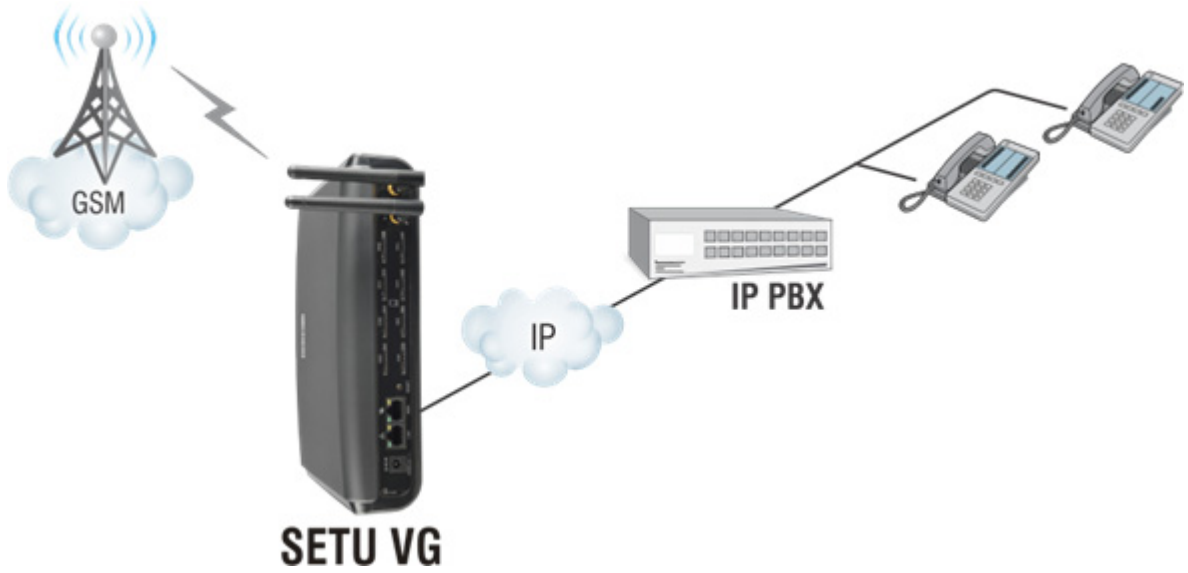
The LEDs indicate the status of the ports and various events occurring on the ports, including errors.


If required, to each port LED—**M1** to **M8** in **SETU VG8** and **M1** to **M4** in **SETU VG4**—you may re-assign a port of your choice. To know more, see “Port LED”.

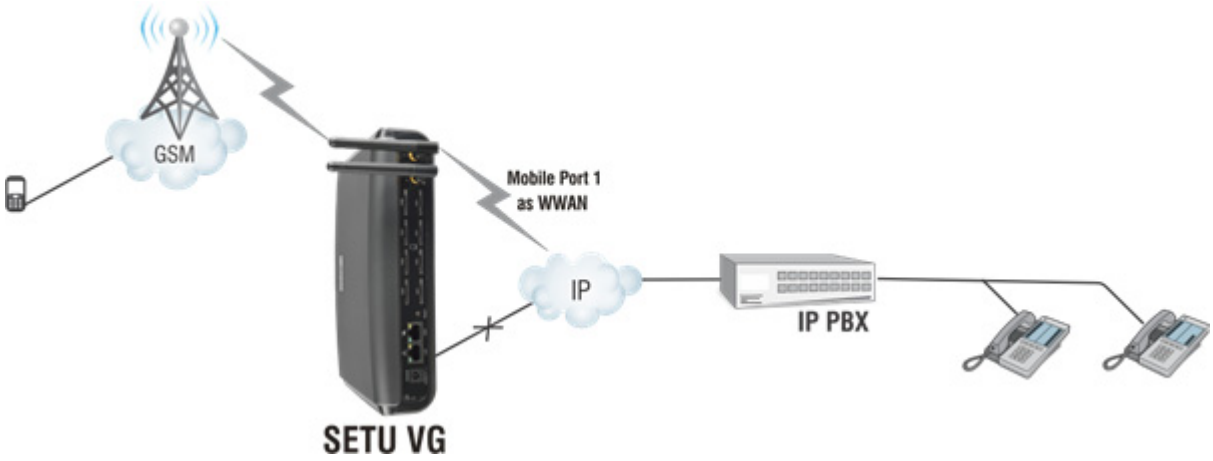
SETU VG is easy to install and operate. The built-in web server, *Jeeves*, allows you to configure the system parameters and features On-site as well as from a remote location.

# Applications of SETU VG

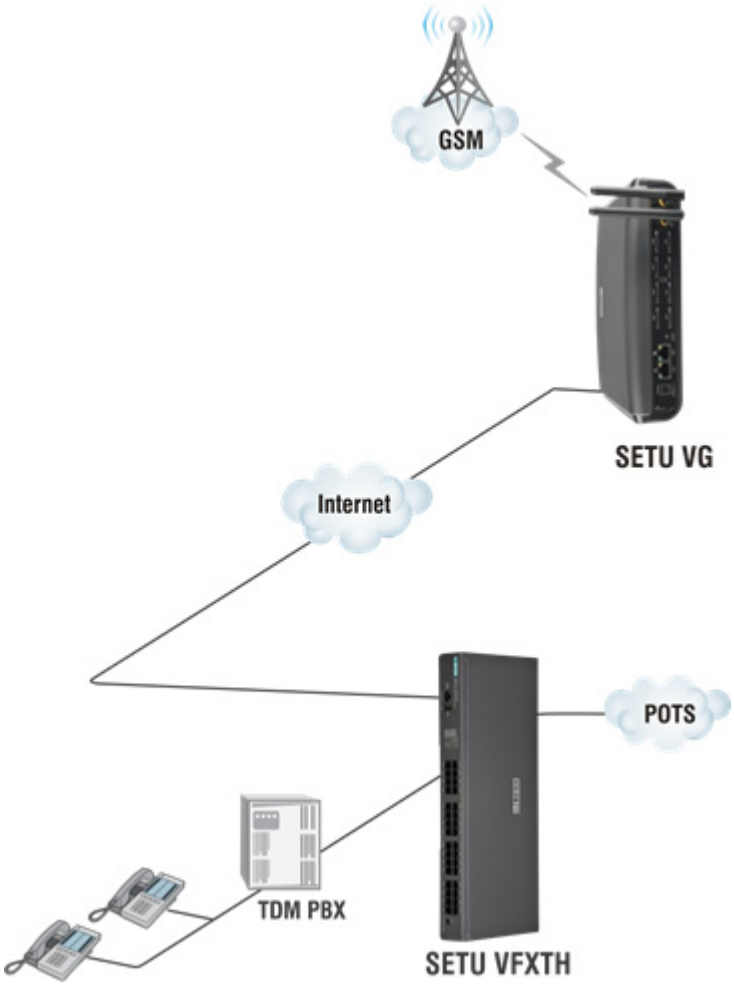
**SETU VG: GSM-VoIP Gateway for IP PBX**




**SETU VG: For Fallback Application**



**SETU VG: The Gateway using Peer-to-Peer calls for VoIP**



CHAPTER 3

# Installing SETU VG

## Before You Start

Before you begin to install and set up the hardware of SETU VG, make sure you have the following ready:

- A suitable location to install SETU VG.
- Power supply.
- A SIP Account from an ITSP to test VoIP connectivity.
- A standalone computer or a computer connected in a LAN to access Jeeves, the web-based configuration tool of SETU VG.
- Appropriate cables and connectors to set up and test the WAN interface of SETU VG and the LAN connection.
- A SIM Card to test Mobile connectivity.

Well begun is half done; plan your hardware installation well.

### Protect SETU VG and Yourself

For safe and efficient operation, observe the guidelines and all necessary safety precautions given in here. While installing and using any electronic appliance, take every safety precaution to reduce the risk of fire, electric shock and injury to persons. Read and understand all the instructions given in the manual.

- Do not install the system at any of the below locations:
    - in any area where it is directly exposed to sunlight, excessive cold or humid atmosphere.
    - any area where sulfuric gases are produced and where there are thermal springs.
    - at any place which is sensitive to vibrations or frequent and strong shocks.
    - at dusty places or places where it comes in direct contact with oil or water.
    - near any water source like a wash bowl, kitchen sink, bath tub or near a swimming pool.
    - on movable or unstable surfaces, which may cause the product to fall and get damaged.

- Always wear an electrostatic discharge preventive wrist strap or belt and use a grounding mat when handling the system.
- Unplug the system from the power outlet before cleaning. Do not use liquid cleaners, use only a dry and soft cloth.
- Do not turn on the power supply until the installation is complete.
- Never open SETU VG in power ON condition.
- Operate the system within the recommended power supply voltage range.
- Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
- Take the system to a qualified service person for repair work.
- Unplug the system from the power outlet and contact the qualified service personnel under the following conditions:
    - If liquid has been spilled onto it.
    - If it has been exposed to rain or water.
    - If it has been dropped or the cabinet has been damaged.
    - If it does not operate normally.

## Battery

SETU VG contains a 3VDC/18mAh (Li-Al) alloy-Manganese Dioxide Coin Battery (ML 1220 - Rechargeable) of diameter 12.5mm and height 2.0mm. The Battery should be replaced only by authorized dealers of Matrix. End Users must not attempt to replace it.

*There is risk of explosion if the Battery is replaced in an incorrect manner. Please dispose-off used Batteries.*

## Warning for RF Safety

This product complies with the RF exposure guidelines as per standard FCC 47 CFR part 2. We recommend that you take the following safety measures:

- Keep the RF Antenna at least 20cm away from other electronic and radio transmission devices.
- Keep the RF antenna at a place at least 20cm away from people's vicinity.
- Do not place the magnetic storage media near the system.
- People carrying medical implants like cardiac pacemakers are advised to maintain appropriate distance from the system. They are also advised to avoid being in the vicinity of the product for a long time.

# Getting Started

- Select an appropriate site to install SETU VG, considering the safety precautions listed earlier in this chapter.

- Unpack SETU VG and verify the package contents. The Package of SETU VG8 contains:
  - SETU VG Unit
  - Power Adapter - 12VDC, 2A (Country Specific)
  - Universal Converter Plug 2 PIN
  - Interchangeable Plug EU
  - Two[1] GSM Antenna with SMA Connector
  - Ethernet Cable (RJ45)
  - Two M7/30 Screws with grips
  - Wall Mounting Template
  - A Warranty Card set

  Make sure the above listed items is present in the package. In case any of these is missing or damaged, contact the dealer/distributor from whom you have purchased it.

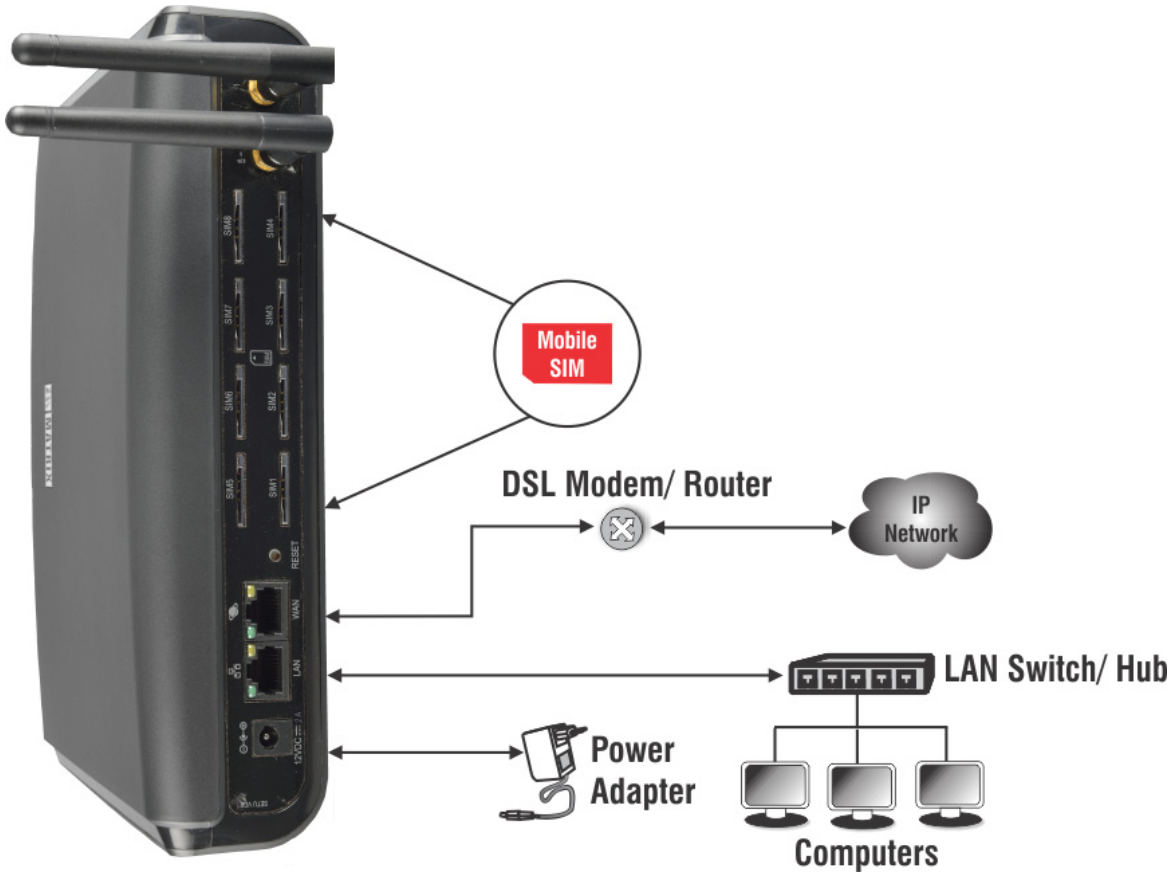
- Place the system at the selected location.

- You may mount the system on a wall. Refer the mounting template for dimensions and accordingly drill the holes on the wall.

1. *The Package of SETU VG4 contains only* one GSM Antenna with SMA Connector.

# Connecting SETU VG

SETU VG8 has a WAN Port, a LAN Port, a Reset Button, 8 Mobile Ports, 9 SIP Trunks, a Power Jack and 10 LEDs.



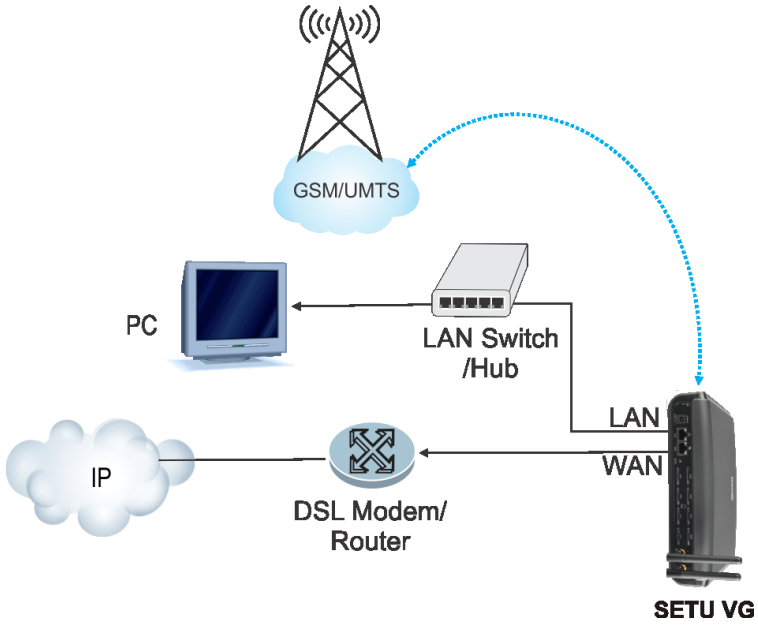

*If you are connecting a GSM Cable Antenna to the SETU VG, make sure the Antenna cable is atleast 4 inches away from the LAN and the WAN cables. It is recommended that you do not pass the Antenna cable through the duct, as it will degrade the signal strength.*

## Connecting to the IP Network

- Connect the **WAN Port** of SETU VG to the IP Network—a DSL modem/router *or* a LAN Switch—using the Ethernet cable supplied for the port.

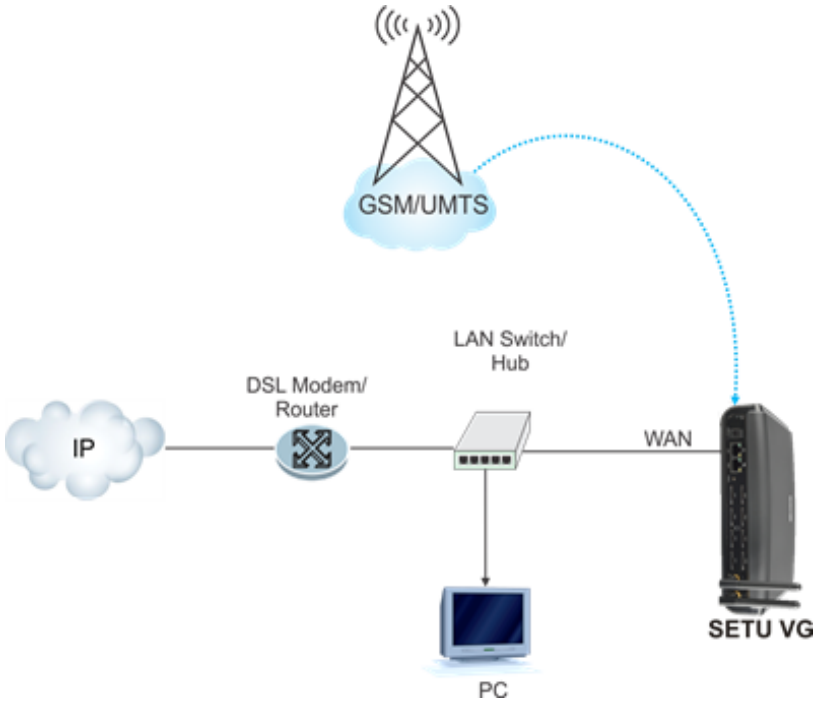
***If connecting to the Public IP Network***,

- Plug one end of the Ethernet cable into the WAN Port of SETU VG and the other end into the DSL modem/ Router.




***If connecting to a Private Network (Behind a NAT Router)***,

- Plug one end of the Ethernet cable into the WAN Port of SETU VG and the other end into the LAN Switch/ Hub.



The default IP Address of the WAN Port is: **192.168.1.100**

The default Subnet Mask of the WAN Port is: **255.255.255.0**

# Connecting to the Mobile Network

Make sure that the site where you have installed the system has sufficient network signal strength.

## Enabling SIM PIN Protection

Protect the SIM Card from unauthorized use with a Personal Identification Number (PIN) on the SIM (in consultation with the customer/owner of the SIM).

To enable SIM PIN protection,

- Get a mobile handset. Insert the SIM Card into the mobile handset.
- From the mobile handset enable PIN Protection.
- Assign a value as the SIM PIN.
- Remove the SIM Card from the mobile handset.

- *If you do not want to use PIN Protection, insert the SIM Card in the Mobile handset and disable PIN protection. Remove the SIM Card from the Mobile handset and insert it in the SIM Slot of the SETU VG.*
- *If your SETU VG has a 3G module, you must disable Call Waiting in the SIM Card before inserting it into the SIM Slot. This will prevent current calls from being disconnected whenever there is a waiting call on the Mobile Port.*

## Inserting the SIM Card

- Insert the SIM Card into the SIM Slot, with its contact side facing down.
- Push the SIM Card backwards into the slot. The SIM Card will be locked inside the slot.

*To unlock the SIM Card, push the protruded portion of the SIM Card backwards again.*

- Repeat the same steps to insert another SIM Card.
- Connect the Antenna to the Antenna Connector.

- *SETU VG supports WWAN over the Mobile Port. To use WWAN over the Mobile Port 1, you must have a 3G module installed in the system and Internet services activated on the SIM.*
- *At every power on, it takes approximate 3 minutes for the Mobile Ports to get registered with the network. Once registration with the mobile network is completed, the Mobile Port can be used.*

# Power ON SETU VG

- Connect the **Power Adapter** into the Power Jack, and plug it into a Power Outlet.
- Switch ON power supply and observe the reset cycle.

## LED Indication

At Power ON, Power LED will turn ON (Continuous Green). Other LEDs will follow the sequence summarized in the table below, during initialization.

| System Status | Color | STS | M1 | M2 | M3 | M4 | M5 | M6 | M7 | M8 | Time in MS |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Kernel UP | | OFF | OFF | OFF | OFF | OFF | OFF | OFF | OFF | OFF | |
| Application and LED Driver Loaded | Green | OFF | **ON** | OFF | OFF | OFF | OFF | OFF | OFF | OFF | |
| Few Initialization (i.e SysConfig, Resolver, SysLog etc.) | Green | OFF | **ON** | **ON** | OFF | OFF | OFF | OFF | OFF | OFF | |
| Few Initialization (i.e WebJvs, CallManager, PortCnfg etc.) | Green | OFF | **ON** | **ON** | **ON** | OFF | OFF | OFF | OFF | OFF | |
| VOPP Program Download Success | Green | OFF | **ON** | **ON** | **ON** | **ON** | OFF | OFF | OFF | OFF | |
| All Init Done, System goes Live | Green | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **1000 ms** |
| | Red | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **ON** | **1000 ms** |
| | | OFF | OFF | OFF | OFF | OFF | OFF | OFF | OFF | OFF | 1000 ms |
| | Green | **ON** | OFF | OFF | OFF | OFF | OFF | OFF | OFF | OFF | **1000 ms** |
| | | OFF | OFF | OFF | OFF | OFF | OFF | OFF | OFF | OFF | 1000 ms |
| | | (Continuous Green blinking as given in Last 2 steps) | | | | | | | | | |

During initialization, System LED (STS) will display following error/events/status:

| LED Status | Colour | Comment |
|---|---|---|
| 1 sec On (Red)<br>1 sec On (Green)<br>(Continuous) | Red and Green | VoPP program download fail. |
| 500 ms On - 500ms Off | Green | Modules not detected. |
| 1sec On - 1sec Off | Green | SETU VG started successfully.<br>Network link is Up.<br>SIP stack is Up.<br>CDR buffer is not full. |
| 500 ms On - 500ms Off -<br>500 ms On - 500ms Off -<br>500 ms On - 500ms Off -<br>500 ms On - 500ms Off (4 Blinks) | Green | Network link is down.<br>SIP stack is down.<br>CDR buffer is not full. |

| LED Status | Colour | Comment |
|---|---|---|
| 500 ms On - 500ms Off -<br>500 ms On - 500ms Off -<br>500 ms On - 1500ms Off (3 Blinks) | Green | Network link is Up.<br>SIP stack is down.<br>CDR buffer is not full. |
| 500 ms On - 500ms Off -<br>500 ms On - 500ms Off -<br>500 ms On - 500ms Off -<br>500 ms On - 500ms Off (4 Blinks) | Red | Network link is down.<br>SIP stack is down.<br>CDR buffer is full. |
| 1 sec On - 1 sec Off | Red | Network link is up.<br>SIP stack is down.<br>CDR buffer is full. |
| 500 ms On - 500ms Off -<br>500 ms On - 500ms Off -<br>500 ms On - 1500ms Off (3 Blinks) | Red | Network link is up.<br>SIP stack is up.<br>CDR buffer is full. |

During initialization, the Mobile Port LEDs will indicate the following error/event/status:

| LED Status - Cadence (in milliseconds)<br>1 cadence = 4000msec | Color | Event/State/Status |
|---|---|---|
| 500ms On- 500ms Off | Green | GSM Initialization |
| 500ms On - 500ms Off | Red | PUK Required |
| 500ms On- 500ms Off - 500ms On-500ms Off-<br>500msOn-1500ms Off (3 Blinks) | Red | SIM PIN Required |
| 500ms On - 500ms Off -<br>500ms On - 2500ms Off (2 Blinks) | Red | SIM PIN Wrong |
| 500ms On - 3500ms Off (1 Blink) | Red | SIM Absent |
| 1sec On - 1sec Off | Red | GSM Network Absent |

During normal functioning, Mobile Port LEDs will display following error/events/status:

| LED Status | Color | Event/State/Status |
|---|---|---|
| Continuous OFF | - | Port Idle/Disable |
| 400ms On - 200ms Off -<br>400ms On - 3000ms Off (2 Blinks) | Red | Incoming Ring Event |
| Continuous On | Red | Off-hook Event |
| Continuous On | Green | Speech |
| Continuous On | Green | Sending SMS/<br>Processing Balance Inquiry / Processing Balance Recharge |

You can assign any of the port LEDs to SIP Trunks, if required. To know more, see “Port LED”.

When an LED is assigned to a SIP Trunk, it will display the following error/event/status:

| LED Status | Color | Event/State/Status |
|---|---|---|
| Continuous Off | - | SIP Disable |

| LED Status | Color | Event/State/Status |
|---|---|---|
| Continuous On | Green | SIP Registered |
| Continuous On | Red | SIP Registration Failed |
| 200ms On - 200ms Off -<br>200ms On - 3400 Off (2 Blinks) | Red | SIP Authentication Failed |

When the Reset Cycle is completed, you may configure the system using the embedded web server, *Jeeves*.

# Configuring SETU VG

SETU VG provides an embedded web server with a Graphic User Interface (GUI), *Jeeves*, for configuration.

To access Jeeves, you will need to connect a computer to SETU VG.

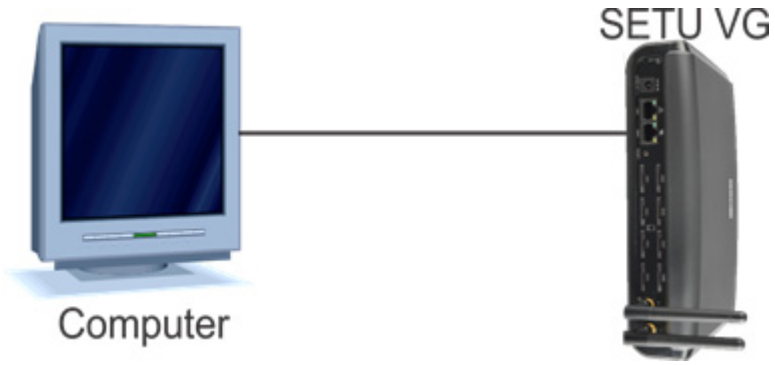
## Connecting a Computer

You may connect a standalone computer to SETU VG or grab any computer connected in the same LAN as SETU VG.

- *Connect a standalone computer to SETU VG, when installing the system for the first time. You may connect it to the LAN after you have finished installation and configuration of the system.*
- *If the computer for accessing Jeeves is connected in a LAN Switch and the WAN Port of SETU VG is connected behind a NAT router, make sure that both the LAN and WAN connections are in different Subnets.*

To connect a standalone computer,

- Plug one end of the Ethernet cable supplied with the system into the LAN Port of SETU VG. Plug the other end into the LAN Port of the computer.




- Make sure, the IP Address of the computer and the LAN Port of SETU VG do not conflict and that both are in the same Subnet.

  The default IP Address of the LAN Port of SETU VG is: **192.168.2.100**

  The default Subnet Mask of the LAN Port of SETU VG is: **255.255.255.000**

  Change the Subnet of the computer, if necessary.

- Make sure a Web-browser, either Internet Explorer version 7 or later *or* Mozilla Firefox version 3.5 or later, is installed on the computer.

- Open the browser on the computer.

- In the address bar of the browser, enter the default IP address of the LAN Port: **192.168.2.100**.


- The **Login** page will open.
- In **Login Password**, enter ***1234***, the default Password.
- Click the **Login** button.


On successful login, the **Home** page of Jeeves opens.

*Before you start configuring the system, if you wish to view or download the SETU VG Quick Start, you can scan the QR Code present on the login page of Jeeves.*

The left navigation bar shows the links **Basic Settings**, **Advanced Settings, Maintenance** and **Status**.


**Basic Settings** break down the complexities of configuration and are sufficient to get your system into operation.

**Advanced Settings** enable you to configure the advanced features and facilities of SETU VG.

**Maintenance** allows you to carry out system maintenance and monitoring activities like uploading/ upgrading firmware and configuration, system debug, system restart.

**Status** allows you to view the system details and the status of all the ports.

You may now configure the Basic Settings of SETU VG.

CHAPTER 4

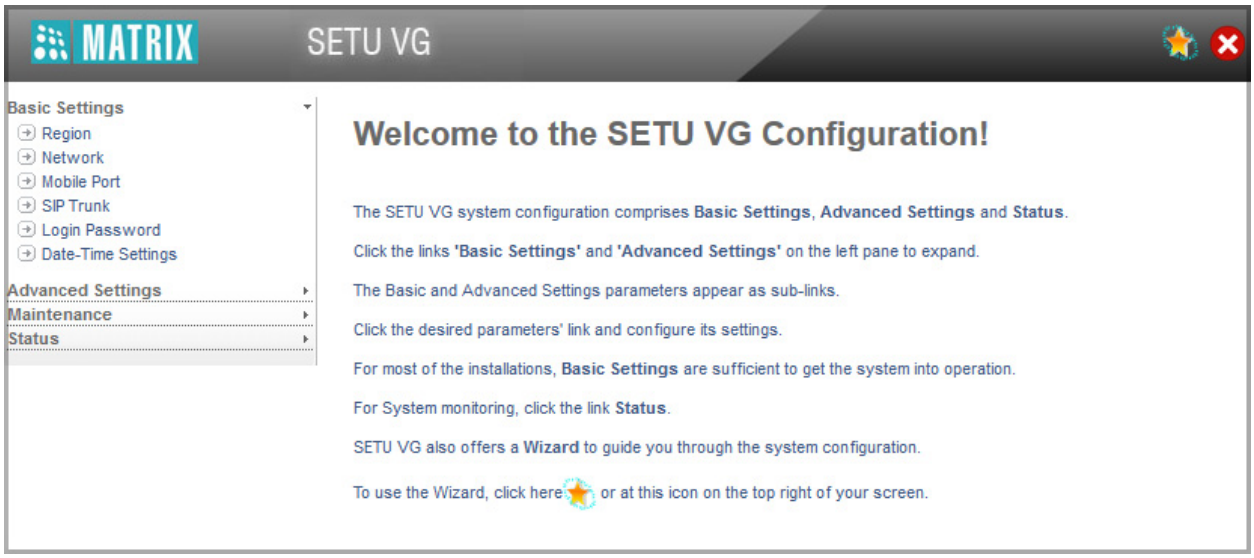
# Basic Settings

The Basic Settings enable you to configure SETU VG for basic functions. You will be able to operate and use the system efficiently, when you configure the Basic Settings.

To configure Basic Settings,

- Click the **Basic Settings** link.

  The links to the different basic parameters appear on the left navigation bar.




  There are two ways to configure Basic Settings.

  - Using the **Wizard**. The Wizard will guide you step-by-step through the configuration.

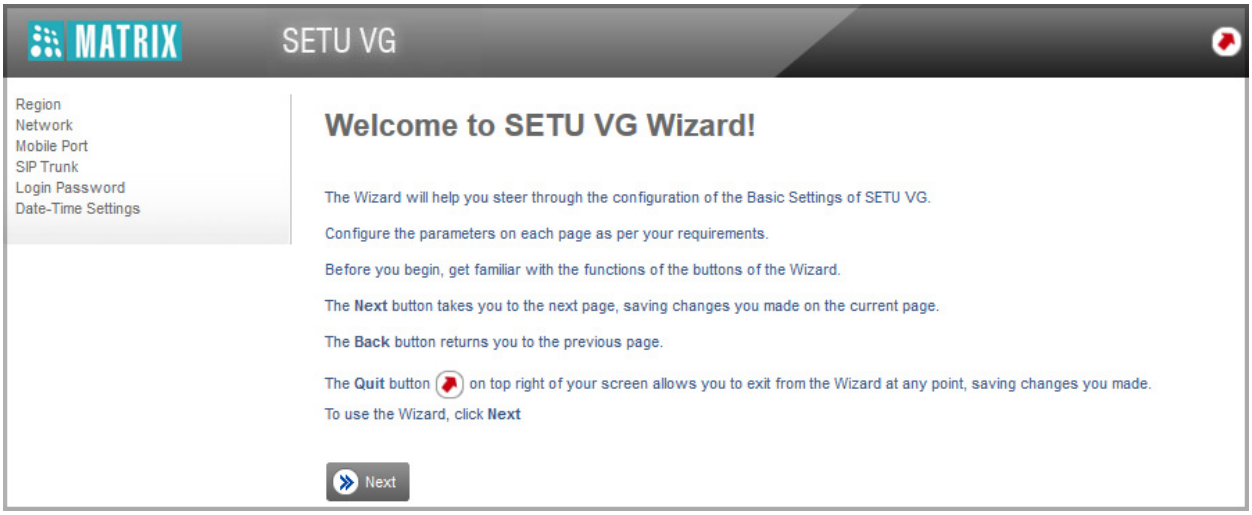
  Or

  - Selectively configuring the Basic Settings parameters, by clicking each link on the left navigation bar.

  To use the **Wizard**,

  - Click the **Wizard** icon on the top right of your screen.

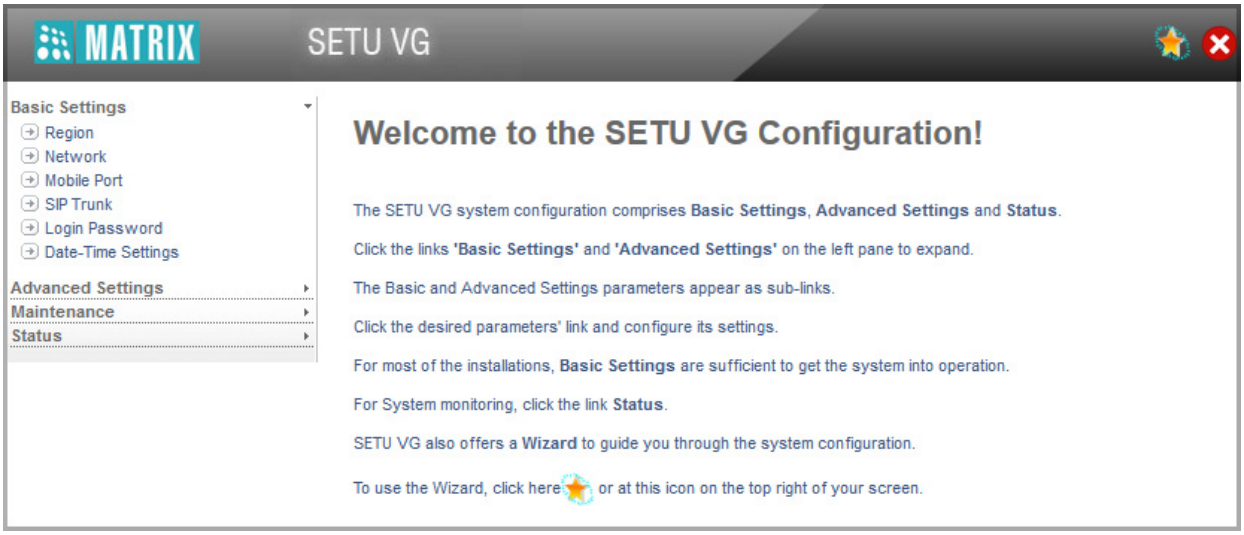
- The welcome page of the Wizard opens.




- Get familiar with the functions of the following buttons of the Wizard before you begin to use them.
  - **Next:** Takes you to the next page, saving the changes you made on the current page.
  - **Back:** Returns you to the previous page.
  - **Expand** : Expands a parameter link to display all parameters under the link.
  - **Collapse** : Collapses a link; hides all parameters under the link.
  - **Settings** : Enables you to configure / edit the settings of a parameter further or to edit an entry or a record.
  - **Default:** Assigns factory set values to all the parameters on the page.
  - **Add:** Enables you to add a new record.
  - **Delete:** Enables you to delete a record.
  - **Close:** Enables you to exit a window.
  - **Copy:** Enables you to copy the parameters of a port to another port.
  - **Quit** : Enables you to exit the Wizard at any stage, saving changes you made before exiting.

To use **Selective Configuration**,

- Click the **Basic Settings** link to expand.




- Click the sublink of the required parameter: **Region**, **Network, Mobile Port**, **SIP Trunk**, **Login Password** and **Date-Time Settings**.
- The selected parameter page opens.
  - Click **Expand** to expand a link and display all parameters under the link.
  - Click **Collapse** to collapse a link and hide all parameters under the link.
  - Click **Settings** to configure / edit the settings of a parameter further.
  - Click the **Submit** button to save changes made on the page.
  - Click the **Default** button to assign factory set values to all the parameters on the page.
  - Click the **Add** button to add a new record.
  - Click the **Delete** button to delete a record.
  - Click the **Close** button to exit a window.
  - Click **Logout** to end the login session and exit Jeeves. You will return to the login page of Jeeves.
- Set the parameters on the page to the desired values and click **Submit** to save.

You may either use the Wizard or selectively configure the Basic Settings pages, whichever works best for you.

This chapter provides instructions for *selective* configuration of the Basic Settings pages.

- Click the **Basic Settings** link to expand.
- The following links appear under Basic Settings:
  - Region

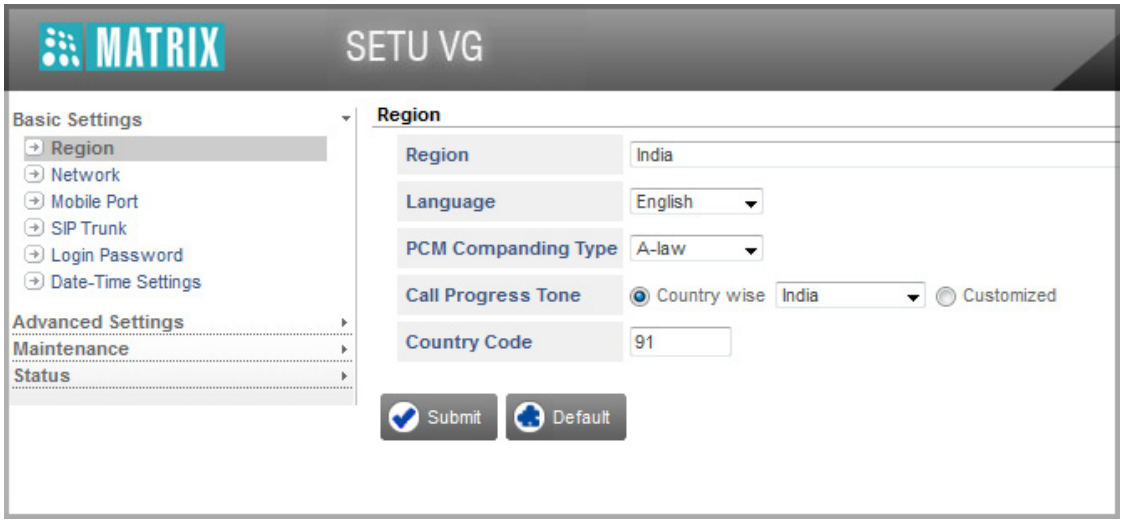
- Network
- Mobile Port
- SIP Trunk
- Login Password
- Date-Time Settings

Each of these is explained in detail in the following.

# Region

To configure Region and other region specific parameters,

- Click the **Region** link.




## Region

- In the **Region** list, click the name of the country where SETU VG is installed. Default: India.

  When you change Region, an alert message will appear on the screen **"Changing Region shall assign default values to all parameters of the system. Do you want to continue?"** Click OK. All country specific parameters will be assigned default values. See "Default Region Table" in the Appendix for country specific default values.

## Language

- In the **Language** list, click the language in which you want the pages of the GUI, Jeeves, to be presented.

  SETU VG can display the pages of the GUI, Jeeves, in English, Italian, Spanish, French, German, and Portuguese. Default: English.

  When you login in again later, all the pages of the GUI will appear in the language you have selected.

  You can also select a Language of your choice on the Login page of Jeeves; however, the language you select on the Login page will be applied for the current session only.

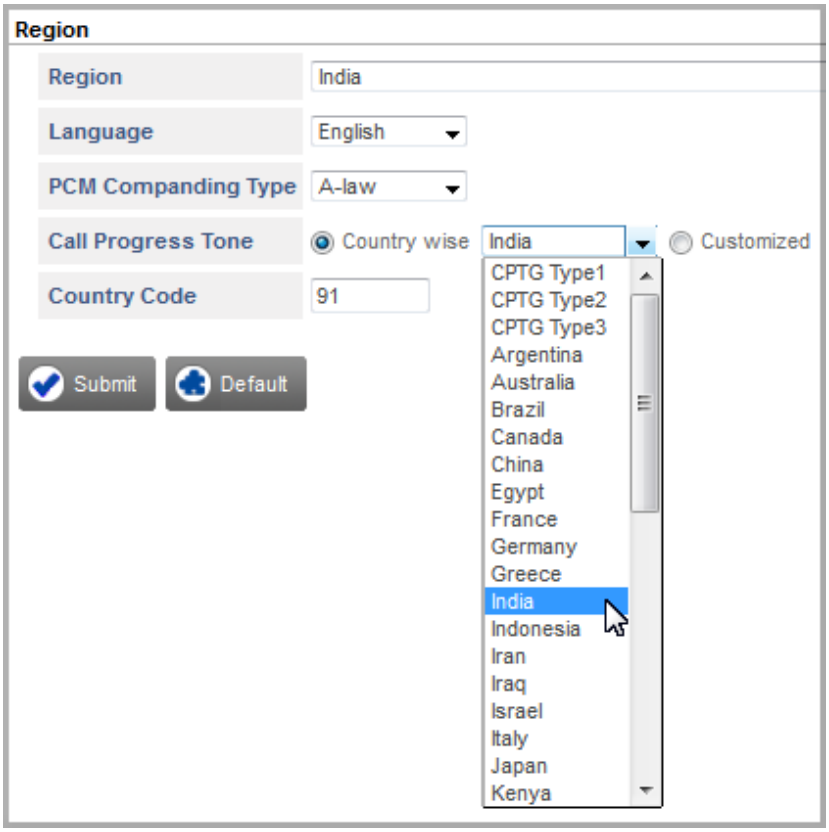
## PCM Companding Type

- If required, you may change the **PCM Companding Type—**A-law or μ–law—set automatically by SETU VG according to the Region you have selected. Default: A-law (for India).

## Call Progress Tones

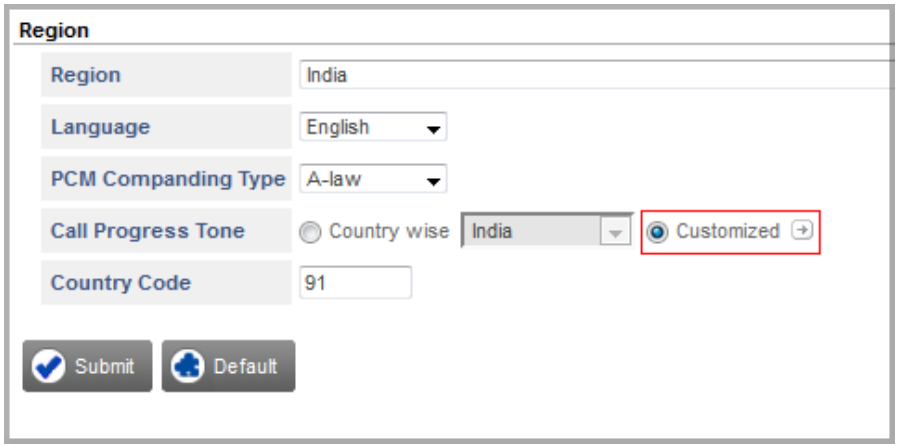
- Select **Call Progress Tone**. SETU VG supports country specific Call Progress Tone Generation (CPTG) to simulate the same tones of the local PSTN to which it is connected. The “Call Progress Tones” supported by the SETU VG for different countries is presented in the “Appendix”.

    - To match the call progress tone of the country where SETU VG is installed, select the **Countrywise** option and select the Country from the list box. Default: India.

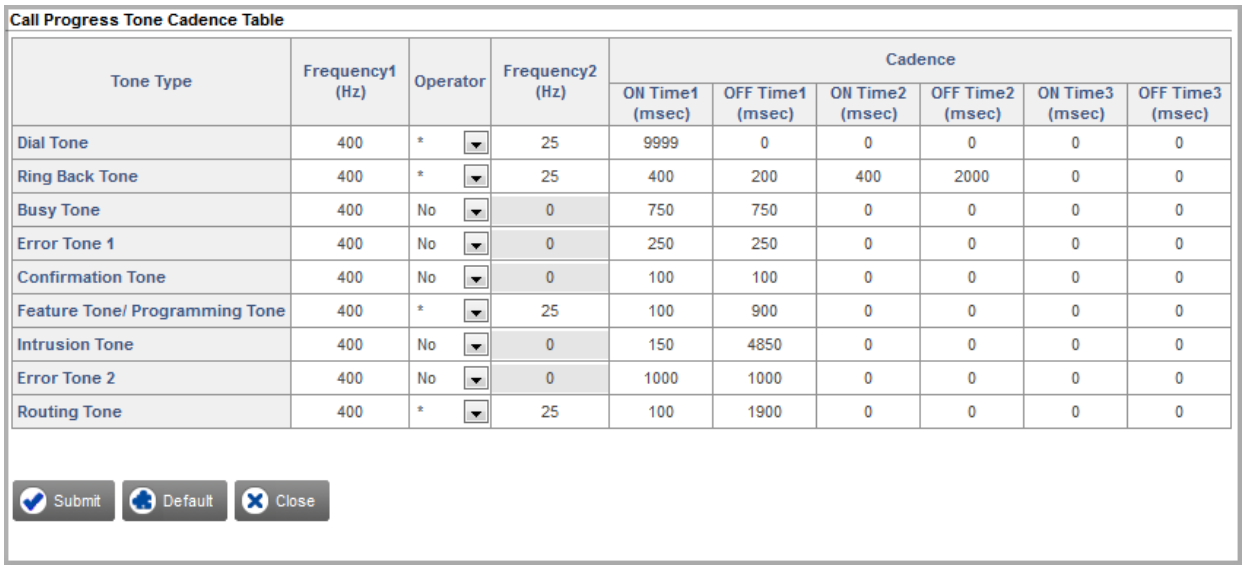



    - If you want to change the cadence of the Call Progress Tones as per your requirement, select the **Customized** option.

- To customize the Call Progress Tones cadence, click **Settings** .




- The **Call Progress Tone Cadence Table** opens.




| Tone Type | Frequency1 (Hz) | Operator | Frequency2 (Hz) | Cadence | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | ON Time1 (msec) | OFF Time1 (msec) | ON Time2 (msec) | OFF Time2 (msec) | ON Time3 (msec) | OFF Time3 (msec) |
| Dial Tone | 400 | * | 25 | 9999 | 0 | 0 | 0 | 0 | 0 |
| Ring Back Tone | 400 | * | 25 | 400 | 200 | 400 | 2000 | 0 | 0 |
| Busy Tone | 400 | No | 0 | 750 | 750 | 0 | 0 | 0 | 0 |
| Error Tone 1 | 400 | No | 0 | 250 | 250 | 0 | 0 | 0 | 0 |
| Confirmation Tone | 400 | No | 0 | 100 | 100 | 0 | 0 | 0 | 0 |
| Feature Tone/ Programming Tone | 400 | * | 25 | 100 | 900 | 0 | 0 | 0 | 0 |
| Intrusion Tone | 400 | No | 0 | 150 | 4850 | 0 | 0 | 0 | 0 |
| Error Tone 2 | 400 | No | 0 | 1000 | 1000 | 0 | 0 | 0 | 0 |
| Routing Tone | 400 | * | 25 | 100 | 1900 | 0 | 0 | 0 | 0 |

Configure the following parameters:

- **Frequency1 (Hz):** Configure frequency1 in this field. The range of frequency1 is 300-1400 Hz for all tones.
- **Frequency2 (Hz):** Configure frequency2 in this field. The range of frequency2 is 20-1400 Hz for all tones.
- **Operator:** Operator parameter has three options:

  **1) No:** If *No* is programmed, Frequency2 will not be applicable.

  **2) * (Modulation):** If *'*' (Modulation)* is programmed, Frequency1 and Frequency2 will be used as modulation (F1 * F2).

  **3) + (Addition):** If *'+' (Addition)* is programmed, Frequency1 and Frequency2 will be used as addition (F1 + F2).

- **Cadence:** Program Cadence ON Time1-OFF Time1, ON Time2-OFF Time2 and ON Time3-OFF Time-3 for all tones. Valid ON Time and OFF Time range for all tones is 0000-9999 msec.

*The Call Progress Tone will not be set to default when the system is set to default.*

- Click **Submit**.
- Close the window to return to the **Region** page.

*When you submit the page after changing the Region or PCM Companding Type or Call Progress Tone, an alert message will appear "Submitting this page will restart the system. Do you want to continue? Click OK. SETU VG will restart and your changes will be saved.*

## Country Code

- If required you may change the **Country Code**, set automatically by SETU VG for the Region you have selected. Default: 91 (India).

  If you have kept **Remove Country Code from CLI received** check box enabled in the System Parameters, the system will remove the Country Code configured here from the CLI received on the source port.

- Click the **Submit** button to save.

# Network

SETU VG may be installed typically, in a Public IP Network or in a Private network, behind a NAT Router.

When SETU VG is installed in a Public IP Network,

- the WAN Port of SETU VG is connected to a Broadband Router/Modem.
- Public IP is assigned to the WAN Port.

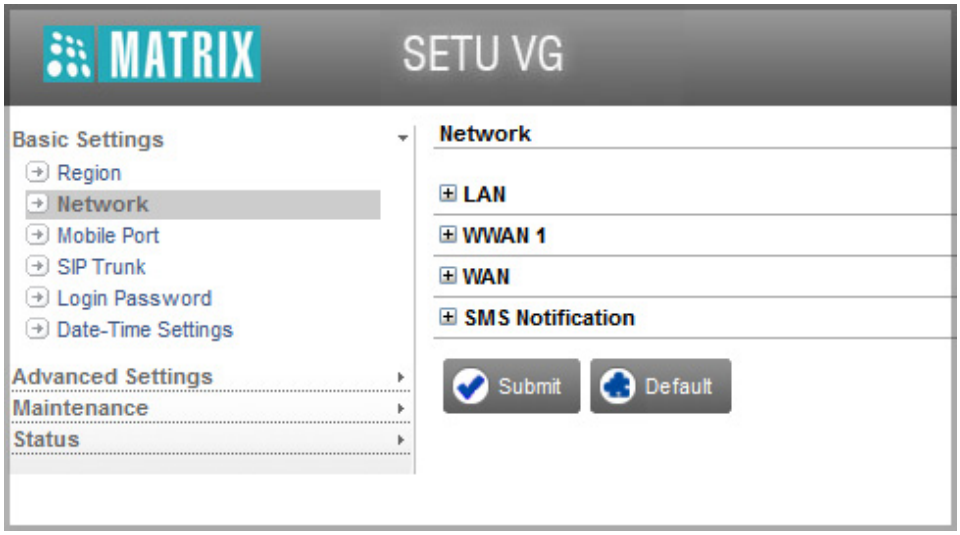
When SETU VG is installed in a Private Network, behind a NAT Router,

- the WAN Port of SETU VG is connected to the LAN Switch/Hub.
- Private IP is assigned to the WAN Port.

Depending on your installation scenario, configure the Network Port Parameters.

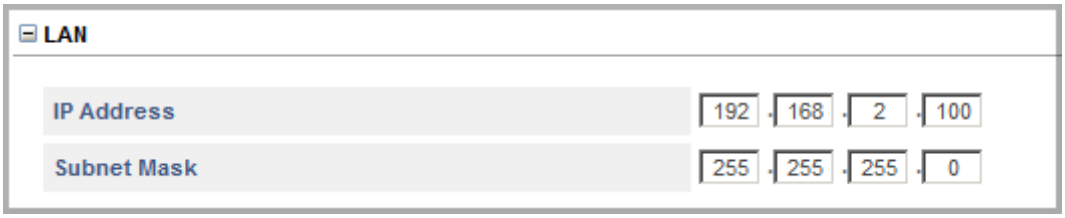
To configure Network parameters,

- Click the **Network** link. The Network Parameters page opens.




## LAN

- Click **LAN** to expand.




- In **IP Address**, the current IP Address of the LAN Port is displayed. Default: **192.168.2.100**
- In **Subnet Mask**, the current Subnet Mask of the LAN Port is displayed. Default: **255.255.255.000**

  If required, you may change the LAN Port IP Address and Subnet Mask.

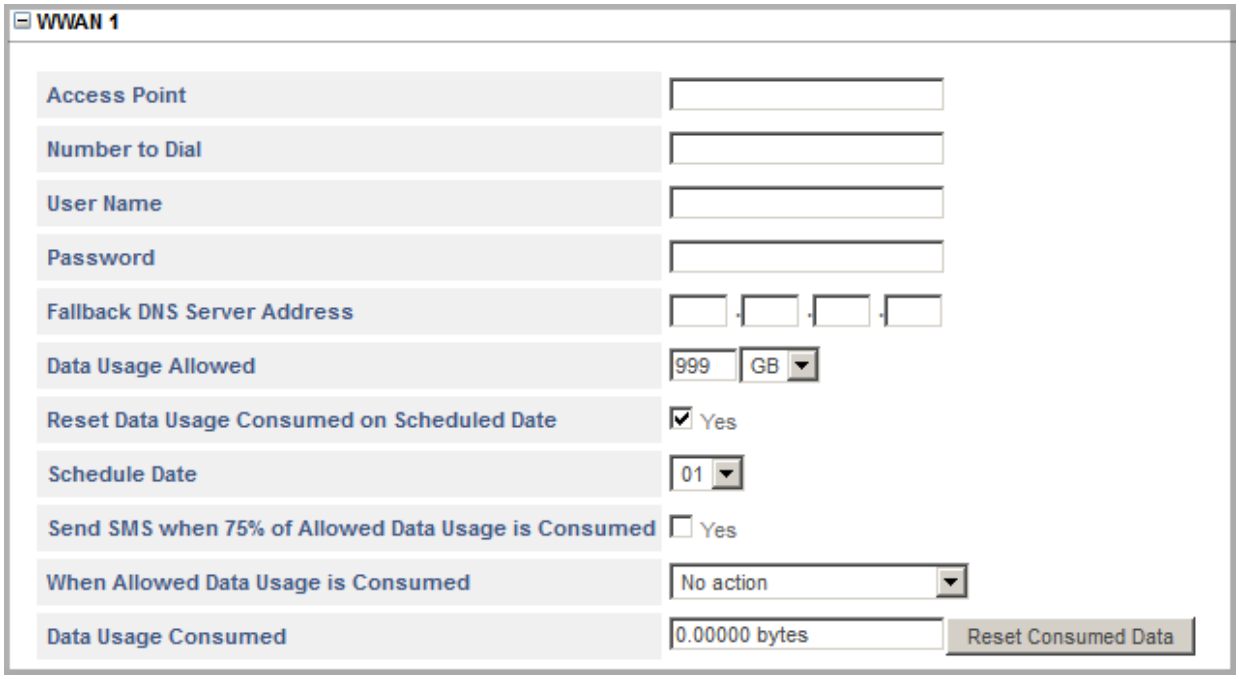
*When your SETU VG is installed in a Private Network, make sure the LAN Port and the WAN Port are connected in different subnets.*

## WWAN (Wireless WAN)

If you are using the Mobile Port 1 of SETU VG as your WAN interface, configure WWAN.

*SETU VG supports WWAN connection on Mobile Port 1 only.*

- To configure WAN interface on Mobile Port 1, click **WWAN 1** to expand.




- Enter the following information:
  - In **Access Point**, enter the access point provided by your Service Provider.
  - Enter the **Number to Dial** provided to you for the internet service by your Service Provider.
  - Enter the **User Name** provided to you for accessing the internet service by your Service Provider.
  - In **Password**, enter the authentication password for the User ID provided by your Service Provider.
  - When we configure the Mobile Port as the WAN interface, the system fetches the DNS Server Address of the Service Provider for connectivity. In the **Fallback DNS Server Address**, enter the DNS Server Address that you want the system to use, when the DNS Server Address of the Service Provider fails to provide connectivity.
  - In **Data Usage Allowed**, enter the data usage as per the scheme provided by your Service Provider. Default: 999 GB.

- Clear the **Reset Data Usage Consumed on Scheduled Date** check box, if you do not want SETU VG to reset the data usage consumed on a particular date. Default: Enabled. The system will automatically reset the value of data usage consumed on a Scheduled Date.

    - In **Schedule Date**, configure the date on which you want the system to reset the data usage consumed. Default: 01.

- Select the **Send SMS when 75% of Allowed Data Usage is Consumed** check box, if you want SETU VG to send SMS to the pre-configured numbers, when 75% of the allowed data usage is consumed. Default: Disabled.

  If you have enabled this parameter, make sure you have configured the mobile numbers in **Send SMS if 75% of Allowed Data Usage is Consumed** under “SMS Notification”.

- You may select one of the following actions to be taken by SETU VG, **When Allowed Data Usage is Consumed**.
    - No action
    - Disconnect
    - Send SMS
    - Send SMS and Disconnect

  Default: No action.

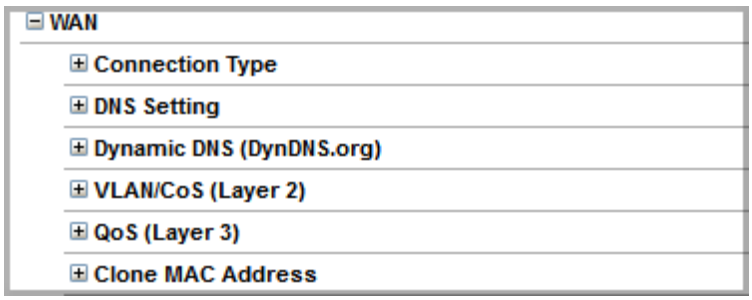
  If you select **Send SMS** or **Send SMS and Disconnect** option, make sure you have configured the mobile numbers in **Send SMS if Allowed Data Usage is Consumed** under “SMS Notification”.

- Total Data consumed on a Mobile Port is displayed in the **Data Usage Consumed** field.

- To reset the Data Usage Consumed manually, click the **Reset Consumed Data** button.

# WAN

- Click **WAN** to expand.



## Connection Type

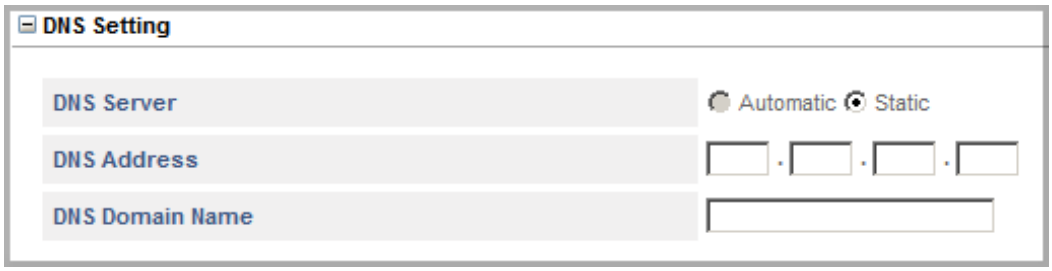
- Click **Connection Type**.


- Select the network connection type, that is, the IP Addressing Scheme used by your network to assign the IP address to the WAN Port: Static, DHCP, PPPoE. Default: Static.
    - **Static:** If your network uses Static IP addressing, select Static and configure the following parameters.
        - **IP Address:** Enter the IP Address you obtained from your Network Administrator for the WAN Port of SETU VG in this field. Make sure that the IP Address does not conflict with that of any other device on the LAN. Default: 192.168.1.100
        - **Subnet Mask:** Enter the Subnet Mask you obtained from your Network Administrator for the WAN Port in this field. Default: 255.255.255.0
        - **Default Gateway:** Enter the IP Address of the Router's LAN Interface as the Default Gateway IP Address.
    - **DHCP:** Whenever SETU VG is restarted, the DHCP server will dynamically assign an IP Address, Subnet Mask and Gateway Address to the WAN Port, if your network uses DHCP Addressing. You have to configure the Domain Name Server (DNS) Address only, if not already provided by your Internet Service Provider.
    - **PPPoE:** If your network uses PPPoE addressing, the PPPoE server will automatically assign an IP Address, Subnet Mask and Gateway Address to the WAN Port of SETU VG. You need to configure the following parameters provided by your Internet Service Provider:
        - **PPPoE User ID:** Enter the User Name provided by the Internet Service Provider. The User ID may be a maximum of 64 characters.
        - **PPPoE Password:** Enter the User Password provided by the Internet Service Provider. The password may be a maximum of 64 characters.
        - **PPPoE Service Name:** Enter the Service Name, if provided by your Internet Service Provider. The Service Name may consist of a maximum of 64 characters. If Service Name is not provided, leave this field blank.

## DNS Server

Configure the Domain Name Server (DNS) settings as provided by your Internet Service Provider. You may consult your Network Administrator in this regard.

- Click **DNS Setting**.




- Select **DNS Server** as **Automatic** or **Static** according to the Connection Type (IP Addressing scheme) used by the network.

  - Select **Static** if:
    - your network uses Static IP Addressing.
    - your network uses DHCP or PPPoE, but the DHCP/PPPoE server does not provide DNS Address automatically.

    If your network does not assign DNS Address automatically, set DNS Address Assignment as **Static** and enter the DNS Server Address in the **DNS Address** field. Enter **DNS Domain Name**, if provided to you by your Network Administrator.

  - Select **Automatic** if:
    - your network uses DHCP or PPPoE IP Addressing.
    - the DHCP/PPPoE server of your network assigns the DNS Address automatically.

## Dynamic DNS (DynDNS.org)

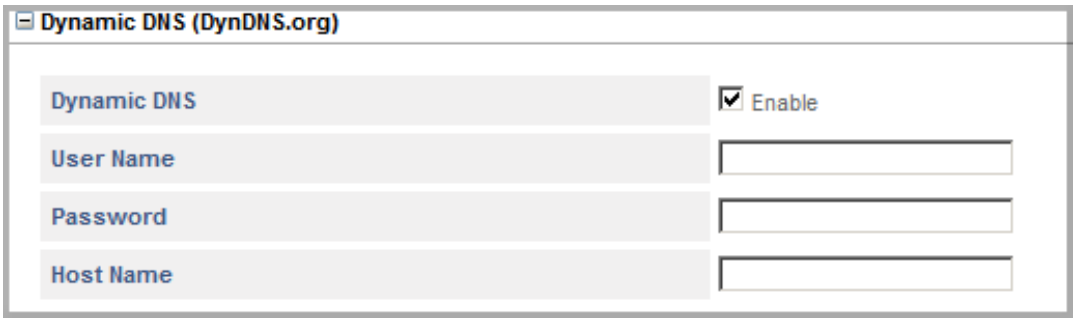
Dynamic DNS (DDNS) is a service that maps internet domain names to IP addresses. DDNS Service Provider provides the host name/domain name to the internet devices and also embeds DDNS client in the internet device. By doing so, whenever a new IP Address is assigned to the internet host, the DDNS client running in the internet host updates its new IP address in the Dynamic DNS server.

When the WAN Port of SETU VG is assigned a dynamic IP, its new IP Address needs to be updated regularly with the various devices or networks which utilise the WAN Port settings to function. Dynamic DNS resolves this by mapping a domain name to the WAN Port IP Address, which SETU VG can update in the Dynamic DNS Server.

Once the IP Address of the system is updated in the DNS server, any caller on the IP network can reach the system by dialing the host name/domain of the system.

SETU VG supports Dynamic DNS Server client of the Service Provider Dynamic DNS.org. To use this service, you must first register with DynDNS.org and then do the following:

- Click **Dynamic DNS (DynDNS.org)**.

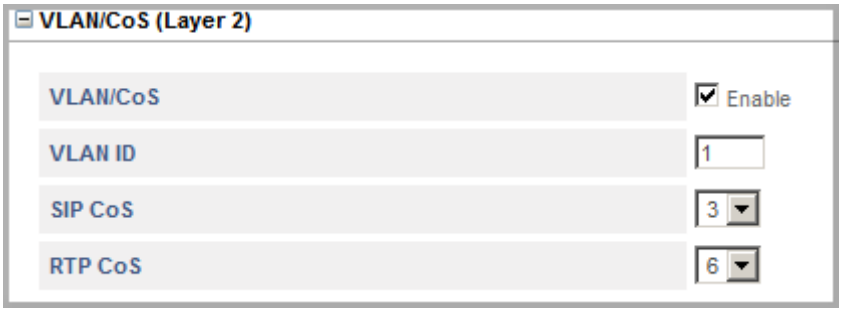



- Select the **Dynamic DNS Enable** check box.
- Enter the **User Name** you created on DynDNS.org. The name can be of maximum 40 characters.
- Enter the **Password** you created for the User Name on DynDNS.org. The password can be of maximum 24 characters.
- Enter the **Host Name** you created on the DynDNS.org here. The Host Name can be of maximum 40 characters.

## VLAN/CoS

If SETU VG is connected in a VLAN, configure the **VLAN/CoS**. This parameter enables the SETU VG to add VLAN header to the packets generated by it. The VLAN header consists of the VLAN ID (12-bit) and Class of Service (CoS, 3-bit) for prioritization of traffic[2].

- Click **VLAN/CoS (Layer 2)**.




- Select the **VLAN/CoS** check box to enable VLAN ID tagging on all packets generated by the system. Default: Disabled.
- Enter the **VLAN ID** that you have assigned to the VLAN in which the SETU VG is connected. The valid range for this is 0-4094. Default: 1.
- For **SIP CoS**, define the CoS (priority) bits which will be added in all SIP packets. The range of CoS bits is from 0 to 7. Default: 3.

2. *The IEEE 802.1P standard allows Layer2 switches to prioritize the traffic, thus providing Quality of Service (QoS), i.e. better handling of data that pass over a network, thereby resulting in greater reliability and quality. Quality of Service (QoS) on Layer2 is referred to as Class of Service (CoS) which is defined by IEEE 802.1P.*

- For **RTP CoS**, define the CoS (priority) bits which will be added in all RTP packets. The range of CoS bits is from 0 to 7. Default: 6.

### QoS (Layer 3)

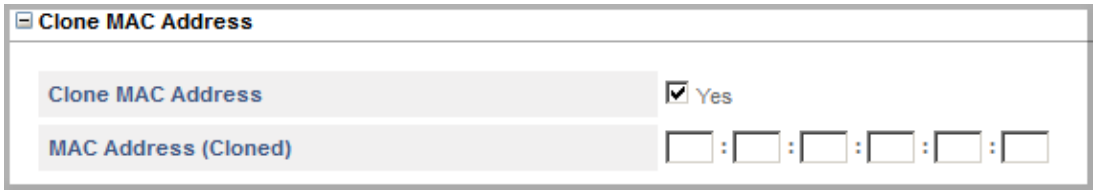
- Click **QoS (Layer 3)**.


- SETU VG will send all SIP messages using SIP QoS setting, enter the **SIP DiffServe/ ToS** as per your requirement. The valid range is from 00-63, Default: 26.

- SETU VG will send all the RTP packets with RTP QoS setting, enter the **RTP DiffServe/ ToS** as per your requirement. The valid range is from 00-63, Default: 46.

### Clone MAC Address

- Click **Clone MAC Address**.




- If you want to clone the MAC address, select the **Clone MAC Address** check box.

  In the **MAC Address (Cloned)** field, enter the desired MAC address you want to clone in hexadecimal format, e.g. 00:50:c2:55:b0:10.

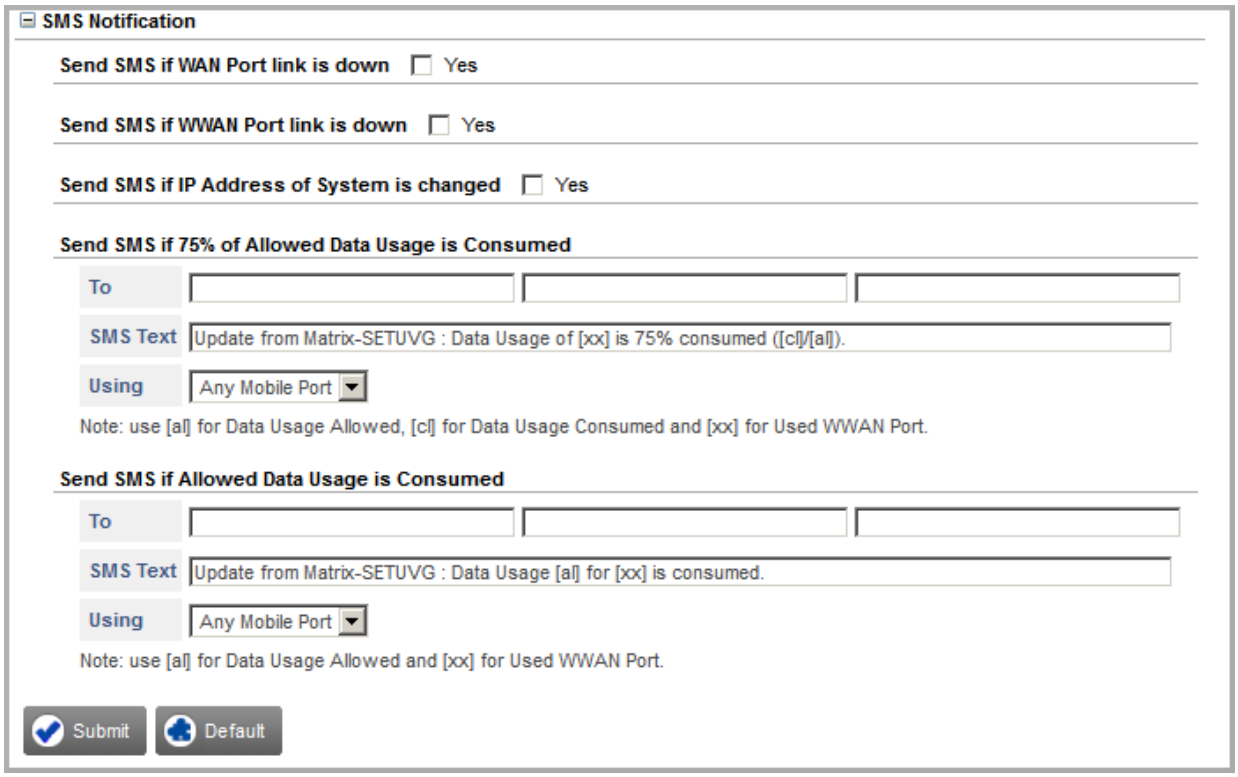
## SMS Notification

SETU VG supports Notification via Short Message Service (SMS) to inform you of the following conditions and events:

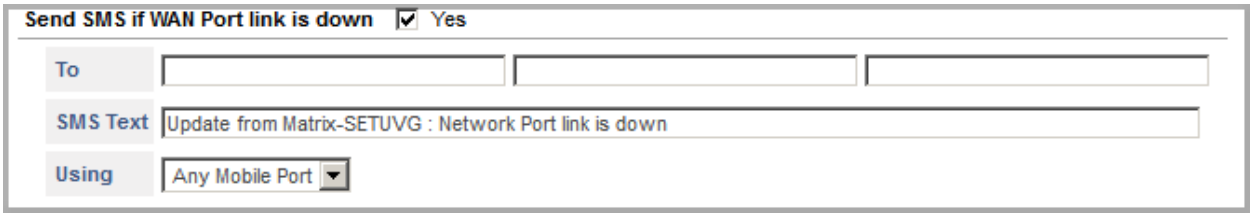
- When the WAN Port or WWAN Port link is down.
- Whenever there is a change in the IP Address of the system.
- SIM Balance Inquiry.
- Call Minutes Consumed.
- Data Usage Consumed.

To use SMS Notification,

- Click **SMS Notification**.

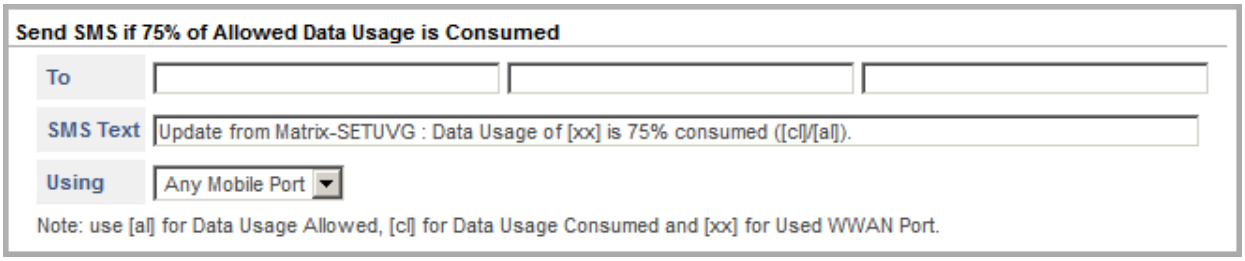



- To request SMS Notification for **WAN Port Link** Status, select the **Send SMS if WAN Port link is down** check box.

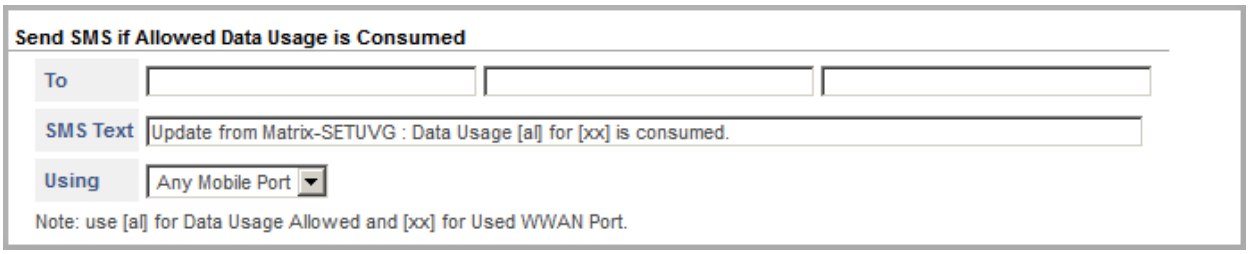



- In the **To** fields, you may enter up to 3 Mobile Numbers to which the SMS should be sent. The numbers can be a maximum of 24 characters. The characters allowed are 0-9, *, # and +.
- In the **SMS Text** field, enter the text you want to be sent in the Notification.The text length can be a maximum of 80 characters.
- In the **Using** box, select the Mobile Port number which the system should use to send the SMS.
- Click **Submit** to save.
- Similarly, configure the parameters for:
  - **Send SMS if WWAN Port link is down**
  - **Send SMS if IP Address of System is changed**

- If you want SETU VG to send SMS to notify that 75% of Allowed Data Usage is consumed, configure the following parameters.




- In the **To** fields, you may enter up to 3 Mobile Numbers to which the SMS should be sent. The numbers can be a maximum of 24 characters. The characters allowed are 0-9, *, # and +.
- In the **SMS Text** field, enter the text you want to be sent in the Notification.The text length can be a maximum of 80 characters.
- In the **Using** box, select the Mobile Port number which the system should use to send the SMS.
- Click **Submit** to save.
- If you want SETU VG to send SMS to notify that the Allowed Data Usage is consumed, configure the following parameters.




- In the **To** fields, you may enter up to 3 Mobile Numbers to which the SMS should be sent. The numbers can be a maximum of 24 characters. The characters allowed are 0-9, *, # and +.
- In the **SMS Text** field, enter the text you want to be sent in the Notification.The text length can be a maximum of 80 characters.
- In the **Using** box, select the Mobile Port number which the system should use to send the SMS.
- Click **Submit** to save.

To request SMS Notification of *SIM Balance Inquiry*, see “SIM Balance Inquiry” under “Mobile Port”.

To request SMS Notification for *Call Minutes Consumed*, see “Call Minutes” under “Mobile Port”.

When you finish configuring all the Network parameters as per your requirement,

- Click **Submit**.
- You will get this message **“Ongoing calls would be disconnected. Do you want to submit this page?”**

- Click **Yes** to save your settings.

## Restoring Default LAN IP Address

You can restore the Default LAN IP Address using the Reset Button. To do so,

- Press the Reset button for more than four seconds.
- Release the Reset button.

The LAN IP Address will be restored to default, **192.168.2.100**

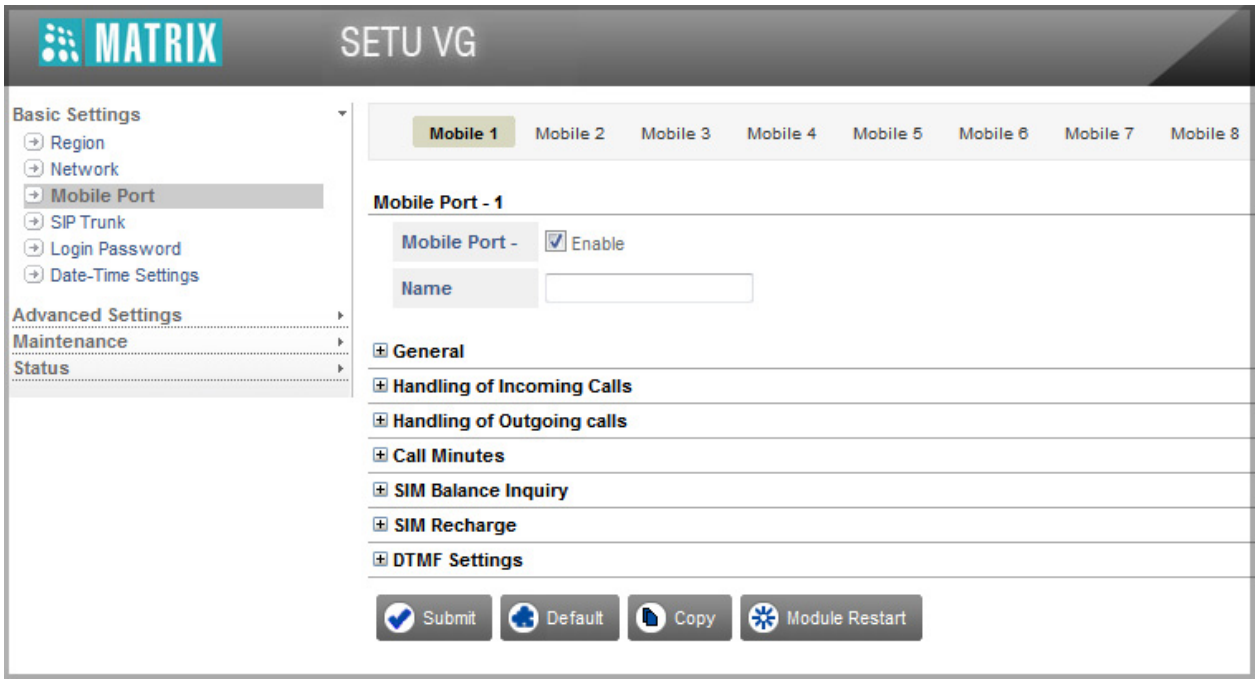
- *If you press the Reset button for less than four seconds, SETU VG will restart.*
- *Along with the LAN IP Address, a few other parameters will also be set to default. See "Restoring Default Settings using the Reset button" for details.*

# Mobile Port

SETU VG8 supports eight Mobile Ports and SETU VG4 supports four Mobile Ports.

To configure a Mobile Port,

- Click the **Basic Settings** link to expand.
- Click the **Mobile Port** link.

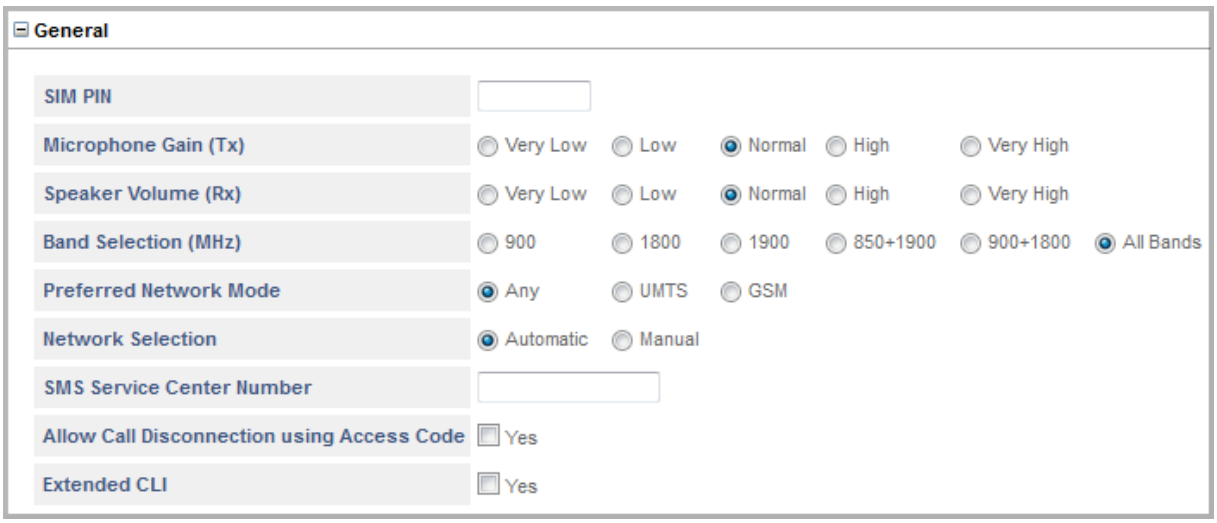



- Click the required Mobile Port number tab from **Mobile 1** to **Mobile 8**, to configure the Mobile Port parameters.
- Keep the **Mobile Port** enabled.

  Clear the **Mobile Port Enable** check box, only if you do not want to use this port. Default: Enabled.
- You can assign a **Name** to each Mobile Port. The name will be displayed as CLIP during incoming calls. The Name can be of maximum 12 characters. Default: Blank.

# General

- Click **General**.




- If you have enabled SIM PIN protection on the SIM Card, in the **SIM PIN** field, enter the same SIM PIN value (4 to 8 digits). Default: Blank.

*SIM PIN is not set to default or does not change, if SETU VG is set to default or when you upgrade/ downgrade firmware.*

- You can adjust the **Microphone Gain (Tx)** Gain of the Mobile Port to improve the audibility of the transmitting speech from SETU VG. Select the desired Tx Gain from these options: **Very Low, Low, Normal**, **High** and **Very High**. Default: Normal.

- You can adjust the **Speaker Volume (Rx)** of the Mobile Port to improve the audibility of incoming speech. Select the desired Rx Gain from these options: **Very Low**, **Low**, **Normal**, **High** and **Very High**. Default: Normal.

- The Frequency **Band Selection (MHz)** supported by the GSM networks varies from country to country. The frequency bands supported by SETU VG are:
  - 900
  - 1800
  - 1900
  - 850+1900
  - 900+1800
  - All Bands

  You can select the Frequency Band used by the GSM Service Provider(s) in the country where SETU VG is installed.

  For instance, select 850 + 1900 GSM frequency band for countries which support both 850 and 1900 MHz frequencies for GSM network. Similarly, set 900 + 1800 frequency band for countries that support 900 or 1800 GSM frequency band.

  Default: All Bands.

- If your SETU VG has a UMTS Mobile Port, the SIM Card of this port will get registered with either GSM (2G) or UMTS (3G) network, whichever is available. You can select the Network with which the SIM should be registered by setting the **Preferred Network Mode**.

  If the SIM you have installed in the UMTS Mobile Port supports both GSM and UMTS services, but you want the SIM to get registered with one of these networks, you can restrict the SIM registration with a particular network by setting the Preferred Network Mode. You may select the Preferred Network Mode from the options:

  - **Any:** The SIM gets registered with the UMTS (3G) network. When the UMTS network is unreachable, the SIM gets registered with the GSM (2G) network automatically.
  - **GSM:** The SIM gets registered with GSM (2G) network only.
  - **UMTS:** The SIM gets registered with UMTS (3G) network only.

    Default: Any.

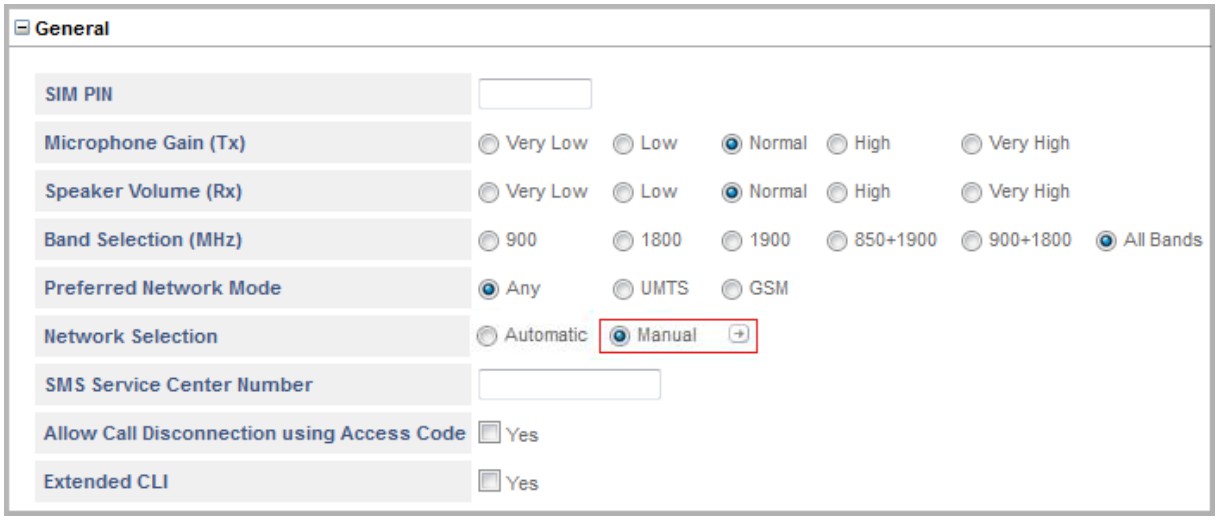
  If your Mobile Port supports GSM only, do not change the default value of this parameter.

- Set the **Network Selection** mode as **Automatic** or **Manual**. Default: Automatic.

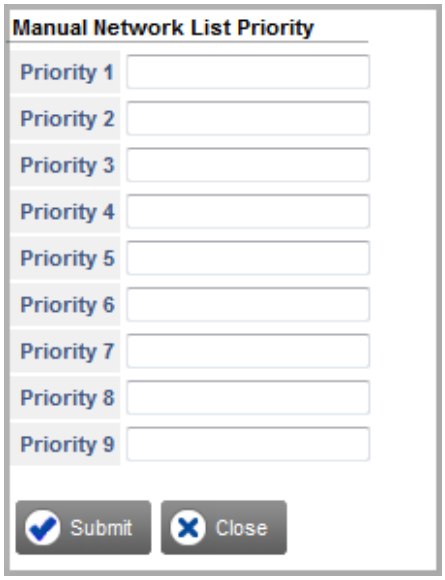
  - Select **Automatic**, if you want the Mobile Port to automatically locate and register with the Network that supports the SIM card. At each power on, the SIM in the Mobile Port will automatically register with the Network.
  - Select **Manual**, if you want the Mobile Port to select the network operator from a list of network operators configured in the order of priority. For this, you need to configure the list of network operators in the **Manual Network List Priority**. Whenever the SIM registers with the network, it will select the Network Operator from this list, according to order of priority you have set.

    To apply **Manual** Network Selection,

    - Select **Manual** and then click **Settings** .



- The **Manual Network List Priority** window opens.




  - In the Priority levels, **Priority1** to **Priority 9**, enter the Network Operator Codes with which you want the SIM to register, as per your preference.

    The Network Operator Code may consist of a minimum of 5 digits and a maximum of 8 digits. Default: Blank.

- Enter the **SMS Service Center Number**, as provided to you by the service provider. This number is used by the system while sending SMS notifications.
- To enable the feature Disconnect Call using Access Code on the Mobile Port, select the **Allow Call Disconnection using Access code** check box. To know more about this feature, see “Disconnecting a Call using Access Code”.
- Select the **Extended CLI** check box if the CLI of the current incoming call displays the last caller’s CLI. When the flag is enabled, the current caller’s CLI will be displayed. By default, it is disabled.
- Click the **Submit** button to save your entries.
- Close the window to return to the main page.

# Handling of Incoming Calls

- Click **Handling of Incoming Calls**.


- If you do not want to route calls received on this Mobile Port, select **Block all calls received on this Mobile Port** check box. Default: Disabled.

## Destination Number Determination

Select the desired destination number determination method for routing incoming calls *with* and *without* CLI.

- To **Route all Incoming calls (with CLI)** on the Mobile Port, you may select from any of these methods:
  - without any Destination Number
  - to the Fixed Destination Number
  - on the basis of Calling Party Number
  - after Answering the Call and Collecting the Digits
    Default: after Answering the Call and Collecting the Digits.

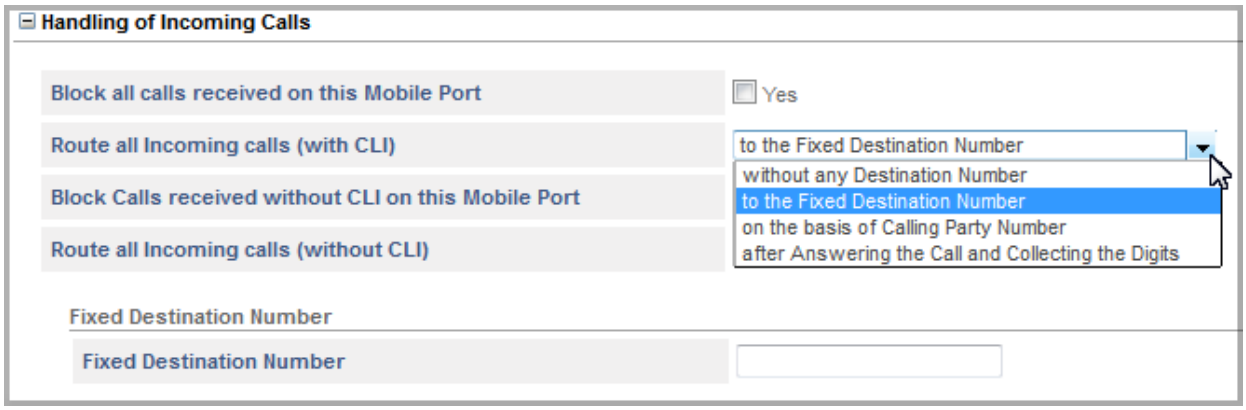
### *Route Calls without any Destination Number*

In this method, all calls received on the Mobile Port are directly routed to a fixed destination port, configured for this port, irrespective of the Destination Number.


- To apply this method, in the **Route all incoming calls (with CLI)** list, click **without any Destination Number**.

### *Route to the Fixed Destination Number*

In this method, calls received on the Mobile Port are routed to a fixed destination number, which is configured for the Mobile Port.




To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, click **to the Fixed Destination Number**.
- In the **Fixed Destination Number** box that appears, enter the desired destination number. The Destination Number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and . (dot). Default: Blank.
- Click **Submit** to save your settings.

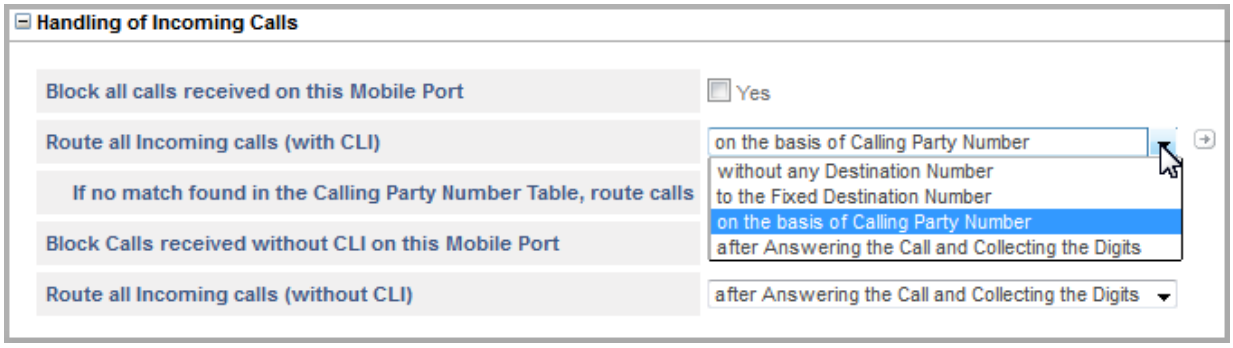
### *Route on the basis of Calling Party Number*

In this method, a call received on the Mobile Port is routed to a specific number, as per the calling party's number. You must configure the calling party numbers in the Calling Party Number Based Table.

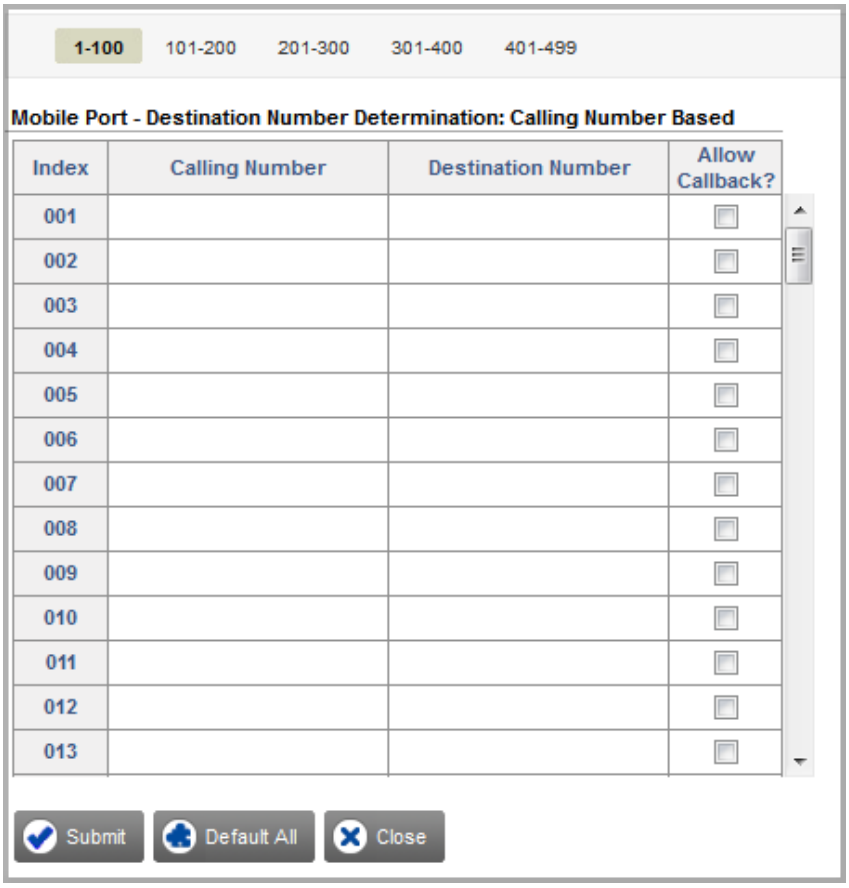
When there is an incoming call on the Mobile Port, SETU VG will match the Calling Party Number with the entries of the Calling Party Number Based Table. If a match is found, the call is routed to the destination number configured for that Calling Party Number.

To apply this method, do the following:

- In **Route all Incoming calls (with CLI)**, click **on the basis of Calling Party Number**.
- Click **Settings** and configure the **Calling Number Based** Table for the Mobile Port.




The **Calling Number Based Table** opens.




- In the **Calling Number** column**,** enter the calling party numbers. Calling party numbers may consist of a maximum of 24 characters. Default: Blank.
- For each calling party number, enter a corresponding destination number in the **Destination Numbers** column. Destination numbers may consist of a maximum of 24 characters. Digits 0 to 9, *, # and (.) dot are allowed. Default: Blank.

- Select the **Allow Callback** check box, if you want the system to automatically call the calling party from whom the call has been received on the Mobile Port.

  The system stores the calling party number for callback in the table. When there is an incoming call from that calling party, the system rejects the call. The system will automatically initiate a call to the calling number after 2-5 seconds. The system will make only one attempt for callback. If the callback fails due to network issues or because the called number is busy, the system will not re-attempt callback.

- Click **Submit** to save and close the window to return to the Mobile Port page.

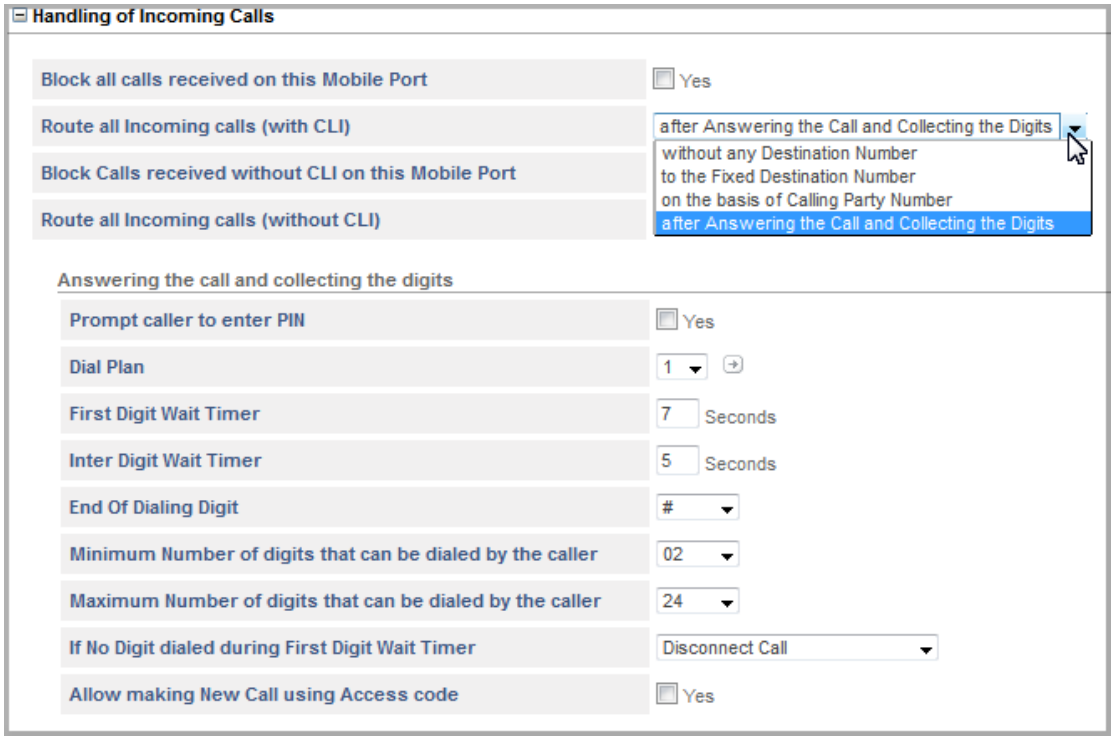
You can also configure the **Calling Number Based** Table from *Advanced Settings.* See "Destination Number Determination" under *Advanced Settings* for instructions.

- Select a method for routing incoming calls with CLI that *do not match* with any entries in the Calling Party Number Based Table.

  In the **If no match found in the Calling Party Number Table, route calls** box, you may select the option **to the Fixed Destination Number** *or* **after Answering the Call and Collecting the Digits**. Default: after Answering the Call and Collecting the Digits.

## *Route After Answering the Call and Collecting the Digits*

In this method, incoming call is answered and dial tone is played to the caller, allowing the caller to dial the desired number. The number dialed by the caller is considered as the destination number.




To apply this method, do the following:

- In the **Route all Incoming calls with CLI** list, click **after Answering the Call and Collecting the Digits**.

The related parameters of this method appear under **Answering the call and collecting the digits**.

- To enable PIN Authentication for incoming calls on this port, select the **Prompt caller to enter PIN** check box.

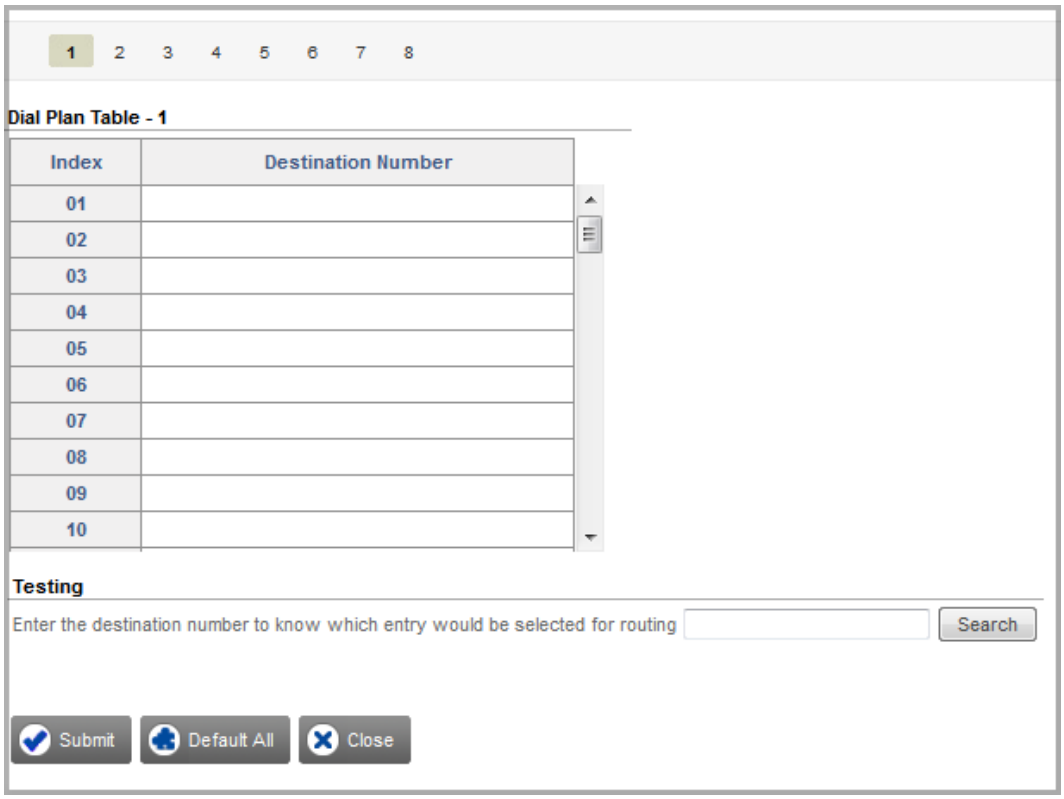
  If you enable this check box, you must also configure the PIN Authentication Table. To know more about this feature and for detail instructions, see "PIN Authentication" under *Advanced Settings*.

- Select the **Dial Plan** that you want the system to use to route the incoming calls received on the Mobile Port. Default: Dial Plan Table - 1.

  If you have not configured the Dial Plan table, you may do so now.

  - Click **Settings** .

  - The Dial Plan page opens in a new window.




  - You may configure the default Dial Plan Table-1 or any other Table (from 2 to 8) for the Mobile Port. You can store upto 64 Numbers at Index Numbers 01 to 64 respectively.

  - In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters: 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

    See "Dial Plan" for more details.

## Wildcard Characters

SETU VG supports following characters.

| Character | Description |
|---|---|
| **X** (letter X) | X represents any single digit from 0 to 9. |
| **#** | When # is configured in a number string, it will not be considered as End of Dialing. |
| ***** | When * is configured in a number string, it will not be considered as End of Dialing. |
| **+** | + (plus) can be configured as a first character of the Destination Number string in the *SIP Trunk-Destination Port Determination-Destination Number Based* table only. |
| **[ - ]** | Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket. |
| **[ , ]** | Comma within a bracket is used as a separator between the groups of numbers. |
| **[ ^ ]** | Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret. |
| **T** (letter T) | Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing. |

- Click **Submit** to save the entries and close the window.
- Return to the Dial Plan parameter and select the Dial Plan Table you configured.

- If required, you may change the duration of the **First Digit Wait Timer (FDWT)**. This is the time for which the system waits for the user to dial the destination number. Valid range: 01–99 seconds. Default: 7 seconds.
- You may configure the following options as End-of-Dialing indication:
  - In the **Inter Digit Wait Timer** field, define the number of seconds the system should wait while receiving the dialing digits, to consider it as end-of-dialing. You may change this timer, if required. Valid range: 01–99 seconds. Default: 5 seconds.
  - In the **End of Dialing Digit** field**,** select # or * as termination digit the system should consider to detect end of dialing. Default: #
  - In the **Minimum number of digits that can be dialed by the caller** field, select the minimum number of digits that the user must dial for the system to route the call. Valid range: 01–24 digits. Default: 2 digits.

***Minimum number of digits that can be dialed by the caller*** *parameter will be applicable when:*
- *the Destination Port Determination method selected is On the basis of Destination Number and the dialed number is not found in the Destination Number Table.*
  *Or*
- *the dialed number is not found in the Dial Plan and the End of Dialing is detected.*

  - In the **Maximum number of digits that can be dialed by the caller** field, select the maximum number of digits to be dialed by the user for the system to consider it as end-of-dialing**.** Valid range: 01–24 digits. Default: 24 digits.

When the caller dials a number, the system will match it with the end-of-dialing indications and accept the one that matches first.

- If the caller fails to dial the number during the First Digit Wait Timer, you can either have the system disconnect the call or route the call to a fixed destination number.

  In the **If No Digit dialed during First Digit Wait Timer (FDWT)** box, select the desired option: **Disconnect the Call** or **Use Fixed Destination Number**. Default: Disconnect Call.

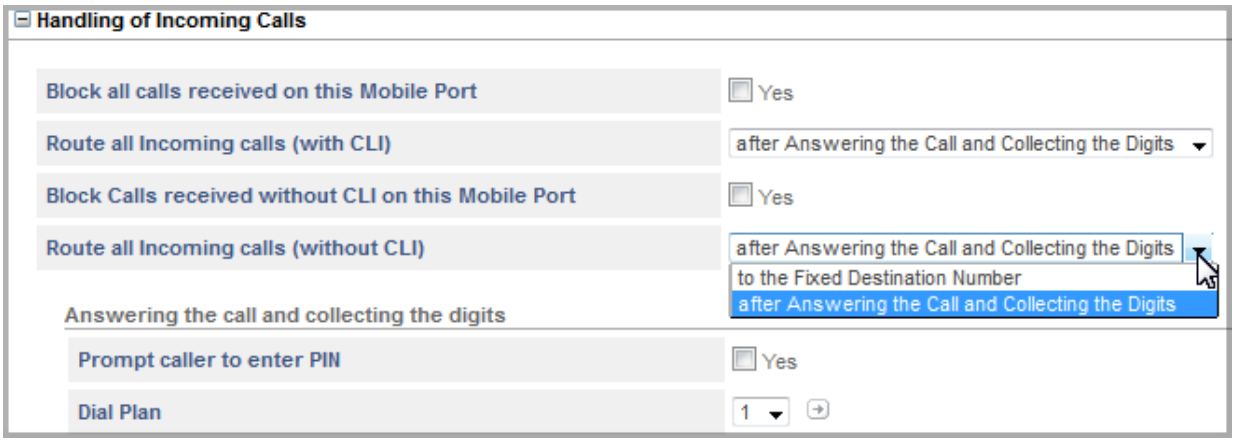
  - If you selected **Use Fixed Destination Number**, enter the desired destination number in the **Fixed Destination Number** field**.** The Destination number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and. (dot/period). Default: Blank.

- Select the **Allow making New Call using Access Code** check box, if you want to enable the feature Making New Call using Access Code on the Mobile Port. See "Making a New Call using Access Code".

- Click **Submit** to save settings.

- If you do not want to route the incoming calls received without CLI, through this Mobile Port, select **Block Calls received without CLI on this Mobile Port** check box.

- To **Route all Incoming calls (without CLI),** you may select from any of the following methods:
  - to a Fixed Destination Number, see "Route to the Fixed Destination Number".
  - after Answering the Call and Collecting the Digits, see "Route After Answering the Call and Collecting the Digits".
    Default: after Answering the Call and Collecting the Digits.




## Destination Port for Routing Calls

Select the Destination Port for routing calls for the selected Mobile Port. You may select from any of the following options:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number
  Default: Fixed

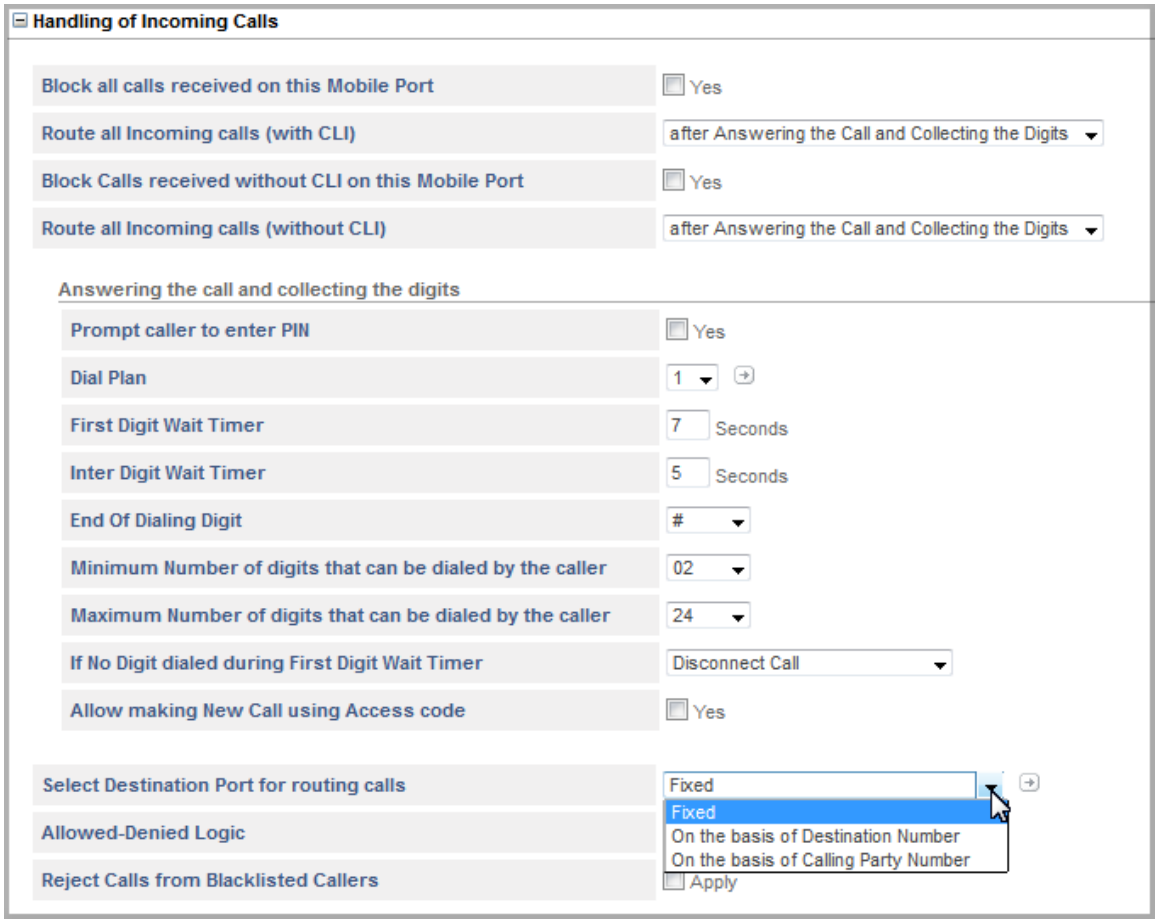
*If the destination number to be dialed out is an IP Address, SETU VG will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. See "IP Dialing" to know more.*

## Fixed

In this method, calls received on the Mobile Port are routed to a fixed destination port, irrespective of the number dialed on the Mobile Port.

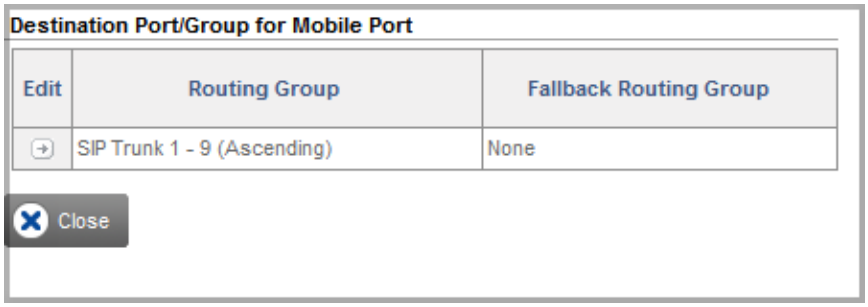
To apply this method, do the following:

- In the **Select Destination Port for routing calls** box, click **Fixed**.



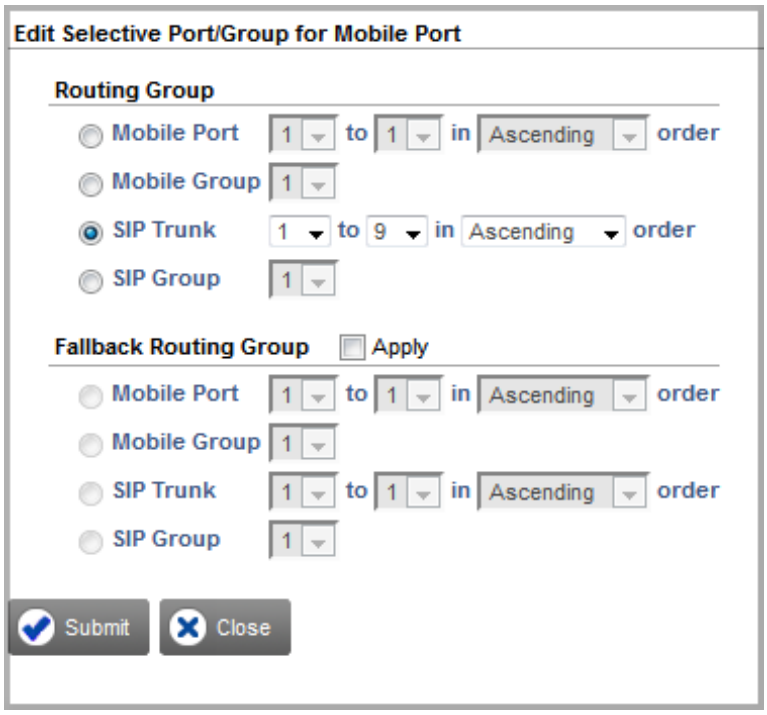

- Click **Settings** .

  The **Destination Port/Group for Mobile Port** window opens.




- Click **Edit**, to change the default Routing Group and create the Fallback Routing Group.

The **Edit Selective Port/Group for Mobile Port** window opens.




- Create the **Routing Group**.
  - To create a group of *sequential* **Mobile Port** as members,
    - Select the desired **Mobile Port** numbers as members. Default: 1.
    - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

      Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.
  - To create a group of *not-sequential* **Mobile Ports** as members,
    - Select **Mobile Group**.
    - Select the **Mobile Group** number. Default:1.
    - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See “Group” for detailed instructions.
  - To create a group of *sequential* **SIP Trunks** as members,
    - Select the desired **SIP Trunk** numbers as members. Default: 1.
    - In the **in - order** field, select the order in which the system should hunt for a free member SIP Trunk to route the call.

Select **Ascending** to start hunting from the first to the last member SIP Trunk. Select **Descending** to start hunting from the last to the first member SIP Trunk. Default: Ascending.

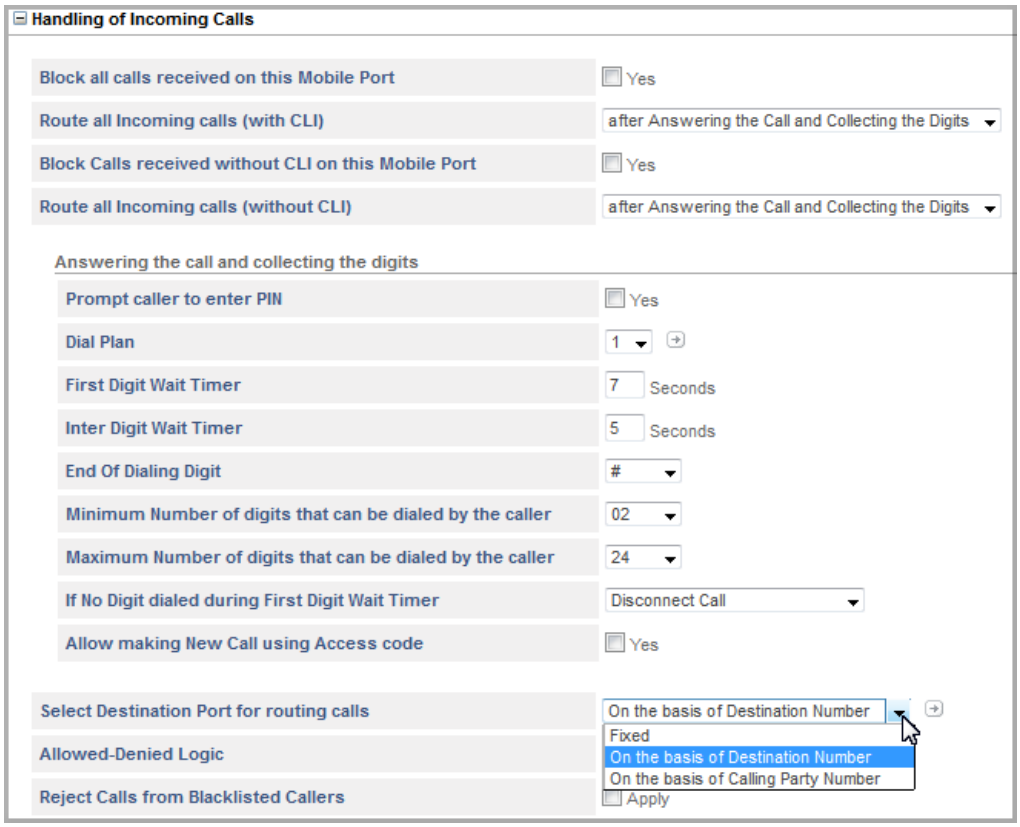
- To create a group of *not-sequential* **SIP Trunks** as members,
  - Select a **SIP Group**.
  - Select **SIP Group** number. Default:1.
  - Click **Settings** . The **SIP Groups** window opens. Create the SIP Group. See "Group" for detailed instructions.

- To create the **Fallback Routing Group**,
  - Select the **Apply** check box.
  - Follow the same instructions as given for creating *sequential* and *not-sequential* groups, for SIP Trunks and Mobile Ports.
  - Click **Submit** to save changes. The **Edit** window closes.

- The edited entry appears in the **Destination Port/Group for Mobile Port** window. Close this window to return to the main page.

### *On the basis of Destination Number*

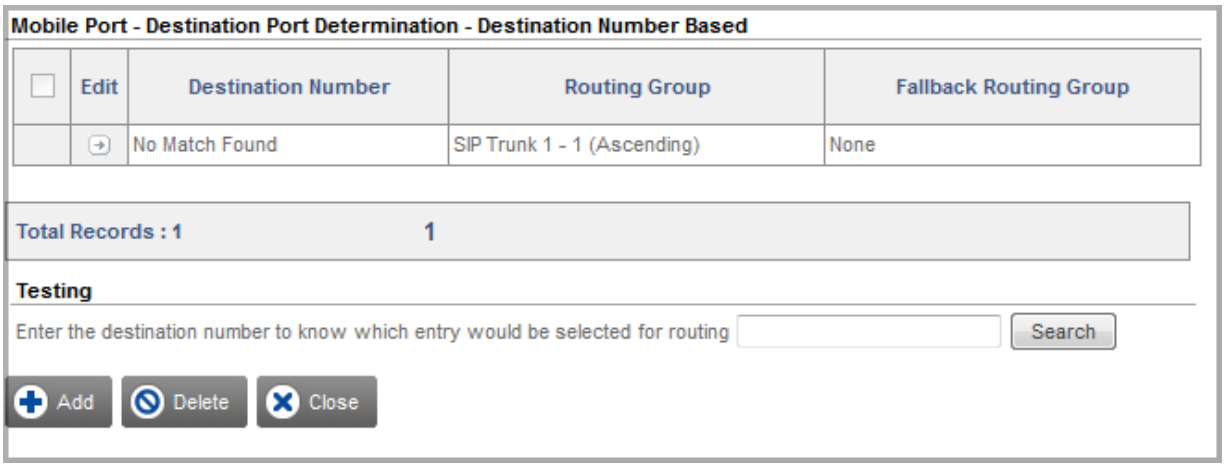
In this method, incoming calls on the source port are routed to the destination port on the basis of the destination number (called party number) dialed by the caller.



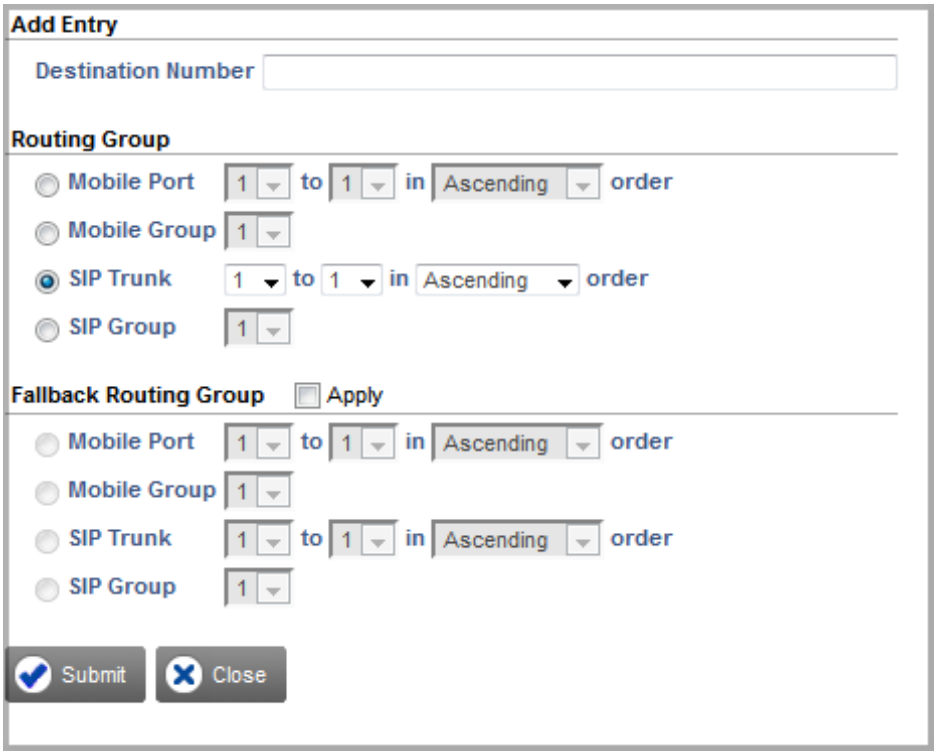
To apply this method, do the following:

- Click **Settings** .

  The **Mobile Port - Destination Port Determination - Destination Number Based** table window opens.




- Click **Add** to add a new entry. The **Add Entry** window opens. You can add upto 100 entries.




  - In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters: 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

  - Create the **Routing Group**.

- To create a group of *sequential* **Mobile Port** as members,
  - Select the desired **Mobile Port** numbers as members. Default: 1.
  - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

    Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.
- To create a group of *not-sequential* **Mobile Ports** as members,
  - Select **Mobile Group**.
  - Select the **Mobile Group** number. Default:1.
  - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See “Group” for detailed instructions.
- To create a group of *sequential* **SIP Trunks** as members,
  - Select the desired **SIP Trunk** numbers as members. Default: 1.
  - In the **in - order** field, select the order in which the system should hunt for a free member SIP Trunk to route the call.

    Select **Ascending** to start hunting from the first to the last member SIP Trunk. Select **Descending** to start hunting from the last to the first member SIP Trunk. Default: Ascending.
- To create a group of *not-sequential* **SIP Trunks** as members,
  - Select a **SIP Group**.
  - Select **SIP Group** number. Default:1.
  - Click **Settings** .The **SIP Groups** window opens. Create the SIP Group. See “Group” for detailed instructions.

- To create the **Fallback Routing Group**,
  - Select the **Apply** check box.
  - Follow the same instructions as given for creating *sequential* and *not-sequential* groups, for SIP Trunks and Mobile Ports.
  - Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **Mobile Port - Destination Port Determination - Destination Number Based** window.
- Follow the same steps as above to add another entry to this table.

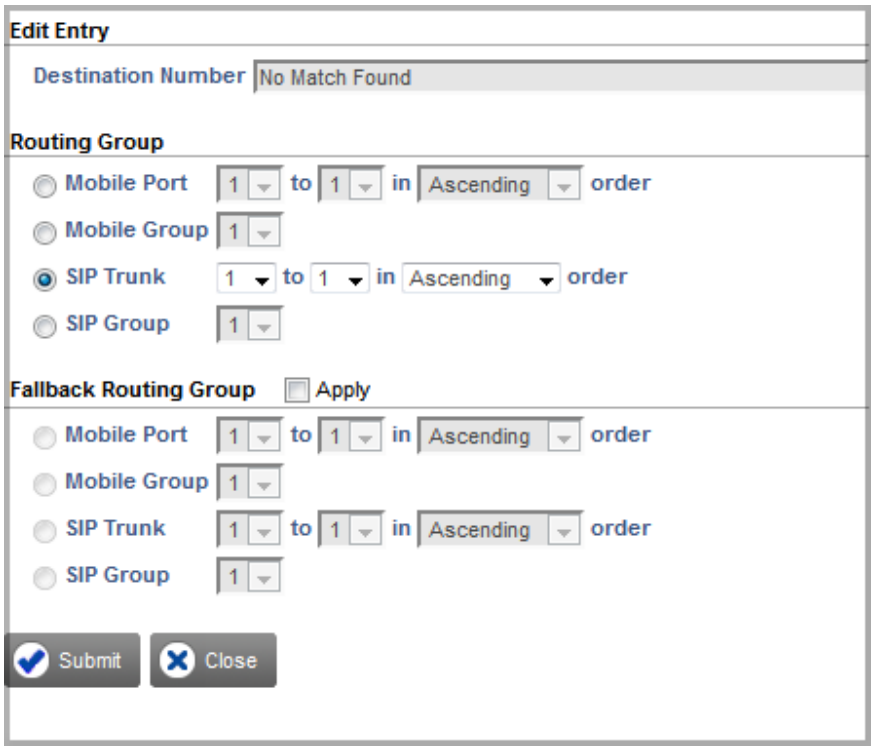
- To delete an entry, select the check box and click **Delete** button.

*If there are multiple entries in the Destination Number Based table, to search a particular entry in the table, under Testing enter the desired number in the **Enter the destination number to know which entry would be selected for routing** search box.*

- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

  To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

  - For the **No Match Found** entry in the table, under **Edit**, click **Settings** .
  - The **Edit Entry** window opens.




  - Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
  - Click **Submit** and close the window.

- Close the window if you have finished adding/editing entries.

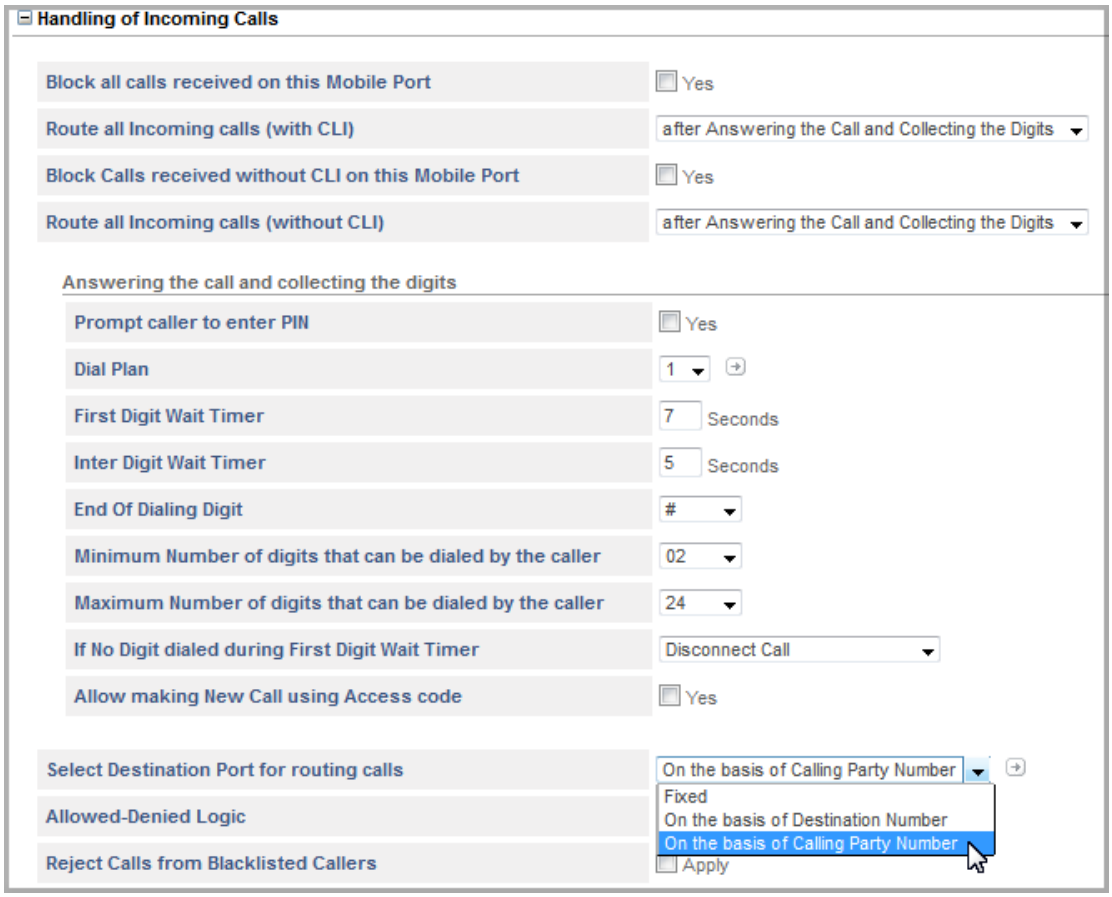
  You can also configure the **Destination Number Based** Table from *Advanced Settings*. See "Destination Port Determination" under Advanced Settings.

### *On the basis of Calling Party Number*

In this method, incoming calls on the Mobile Port are routed to a specific port, as per the calling party's number.

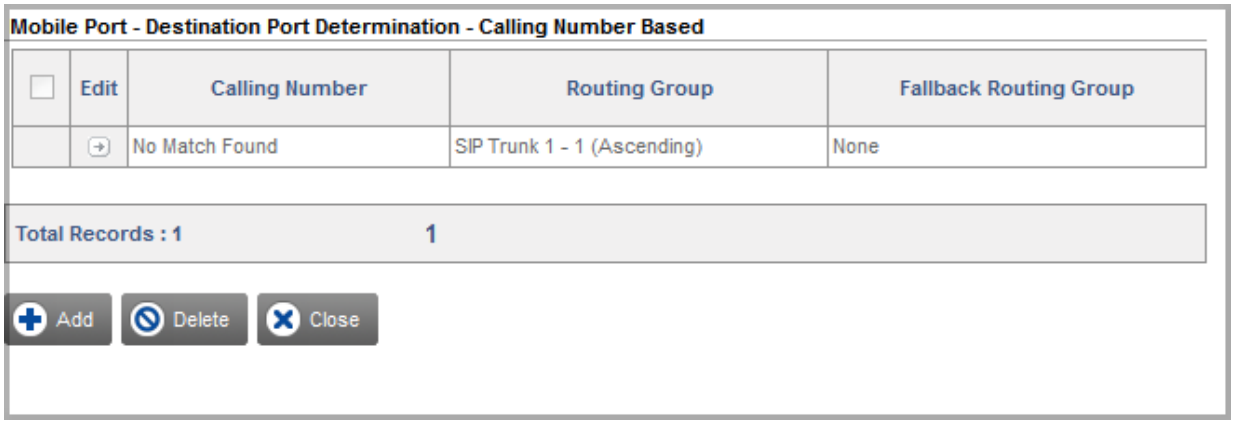
To apply this method, do the following:

- In the **Select Destination Port for routing calls** box, click **on the basis of Calling Party Number**.

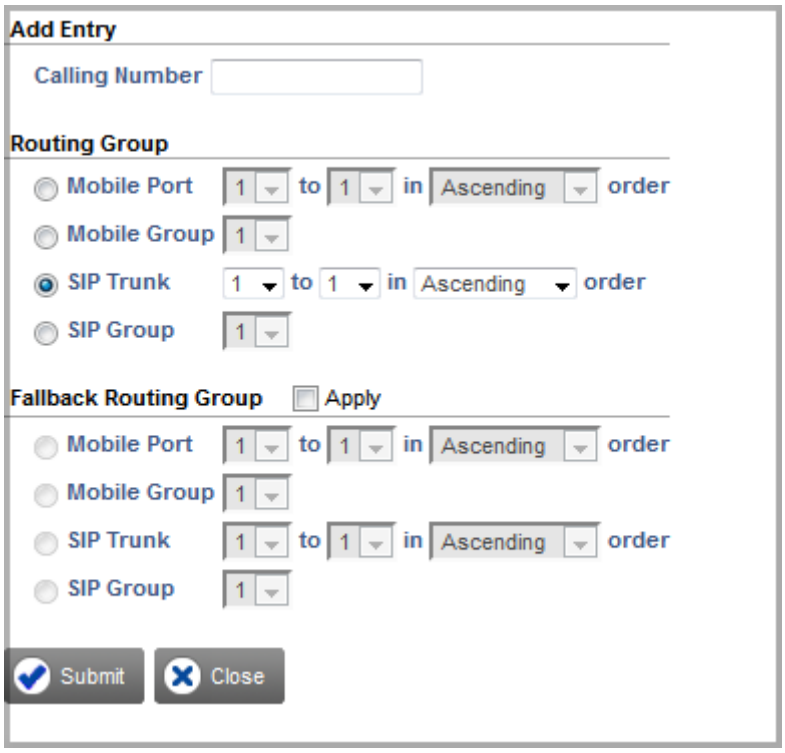



- Click **Settings** .

  The **Mobile Port - Destination Port Determination - Calling Number Based** table window opens.



- Click **Add** to add a new entry. The **Add Entry** window opens. You can add upto 500 entries.




  - In the **Calling Number** field, enter numbers (max. 24 characters) from which you expect calls to be received. Valid digits: 0 to 9, *, #, . (dot). Default: blank.
  - Create the **Routing Group**.
    - To create a group of *sequential* **Mobile Port** as members,
      - Select the desired **Mobile Port** numbers as members. Default: 1.
      - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

        Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.
    - To create a group of *not-sequential* **Mobile Ports** as members,
      - Select **Mobile Group**.
      - Select the **Mobile Group** number. Default:1.
      - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See “Group” for detailed instructions.
    - To create a group of *sequential* **SIP Trunks** as members,
      - Select the desired **SIP Trunk** numbers as members. Default: 1.

- In the **in - order** field, select the order in which the system should hunt for a free member SIP Trunk to route the call.

  Select **Ascending** to start hunting from the first to the last member SIP Trunk. Select **Descending** to start hunting from the last to the first member SIP Trunk. Default: Ascending.

- To create a group of *not-sequential* **SIP Trunks** as members,

  - Select a **SIP Group**.

  - Select **SIP Group** number. Default:1.

  - Click **Settings** . The **SIP Groups** window opens. Create the SIP Group. See “Group” for detailed instructions.

- To create the **Fallback Routing Group**,

  - Select the **Apply** check box.

  - Follow the same instructions as given for creating *sequential* and *not-sequential* groups, for SIP Trunks and Mobile Ports.

  - Click **Submit** to save changes. The **Add Entry** window closes.

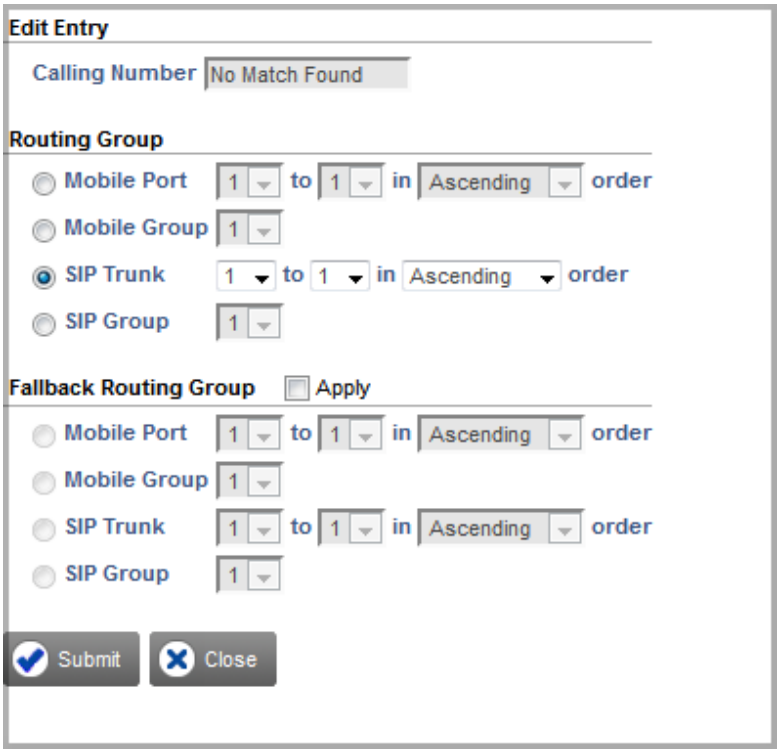
- The entry you added appears in the **Mobile Port- Destination Port Determination - Calling Number Based** window.

- By default SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

  To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

  - For the **No Match Found** entry, under **Edit**, click **Settings** .

- The **Edit Entry** window opens.




  - Create the **Routing Group** and **Fallback Routing Group**.
  - Click **Submit** and close the window.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click **Delete** button.
- Close the window if you have finished adding/editing entries.

  You can also configure the **Calling Number Based** Table from *Advanced Settings*. See “Destination Port Determination” under Advanced Settings.

## Allowed - Denied Logic

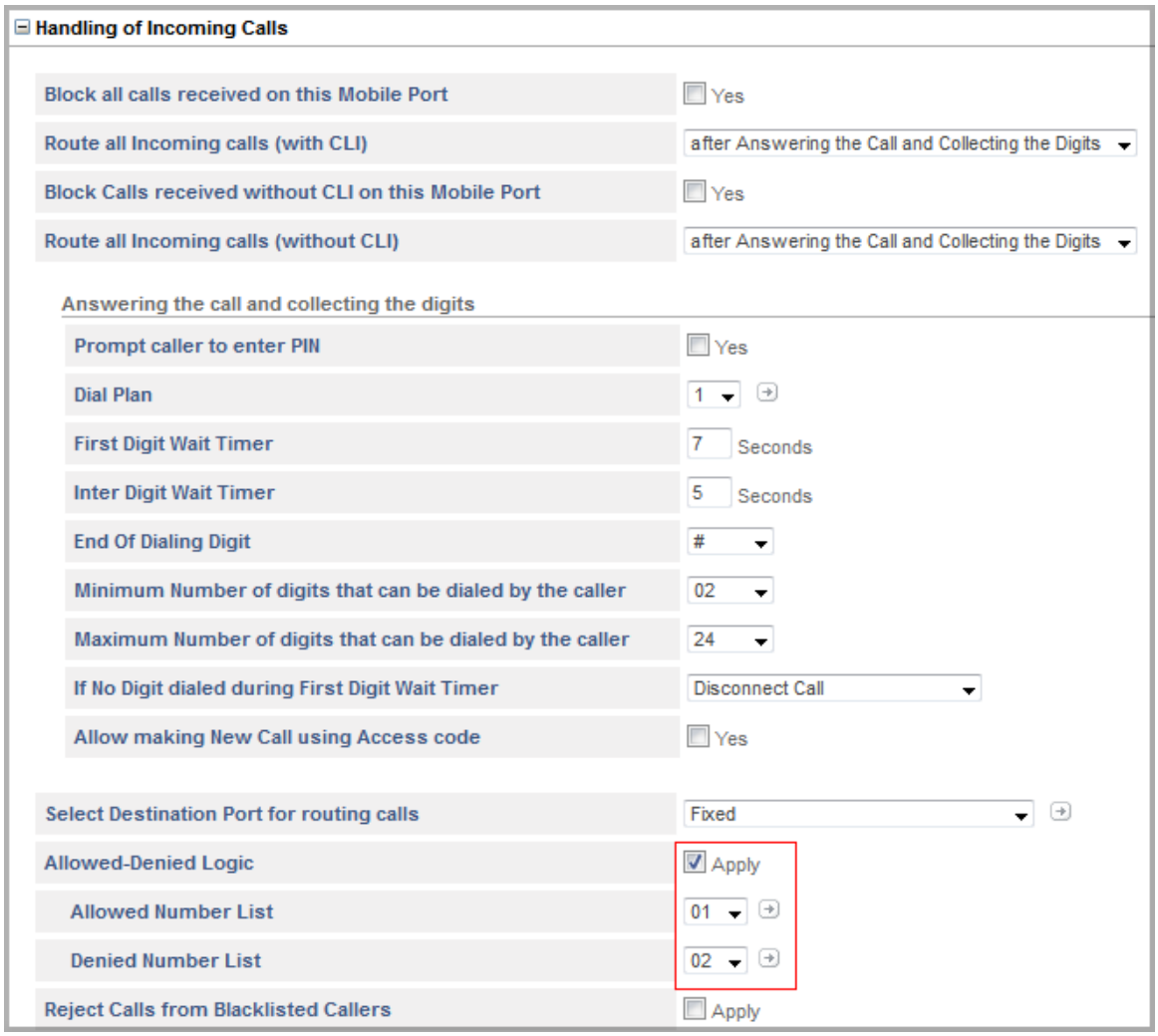
With the Allowed-Denied Numbers feature you can permit and restrict the dialing of particular numbers from the Mobile Port.

Allowed Denied Number Logic makes use of two Number lists:

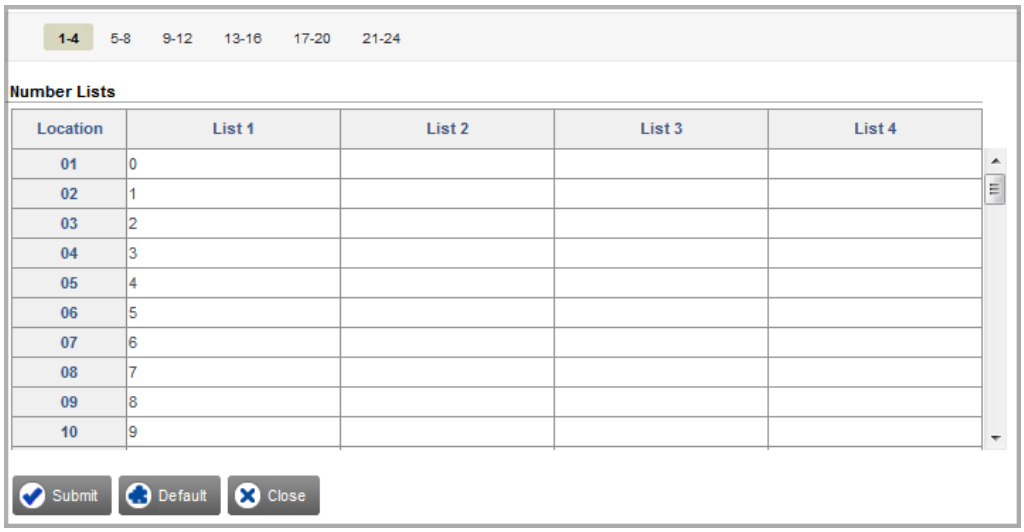
- **Allowed Numbers List:** This is the list of numbers that are allowed to be dialed out by the caller on the Mobile Port. By default, List Number 1 is assigned to the Mobile Port.
- **Denied Numbers List:** This list contains the numbers that are denied to be dialed out by the caller on the Mobile Port. By default, List Number 2 is assigned to the Mobile Port.

To apply Allowed - Denied Logic on the Mobile Port,

- Click the **Allowed - Denied Logic** check box.




- To configure the **Allowed Number List**, click **Settings** .
  - The Number List page opens in a new window.



    - By default, Number List 1 is assigned as Allowed Number List.
    - Enter the numbers you want the system to allow to be dialed in this list.
    - Click **Submit** to save the entries and close the window.
- To configure the **Denied Number List**, click **Settings** .
    - The Number List page opens in a new window.
    - By default, Number List 2 is assigned as Denied Number List.
    - Enter the numbers you want the system to restrict from being dialed out in this list.
    - Click **Submit** to save the entries and close the window.

You may configure a different Number List as Allowed and Denied List. See “Allowed - Denied Logic” under “Number Lists”.

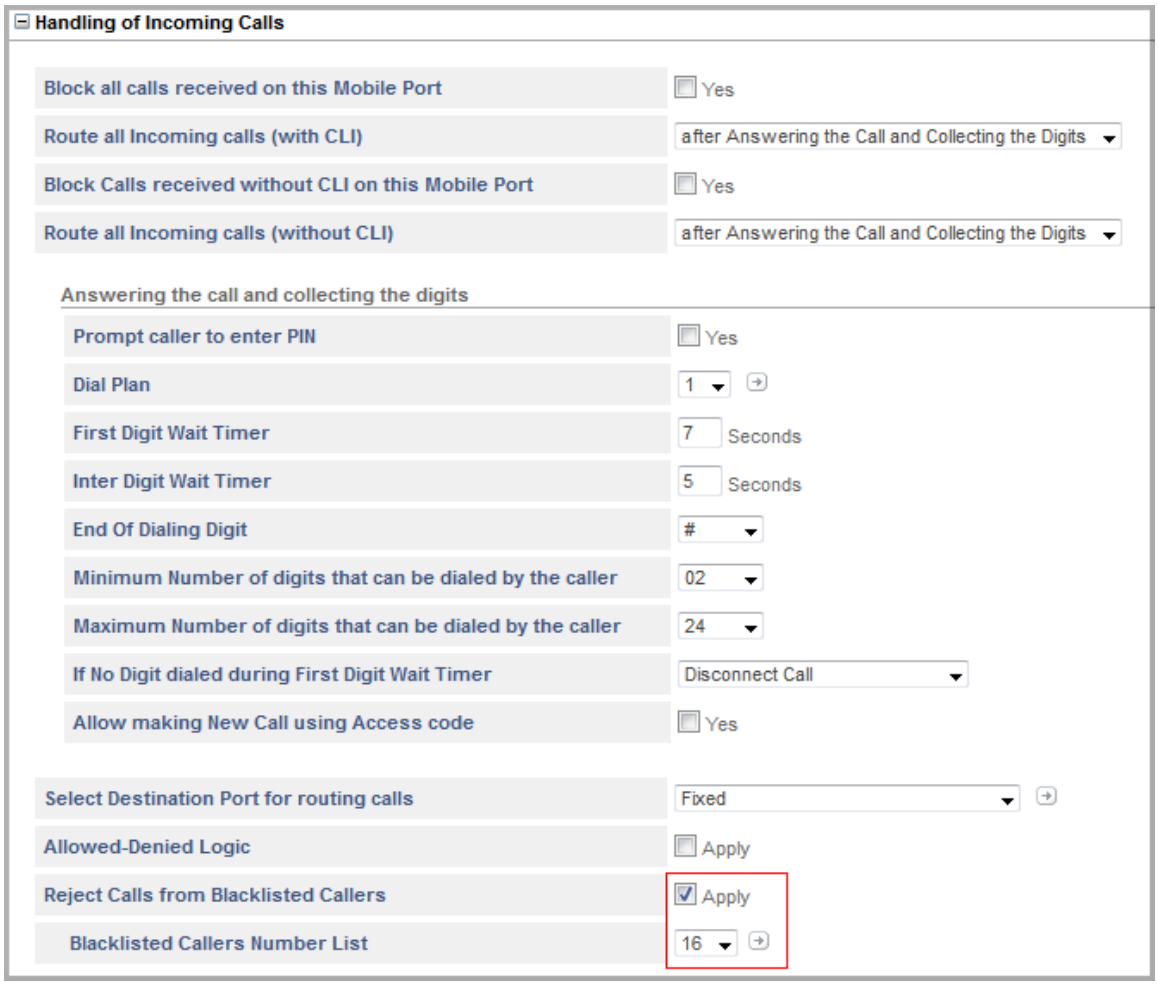
## Black Listed Callers

With the Black Listed Callers feature you can block incoming calls from specific numbers on the Mobile Port. Thus all incoming calls from the numbers you have 'blacklisted' will be automatically rejected by SETU VG.

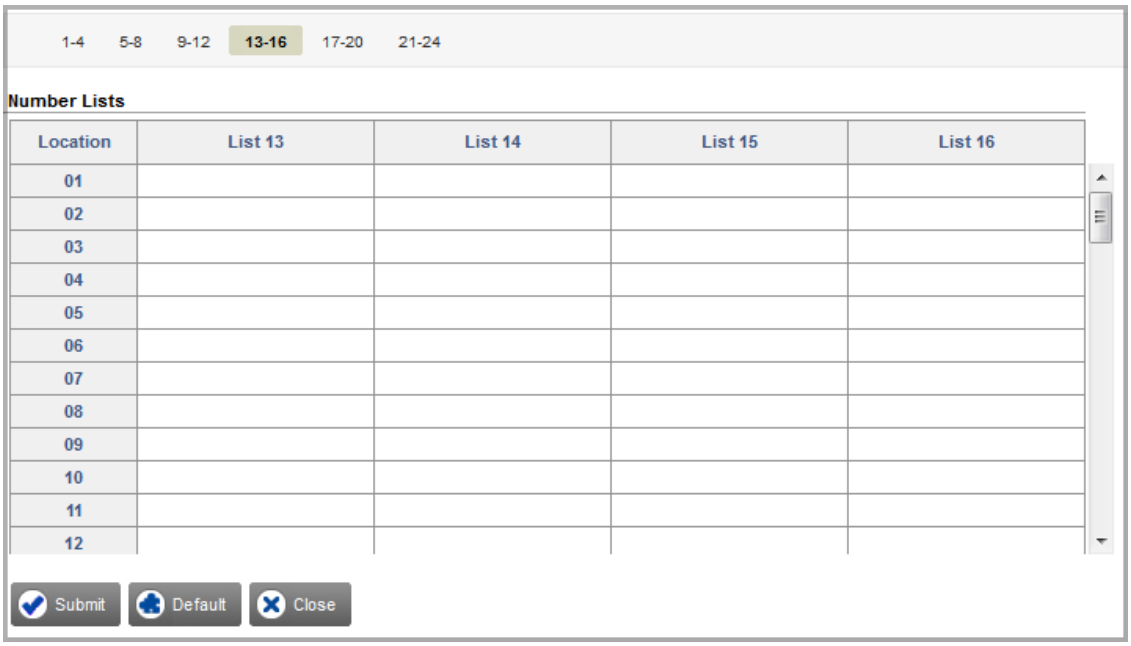
To apply Black Listed Callers on Mobile Port,

- Select the **Reject Calls from Blacklisted Callers** check box.
- Configure the **Black Listed Callers** table. To do this,

- Click **Settings** .




- The Number List page opens in a new window.

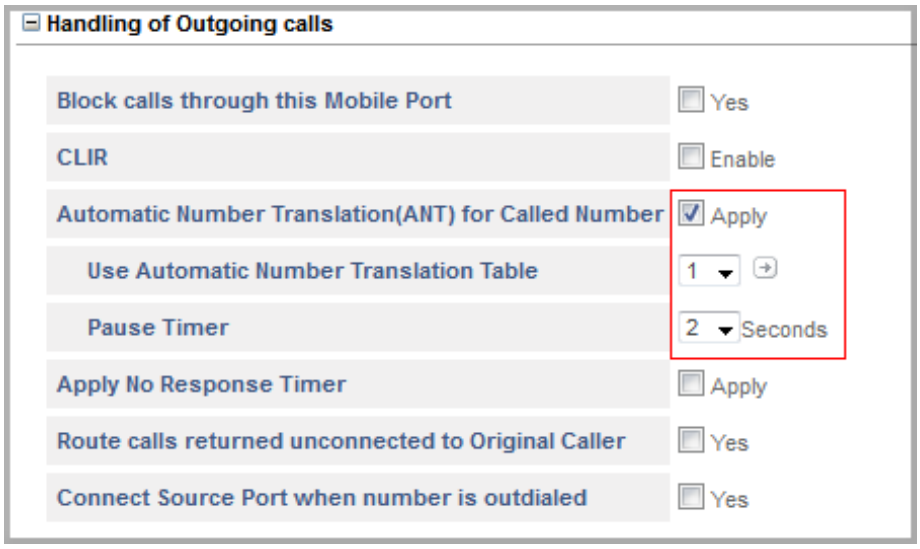


- By default, Number List 16 is assigned as Black Listed Callers List.
- Enter the numbers of unwanted callers in this list.
- Click **Submit** to save the entries and close the window to return to the main page.

## Handling of Outgoing Calls

When Mobile Port is determined as the destination port, numbers dialed from this port constitute outgoing calls.

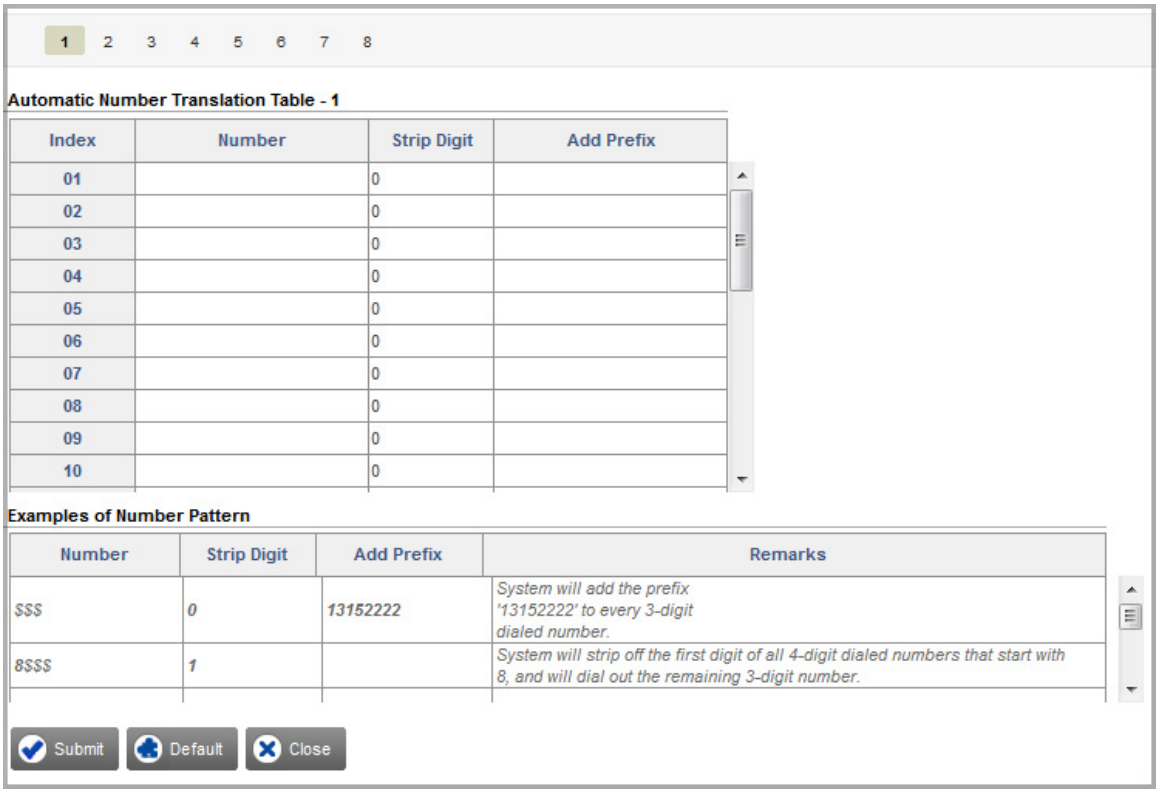

- If you do not want to route outgoing calls though this Mobile Port, select the **Block calls through this Mobile Port** check box. Default: Disabled.
- By default, the CLI of the Mobile Port is sent to the called party when outgoing calls are made using the Mobile Port. If you do not want to send CLI, enable the **CLIR** check box. Default: Disabled.
- You can apply **Automatic Number Translation logic** on outgoing calls made from the Mobile Port.
  - To apply ANT logic on the Called Numbers, click the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.



- In the **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Mobile Port. By default, Table 1 is assigned to the Mobile Port.

  If you have not configured the Automatic Number Translation Table,

  - Click **Settings** . The Automatic Number Translation Table page will open in a new window.




  - You may configure the default Automatic Number Translation Table 1 or any other Table number (2 to 8) for the Mobile Port. See "Automatic Number Translation (ANT)" to configure the ANT Table.

  - Click **Submit** to save the ANT Table and close the window.

- Return to ANT parameter and assign the ANT Table you configured.

- Click **Submit** to apply List.

- Configure the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. The valid range of the Pause Timer is 1 to 9 seconds. Default: 2 seconds.

- Enable **Apply No Response Timer.** The system will route the call through a Fallback Routing Group or Port, if a response other than—Alert, Connect, Busy, No Reply, Disconnect with cause as Busy or No Reply—is received from the network within the specified time period. Default: Disabled.

- Set the **No Response Timer**, if you have enabled the *Apply No Response Timer* parameter. It is the time for which SETU VG will wait for the valid response from the network for any request. If no valid response is received before the expiry of this timer, SETU VG will fallback to alternate Routing Group or Port for further processing of the call. Valid range: 01–99 seconds. Default: 10 seconds.

*To apply Fallback logic on the Mobile Port, make sure you have enabled Fallback Routing Group under "Destination Port for Routing Calls".*

- Enable **Route calls returned unconnected to original caller**, if you want SETU VG to route outgoing calls made from this port that returns unconnected back to the original caller.

  If you enable this feature, when an outgoing call is made using this Trunk, and the Called Party is found busy or does not respond, SETU VG stores the number of the Calling Party, the number of the Called Party, the source port type and number and the trunk port type and number used for routing the outgoing call in the RCOC table. A record of each such call is stored for the duration of the *Unconnected Calls Record Delete Timer* (configurable; default: 999 minutes).

  If the called party returns the call before the expiry of this timer, SETU VG checks whether *Apply RCOC only if the caller calls back on the same trunk from which the call was made* is enabled or not, and accordingly place the incoming call to the original calling party. See "System Parameters" to configure the *Unconnected Calls Record Delete Timer* and *Apply RCOC only if the caller calls back on the same trunk from which the call was made* check box.

- To connect the Source Port with the Destination Port without waiting for the call on the Destination Port to mature, enable the **Connect Source Port when number is outdialed** check box. Default: Disabled.

  In all Destination Number Determination methods except *After Answering the Call and Collecting the Digits*, the Source Port gets connected to the Destination Port only after the call has matured, i.e. the called party has answered the call. Until the call matures, the caller hears only Ring Back Tone played by the network.

  By connecting the Source Port with the Destination Port immediately after the number is dialed, the caller can know the state of the call; if the called party is busy, not responding, not reachable or is rejecting the call.

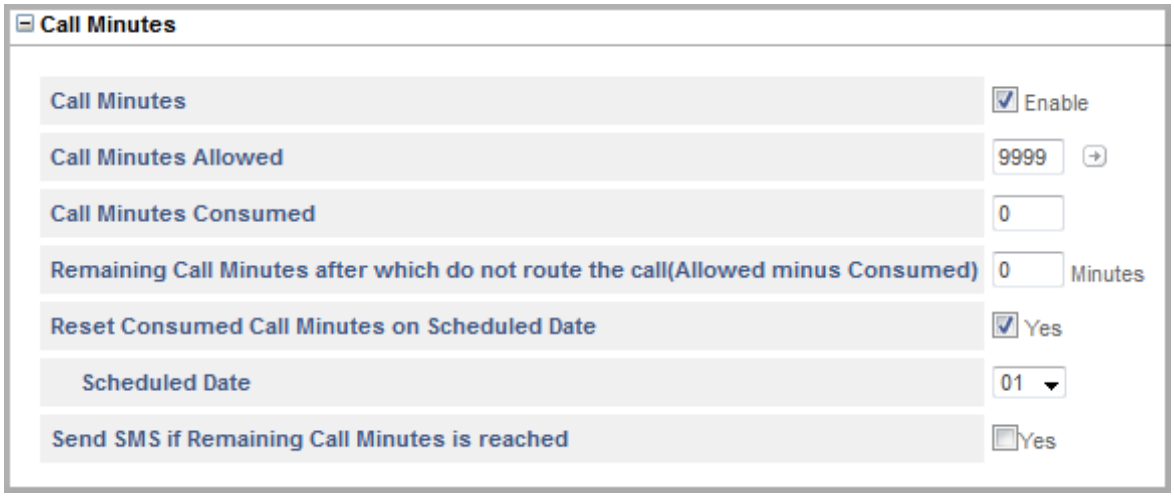
- Click **Submit** to save.

*If you enable **Connect Source Port when number is outdialed**, you will not be able to provide the features "Making a New Call using Access Code" and "Disconnecting a Call using Access Code" to users.*

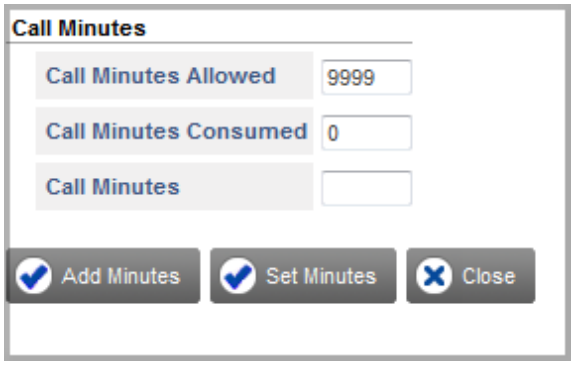
## Call Minutes

Mobile Service Providers offer different tariff schemes to their subscribers. For example, mobile service providers in India offer first 500 Minutes free, CUG calling, first 500 minutes calling at 30 paise. SETU VG allows you to take advantage of these tariff schemes by configuring Call Minutes on the Mobile Port.

- Click **Call Minutes**.

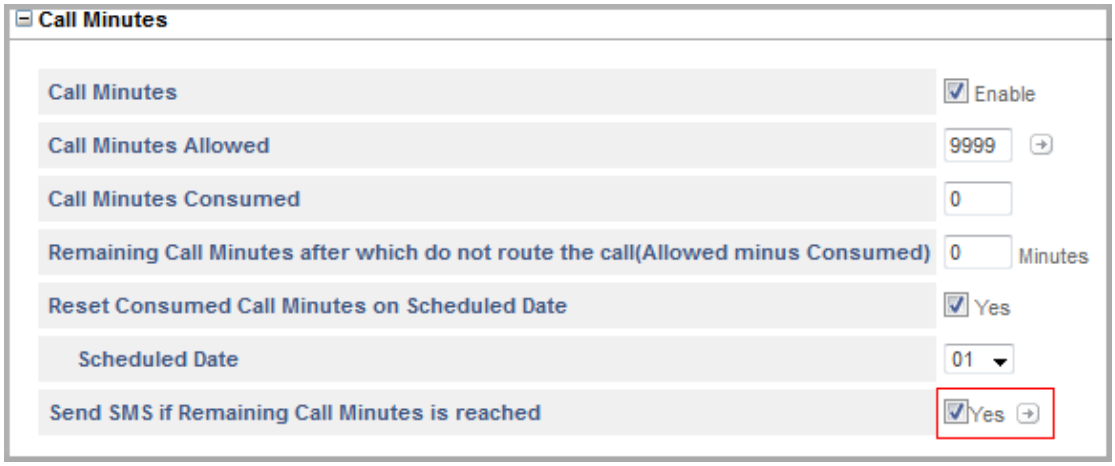



- Select the **Call Minutes** check box to apply this feature.
- The **Call Minutes Allowed** field displays the minutes allotted to the Mobile Port for making outgoing calls. Default: 9999. Valid Range: 0000 to 9999. To change the value of Call Minutes Allowed,
    - Click the **Call Minutes Allowed Settings** .

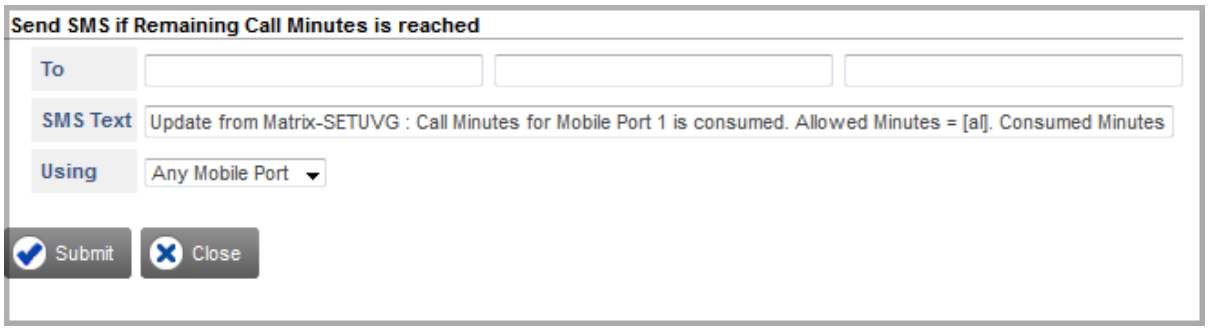



    - The **Call Minutes** window opens.
        - In the **Call Minutes** field, enter the desired value.
        - Click the **Set Minutes** button. The value entered appears in the **Call Minutes Allowed** field.
    - If you want to add minutes to the existing value,
        - In the **Call Minutes** field, enter the desired value you want to add.
        - Click the **Add Minutes** button. The value you entered gets added to the existing minutes and appears in the **Call Minutes Allowed** field.
- Close the window to return to the main page.
- The **Call Minutes Allowed** field, displays the Call Minutes set/added by you.

- The minutes consumed are displayed in the **Call Minutes Consumed** field.
- You may block outgoing calls from the Mobile Port after a certain number of call minutes have been consumed. To do this, in the **Remaining Call Minutes after which do not route the call (Allowed minus Consumed)** field, enter the minutes that the system should consider as call minutes remaining. Valid Range: 000 to 999. Default: 000.
- To have the system automatically reset the value of Call Minutes on a scheduled date, select the **Reset Consumed Call Minutes on Scheduled Date** check box and select the date from the **Scheduled Date** drop box.
- If you want the system to send SMS notification for the Remaining Call Minutes after which the call will not be routed,
  - Select the **Send SMS if Remaining Call Minutes is reached** check box.
  - Click **Settings** .




The **Send SMS if Remaining Call Minutes is reached** window opens.




- In the **To** fields, you may enter up to 3 different Mobile Numbers to which the SMS should be sent. The numbers can be a maximum of 24 digits. The digits allowed are 0-9, *, # and +.
- In the **SMS Text** field, enter the text you want to be sent in the SMS Notification. The text length can be a maximum of 80 characters.

- In the **Using** field, select the Mobile Port number which the system should use to send the SMS.

- Click **Submit** to save and close the window to return to the main page.

# SIM Balance and Recharge

SETU VG supports Balance Inquiry and Recharging of the SIM Card installed in its Mobile Ports[3].

To be able to use this feature, first get information about the following from your Network Operator:

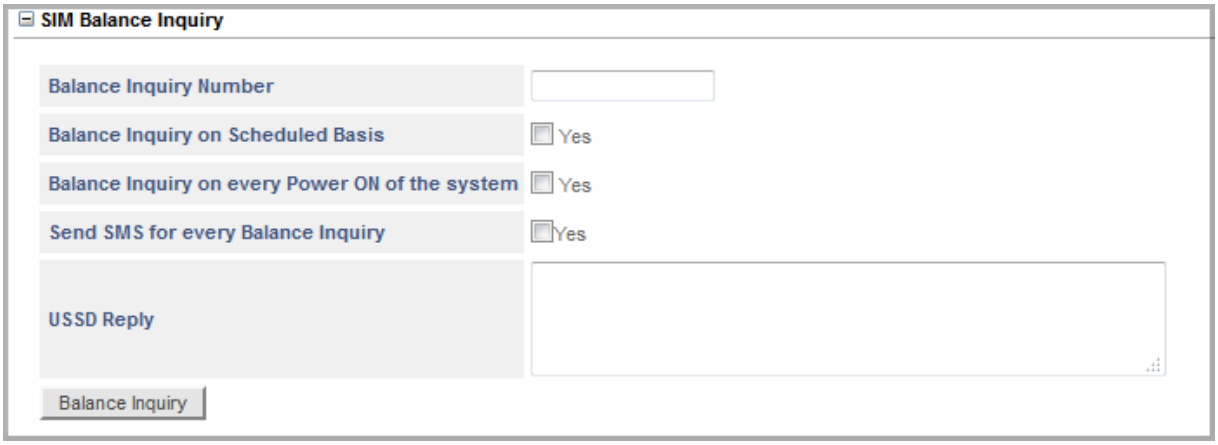
- **Balance Inquiry Number:** This is the number provided by the Network Operator to the subscribers to check Balance. Different Network Operators have different numbers. For example, the Balance Inquiry number of Vodafone is ****141#.***

- **Recharging Service Number:** This is the number provided by the Network Operators to their subscribers for Recharging Service. Different Network Operators have different numbers for Recharging Service. For example, the Recharging Service Number of Vodafone is ****140****.

## SIM Balance Inquiry

To check the SIM Balance using Jeeves,

- Click **SIM Balance Inquiry**.



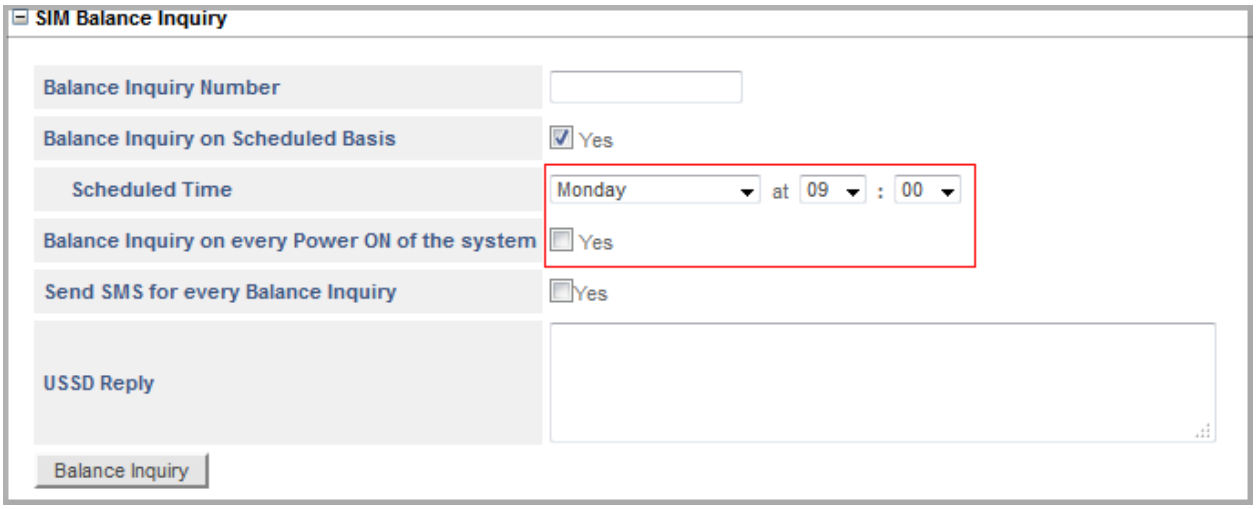

- In the **Balance Inquiry Number** field, enter the number provided to you by the Network Operator to check Balance. The number can be a maximum of 16 digits. The digits allowed are 0-9, * and #.

- Click **Submit**.

- To run the query click the **Balance Inquiry** button.

3. *SETU VG supports Unstructured Supplementary Service Data (USSD), the standard for transmitting information over CSM signaling channels and a commonly used method to query the available balance and other similar information in pre-paid GSM services.*

- If you want the system to check the SIM Balance at fixed intervals, select the **Balance Inquiry on Scheduled Basis** check box and configure the following:



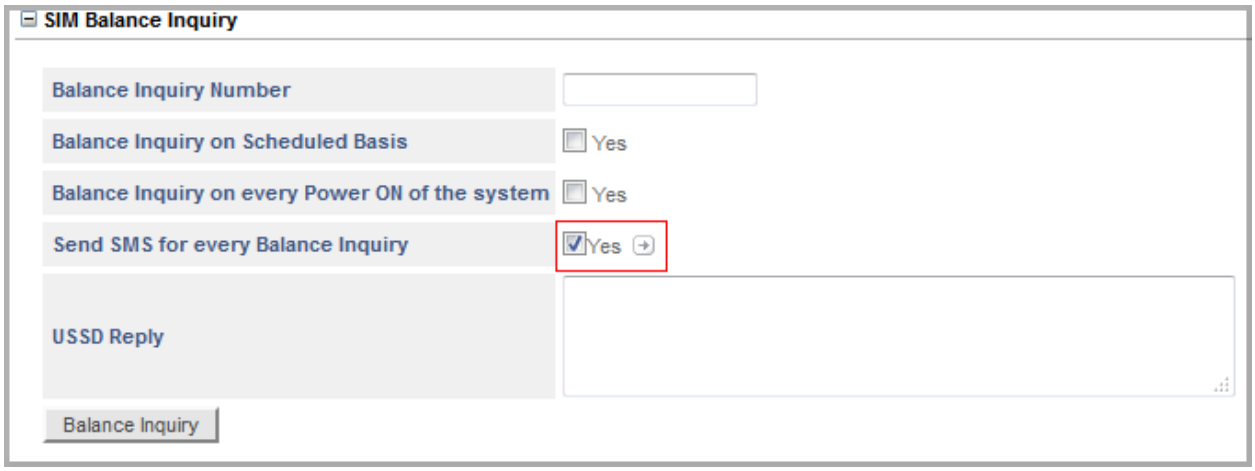

  - In the **Schedule Time - at** field, enter the day and the time when you want the system to make the Balance query.

- Select the **Balance Inquiry on every Power ON of the system** check box, if you want the system to make the SIM Balance query at every Power ON.

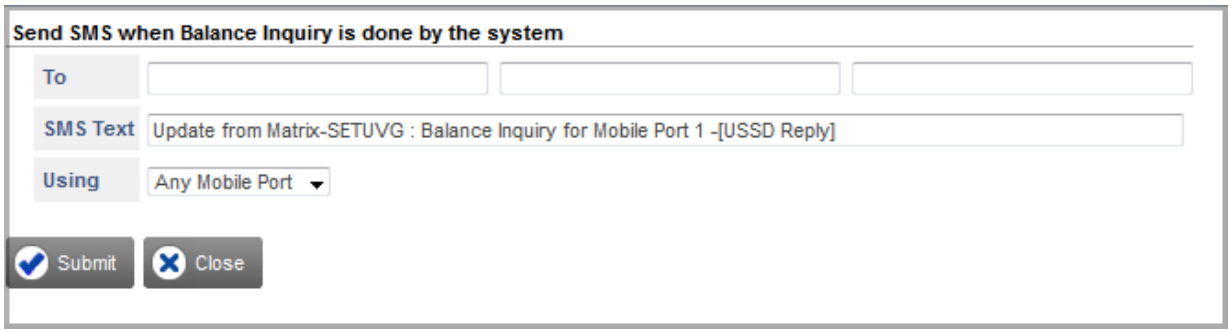
- Select the **Send SMS for every Balance Inquiry** check box, if you want the system to send a SMS notification for every Balance Inquiry query.

  You must configure the following if you have enabled SMS Notification:

  - Click **Settings** .



- the **Send SMS when Balance Inquiry is done by the system** window opens.




  - in the **To** fields, enter three mobile numbers on which you to want the system to send the SMS notification. The numbers can be a maximum of 24 digits. The digits allowed are 0-9, *, # and +.
  - in the **SMS Text** field, enter the message that you want the system to send. The text length can be a maximum of 80 characters.
  - from the **Using** options, select the Mobile Port through which you want the system to send the SMS.
  - click **Submit** to save and close the window to return to the main page.
- The response received from the GSM network (including possible error messages) will be displayed under **USSD-Reply**.

## SIM Recharge

To Recharge the SIM,

- Click **SIM Recharge**.


- In the **Recharge Number** field, enter the number provided to you by the Network Operator to recharge the SIM. The number can be a maximum of 8 digits. The digits allowed are 0-9, * and #.
- Click **Submit**.
- Click the **Recharge** button.
- A new window opens. In the **Enter Recharge PIN Number** field, enter the number printed on the Recharge Voucher.
- Click **OK**.

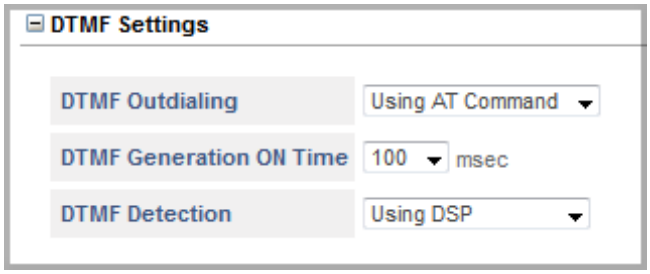
- The response received from the mobile network (including possible error messages) will be displayed under **USSD-Reply**.

*If no number is entered the SMS will not be sent.*

### DTMF Settings

To configure the DTMF Settings for the Mobile Port,

- Click **DTMF Settings**.

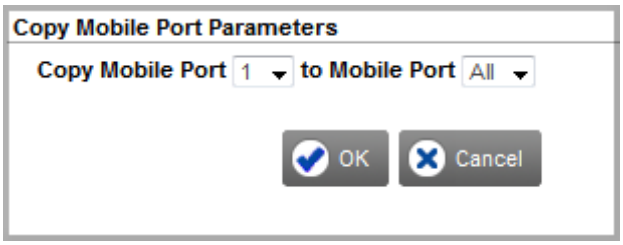



- Select the desired **DTMF Outdialing** option as **Inband** or **Using AT Command**. Default: Using AT Command.
- Select the appropriate **DTMF Generation ON Time** for the Mobile Port. This parameter determines the time for which the DTMF digit will remain ON, while being out dialed by the system. You may select 100 msec or 200 msec. Default: 100 msec.
- Select the appropriate **DTMF Detection** option. You may select **Using DSP** or **Using GSM Engine**. Default: Using DSP.
- If you have selected DTMF Detection option as *Using GSM Engine*, configure the appropriate **DTMF Detection Minimum ON Duration**. Valid range of DTMF Detection Minimum ON Duration is from 20-100 milliseconds. Default: 30 milliseconds.
- To configure the next Mobile Port, click the Mobile Port number tab and follow the same instructions as given earlier.
- If required, you may restart the GSM/ UMTS Module by clicking the **Module Restart** button.

## Copy Port Settings

- You can also copy the settings of a Mobile Port to another Mobile Port using the **Copy** button. To do this,

- Click the **Copy** button. The **Copy Mobile Port Parameters** window opens.




- In the **Copy Mobile Port** box, select the number of the port you want to copy *From*. In the **to Mobile Port** box, select the number of the port you want to copy the settings *To*.
- Click the **OK** and close the window.

  Once you have copied the settings, you can again edit the specific parameters of the Mobile Port you copied the settings to.

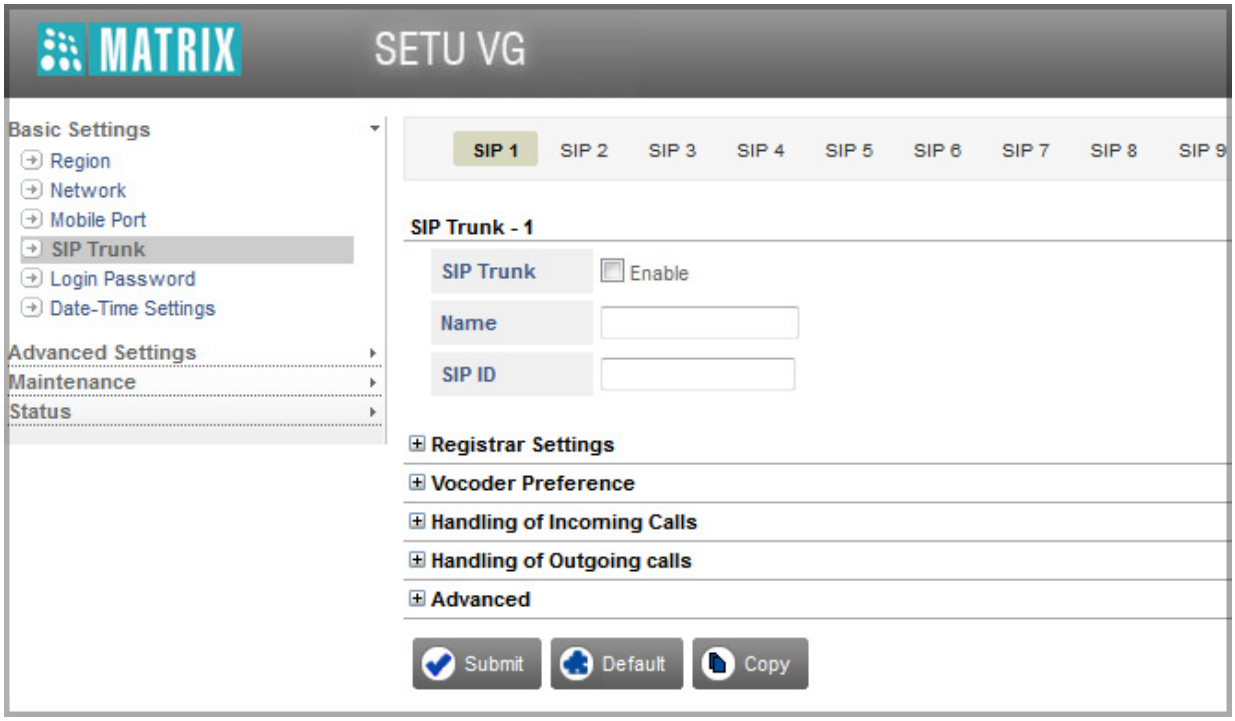
# SIP Trunk

SETU VG supports nine SIP Trunks. You can register all SIP Trunks with the same ITSP or with different ITSPs. These SIP Trunks may be configured as Proxy or Peer-to-Peer (non-proxy).

To configure a SIP Trunk,

- Click the **Basic Settings** link to expand.
- Click the **SIP Trunk** link.
- Click the SIP Trunk number tab, **SIP 1** to **SIP 9**, you want to configure.

  The desired **SIP Trunk** page opens.




- Select the **SIP Trunk Enable** check box to use the SIP Trunk. You may disable the SIP Trunk, if you do not want to route calls through this Trunk. Default: Disabled.
- You can assign a **Name** to the SIP Trunk for identification of this trunk. Default: Blank.

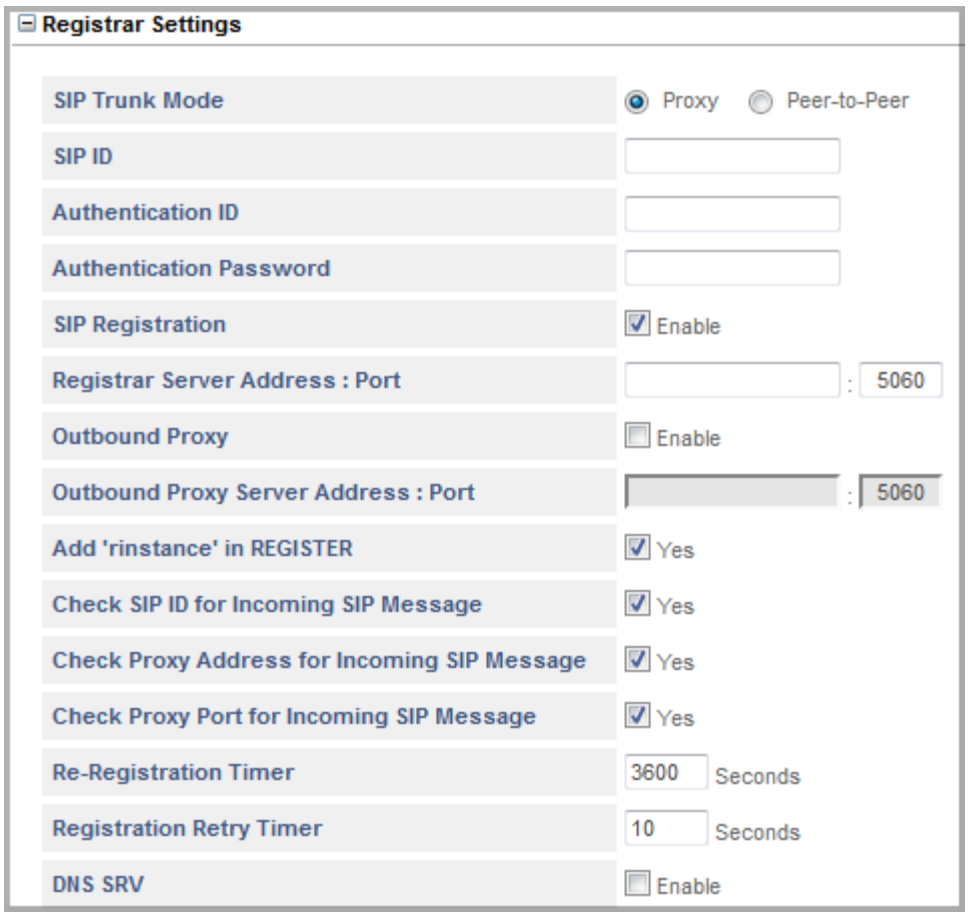
  You may assign the name of the ITSP with which the trunk is registered, or any other name of your choice.

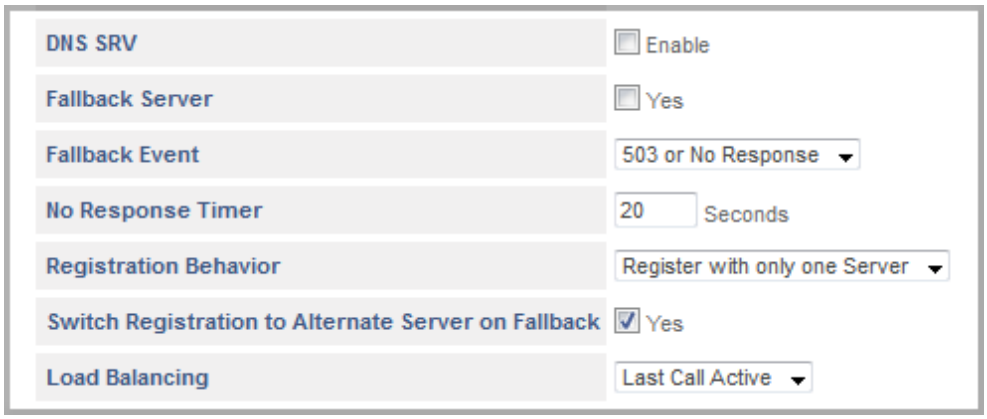
  The name you assign to the SIP Trunk will appear on the display of the remote party's phone, when a call is made through this Trunk.
- In **SIP ID**, the SIP ID that you assign under *Registrar Settings* will appear.

## Registrar Settings

- Click **Registrar Settings**.


- Select **SIP Trunk Mode** according to the type of your installation. Default: Peer-to-Peer.
  - Select **Proxy**, if you want to register the SIP Trunk with an ITSP or a Registrar Server.
  - Select **Peer-to-Peer**, if you want to use the SIP Trunk for Peer-to-Peer (non-proxy) calls.
- To configure **SIP Trunk Mode** as **Proxy**, do the following:






- Select **Proxy**. You will be presented with the related registrar settings.
- In **SIP ID**, enter the SIP ID provided by your ITSP. For example, if the SIP URI provided by the ITSP is 12345@abc.com, enter 12345 in this field. Default: Blank.

  The SIP ID is the number which remote parties will use to call this SIP Trunk.

  The SIP ID may be a number or text consisting of a maximum of 40 characters.
- Enter the **Authentication ID** (User ID) provided by your ITSP. Default: Blank.
- Enter the **Authentication Password** provided by your ITSP. Default: Blank.
- Keep the **SIP Registration** check box enabled.

  SETU VG will send the REGISTER message to Registrar proxy or Outbound proxy as applicable.

  Clear the check box only if you want to disable registration. Default: Enabled.
- In the **Registrar Server Address: Port** field, enter the Registrar Server Address and the Registrar Server's listening port for SIP messages. The registrar server address may be an IP address or a domain. The Registrar Server Address can be of maximum 64 characters. Valid port range: 1025–65534. Default Port: 5060.
- If your Service Provider uses outbound proxy for handling voice calls, select the **Outbound Proxy** check box. Default: Disabled.
- In the **Outbound Proxy Server Address: Port** field, enter the Outbound Proxy Server's IP Address and the Outbound Proxy Server's Listening Port for SIP. The Outbound Proxy Server Address may be of maximum 64 characters. Valid port range:1025–65534. Default Port: 5060.
- To add 'rinstance' in REGISTER message, keep the **Add 'rinstance' in REGISTER** check box enabled.

  'rinstance' is any random value which can be used by SETU VG to fetch its own contact binding, that is, to know the Registration Expiry Timer assigned by the server.

When you enable ‘rinstance’ in REGISTER, SETU VG will generate any random value of 'rinstance' and include it in the REGISTER message. The system will use the registration expiry timer of that contact binding.

- Keep the **Check SIP ID for Incoming SIP Message** check box enabled, if you want SETU VG to validate the SIP ID during an incoming call. Default: Enabled.

- Keep the **Check Proxy Address for Incoming SIP Message** check box enabled, if you want SETU VG to validate the Proxy Address during an incoming call. Default: Enabled.

- Keep the **Check Proxy Port for Incoming SIP Message** check box enabled, if you want SETU VG to validate the Proxy Port during an incoming call. Default: Enabled.

- Select **Send OPTIONS message as Heartbeat** check box, if you want SETU VG to send OPTIONS messages periodically to the Proxy Server to monitor its availability. Default: Disabled.

  Calls can be made and received only if the Proxy Server is alive. If the Proxy Server is unavailable (no response is received from the server), the status of the SIP Trunk will display *“Inactive”* along with the Reason for Failure.

- *To view status of the Proxy Server, go to “SIP Trunk” Status.*

- *The **Send OPTIONS message as Heartbeat** will work only if,*
  - ***SIP Trunk Mode** is configured as Proxy.*
  - ***SIP Registration** is disabled.*

  If you enable *Send OPTIONS message as Heartbeat*, you must configure the **Heartbeat Interval**.

- Set the **Heartbeat Interval** (Seconds). It is the time period after which SETU VG will send the OPTIONS message to the Proxy Server to check its availability. Valid range of Heartbeat Interval is from 10 to 999 seconds. Default: 60 seconds.

- Set the **Re-registration Timer**. This is the time period after which the SETU VG will send registration request to maintain registration binding with the Registrar server. Valid range: 00001–65535 seconds. Default: 3600 seconds.

*The **Re-registration Timer** will be applicable only if, **SIP Registration** is enabled.*

- Set the **Registration Retry Timer**. When a registration attempt fails, SETU VG will resend registration request to the Registrar Server after the expiry of the Re-registration Timer. Valid range: 00001–65535. Default: 10 seconds.

*The **Registration Retry Timer** will be applicable only if, **SIP Registration** is enabled.*

- If you want the system to send DNS SRV query to the configured domain server, enable **DNS SRV**. When disabled, the system will send DNS A query to the configured domain server. Default: Disabled.

*If you enable DNS SRV, Fallback Server logic will not be applicable.*

- Select the **Fallback Server** check box, if your Service Provider supports multiple servers in its network. Default: Disabled.

  If you have enabled Fallback Server and Outbound Proxy is disabled,

- In the **Fallback Registrar Server Address 1: Port** and **Fallback Registrar Server Address 2: Port** field, enter addresses of the alternate Registrar Servers and their respective listening ports. The Fallback Registrar Server Address can be of maximum 64 characters. Valid port range: 1025–65534. Default Port: 5060.

If you have enabled Fallback Server and Outbound Proxy is enabled,

- In **Fallback Outbound Proxy Server Address 1: Port** and **Fallback Outbound Proxy Server Address 2: Port** field, enter addresses of the alternate Outbound Proxy Servers and their respective listening ports. The Fallback Outbound Proxy Server Address can be of maximum 64 characters. Valid port range:1025–65534. Default Port: 5060.

- In the **Fallback Event** list, select the event on occurrence of which SETU VG should fallback to an alternate Registrar/Outbound Proxy Server, if available.
  - No Response
  - 503 or No Response
  - 5xx or No Response

  Default: 503 or No Response

  In case, the Fallback Server does not respond and the call is not routed to the destination port, the call will be routed to another port type as per the Routing/Fallback Routing Group configured for the SIP Trunk.

- Set the **No Response Timer**. It is the time for which SETU VG will wait for the response from the server for any request. If no valid response is received before the expiry of this timer, SETU VG will fallback to alternate Registrar/Outbound Proxy Server or Routing Group/Fallback Routing Group for further processing of the call. Valid range: 01–99 seconds. Default: 20 seconds.

*If the SIP General Request Timer configured in the System Parameters is less than the No Response Timer, then SETU VG will fallback to alternate Registrar/Outbound Proxy Server or Routing Group/ Fallback Routing Group on the expiry of the SIP General Request Timer and the No Response Timer will stop.*

- In the **Registration Behavior**, select the desired option:
  - Register with all Servers
  - Register with only one Server

  If you select **Register with only one Server**, SETU VG will get registered with the Registrar/Outbound Proxy Server. If registration with the Registrar/Outbound Proxy Server fails, it will get registered with Fallback Registrar/Outbound Proxy Server 1 or Fallback Registrar/Outbound Proxy Server 2 respectively for further processing of call.

  If you select **Register with all Servers**, SETU VG will get registered with Registrar/Outbound Proxy Server as well as Fallback Registrar/Outbound Proxy Servers. It will not apply Fallback logic even if *Fallback Server* is enabled.

*The **Registration Behavior** will be applicable only if, **SIP Registration** is enabled.*

- Keep the **Switch Registration to Alternate Server on Fallback** check box enabled. SETU VG will get unregistered with the current server and will register with the alternate server, if fallback occurs while sending the INVITE message.

*The **Switch Registration to Alternate Server on Fallback** will be applicable only if, **SIP Registration** is **enabled** and **Registration Behavior** is set as **Register with only one Server**.*

- Select the desired option for **Load Balancing** from the following:

  - **Last Call Active**: Each new call will be processed through the Registrar/Outbound Proxy Server through which the last active call has been processed.

    For example, if the last call has been processed by Fallback Registrar/Outbound Proxy Server 2, the new call will also be processed through Fallback Registrar/Outbound Proxy Server 2 only.

  - **First Active**: Each new call will be processed through the first active Registrar/Outbound Proxy Server only.

  - **Cyclic**: Each new call will be processed through the next active Registrar/Outbound Proxy Server.

    For example, if the last call has been processed by Fallback Registrar/Outbound Proxy Server 1, the new call will be processed through Fallback Registrar/Outbound Proxy Server 2 and the subsequent new call will be processed through the Registrar/Outbound Proxy Server.

  Default: Last Call Active.

*If you have disabled **SIP Registration**, it is recommended that you enable **Send OPTIONS message as Heartbeat** to use Fallback facility efficiently.*

- To configure **SIP Trunk Mode** as **Peer-to-Peer**, do the following:


- Select the **Peer-to-Peer** option. You will be presented with the related peer-to-peer SIP Trunk parameters.

- In the **SIP ID** field, enter the desired SIP ID which the remote parties will use to call this SIP Trunk. Default: Blank.

  The SIP ID may be a number or text consisting of a maximum of 40 characters.

- In the **Authentication ID** field, enter the ID of your preference as Authentication ID. Default: Blank.

- In the **Authentication Password** field, enter a password of your choice as Authentication Password for the Authentication ID you have assigned. Default: Blank.

- To configure the Peer-to-Peer Number strings, click **Settings** .

  The **Peer-to-Peer Dialing** table window opens.


You can add as many as 500 number strings to this table. Each entry in the table consists of the Destination Number, Destination Address and Name.

The first entry in the table is reserved for numbers that do no match with any of the entries in the table, the **No Match Found** entry. When the number dialed by users does not match with any of the entries in the table, the system uses the **Destination Address** assigned to the **No Match Found** entry in the table to route the call.

- To enter a number, click **Add**.

  The **Add Entry** window opens.


- In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters: 0 to 9, *, #, +, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

  If the number to be dialed out is <dialednumber@destination address>, for example, 123@abc.com, you must enter 123 in this field.

## Wildcard Characters

SETU VG supports following characters.

| Character | Description |
|---|---|
| **X** (letter X) | X represents any single digit from 0 to 9. |
| **#** | When # is configured in a number string, it will not be considered as End of Dialing. |
| ***** | When * is configured in a number string, it will not be considered as End of Dialing. |
| **+** | + (plus) can be configured as a first character of the Destination Number string in the *SIP Trunk-Destination Port Determination-Destination Number Based* table only. |
| **[ - ]** | Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket. |
| **[ , ]** | Comma within a bracket is used as a separator between the groups of numbers. |
| **[ ^ ]** | Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret. |
| **T** (letter T) | Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing. |

- In the **Destination Address** field, enter the domain name or IP Address where the dialed peer-to-peer number string is to be sent. The Destination Address may have up to 40 characters. Default: Blank.

  For example, if the peer-to-peer number to be dialed out is 123@abc.com, enter abc.com as Destination Address. If the number is 1234@ 192.168.1.197, enter 192.168.1.197 as the Destination Address. The Destination Address can also be in the form of Address: Port number.

- Enter a name in the **Name** field to identify the number string you configured. It may be the name of your contact or any name you want to assign to the number string. The name may consist of 12 characters (maximum). Default: Blank.

- Click **Submit** to save entries. The window closes.

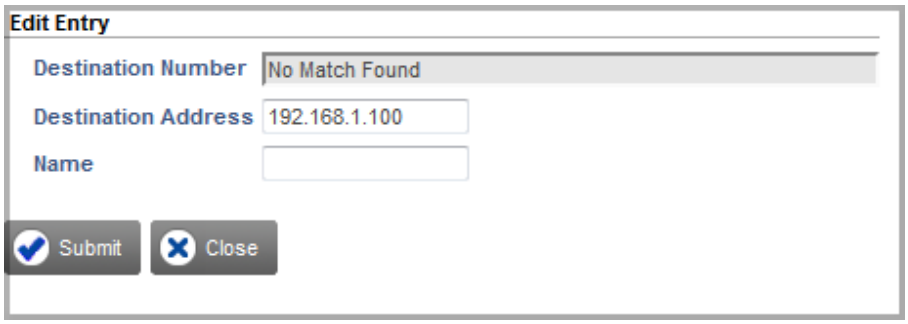
- The records appear in the Peer-to-Peer Dialing table.

*If there are multiple entries in the Peer to Peer Dialing table, to search a particular entry in the table, under Testing enter the desired number in the **Enter the destination number to know which entry would be selected for routing** search box.*

- You may also change the default values of the **No Match Found** entry in the table.

  - To change the default values of the No Match Found entry, under **Edit**, click **Settings** of the **No Match Found** entry.

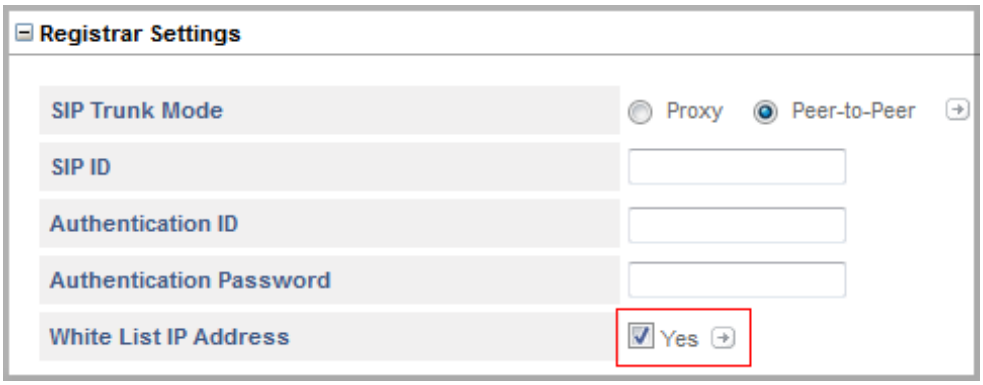
- The **Edit Entry** window opens.




  - Change the default values of the **Destination Address** and **Name** as per your requirement.
  - Click **Submit** and close the window.
- To delete an entry in the Peer-to-Peer Dialing Table, select the check box of the entry, and then click **Delete**.
- Close the window to return to the main page.

To know more about the Peer-to-Peer application, *see* "Peer to Peer Dialing" under *Advanced Settings*.

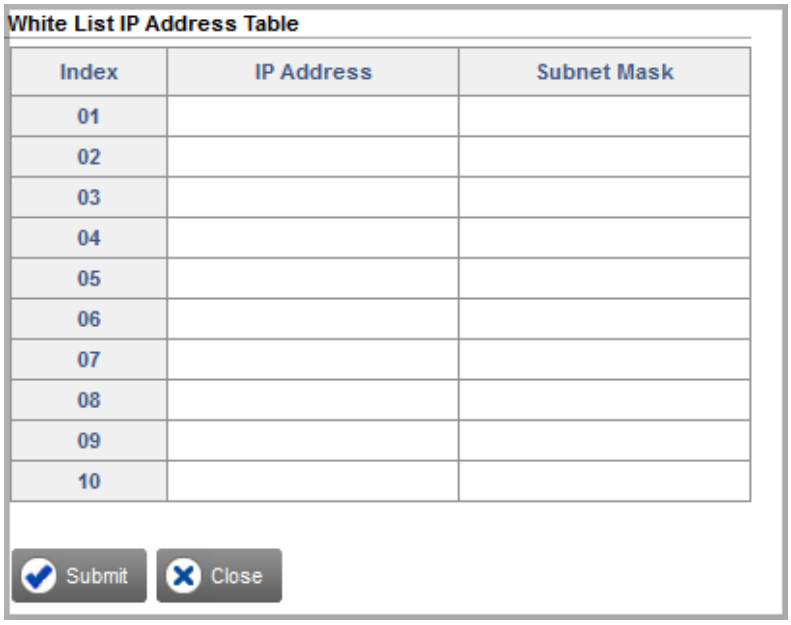
- To apply call restriction based on IP Address, select the **White List IP Address** check box and configure the White List IP Address table. Default: Disabled.




When the WAN Port of SETU VG is connected to a public IP network, it may be necessary that the system allows incoming calls from trusted IP addresses only. Make a list of trusted IP Addresses from which you want to allow incoming calls. You may list up to 10 such IP Addresses and their Subnet Masks.

- To configure the **White List IP Address table**, click **Settings** .

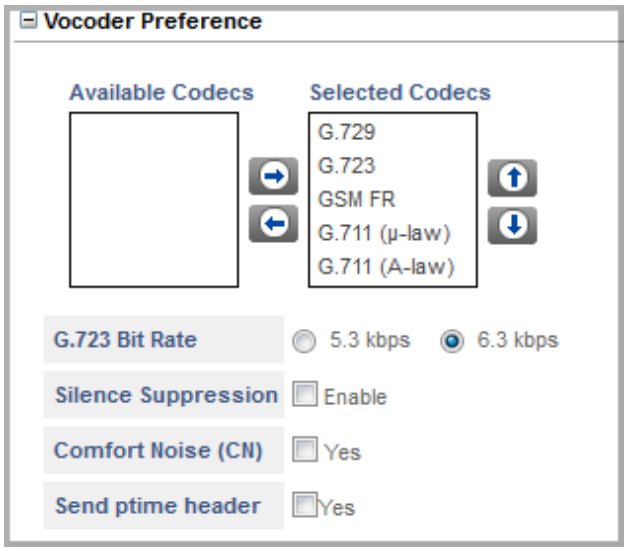
- The **White List IP Address Table** opens in a new window.




- Enter the **IP Addresses** and their respective **Subnet Mask** in the table.
- Click **Submit** and close the window.

## Vocoder Preference[4]

- Click **Vocoder Preference**.




4. *Codec list for SETU VG8 and SETU VG4 vary according to the DSP channel used in the system. The Vocoders supported by SETU VG4 appears in the Selected Codecs list in the following order of preference:*
   1. G. 729
   2. G.723
   3. GSM FR
   4. iLBC_30ms
   5. iLBC_20ms
   6. G.711 (μ – Law)
   7. G.711 (A - Law)

Vocoders are voice codecs used to compress the data in RTP packets for optimum use of bandwidth and for ensuring voice quality.

The Vocoders supported by SETU VG8 appears in the **Selected Codecs** list in the following order of preference:

1. G. 729
2. G.723
3. GSM FR
4. G.711 (μ – Law)
5. G.711 (A - Law)

- You can change the order of preference by moving the desired Vocoders up or down the list. To move a Vocoder up or down the list, do the following:
  - In the **Selected Codecs** list, click the Vocoder you want to move.
  - Click the UP/DOWN ARROW to move the Vocoder to the desired position in the list.
- To remove a Vocoder from the **Selected Codecs** list, click the Vocoder you want to remove, and then click the LEFT ARROW. The Vocoder is moved to the **Available Codecs** list.
- To move a Vocoder from the **Available Codecs** list to the **Selected Codecs** list, click the Vocoder you want to move, and then click the RIGHT ARROW.

- If you have **G.723** as a Preferred Vocoder, select the **G.723 Bit Rate** as **5.3 Kbps** or **6.3 Kbps**. Default: 6.3kpbs.

  When G.723 is negotiated, the selected Bit Rate will be applied only when sending the RTP packets. When receiving RTP packets from the remote end, both the Bit Rates of G.723 will be accepted.

- Select the **Silence Suppression Enable** check box, if you want SETU VG to suppress the *Silence* packets and allow only the *Voice* packets to pass through. Default: Disabled.

*Silence Suppression is applicable only when you have selected G.729 as Preferred Vocoder.*

- Select the **Comfort Noise (CN)** check box, if you want SETU VG to negotiate the Comfort Noise received in the SDP body with the remote peer. Default: Disabled.

- Select the **Send ptime header** check box, if you want SETU VG to add ptime header in the SDP offer and answer. Default: Disabled.

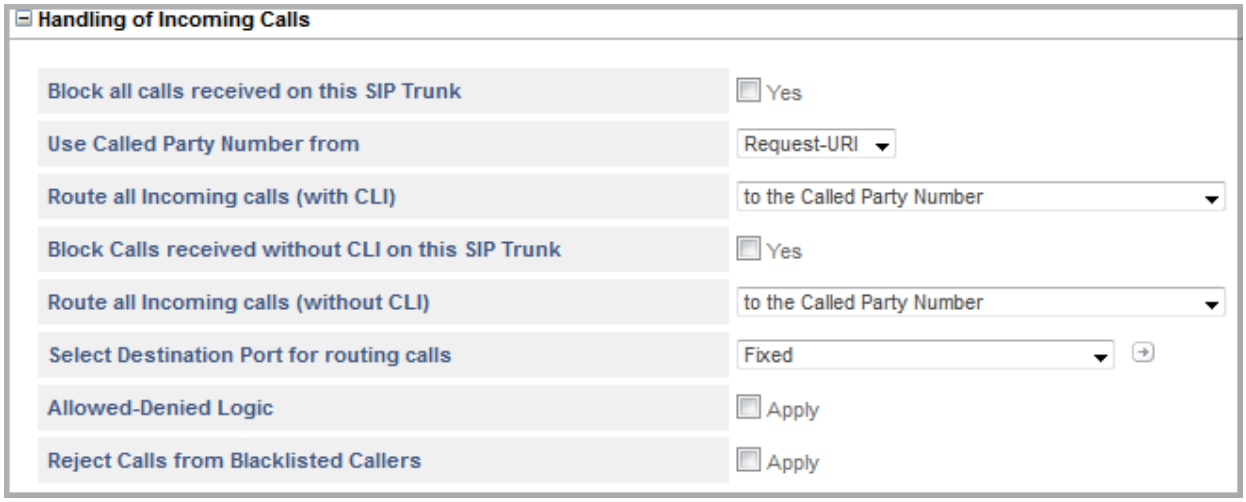
- You must select the **ptime value**, if you have enabled *Send ptime header* check box and have selected codec as—G. 729 and/or G.711 (μ – Law) and/or G.711 (A - Law). You can select from the following:
  - 10 msec
  - 20 msec
  - 30 msec
  - 40 msec

  Default: 20 msec

*For Passthrough FAX, SETU VG will use the default ptime value (20 msec) only.*

# Handling of Incoming Calls

- Click **Handling of Incoming Calls**.




- If you do not want to route calls received on this SIP Trunk, select the **Block all calls received on this SIP Trunk** check box. Default: Disabled.

- By default, SETU VG identifies the Called Party Number for routing the incoming call on the SIP Trunk further, by the number received in the **Request-URI** of the INVITE message.

  If you want the system to identify the Called Party Number from the 'To Field' of the INVITE message, in the **Use Called Party Number From** parameter, select the **To Field** option.

## Destination Number Determination

Select the desired destination number determination method for routing incoming calls *with* and *without* CLI.

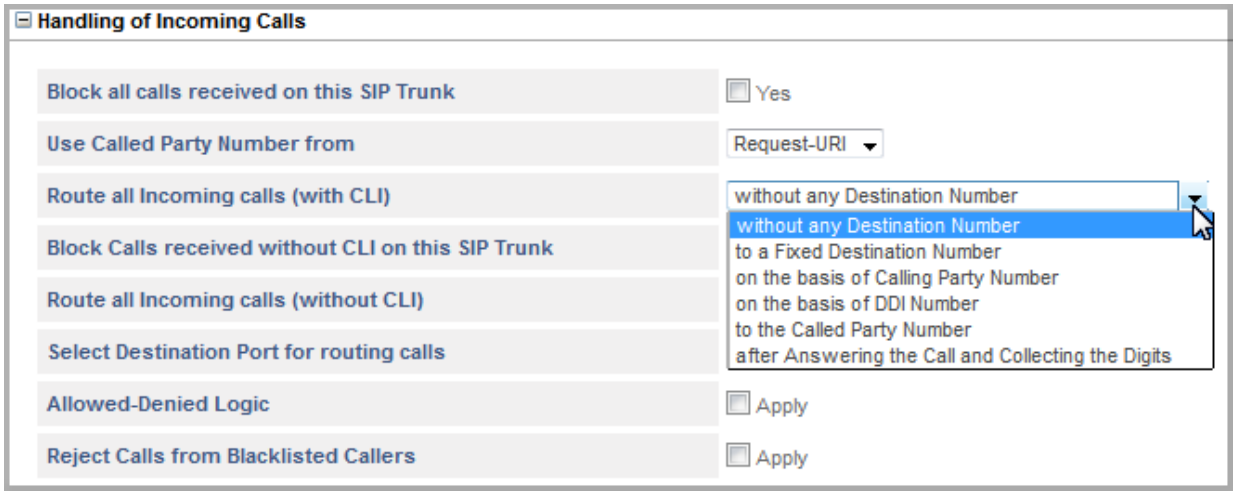
- To **Route all Incoming calls (with CLI)**, you may select from any of the following methods.
  - without any Destination Number
  - to the Fixed Destination Number
  - on the basis of Calling Party Number
  - on the basis of DDI Number
  - to the Called Party Number
  - after Answering the Call and Collecting the Digits

  Default: to the Called Party Number

  Read further for instructions on selecting and configuring each of these destination number determination methods.

### *Route Calls without any Destination Number*

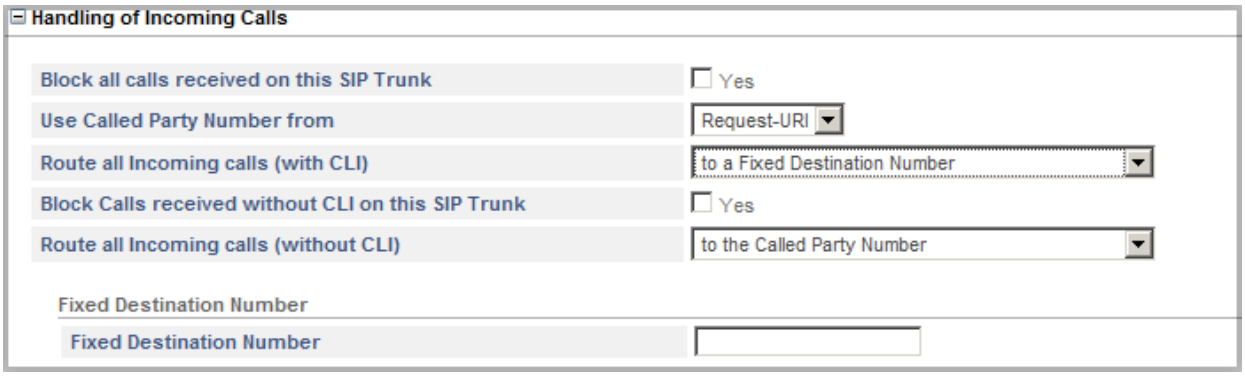
In this method, all calls received on the SIP Trunk are directly routed to a fixed destination port configured for the SIP Trunk, irrespective of the Destination Number.




- To apply this method, in the **Route all incoming calls (with CLI)** list, click **without any Destination Number**.

### *Route to the Fixed Destination Number*

In this method, calls received on the SIP Trunk are routed to a fixed destination number configured for the SIP Trunk.




To apply this method, do the following:

- In the **Route all Incoming calls with CLI** list, click **to a Fixed Destination Number**.
- In the **Fixed Destination Number** box that appears, enter the desired destination number. The Destination Number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and (.) dot. Default: Blank.
- Click **Submit** to save the changes.

### *Route on the basis of Calling Party Number*

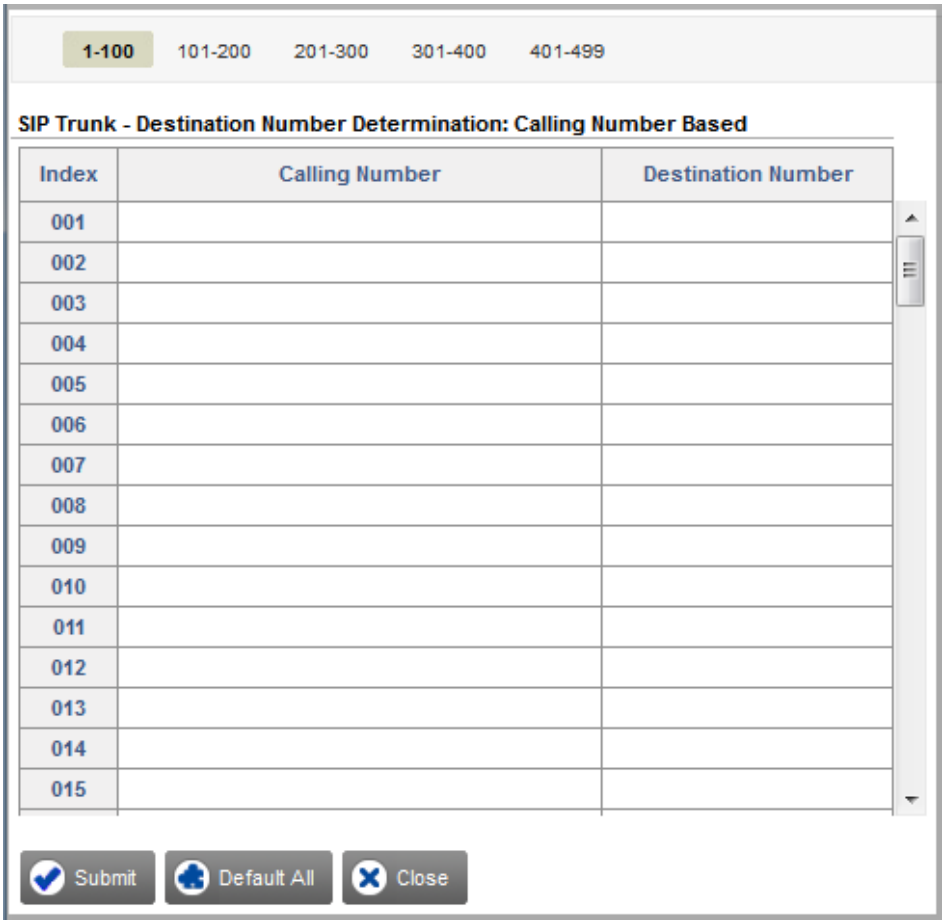
In this method, a call received on the SIP Trunk is routed to a specific number, as per the calling party's number.

You must configure the calling party numbers in the Calling Party Number Based Table. When there is an incoming call on the SIP Trunk, SETU VG will match the CLI of the number received with the entries of this table. If a match is found for the number in the table, the call is routed to the destination port.

To apply this method, do the following:

- In the **Route all Incoming calls with CLI** list, click **on the Basis of Calling Party Number**.
- Click **Settings** .

The **Calling Number Based Table** page opens. You can store up to 500 numbers in this table.




- In the **Calling Number** column**,** enter the calling party numbers. The Calling numbers may consist of a maximum of 24 characters. All ASCII characters are allowed. Default: Blank.

- For each calling party number, enter a corresponding destination number in the **Destination Number** column. Destination numbers may consist of a maximum of 24 characters. Characters 0-9, *, # and dot (.) are allowed. Default: Blank.

- Click **Submit** to save your entries. Close the window to return to the SIP Trunk page.

  You can also configure the **Calling Number Based** Table from *Advanced Settings.* See “Destination Number Determination” under *Advanced Settings* for instructions.

- Select a method for routing incoming calls with CLI that *do not match* with any entries in the Calling Party Number Based Table.

  In the **If no match found in the Calling Party Number Table, route calls** box, click the desired method from the following options for processing the call:
  - to a Fixed Destination Number
  - to the Called Party Number
  - on the basis of DDI Number
  - after Answering the Call and Collecting the Digits

  Default: to the Called Party Number.

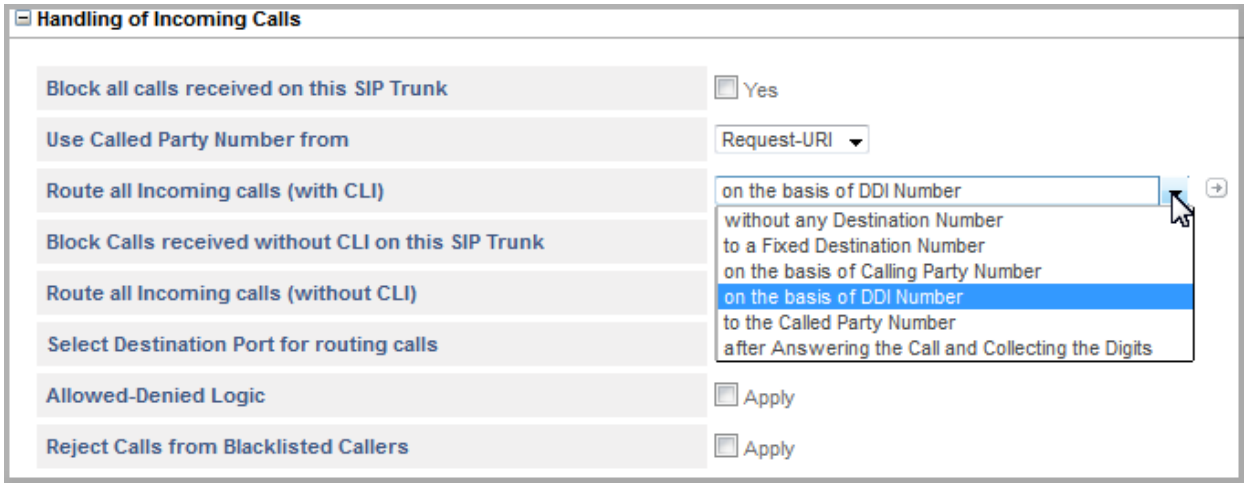
### *Route on the basis of DDI Number*

In this method, a call received on the SIP Trunk is routed to a specific number as per the DDI number received in the SIP INVITE message.

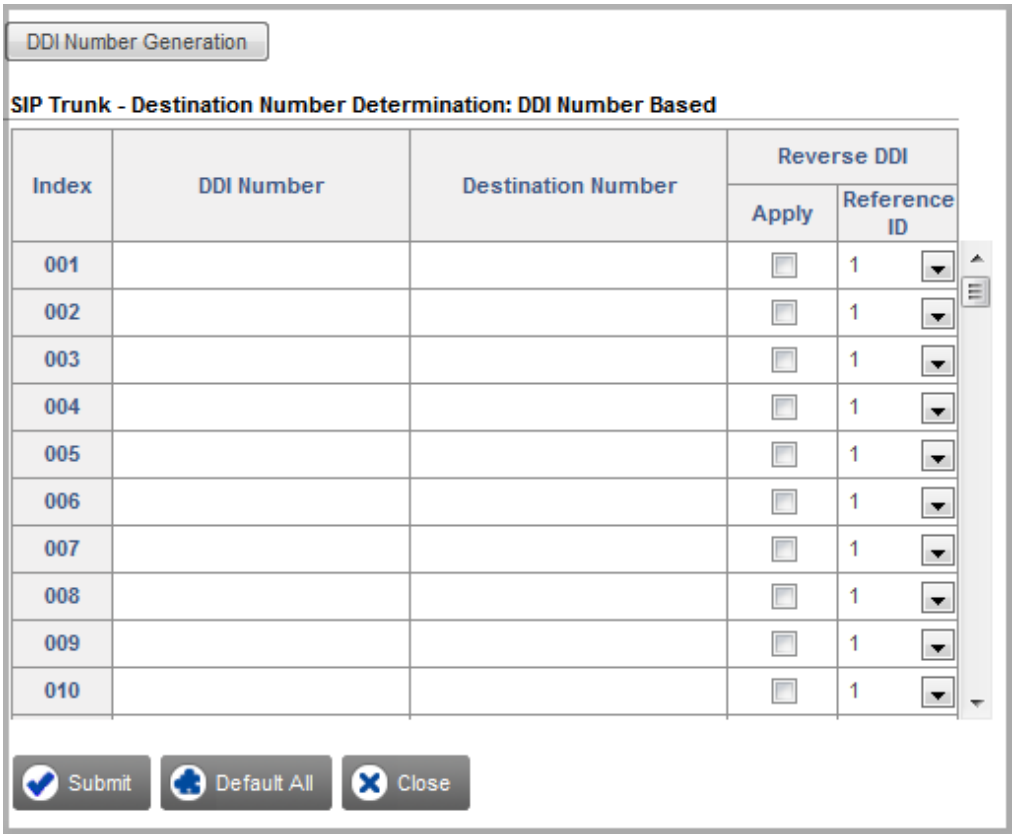
You must configure the DDI numbers in the DDI Number Based Table. When there is an incoming call on the SIP Trunk, SETU VG will match the CLI of the number received with the entries of this table. If a match is found for the number in the table, the call is routed to the destination port.

To apply this method, do the following:

- In the **Route all Incoming calls with CLI** list, click **on the Basis of DDI Number**.
- Click **Settings** .



The **DDI Number Based Table** page opens. You can store up to 100 numbers in this table.




- There are two ways to generate the DDI Numbers:
  - Using the DDI Number Generation Button to automatically generate the DDI Number Table. See "Configuring SIP-DDI Number Based Table" in *Destination Number Determination* topic for instructions.

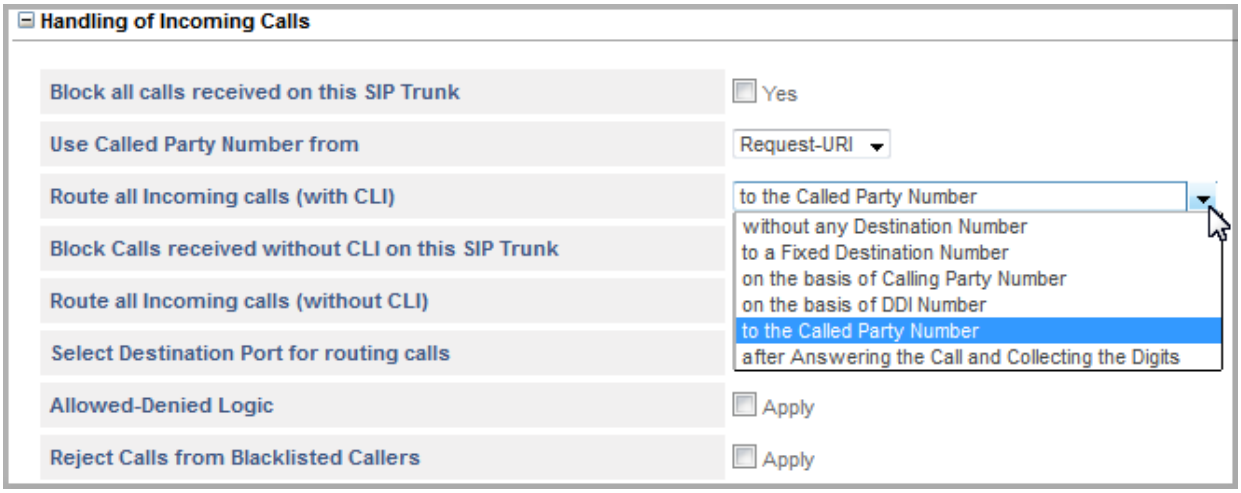
    **OR**

  - Entering each DDI Number manually.
    - In the **DDI Number** column**,** enter the DDI numbers allotted by your service provider. The DDI numbers may consist of a maximum of 24 characters. Characters 0-9, +, * and # are allowed. Default: Blank.
    - In the **Destination Number** column, enter a corresponding destination number for each DDI number. Destination numbers may consist of a maximum of 24 characters. Characters 0 to 9, * and # are allowed. Default: Blank.
    - To apply **Reverse DDI** for each number, select the **Reverse DDI Apply** check box and select the **Reference ID** for the number. Default: Apply Reverse DDI is disabled and Reference ID is 1.
  - Click **Submit** to save your entries. Close the window to return to the SIP Trunk page.

    You can also configure the DDI Number Based Table from Advanced Settings. See "Destination Number Determination" under *Advanced Settings* for instructions.

### *Route to the Called Party Number*

In this method, a call is routed to a specific number depending upon the called party number received in the SIP ID of the Request URI of the INVITE message.



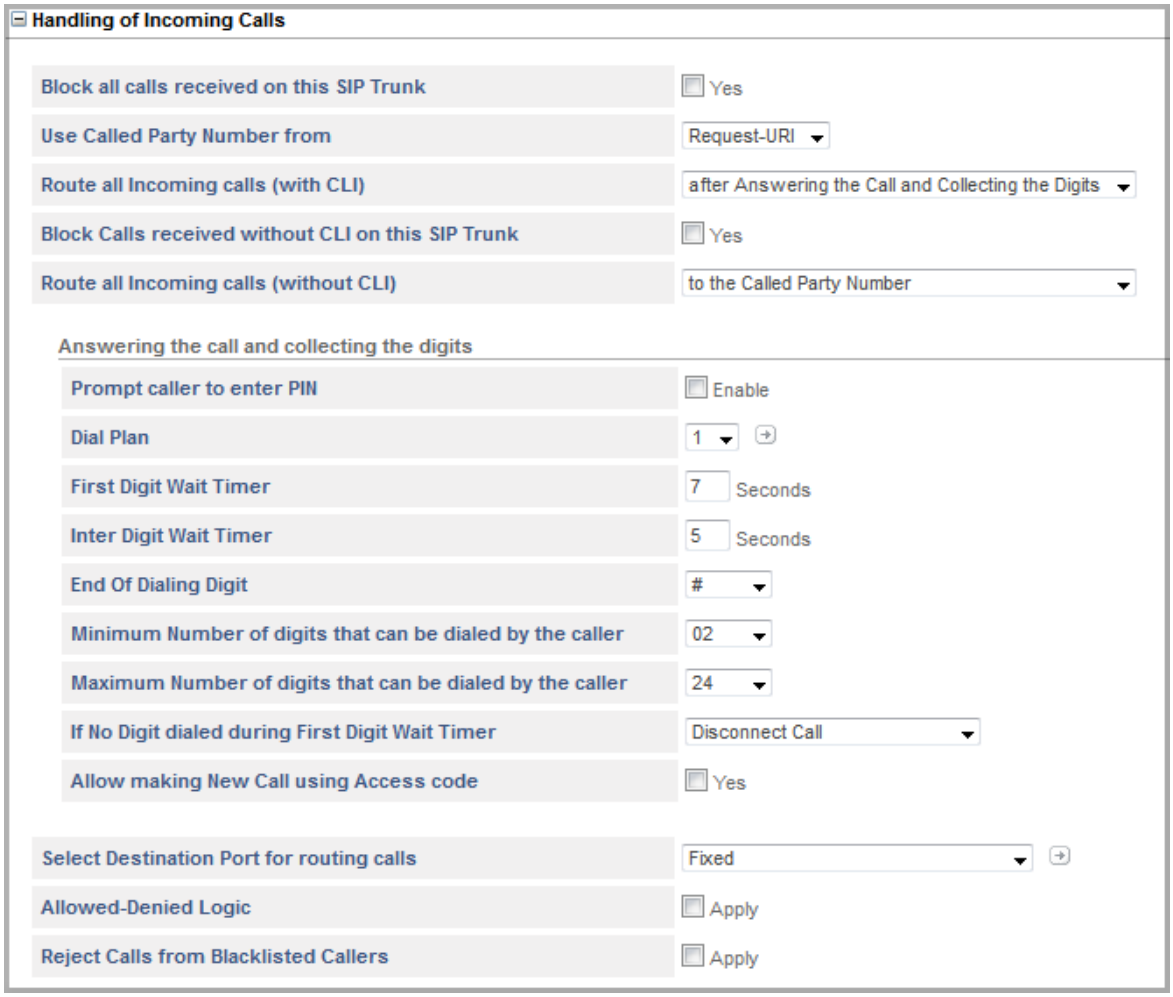

- To apply this method, in the **Route all Incoming calls with CLI** list, click **to the Called Party Number**.

### *Route After Answering the Call and Collecting the Digits*

In this method, the Incoming call is answered and dial tone is played to the caller, allowing the caller to dial the desired number. The number dialed by the caller is considered as the destination number.

To apply this method, do the following:

- In the **Route all Incoming calls with CLI** list, click **after Answering the Call and Collecting the Digits**.




The related parameters of this method appear under **Answering the call and collecting the digits**.

- To enable PIN Authentication for incoming calls on this port, select the **Prompt caller to enter PIN** check box.

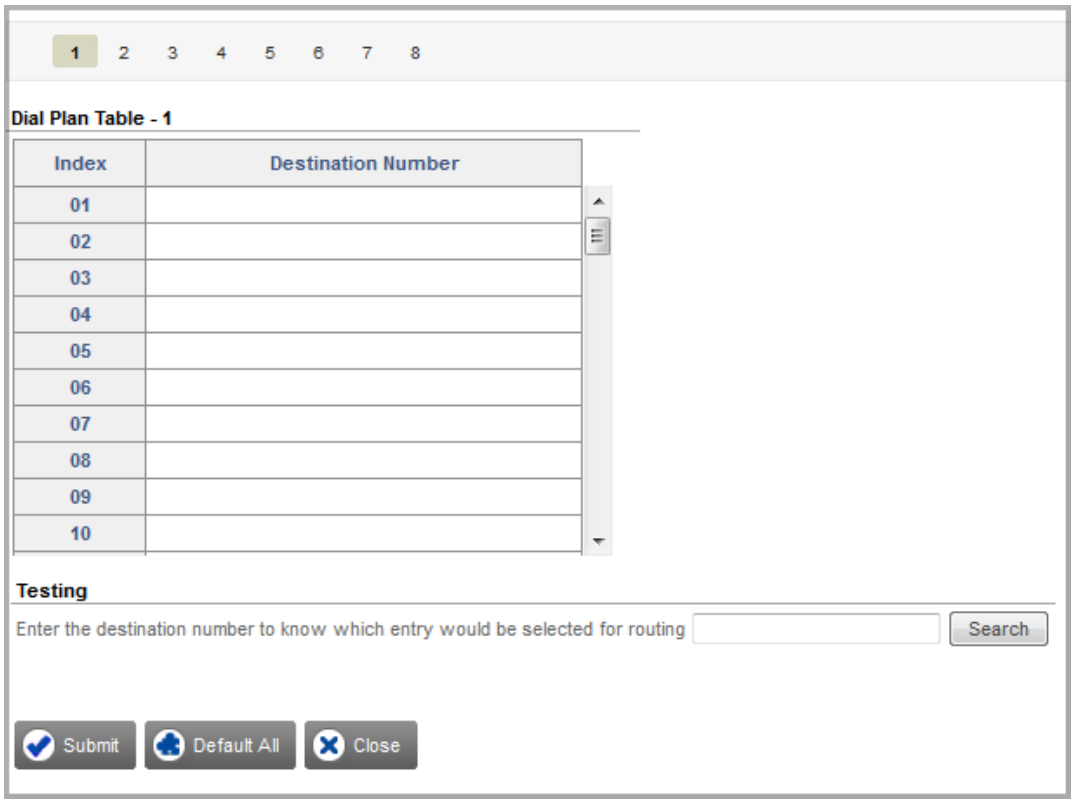
  If you enable this check box, you must also configure the PIN Authentication Table. To know more about this feature and for detail instructions, see "PIN Authentication" under *Advanced Settings*.

- Select the **Dial Plan** that you want the system to use to route the incoming calls received on the SIP Trunk. Default: Dial Plan Table - 1.

  If you have not configured the Dial Plan table, you may do so now.

  - Click **Settings** .

- The Dial Plan page opens in a new window.




- You may configure the default Dial Plan Table-1 or any other Table (from 2 to 8) for the SIP Trunk. You can store 64 Numbers at Index Numbers 01 to 64 respectively.
- In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters: 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

  See "Dial Plan" for more details.
- Click **Submit** to save the entries and close the window.
- Return to the Dial Plan parameter and select the Dial Plan Table you configured.
- If required, you may change the duration of the **First Digit Wait Timer (FDWT)**. This is the time for which the system waits for the user to dial the destination number. Valid range: 01–99 seconds. Default: 7 seconds.
- You may configure the following options as End-of-Dialing indication:
  - In the **Inter Digit Wait Timer** field, define the number of seconds the system should wait while receiving the dialing digits, to consider it as end-of-dialing. You may change this timer, if required.The valid range is 01 to 99 seconds. Default: 05 seconds.
  - In the **End of Dialing Digit** field**,** select # or * as termination digit the system should consider to detect end-of-dialing. Default: #

- In the **Minimum number of digits that can be dialed by the caller** field, select the minimum number of digits that the user must dial for the system to route the call. Valid range: 01–24 digits. Default: 2 digits.

***Minimum number of digits that can be dialed by the caller*** *parameter will be applicable when:*

- *the Destination Port Determination method selected is On the basis of Destination Number and the dialed number is not found in the Destination Number Table.*
  *Or*
- *the dialed number is not found in the Dial Plan and the End of Dialing is detected.*

- In the **Maximum number of digits that can be dialed by the caller** field, select the maximum number of digits to be dialed by the user for the system to consider it as end-of-dialing**.** The valid range is 01 to 24 digits. Default: 24 digits.

When the caller dials a number, the system will match it with the end-of-dialing indications and accept the one that matches first.

- If the caller fails to dial the number during the First Digit Wait Timer, you can either have the system disconnect the call or route the call to a fixed destination number.

  In the **If No Digit dialed during First Digit Wait Timer (FDWT)** box, select the desired option: **Disconnect the Call** or **Use Fixed Destination Number**. Default: Disconnect Call.

  - If you selected **Use Fixed Destination Number**, enter the desired destination number in the **Fixed Destination Number** field**.** The Destination number may consist of a maximum of 24 digits. Valid digits are 0 to 9, *, # and (.) dot. Default: Blank.

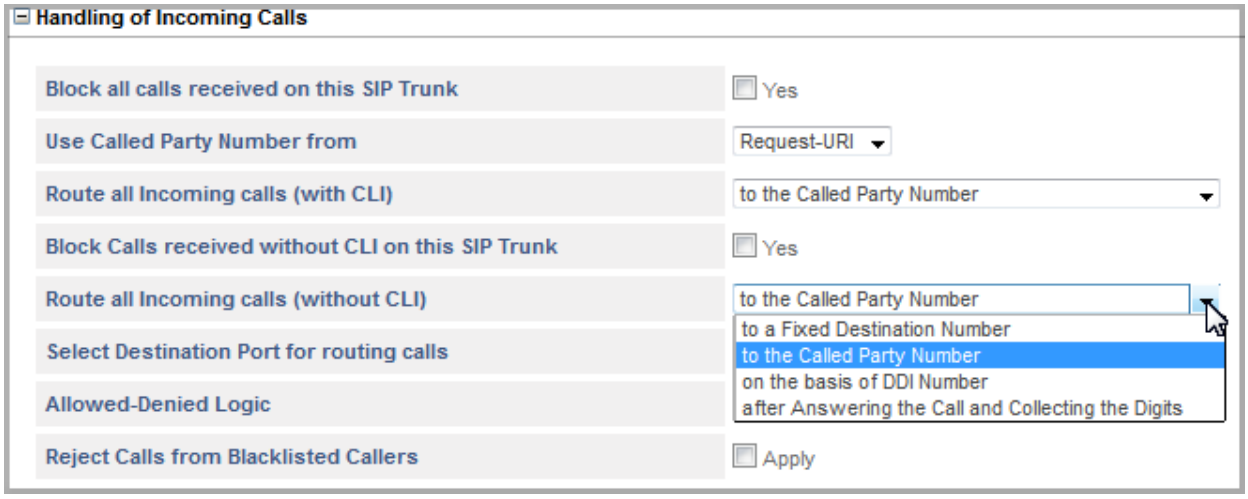
- Select the **Allow making New Call using Access Code** check box, if you want to enable the feature Making New Call using Access Code on the SIP Trunk. See “Making a New Call using Access Code”.

- Click **Submit** to save settings.

- If you do not want to route calls without CLI through this SIP Trunk, select the **Block Calls received without CLI on this SIP Trunk** check box.

- To **Route all Incoming calls (without CLI),** you may select from any of the following methods: Default: to the Called Party Number.
  - to a Fixed Destination Number, see “Route to the Fixed Destination Number”.
  - to the Called Party Number, see “Route to the Called Party Number”.
  - on the basis of DDI Number, see “Route on the basis of DDI Number”
  - after Answering the Call and Collecting the Digits, see “Route After Answering the Call and Collecting the Digits”.

Default: to the Called Party Number.




## Destination Port Determination

- In **Select the Destination Port for routing calls**, select from any of the following options:
  - Fixed
  - on the basis of Destination Number
  - on the basis of Calling Party Number

  Default: Fixed

- *SETU VG supports maximum two SIP to SIP Calls.*
- *If the destination number to be dialed out is an IP Address, SETU VG will not check the Destination Port Determination Method. Instead, it will route the call using the SIP Trunk / Group programmed for IP Dialing. See "IP Dialing" to know more.*

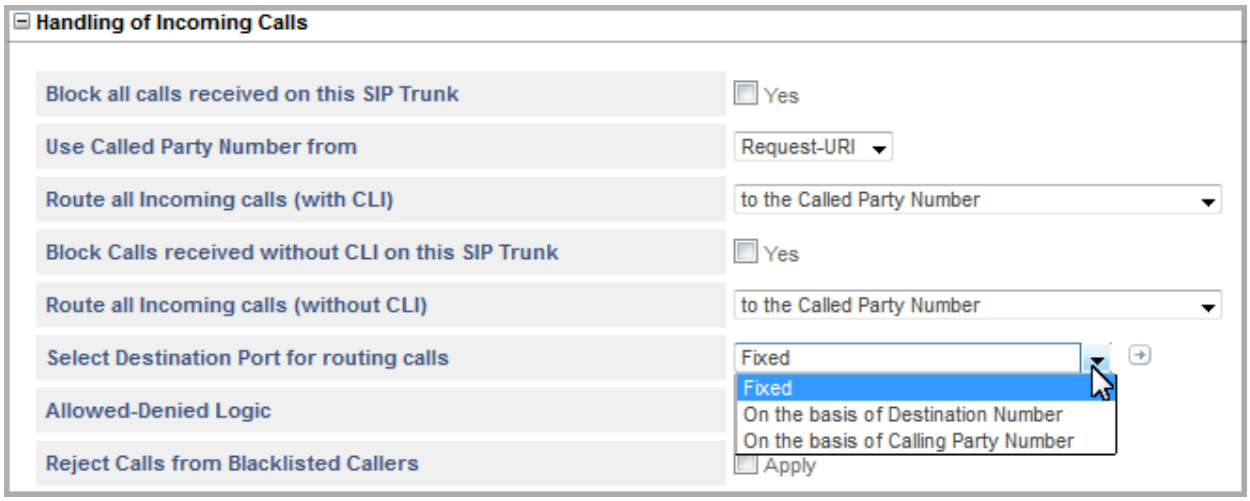
### *Fixed*

In this method, calls received on the SIP Trunk are routed to a fixed destination port, irrespective of the number dialed on the SIP Trunk.

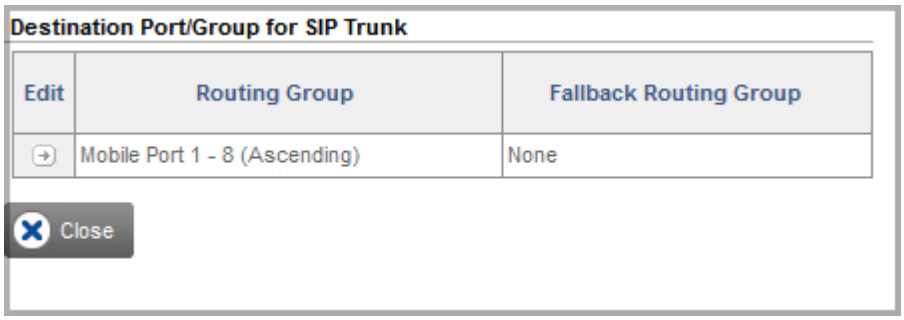
To apply this method, do the following:

- In the **Select Destination Port for routing calls** box, click **Fixed**.

- Click **Settings** .

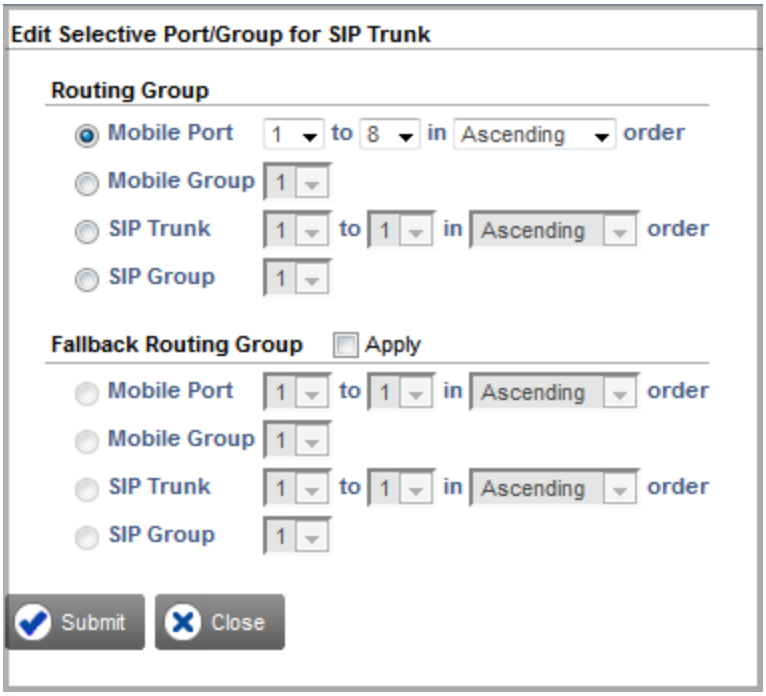



The **Destination Port/Group for SIP Trunk** window opens.




- To change the default Routing Group and create the Fallback Routing Group, under **Edit**, click **Settings** .

The **Edit Selective Port/Group for SIP Trunk** window opens.




- Create the **Routing Group**.
- To create a group of *sequential* **Mobile Port** as members,
  - Select the desired **Mobile Port** numbers as members. Default: 1.
  - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

    Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.
- To create a group of *not-sequential* **Mobile Ports** as members,
  - Select **Mobile Group**.
  - Select the **Mobile Group** number. Default:1.
  - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See “Group” for detailed instructions.
- To create a group of *sequential* **SIP Trunks** as members,
  - Select the desired **SIP Trunk** numbers as members. Default: 1.
  - In the **in - order** field, select the order in which the system should hunt for a free member SIP Trunk to route the call.

Select **Ascending** to start hunting from the first to the last member SIP Trunk. Select **Descending** to start hunting from the last to the first member SIP Trunk. Default: Ascending.

- To create a group of *not-sequential* **SIP Trunks** as members,
  - Select a **SIP Group**.
  - Select **SIP Group** number. Default:1.
  - Click **Settings** . The **SIP Groups** window opens. Create the SIP Group. See "Group" for detailed instructions.

- To create the **Fallback Routing Group**,
  - Select the **Apply** check box.
  - Follow the same instructions as given for creating *sequential* and *not-sequential* groups, for SIP Trunks and Mobile Ports.
  - Click **Submit** to save changes. The **Edit** window closes.
- The changes you made appear in the **Destination Port/Group for SIP Trunk** window. Close this window to return to the main page.

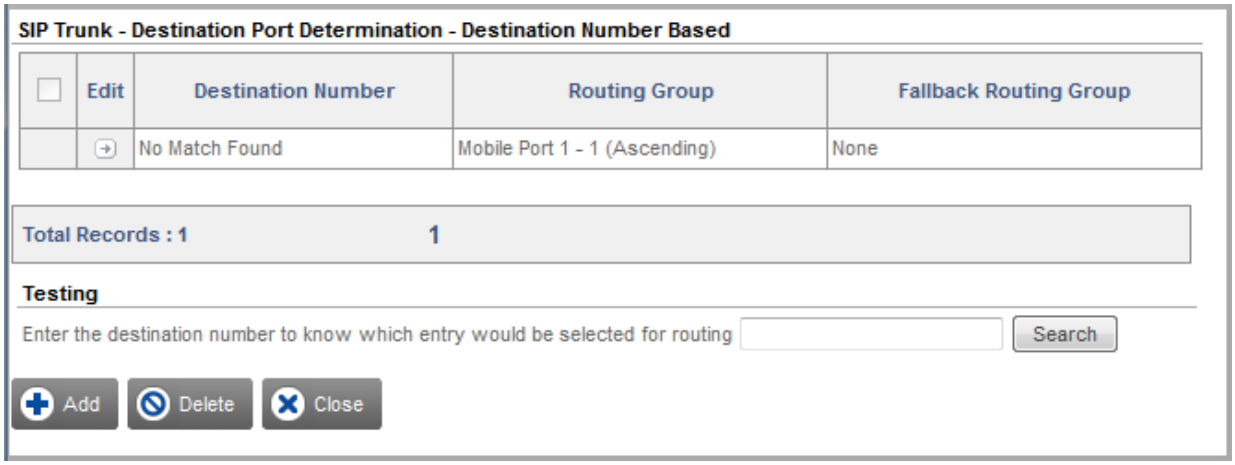
### *On the basis of Destination Number*

In this method, incoming calls on the source port are routed to the destination port on the basis of the destination number (called party number) dialed by the caller.

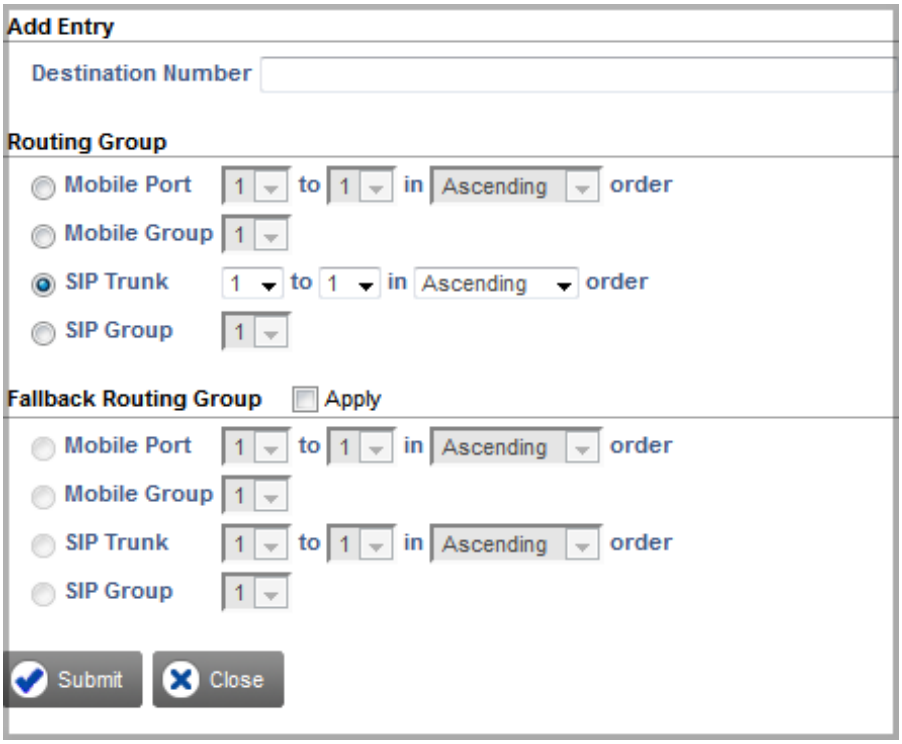
To apply this method, do the following:

- In the **Select Destination Port for routing calls** box, click **On the basis of Destination Number**.
- Click **Settings** .

The **SIP Trunk - Destination Port Determination - Destination Number Based** table window opens.




- Click **Add** to add a new entry. The **Add Entry** window opens. You can add upto 100 entries.




- In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters: 0 to 9, *, #, +, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.
- Create the **Routing Group**.
  - To create a group of *sequential* **Mobile Port** as members,
    - Select the desired **Mobile Port** numbers as members. Default: 1.
    - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.

- To create a group of *not-sequential* **Mobile Ports** as members,
  - Select **Mobile Group**.
  - Select the **Mobile Group** number. Default:1.
  - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See "Group" for detailed instructions.
- To create a group of *sequential* **SIP Trunks** as members,
  - Select the desired **SIP Trunk** numbers as members. Default: 1.
  - In the **in - order** field, select the order in which the system should hunt for a free member SIP Trunk to route the call.

    Select **Ascending** to start hunting from the first to the last member SIP Trunk. Select **Descending** to start hunting from the last to the first member SIP Trunk. Default: Ascending.
- To create a group of *not-sequential* **SIP Trunks** as members,
  - Select a **SIP Group**.
  - Select **SIP Group** number. Default:1.
  - Click **Settings** .The **SIP Groups** window opens. Create the SIP Group. See "Group" for detailed instructions.

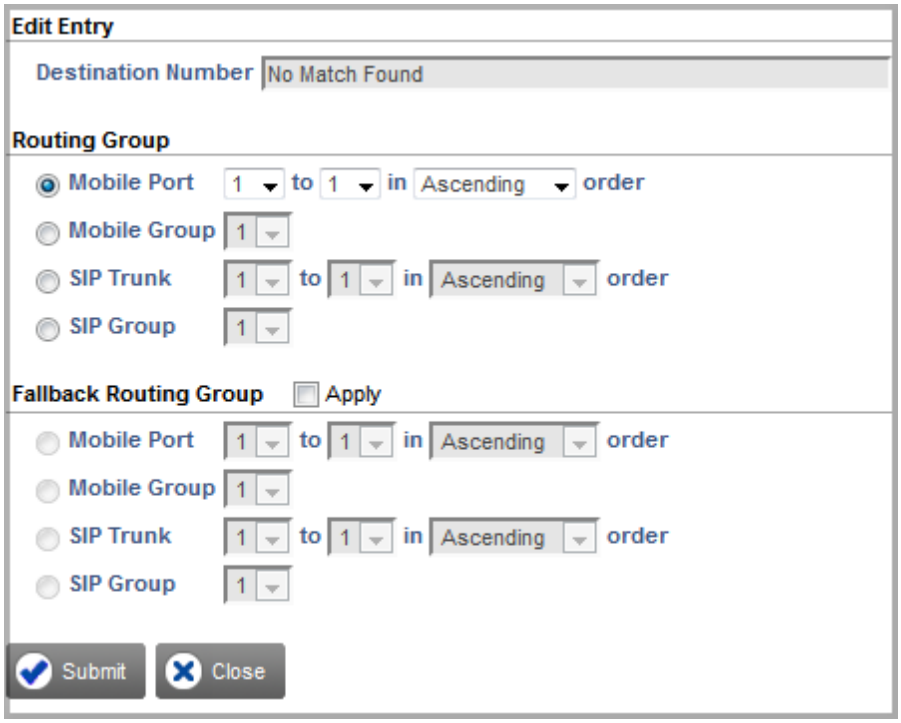
- To create the **Fallback Routing Group**,
  - Select the **Apply** check box.
  - Follow the same instructions as given for creating *sequential* and *not-sequential* groups, for SIP Trunks and Mobile Ports.
  - Click **Submit** to save changes. The **Add Entry** window closes.
- The entry you added appears in the **SIP Trunk - Destination Port Determination - Destination Number Based** window.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click **Delete** button.

*If there are multiple entries in the Destination Number Based table, to search a particular entry in the table, under Testing enter the desired number in the **Enter the destination number to know which entry would be selected for routing** search box.*

- By default, SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

  To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

  - For the **No Match Found** entry in the table, under **Edit**, click **Settings** .




  - The **Edit Entry** window opens.
  - Create the **Routing Group** and **Fallback Routing Group** as per your requirement.
  - Click **Submit** and close the window.

- Close the window if you have finished adding/editing entries.

  You can also configure the **Destination Number Based** Table from *Advanced Settings*. See “Destination Port Determination” under Advanced Settings.

### *On the basis of Calling Party Number*

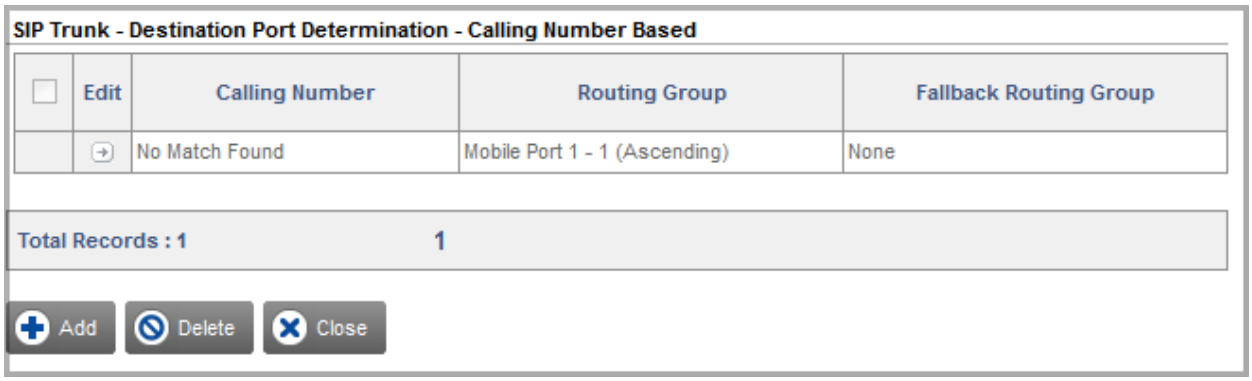
In this method, incoming calls on the SIP Trunk are routed to a specific port, as per the calling party's number.

To apply this method, do the following:

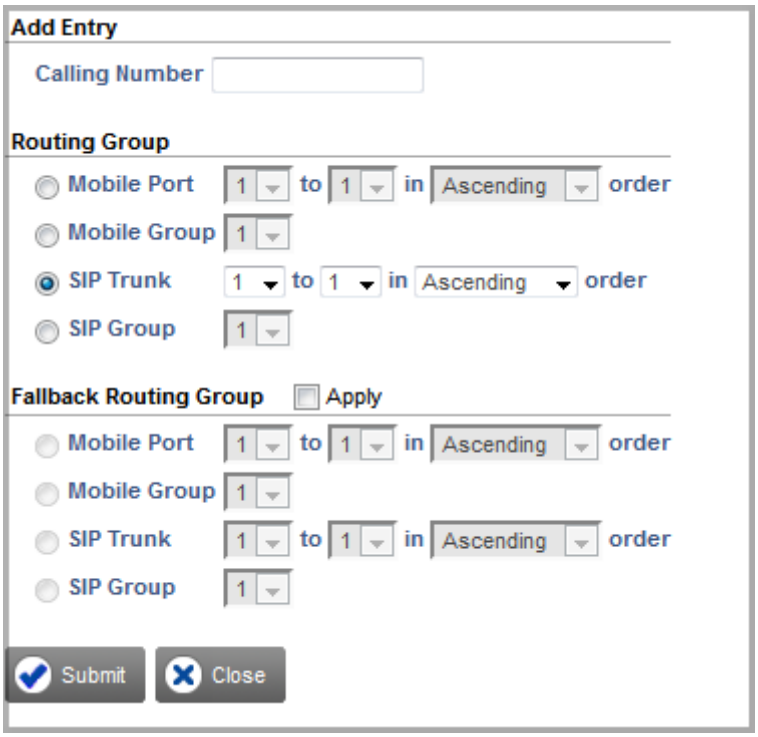
- In the **Select Destination Port for routing calls** box, click **on the basis of Calling Party Number**.

- Click **Settings** .


The **SIP Trunk - Destination Port Determination - Calling Number Based** table window opens.



- Click **Add** to add a new entry. The **Add Entry** window opens. You can add upto 500 entries.




  - In the **Calling Number** field, enter numbers (max. 24 characters) from which you expect calls to be received. All ASCII characters are allowed. Default: blank.
  - Create the **Routing Group**.
    - To create a group of *sequential* **Mobile Port** as members,
      - Select the desired **Mobile Port** numbers as members. Default: 1.
      - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

        Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.
    - To create a group of *not-sequential* **Mobile Ports** as members,
      - Select **Mobile Group**.
      - Select the **Mobile Group** number. Default:1.
      - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See “Group” for detailed instructions.
    - To create a group of *sequential* **SIP Trunks** as members,
      - Select the desired **SIP Trunk** numbers as members. Default: 1.

- In the **in - order** field, select the order in which the system should hunt for a free member SIP Trunk to route the call.

  Select **Ascending** to start hunting from the first to the last member SIP Trunk. Select **Descending** to start hunting from the last to the first member SIP Trunk. Default: Ascending.

- To create a group of *not-sequential* **SIP Trunks** as members,

  - Select a **SIP Group**.

  - Select **SIP Group** number. Default:1.

  - Click **Settings** . The **SIP Groups** window opens. Create the SIP Group. See “Group” for detailed instructions.

- To create the **Fallback Routing Group**,

  - Select the **Apply** check box.

  - Follow the same instructions as given for creating *sequential* and *not-sequential* groups, for SIP Trunks and Mobile Ports.

  - Click **Submit** to save changes. The **Add Entry** window closes.

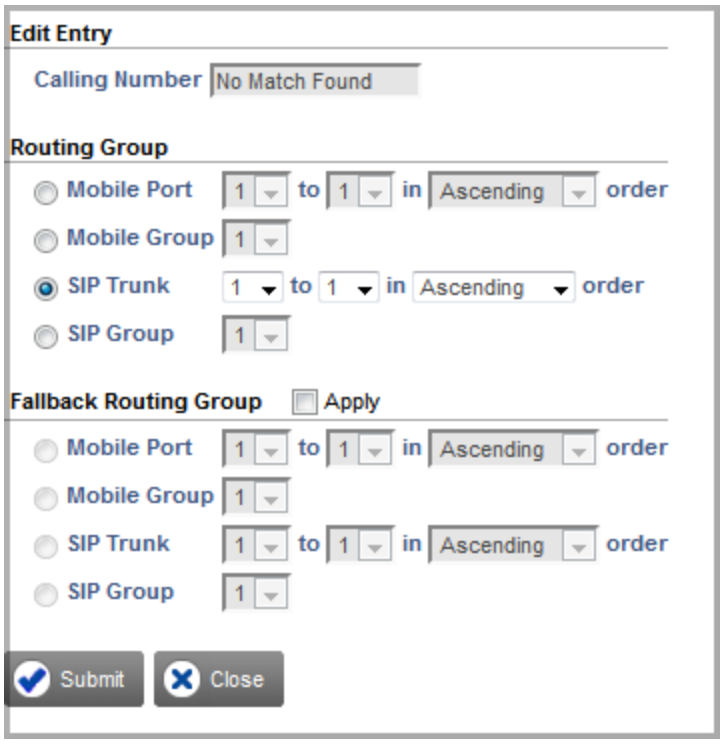
- The entry you added appears in the **SIP Trunk- Destination Port Determination - Calling Number Based** window.

- By default SIP Trunk 1-1 (Ascending) is assigned as the Routing Group, for routing calls from numbers that do not match with any of the destination numbers you configured (No Match Found).

  To change the default Routing Group and to create the Fallback Routing Group for the No Match Found numbers entry,

  - For the **No Match Found** entry, under **Edit**, click **Settings** .

- The **Edit Entry** window opens.




  - Create the **Routing Group** and **Fallback Routing Group**.
  - Click **Submit** and close the window.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click **Delete** button.
- Close the window if you have finished adding/editing entries.

  You can also configure the **Calling Number Based** Table from *Advanced Settings*. See “Destination Port Determination” under Advanced Settings.

## Allowed - Denied Logic (Toll Control)

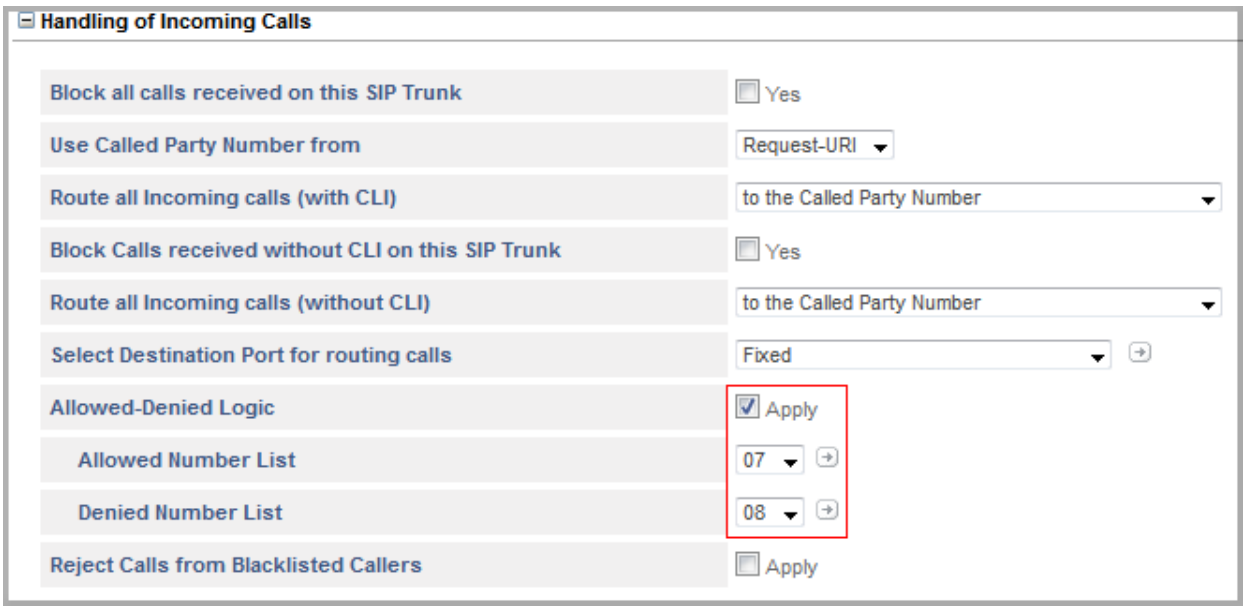
With the Allowed-Denied Numbers feature you can permit and restrict the dialing of particular numbers from the SIP Trunk. You can use this feature for applying Toll Control on the SIP Trunk.

Allowed Denied Number Logic makes use of two Number lists:

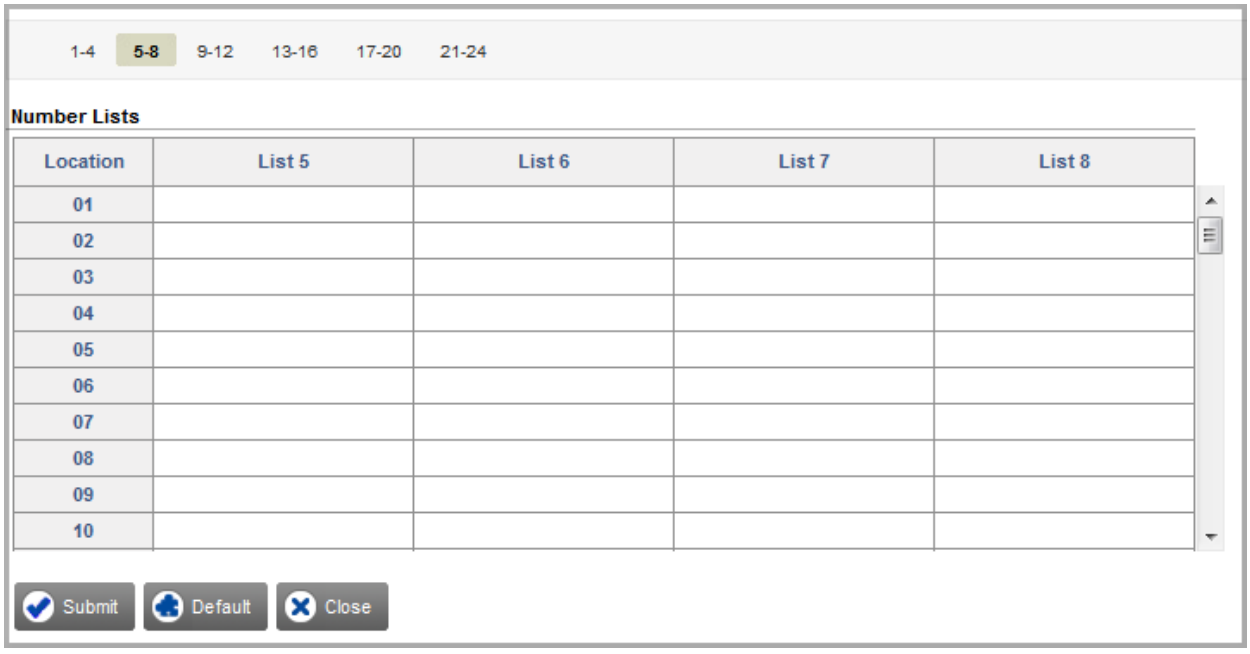
- **Allowed Numbers List:** This is the list of numbers that are allowed to be dialed out by the caller on the SIP Trunk. By default, List Number 7 is assigned to the SIP Trunk.
- **Denied Numbers List:** This list contains the numbers that are denied to be dialed out by the caller on the SIP Trunk. By default, List Number 8 is assigned to the SIP Trunk.

To apply Allowed - Denied Logic on the SIP Trunk,

- Select the **Allowed - Denied Logic** check box.




- To configure the **Allowed Number List**, click **Settings** .




- The Number List page opens in a new window.
- By default, Number List 7 is assigned as Allowed Number List.
- Enter the numbers you want the system to allow to be dialed in this list.
- Click **Submit** to save the entries and close the window.

- To configure the **Denied Number List**, click **Settings** .
  - The Number List page opens in a new window.
  - By default, Number List 8 is assigned as Denied Number List.
  - Enter the numbers you want the system to restrict from being dialed out in this list.
  - Click **Submit** to save the entries and close the window.

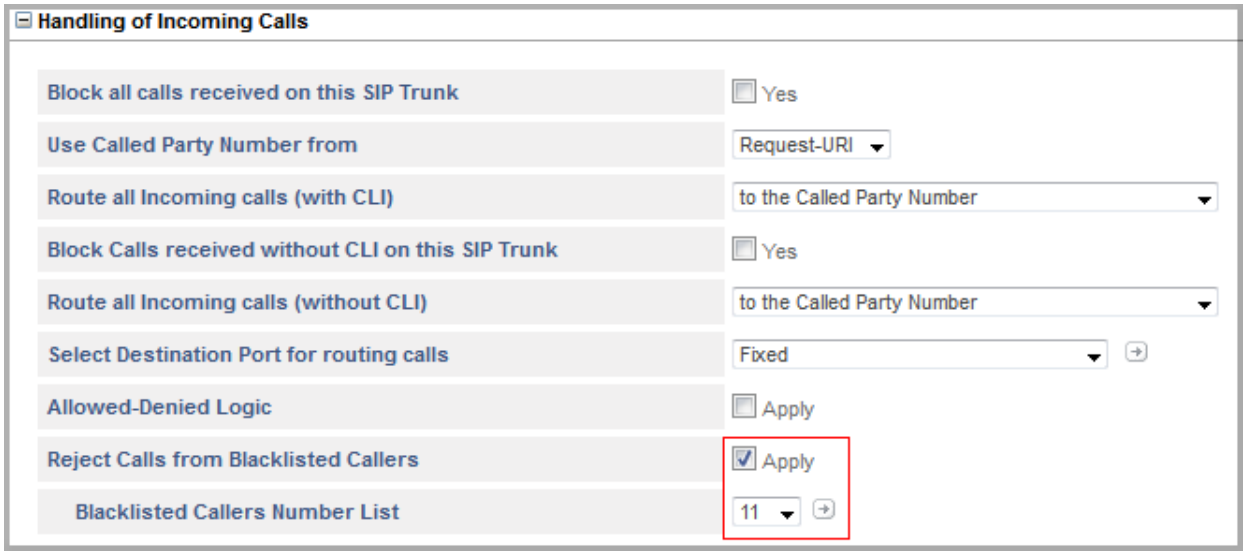
You may configure a different Number List as Allowed and Denied List. See “Allowed - Denied Logic” under “Number Lists”.

## Black Listed Callers

With the Black Listed Callers feature you can block incoming calls from specific addresses/numbers on SIP Trunks. Thus all incoming calls from the numbers you have 'blacklisted' will be automatically rejected by SETU VG.

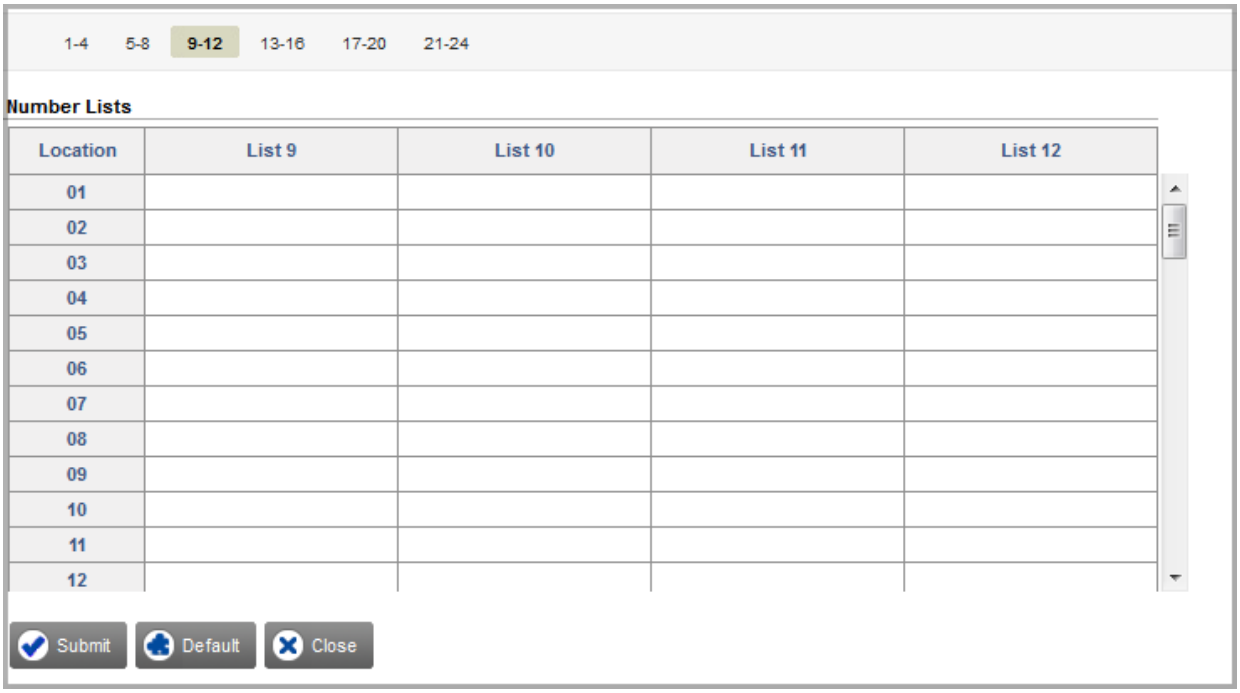
To apply Black Listed Callers on SIP Trunk,

- Select the **Reject Calls from Blacklisted Callers** check box.




- Configure the **Black Listed Callers** table. To do this,
  - Click **Settings** .

- The Number List page opens in a new window.




- By default, Number List 11 is assigned as Black Listed Callers List.
- Enter the numbers of unwanted callers in this list.

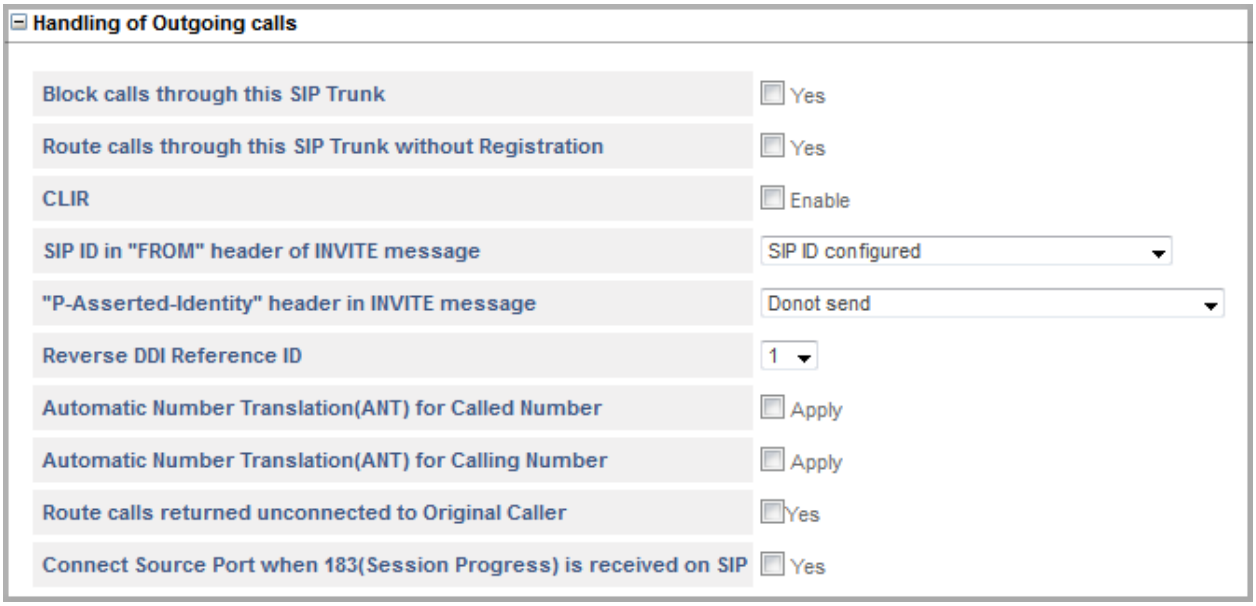
*Make sure you have configured the full SIP URI (for example: 12345@abc.com) of the unwanted callers in the Blacklisted Callers Number List.*

- Click **Submit** to save the entries and close the window to return to the main page.

## Handling of Outgoing Calls

When a SIP Trunk is determined as the destination port, numbers dialed from this port constitute outgoing calls.

- Click **Handling of Outgoing calls**.




- If you do not want to route outgoing calls through this SIP Trunk, select the **Block calls through this SIP Trunk** check box.

- To allow the users to make outgoing calls irrespective of whether the SIP Trunk has been successfully registered with the proxy or not, select the **Route Calls through this SIP Trunk without Registration** check box.

  By default, the system does not allow outgoing calls to be made if the status of the SIP Trunk is 'not registered'.

- By default, the CLI of the SIP Trunk is sent to the called party when outgoing calls are made using the SIP Trunk. If you do not want to send CLI, enable the **CLIR** check box. Default: Disabled.

- Select an option you want to send as **SIP ID in "FROM" header of INVITE message**. You may select:
  - SIP ID configured
  - Caller ID received on Source Port
  - Caller ID after applying Reverse DDI logic

  Default: SIP ID configured

- Select an option you want to send as **"P-Asserted-Identity" header in INVITE message**. You may select:
  - Do not send
  - Send SIP ID configured
  - Send Caller ID received on Source Port
  - Send Caller ID after applying Reverse DDI logic
    - Configure an option you want to send as *"P-Asserted-Identity" header in INVITE message*, **If no match found using Reverse DDI logic**. You may select:
      - Send SIP ID configured.

    - Send Caller ID received on Source Port
    - Send Fixed Number.
- Send Fixed Number

Default: Do not send

If you have selected *Send Fixed Number* as an option for *"P-Asserted-Identity" header in INVITE message* or *If no match found using Reverse DDI logic*, configure the **Fixed Number**. The Fixed Number can be a maximum of 24 characters. Characters 0-9, +, * and # are allowed. Default: Blank.

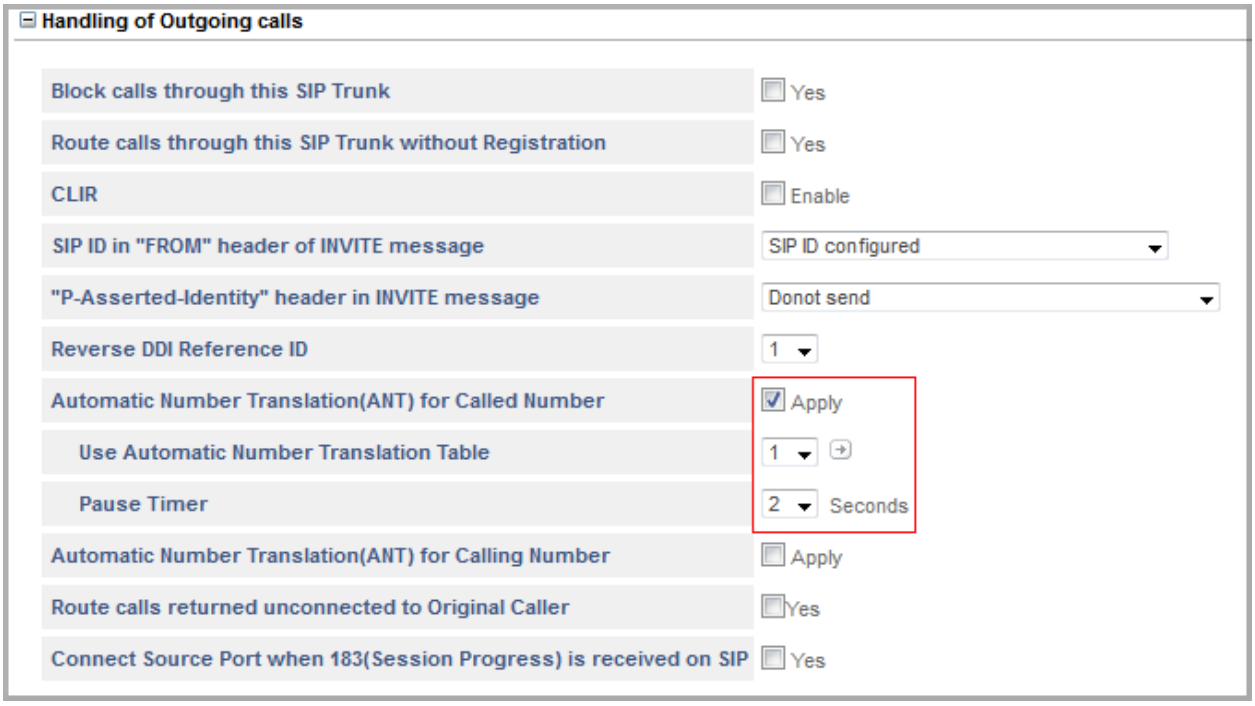
*If you have enabled **CLIR** and **"P-Asserted-Identity" header in INVITE message** is configured other than Do not send, then SETU VG will add **Privacy = ID** header in the INVITE message during an outgoing call from SIP Trunk.*

- Select the **Reverse DDI Reference ID**, if you have selected *Caller ID after applying Reverse DDI logic* as SIP ID in "FROM" header of INVITE message and/or *Send Caller ID after applying Reverse DDI logic* as "P-Asserted-Identity" header in INVITE message.

  SETU VG will compare the Reference ID configured on the SIP Trunk with the one configured in the SIP Trunk - Destination Number Determination: DDI Number Based Table. If a match is found, SETU VG will send the corresponding DDI Number to the Called Party.

- You can apply **Automatic Number Translation logic** on outgoing calls made from the SIP Trunk.

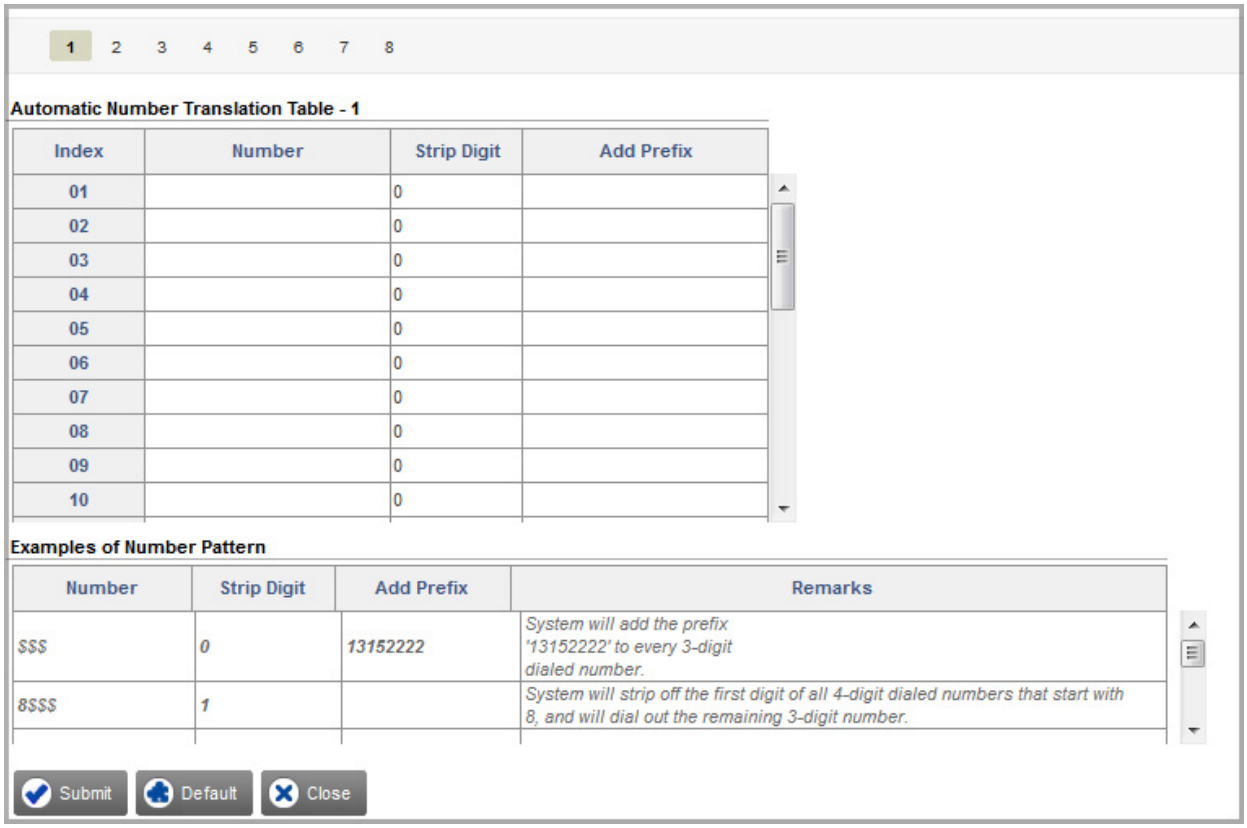
    - To apply ANT logic on the Called Numbers, click the **Automatic Number Translation (ANT) for Called Number** check box. Default: Disabled.




    - In the **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Called Numbers. Default: Table 1.

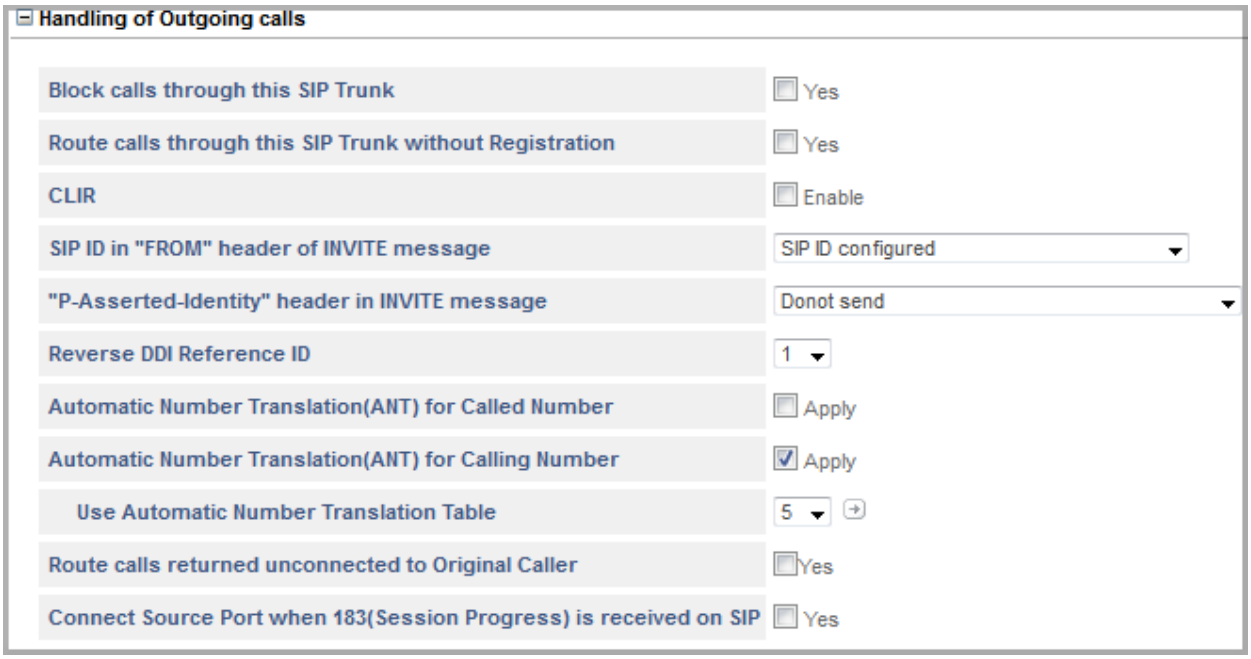
      If you have not configured the Automatic Number Translation Table,

- Click **Settings** . The Automatic Number Translation Table page will open in a new window.




  - You may configure the default Automatic Number Translation Table 1 or any other Table (2 to 8). See “Automatic Number Translation (ANT)” to configure the ANT Table.
  - Click **Submit** to save the ANT Table and close the window.
  - Return to ANT parameter and assign the ANT Table you configured.
  - Click **Submit** to apply List.
- Configure the **Pause Timer**, if you have configured ^ (Pause) in the Add Prefix column of the ANT Table. The valid range of the Pause Timer is 1 to 9 seconds. Default: 2 seconds.

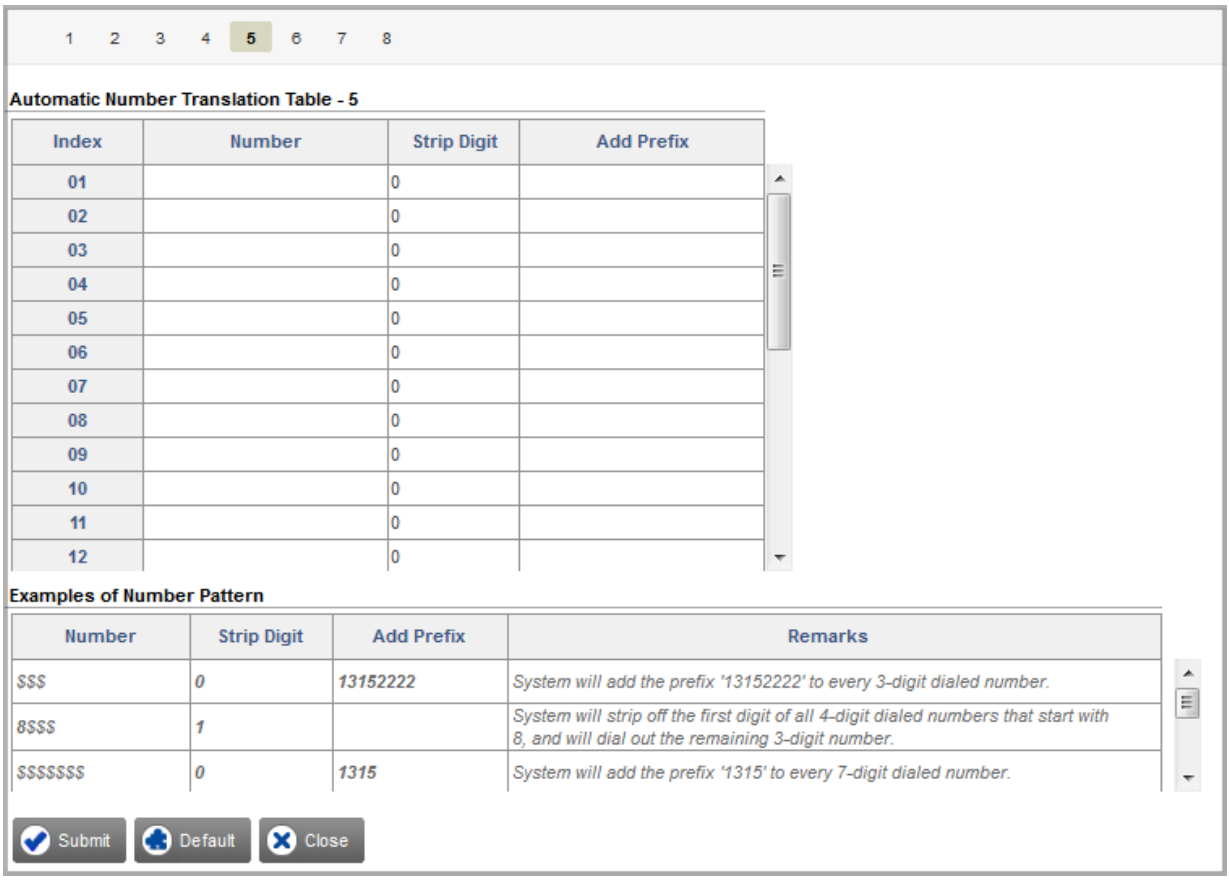
- To apply ANT logic on the Calling Numbers, click the **Automatic Number Translation (ANT) for Calling Number** check box. Default: Disabled.




- In the **Use Automatic Number Translation Table**, select the ANT Table number you have configured for the Calling Numbers. Default: Table 5.

  If you have not configured the Automatic Number Translation Table,

- Click **Settings**. The Automatic Number Translation Table page will open in a new window.




  - You may configure the default Automatic Number Translation Table 5 or any other Table. See "Automatic Number Translation (ANT)" to configure the ANT Table.
  - Click **Submit** to save the ANT Table and close the window.
  - Return to ANT parameter and assign the ANT Table you configured.
  - Click **Submit** to apply List.

- Select the **Route calls returned unconnected to original caller** check box, if you want SETU VG to route outgoing calls made from this port that returns unconnected back to the original caller.

  If you enable this feature, when an outgoing call is made using this Trunk, and the Called Party is found busy or does not respond, SETU VG stores the number of the Calling Party, the number of the Called Party, the source port type and number and the trunk port type and number used for routing the outgoing call in the RCOC table. A record of each such call is stored for the duration of the *Unconnected Calls Record Delete Timer* (configurable; default: 999 minutes).

  If the called party returns the call before the expiry of this Timer, SETU VG checks whether *Apply RCOC only if the caller calls back on the same trunk from which the call was made* is enabled or not, and accordingly place the incoming call to the original calling party. See "System Parameters" to configure the *Unconnected Calls Record Delete Timer* and *Apply RCOC only if the caller calls back on the same trunk from which the call was made* check box.

- To connect the Source Port with the Destination Port without waiting for the call on the Destination Port to mature, select to enable the **Connect Source Port when 183 (Session Progress) is received on SIP** check box. Default: Disabled.

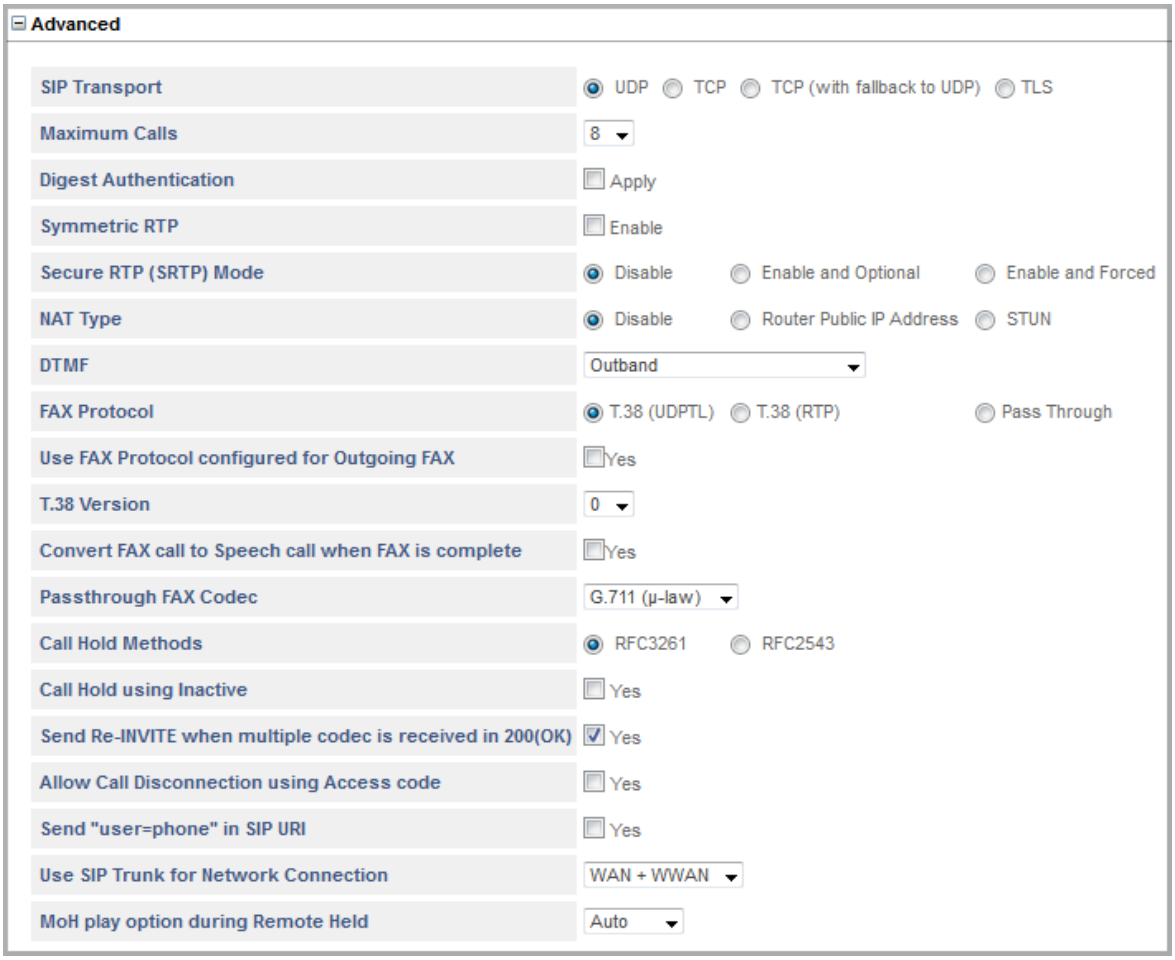
  In all Destination Number Determination methods except *After Answering the Call and Collecting the Digits*, the Source Port gets connected to the Destination Port only after the call has matured, that is, the called party has answered the call. Until the call matures, the caller hears only Ring Back Tone played by the network.

  By connecting the Source Port with the Destination Port immediately after the number is dialed, the caller can know the state of the call; if the called party is busy, not responding, not reachable or is rejecting the call.

*If you enable **Connect Source Port when 183(Session Progress) is received on SIP**, you will not be able to provide the features "Making a New Call using Access Code" and "Disconnecting a Call using Access Code" to users.*

- Click **Submit** to save the changes.

## Advanced




- Click **Advanced** and configure the following parameters:

  - Select the default **SIP Transport** for outgoing SIP messages from the following options:

- **UDP:** Outgoing messages are transported using UDP.
- **TCP:** Outgoing messages are transported using TCP.
- **TCP (with fallback to UDP):** TCP is used for outgoing messages. However, if the TCP connection fails, the system will attempt to send the message again over UDP.
- **TLS:** Outgoing messages are transported using TLS.

  Default: UDP

- *To use TCP or TCP (Fallback to UDP), you must enable **SIP over TCP** in the "System Parameters".*
- *To use TLS, you must enable **SIP over TLS** in "System Parameters".*
- In the **Maximum Calls** field, configure the number of simultaneously calls you want to allow on this SIP Trunk. Default: 8.

  The number of simultaneous SIP calls depends on the number of simultaneous calls allowed by the ITSP with whom you have subscribed this SIP Trunk.

  The SETU VG supports 8 simultaneous calls. Ask your ITSP about the number of simultaneous SIP calls supported on this SIP Trunk.
- If you want to allow incoming calls on the SIP Trunk only after callers have authenticated themselves with their User ID and Password, enable **Digest Authentication**. Default: Disabled.

  If you enable Digest Authentication feature on the SIP Trunk, you must configure the Digest Authentication Table. To know more about this feature, see "Digest Authentication".
- If you want the system to send RTP packets to original IP and Port from where RTP packets are received, by ignoring the contact information received in SDP, enable the **Symmetric RTP** check box. Default: Disabled.
- Select the appropriate **Secure RTP (SRTP)** mode from the following options:
  - **Disable:** SRTP will not be used.
  - **Enable and optional:** Either RTP or SRTP will be used. If you select this mode, you must select the SRTP Media Type. You can select AVP or SAVP. Default: AVP.
  - **Enable and forced:** Only SRTP will be used.

    Default: Disable.
- When the system is installed behind a NAT Router, select specific NAT traversal mechanism to be used as **NAT Type**. Default: Disabled.
  - Select **Router's IP Address,** if your SETU VG is located behind the NAT router (any type).

    Make sure you disable Outbound Proxy on SIP Trunk and configure the same IP Address under NAT settings in the "System Parameters" page.

- Select **STUN**, if your system is located behind the NAT router other than Symmetric.

  Make sure you disable Outbound Proxy on SIP Trunk and configure the STUN Server Address and port in “System Parameters”.

- Select the appropriate **DTMF** sending/receiving mechanism that is compatible with the DTMF sending/receiving mechanism of your ITSP or remote peer. SETU VG supports:

  - **In-band:** System will send and detect digits in In-band only.
  - **Outband:** System will send and detect digits in Outband events only.
  - **SIP INFO:** System will send and detect digits in SIP INFO message only.
  - **Outband-->In-band:** System will send and detect digits in Outband, if negotiated in offer-answer else it will use In-band.
  - **SIP INFO-->In-band:** System will send and detect digits in SIP INFO, if negotiated in offer-answer else it will use In-band.
  - **Outband-->SIP INFO-->In-band:** System will send and detect digits in Outband or SIP INFO, if negotiated in offer-answer else it will use In-band. If both Outband and SIP INFO is negotiated, Outband will have priority over SIP INFO.
  - **SIP INFO-->Outband-->In-band:** System will send and detect digits in SIP INFO or Outband, if negotiated in offer-answer else it will use In-band. If both SIP INFO and Outband is negotiated, SIP INFO will have priority over Outband.

    Default: Outband

- Select the desired **Fax Protocol**, to send and receive the Fax over IP:

  - **T.38(UDPTL):** If you select this option, the device you are sending the fax to, must also support this protocol.
  - **T.38(RTP):** If you select this option, the device you are sending the fax to, must also support this protocol.
  - **Pass Through:** Select this option, if you need to send fax over G.711. The device you are sending fax to must also use G.711.

    Default: T.38 (UDPTL).

- Select the **Use FAX Protocol configured for Outgoing FAX** check box, if you want SETU VG to use the Fax Protocol configured for outgoing fax for this SIP Trunk and not the one that is received in RE-INVITE message from the remote end. Default: Disabled.

- If you have selected *T.38(UDPTL)* or *T.38(RTP)* as Fax Protocol, you must select an appropriate **T.38 Version** that is compatible with your ITSP proxy server/remote peer. You may select:
  - 0
  - 1
  - 2

Default: 0

- Select the **Convert FAX call to Speech call when FAX is complete** check box, if you want SETU VG to convert the fax call to a speech (voice) call after the fax complete event is received. Default: Disabled.

- If you have selected *Pass Through* as Fax Protocol, you must select an appropriate **Passthrough FAX Codec** that is compatible with your ITSP proxy server/remote peer. You may select the Codec as:
  - G.711(μ-law)
  - G.711 (A-law)

  Default: G.711 (μ-law)

- Select an appropriate **Call Hold Method** that is compatible with your ITSP proxy server/remote peer. You may select:
  - RFC 2543
  - RFC 3261

  Default: RFC 3261

- Select the **Call Hold using Inactive** check box, if you want the system to send '*a=inactive'* message instead of *'a=sendonly'* message on the SIP Trunk, when the user puts the call on hold. Default: Disabled.

- Clear the **Send Re-INVITE when multiple codec is received in 200(OK)** check box, if you do not want SETU VG to send Re-INVITE message and use only the first codec from the multiple codec received in 200(OK). Default: Enabled.

- Select the **Allow Call Disconnection using Access code** check box, if you want to enable the feature Disconnect Call using Access Code on the SIP Trunk. Default: Disabled. See "Disconnecting a Call using Access Code".

- Select **Send "user=phone" in SIP URI** check box, if you want SETU VG to add user=phone in the Request URI/From/To header of the INVITE message. Default: Disabled.

  SETU VG will send user=phone in SIP URI, only if the SIP ID is numeric.

- Select the desired option to **Use SIP Trunk for Network Connection**. You may select:
  - WAN
  - WWAN
  - WAN+WWAN

  Default: WAN+WWAN

- Select the desired **MoH play option during Remote Held**. You may select:
  - Auto
  - Local
  - Remote

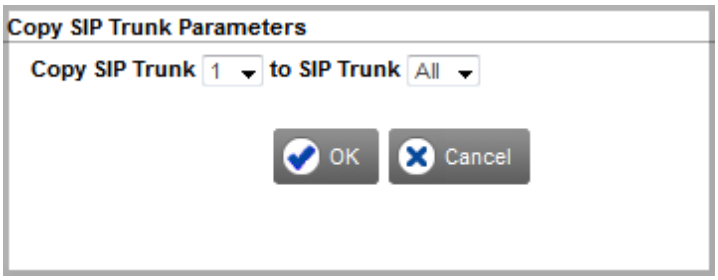
  Default: Auto

- If you have completed the configuration of SIP Trunk 1, click **Submit** to save settings.

- To configure the next SIP Trunk, click the SIP Trunk number tab and follow the same instructions as given earlier.

## Copy Port Settings

- You can also copy the settings of a SIP Trunk to another SIP Trunk using the **Copy** button. To do this,
  - Click the **Copy** button. **The Copy SIP Trunk Parameters** window opens.



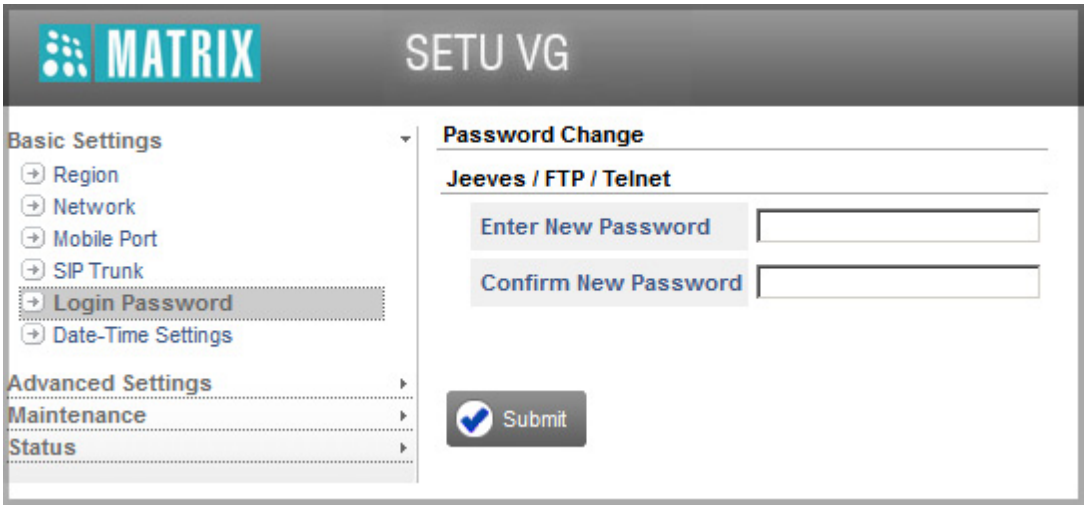

  - In the **Copy SIP Trunk** box, select the number of the port you want to copy settings *From*. In the **to SIP Trunk** box, select the number of the port you want to copy the settings *To*.
  - Click **OK** and close the window.
  - Once you have copied the settings, you can again edit the specific parameters of the SIP Trunk you copied the settings to.

# Login Password

You can configure SETU VG using Jeeves. To configure the system, you must log into the Jeeves using the Jeeves (login) Password. This Password must not be less than 4 characters and can be of upto 16 characters. All ASCII characters are allowed except **White Space & ( ) ` ; " ' < > | \ dot (.)**. The default Jeeves Password is **1234.** You may change this Password using the Jeeves, if required.

To change the Jeeves (login) Password:

- Log into Jeeves.
- Click the **Basic Settings** link to expand.
- Click **Login Password.**




Under **Jeeves/FTP/Telnet**,

- Enter the new password in the **Enter New Password** field.
- Type the new password again for confirmation in the **Confirm New Password** field.
- Click **Submit** to save.

- *Password for Jeeves is case sensitive.*
- *When you default the system using the Web Jeeves, Jeeves Password will not be set to default.*

## Forgot the Login Password?

If you have already changed the default Jeeves Password (1234) and are unable to recall or locate it, you must restore the default Jeeves Password. You may restore the default Jeeves Password using the Reset button.

To restore the default Jeeves Password,

- Press the Reset button for more than four seconds.

- Release the Reset button.

- *If you press the Reset button for less than four seconds, SETU VG will restart.*
- *When you restore the default Jeeves Password (1234), a few other parameters will also be set to default. See "Restoring Default Settings using the Reset button" for details.*

# Date-Time Settings

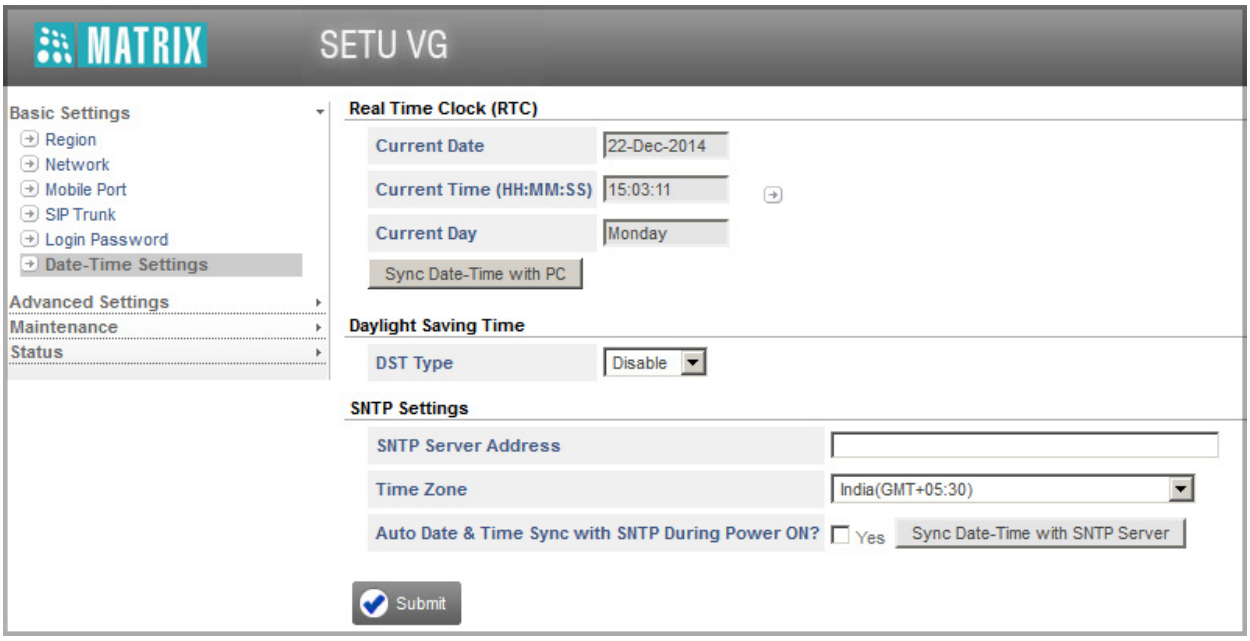
## Real Time Clock

SETU VG has a Real Time Clock (RTC) to store date and time. When you select the Region, the RTC parameters are set automatically.

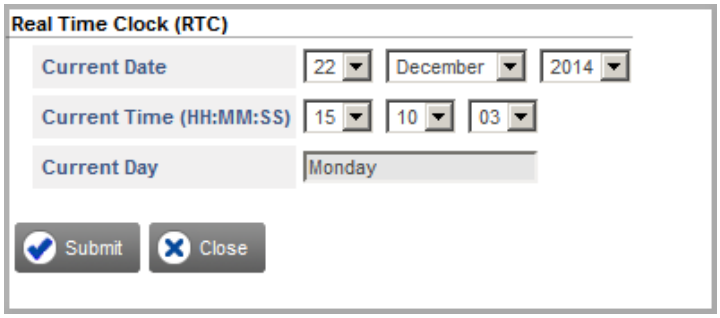
However, the RTC can drift over a long period. So, you may check and reset the RTC values at regular intervals to correct this drift.

To set the Real Time Clock,

- Under **Basic Settings**, click the **Date-Time Settings** link.
- The **Real Time Clock** parameters appear on your screen.




- Under **Real Time Clock (RTC)**, click **Settings** of the **Current Time (HH:MM:SS)**.
  - A new window opens.




  - Set the **Current Date** in date-month-year format.

- Set the **Current Time** in hours-minutes-seconds format.

  The current day will be displayed automatically for the date and time you set.

- Close the window.

- Click **Submit** to save RTC settings.
- Click **Sync Date-Time with PC** button, if you want to sync the system's date and time with that of your PC.

## Daylight Saving Time

Daylight Saving Time (DST) is the practice of advancing clocks so that afternoons have more daylight and mornings have less. Typically clocks are adjusted forward one hour near the start of spring and are adjusted backward in autumn. Many countries of the world[5] use it, though the start and end dates of DST vary by location and year.

SETU VG supports Daylight Saving Time adjustment to enable you to set the Date and Time[6] of SETU VG forward and backward according to the DST convention followed in your country.

You can set DST by: **Day and Month** or **Date and Month**.

*When SETU VG is set to default, your DST settings will remain unchanged.*

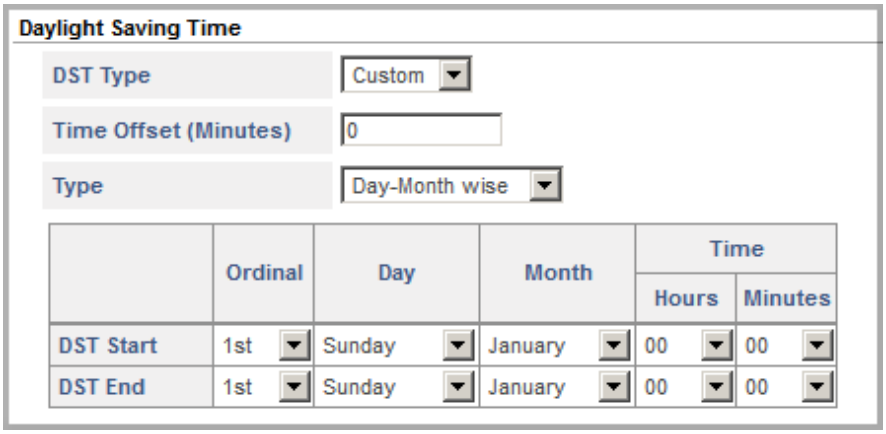
To configure DST,

- Under **Basic Settings**, click the **Date and Time Settings** link.
- Go to **Daylight Saving Time** and do the following:
  - Select the **DST Type**. You may select **Auto** or **Custom**. If you do not want to apply DST select Disable. Default: Disabled.

5. *In most countries in Asia and Africa, and in certain countries of South America, DST is not observed.*
6. *SETU VG sets its Date and Time according to the **Time Zone** you selected, and synchronizes the time according to the **SNTP Server** you selected.*

- If you select **Auto**, you must select the **Region**. DST will be set automatically for the region you select.


- If you select **Custom**, you must configure the Time Offset and choose whether you want the DST to be applied by Day and Month or by Date and Month and define the DST Start and End time.




- In the **Time Offset** field, enter the time in minutes which the system should consider to forward the clock at the start of DST and to set the clock back when DST ends. Default: 60 minutes.
- Select the desired **Type** of DST as:
  - **Day-Month Wise**, if the DST in your country starts and ends on a particular day of the month. For example, if DST starts on the Second Sunday of March and ends on the First Sunday of October.

  –or–

  - **Date-Month Wise**, if the DST in your country starts and ends on a particular date of the month. For example, if DST starts on October 12 and ends on March 15.

  Default: Day-Month Wise.

- If you selected the **Day-Month Wise** option, configure the Start and End time for DST.

  **DST Start**
  - Select the **Ordinal** day of the month when DST begins: 1st, 2nd, 3rd, 4th or 5th.
  - Select the **Day** of the month when DST begins: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
  - Select the **Month** when DST begins: January to December.
  - Set the **Time** when you want DST to begin in 24 hours format.

  Default: 1st Sunday March, Time 00 hours and 00 minutes.

  **DST End**
  - Select the **Ordinal** day of the month when DST ends: 1st, 2nd, 3rd, 4th or 5th.
  - Select the **Day** of the month when DST ends: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
  - Select the **Month** when DST ends: January to December.
  - Set the **Time** when you want DST to end in 24 hours format.

  Default: 1st Sunday September, Time 00 hours and 00 minutes.

*When the DST of a particular country starts or ends on the Last Sunday or any other day, for instance, the last Tuesday, last Friday of the month, always set the Ordinal Number as '5th'.*

- If you select **Date-Month Wise** option, configure the following parameters:

  **DST Start**
  - Select the **Month** when DST begins: January to December.
  - Select the **Date** on which DST begins: 1 to 31.
  - Set the **Time** when DST begins in 24 hours format.

  **DST End**
  - Select the **Month** when DST ends: January to December.
  - Select the **Date** on which DST ends: 1 to 31.
  - Set the **Time** when DST ends in 24 hours format.

- Click **Submit** to save your DST settings.

**Example:** If you are installing SETU VG in a country in the European Union, as per the European Summer Time, the DST would start on the Last Sunday in March and end on the Last Sunday in October each year. Clocks are advanced by one hour at 01:00 hours GMT at the start of DST and set back by one hour at 01:00 hours GMT when DST ends. Let us take the example of setting DST, if SETU VG were installed in Berlin, Germany. In the year 2011, the DST in Berlin starts on Sunday, 27 March at 02:00:00 hours and ends on Sunday 30 October at 03:00:00 hours.

To set DST you must do the following:

1. Select the **DST Type** as **Custom**.
2. Set the **Time Offset** as 60 minutes.
3. Select the option **Date-Month Wise** as **Type**[7].

7. *You can also select Day-Month-wise as Type.*

4. Configure the **DST Start** as follows:
   - Select **March** as the **Month.**
   - Select **27th** as the **Date**.
   - Set **Time** to 01:59:59

5. Now, go to the option **DST End**, and configure as follows.
   - Select **October** as the **Month**.
   - Select **30th** as the **Date**.
   - Set **Time** to 02:59:59.

6. Click **Submit** to save DST settings.

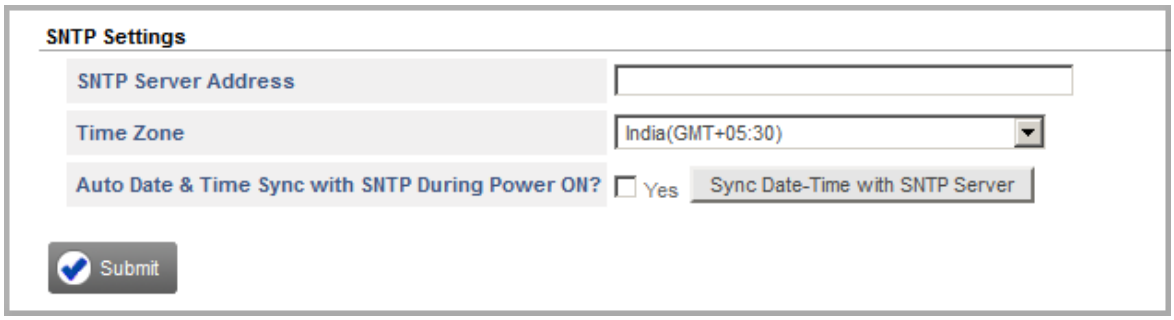
On Sunday 27 March at 01:59:59 the SETU VG will set the clock forward by 1 hour. On Sunday 30 October, SETU VG sets the clock back by 1 hour at 02:59:59.

## SNTP Settings

To use SNTP for synchronizing with the Real Time Clock,

- Under **Basic Settings**, click the **Date and Time Settings** link.

- Go to **SNTP Settings** on this page.




- In the **SNTP Server Address** field, enter the Time Server Address. The SNTP Server address can be of maximum 40 characters. Default: Blank.

- By default, the time zone for the country/region where SETU VG is installed is automatically selected when you select 'Region'. If required you may change the time zone by selecting the desired country/region from the **Time Zone** list. Default: India (GMT+05:30).

- If you want the system to synchronize date and time with the SNTP server automatically at Power On, select the **Auto Date & Time Sync with SNTP During Power ON?** check box.

  At every power ON, SETU VG will synchronize its date and time with the Time Server address you have entered as SNTP Server Address.

  By default, Auto Date & Time Sync with SNTP During Power ON is disabled.

- To synchronize date and time of SETU VG with the SNTP server whenever required, click the **Sync Date-Time with SNTP Server** button.

- Click **Submit** to save the changes.

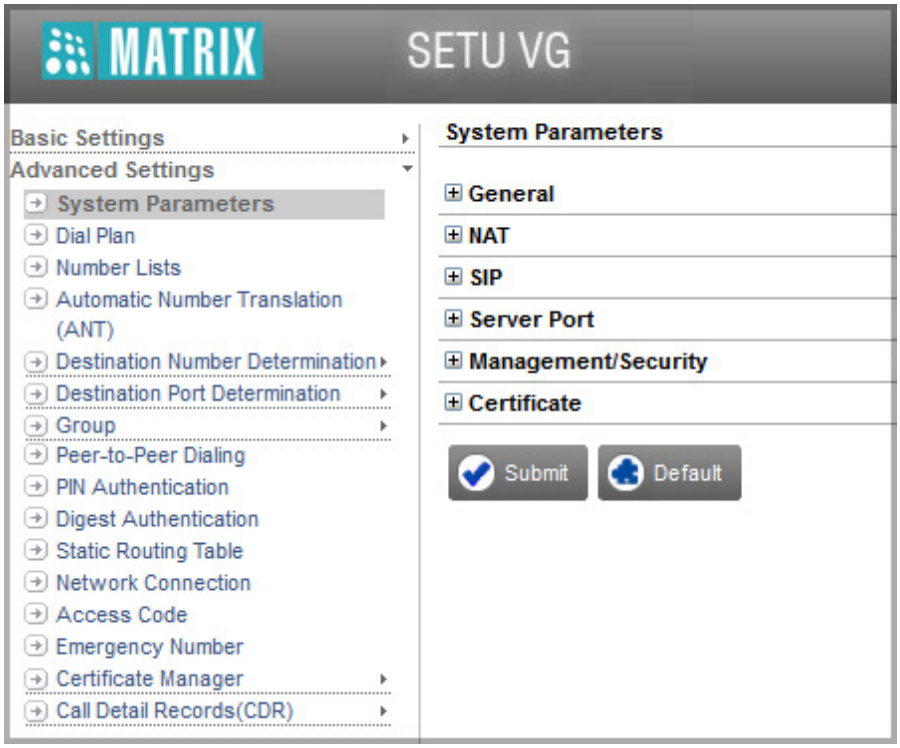
CHAPTER 5 **Advanced Settings**

# System Parameters

System Parameters are general parameters, related to features and facilities that are applied system-wide, such as System Name, NAT and SIP related parameters, Server Port, Certificates etc.

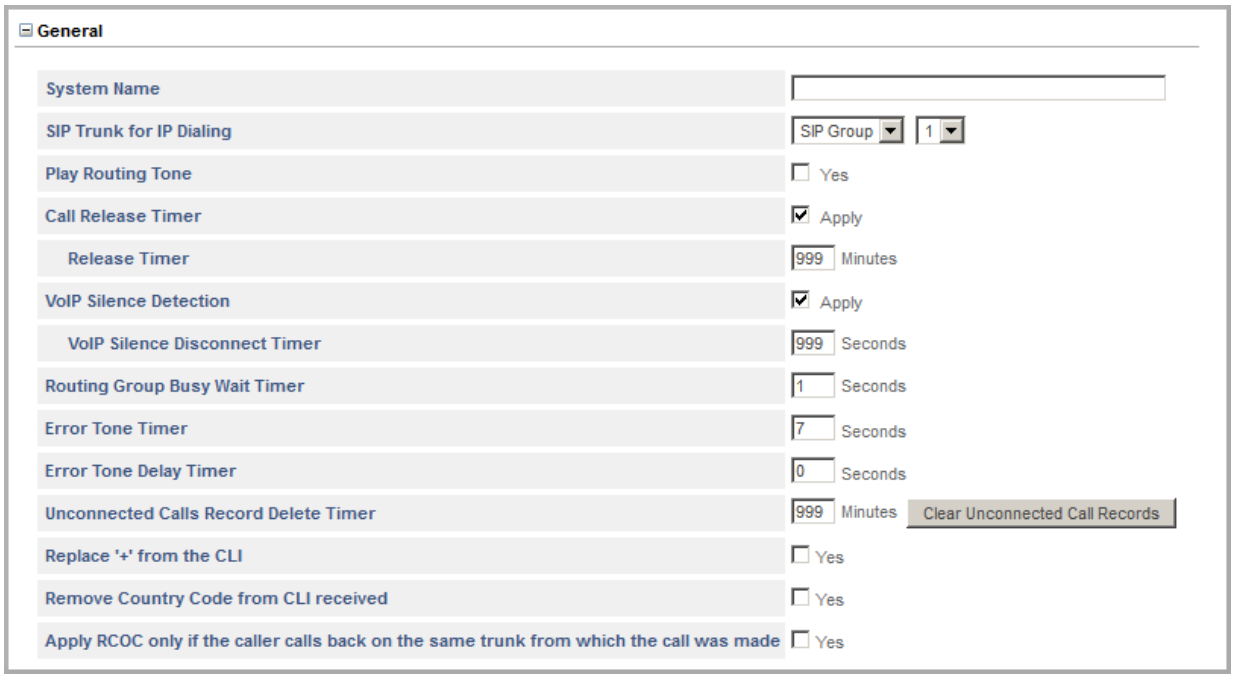
To change the settings of System Parameters,

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **System Parameters** link to open the page.



## General Parameters

- Click **General** to expand and configure the following.




- **System Name:** You can assign a name to SETU VG. This name can serve as an identifier, when there is more than one SETU VG connected in the same LAN network.

  System Name can be of a maximum of 40 characters. Default: Blank.

- **SIP Trunk for IP Dialing:** To use the IP Dialing feature, i.e. to directly dial IP Addresses, you must select a **SIP Trunk** or **SIP Group** for routing the call to the IP Address. For example, if you configured SIP Trunk Group 3 for IP Dialing, you must select 3. See "IP Dialing" to know more about this feature.

  The valid range for the SIP Trunk is 1 to 9 and 1 to 9 for SIP Group. Default: SIP Group 1.

  When you assign a SIP Trunk, make sure it is enabled and has the necessary configuration done. For instructions, see "SIP Trunk" under *Basic Settings*.

  When you assign a SIP Group, you must configure the SIP Group first. See "Group" for instructions.

- **Play Routing Tone:** Routing Tone is played at the time of routing the call to the destination port. During an outgoing call, the routing tone indicates that the call is in progress. Select this check box, to enable the routing tone. Default: Disabled.

- **Call Release Timer:** Keep this check box enabled, if you want the system to release the ports involved in a call after a definite time, if they are not released due to any reason. Else, clear the check box. Default: Enabled.

  This timer is loaded as soon as a call gets matured and it is stopped if one of the ports involved in a call is released.

  - **Release Timer:** Configure the Call **Release Timer**, if you have enabled the Call Release Timer check box. The valid range of Call Release Timer is 001 to 999 minutes. Default: 999 minutes.

- **VoIP Silence Disconnect:** Keep this check box enabled, if you want the system to disconnect the SIP call, if continuous silence (no RTP Packets) is detected for the set time period.

  The VoIP Silence Disconnect Timer is loaded as soon as silence is detected during an IP call. The IP call is disconnected if continuous silence is detected after the expiry of this timer. This timer is applicable for all types of calls received or made through the SIP Trunks

  - **VoIP Silence Disconnect Timer**: Configure the **VoIP Silence Disconnect Timer**, if you have enabled the VoIP Silence Disconnect check box. The valid range of the VoIP Silence Disconnect Timer is 001 to 999 seconds. Default: 999 seconds.

- **Routing Group Busy Wait Timer:** It is the duration for which SETU VG searches for a free destination port in the Routing Group and the Fallback Routing Group to route and place the call. The Routing Group Busy Wait Timer is loaded when no destination port is free in both the Routing Group and the Fallback Routing Group.

  The valid range of the Routing Group Busy Wait Timer is 1 to 99 seconds. Default: 1 second.

- **Error Tone Timer:** It is the duration for which the system will play the Error Tone. The valid range of the Error Tone Timer is 0 to 9 seconds. Default: 7 seconds.

- **Error Tone Delay Timer:** It is the duration after which the system will play the Error Tone, if the call is disconnected during speech. The valid range of the Error Tone Delay Timer is 00 to 99 seconds. Default: 00 seconds.

- **Unconnected Calls Record Delete Timer:** SETU VG offers a feature on the Mobile Port and SIP Trunks whereby outgoing calls made from these ports that return unconnected are routed to the original caller.

  To use this feature on a Mobile Port or a SIP Trunk, you must enable **Route calls returned unconnected to Original Caller** under *Handling of Outgoing Calls* on the port.

  When an outgoing call is made using the port on which this feature is enabled, and the Called Party is found busy or does not respond, SETU VG stores the number of the Calling Party, the number of the Called Party, the source port type and number through which the outgoing call was made and the trunk port type and number used for routing the outgoing call in the RCOC table. A record of each such call is stored for the duration of the *Unconnected Calls Record Delete Timer* (configurable; default: 999 minutes). If the called party returns the call before the expiry of this Timer, this incoming call is placed to the original calling party.

  The records of 200 such Unconnected Calls are stored using FIFO method, and deleted on the expiry of the Record Delete Timer, or when the call returned by the called party is returned to the original caller and answered by the original caller.

  By default, the Unconnected Calls Record Delete Timer is set to 999 minutes. If required, you may change, this timer to the desired duration.

  You can also delete the records of unconnected calls any time, without waiting for this timer to expire. To do this, click the **Clear Unconnected Call Records** button.

- **Replace '+' from CLI received:** The mobile network presents the calling party number with the prefix '+' to the called party. However, not all equipments can present the calling party number containing '+'.

SETU VG enables you to remove the prefix '+' and replace it with an appropriate number string, if required.

If you want the system to replace '+' in the CLI received, select this check box. Default: Disabled.

You may also program the number string with which '+' is to be replaced in the CLI. In the **Replace '+' from CLI with the number string** field, enter the number string with which you want to replace '+' received as prefix of the calling party number**.**

If you keep the number string field blank, SETU VG will remove the '+' sign from the CLI of the calling party and present the remaining digits to the Called Party.

For example:
The number string +919327237228 is received as CLI.
If '00' is configured as the replacement string, the CLI number would be presented as 00919327237228.
If no replacement string is configured (left blank), the CLI number would be presented as 919327237228.

- **Remove Country Code from CLI received:** You may remove country code from the CLI received on the source port, before presenting it on the destination port, if required.

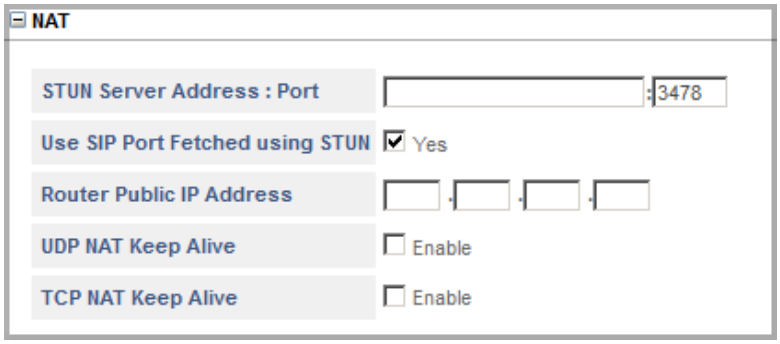
  If you want the system to remove country code from the CLI received, select this check box. Default: Disabled. Make sure you configure "Region" under *Region* in Basic Settings.

- **Apply RCOC only if the caller calls back on the same trunk from which the call was made:** If you want SETU VG to match the Trunk Port Parameters (Trunk Port Number and Type) of an incoming call with the entry in the RCOC table while applying RCOC logic on the "SIP Trunk" and the "Mobile Port", select this check box. Default: Disabled.

  If this check box is enabled, SETU VG will match Trunk port parameters of the incoming call with the entry stored in RCOC table. If a match is found, it will route the incoming call to original caller.

## NAT

- Click **NAT** to expand and configure the following.




- **STUN Server Address: Port:** STUN (Simple Traversal of UDP through NAT) server facilitates traversing through most NATs, except symmetric NATs. So, if your router has Symmetric NAT, do not configure STUN. If your SETU VG is located behind a NAT router that is other than symmetric, use STUN.

In the **STUN Server Address: Port** field, enter the STUN Server Address and the Listening Port of the STUN Server.

The STUN Server Address can have a maximum of 40 characters. Default: Blank.

The valid range of the STUN Server Port is from 1024–65535. Default: 3478.

- **Use SIP Port Fetched using STUN:** Clear this check box, if your SETU VG is located behind the NAT router and you have forwarded the SIP listening port of the SETU VG in the router.

  Keep the **SIP Port fetched using STUN** check box enabled, if you have *not* forwarded the SIP Listening Port in the router.

*Make sure you configure the **NAT Type** on the SIP Trunk as **STUN**. See "SIP Trunk".*

- **Router's Public IP Address:** The Router's public IP address specifies the public IP address of the NAT router behind which system is located. Default: Blank.

  You need to configure this field only if the system is located behind the NAT router and a Static IP Address is assigned as Public IP Address of the Router.

*Make sure you configure the **NAT Type** on the SIP Trunk as **Router's IP Address**. See "SIP Trunk".*

- **UDP NAT Keep Alive:** When SETU VG is connected behind a NAT router and SIP messages are transported over UDP, NAT Keep Alive messages must be sent to refresh the binding in the NAT router.

  Select the **UDP NAT Keep Alive** check box to enable. Default: Disabled.

  - **Keep Alive Message:** Select the type of **Keep Alive Message** to be sent. You may select either REGISTER or NOTIFY. Default: NOTIFY.

  - As **Interval**, set the time period after which the system should send Keep Alive messages. This time period should be less than the NAT binding timer of the router. The valid range for the UDP NAT Keep Alive Interval is 001–999 seconds. Default: 120 seconds.

- **TCP NAT Keep Alive:** When SETU VG is connected behind a NAT router, and SIP messages are transported over TCP, NAT Keep Alive messages must be sent to refresh the binding in the NAT router.

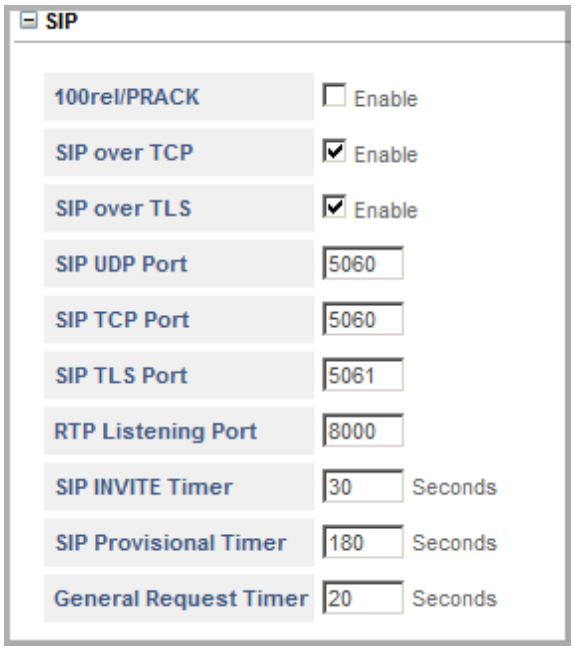
  Select the **TCP NAT Keep Alive** check box, if you want the system to send Keep Alive messages periodically to refresh the binding in the NAT router. Default: Disabled.

  - As **Interval**, set the time period after which the system should send Keep Alive messages. This time period should be less than the NAT binding timer of the router. The valid range for the TCP NAT Keep Alive Interval is 001–999 seconds. Default: 120 seconds.

- Click **Submit** to save changes.

## SIP

- Click **SIP** to expand and configure the following.




- **100rel/PRACK:** This parameter is to be configured if you want to support reliable transmission of (SIP) provisional responses.

  Select the **100rel/PRACK Enable** check box, if you want the SETU VG to use 100rel SIP extension for reliable transmission of SIP provisional responses and to use PRACK (Provisional Acknowledgement). Default: Disabled.

- **SIP Over TCP:** SETU VG supports transporting of SIP messages over User Datagram Protocol (UDP) as well as Transfer Control Protocol (TCP) connection. Despite the advantages that SIP over TCP offers, it is more common to use UDP to transport SIP messages.

  By default, SIP over TCP is enabled. If you want to receive SIP messages over TCP keep this option enabled.

  You must also enable ‘TCP' or 'TCP (Fallback to UDP)' on the SIP Trunk.

- **SIP Over TLS:** SETU VG supports transporting of SIP messages over TLS. TLS protects SIP signaling against loss of integrity, confidentiality and against replay.

  By default, SIP over TLS is enabled. If you want to receive SIP messages over TLS, keep this option enabled.

  You must also enable ‘TLS' on the SIP Trunk.

- **SIP UDP Port:** This is the port on which the SETU VG listens for SIP messages transported over UDP. This port is also used as the source port for sending SIP messages to the remote peer. The valid range for this port is 1031–65534. Default: 5060.

- **SIP TCP Port:** This is the port on which the SETU VG listens for SIP messages transported over TCP. This port is also used as the source port for sending SIP messages to the remote peer. The valid range for this port is 1031–65534. Default: 5060.

- **SIP TLS Port:** This is the port on which the SETU VG listens for SIP messages transported over TLS. This port is also used as the source port for sending SIP messages to the remote peer. The valid range for this port is 1031–65534. Default: 5061.

- **RTP Listening Port:** This is the port on which the SETU VG listens for RTP Packets. This port is also used as the source port for sending RTP packets to the remote peer. The valid range for this port is 1032–65535. Default: 8000.

- **SIP INVITE Timer:** This is the time in seconds for which SETU VG waits for a response from the called party after sending INVITE message. This timer starts after sending INVITE message to the called party and stops on receipt of the provisional response or the final response or when the user disconnects the call. On expiry of the timer, the SETU VG terminates the call process and gives an error tone to the user. The range of the SIP INVITE TIMER is 10–200 seconds. Default: 30 seconds.

- **SIP Provisional Timer:** This is the time in seconds for which SETU VG waits for final response after receiving the provisional response from the called party. This timer starts on the receipt of the provisional response from the called party and stops on receipt of the final response from the called party or when the user disconnects the call. On the expiry of the timer, the SETU VG terminates the call process and gives error tone to the user. The range of the SIP Provisional Timer is 10–200 seconds. Default: 180 seconds.

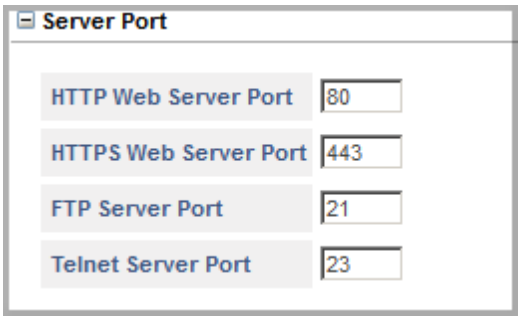
- **General Request Timer:** This is the time in seconds for which the SETU VG waits for response for a transaction request. This timer starts on initiating a transaction and stops on the receipt of a response for the request. On expiry of the timer, the SETU VG clears the transaction. The range of the General Request Timer is 10–60 seconds. Default: 20 seconds.

- Click **Submit** to save changes.

*If you have made any changes in the NAT or SIP Parameters, all the current ongoing calls will be disconnected when you submit the page to save the changes.*

## Server Port

- Click **Server Port** to expand and configure the following.




- **HTTP Web Server Port:** SETU VG has an embedded web server called *Jeeves*, for system configuration. You can access *Jeeves* using HTTP. By default, HTTP Web Server Port is 80. You can change it as per your requirement. Valid range of the port is: 80, 1031-65535.

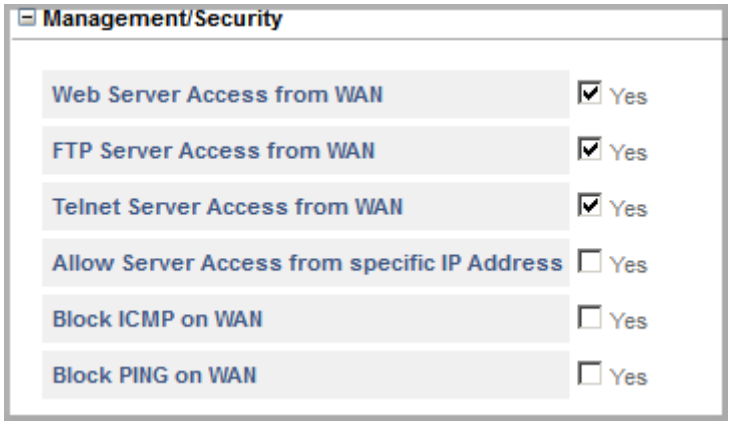
- **HTTPS Web Server Port:** You can access *Jeeves* of SETU VG using HTTPS. By default, HTTPS Web Server Port is 443. You can change it as per your requirement. Valid range of the port is: 443, 1031-65535.

- **FTP Server Port:** SETU VG has an embedded FTP server for Software Upgrade. By default, FTP Server Port is 21.You can change it as per your requirement. Valid range of the port is: 21, 1031-65535.

- **Telnet Server Port:** You can access SETU VG using Telnet. By default, Telnet Server Port is 23. You can change it as per your requirement. Valid range of the port is: 23, 1031-65535.

## Management/Security

- Click **Management/Security** to expand and configure the following.




- **Web Server Access from WAN:** Keep this check box enabled, if you want to allow users to access the system's Web Server (Jeeves) from the WAN Port.

  You may clear this check box, if required. Default: Enabled.

- **FTP Server Access from WAN:** Keep this check box enabled, if you want to allow users to access the system's FTP Server from the WAN Port.

  You may clear this check box, if required. Default: Enabled.

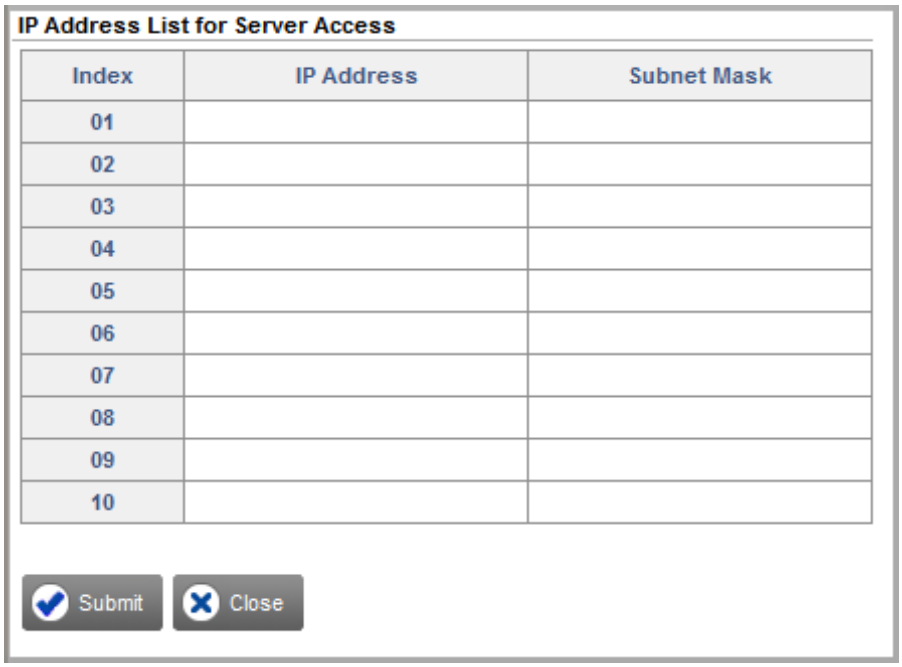
- **Telnet Server Access from WAN:** Keep this check box enabled, if you want to allow users to access the system using Telnet from the WAN Port.

  You may clear this check box, if required. Default: Enabled.

- **Allow Server access from specific IP Address:** Enable this check box, if you want to allow users to access system from specific IP Addresses only. Default: Disabled.

  If you enable this parameter, you must configure the IP Address table for Server Access. To configure the IP Address table, Click **Settings** .


The **IP Address List for Server Access** opens in a new window. You can store 10 entries in this table.




- Enter the IP Addresses and their respective Subnet Mask in the table.
- Click Submit and close the window.

SETU VG will allow system access only to those users whose IP Address matches with the one configured in the IP Address List for Server Access.

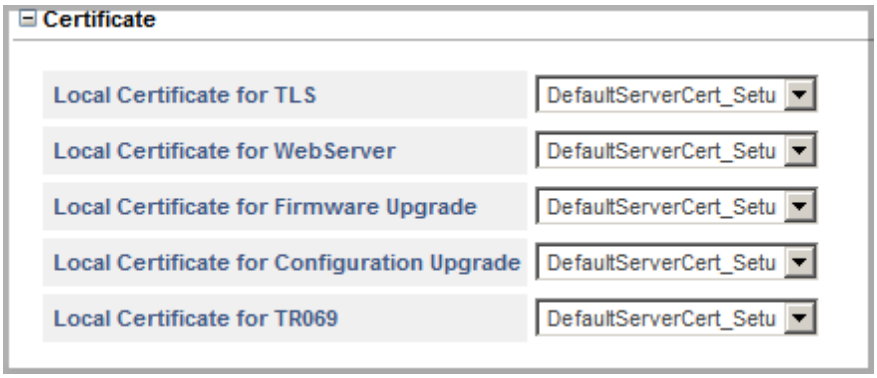
- **Block ICMP on WAN:** Enable this check box, if you want the system to discard the ICMP packets received on WAN. Default: Disabled.
- **Block PING on WAN:** Enable this check box, if you want the system to discard the PING request received on WAN. Default: Disabled.

  Blocking of PING on WAN will prevent your network from being pinged or detected by other Internet users and acquire your IP Address.

***Block PING on WAN** will not be applicable, if you have enabled **Block ICMP on WAN**.*

## Certificate

- Click **Certificate** to expand and select the certificate for each of the following.




  - In **Local Certificate for TLS**, select the certificate to be used by the system for TLS.
  - In **Local Certificate for WebServer**, select the certificate to be used by the system for accessing the WebServer.
  - In **Local Certificate for Firmware Upgrade**, select the certificate to be used by the system for Firmware Upgrade.
  - In **Local Certificate for Configuration Upgrade**, select the certificate to be used by the system for Configuration Upgrade.
  - In **Local Certificate for TR069**, select the desired certificate to be used by the system for TR069.

  To create and Upload /Download Certificates, see “Certificate Manager”.

- Click **Submit** to save changes.

# Dial Plan

SETU VG supports 8 Dial Plans with total 64 entries in each table. The Dial Plan contains a series of digits and/or wildcard characters.

When a user dials a number, it is compared with the Destination Number configured in the Dial Plan. If a match is found, the system routes the call immediately without waiting for End of Dialing and if a match is not found, the system will wait for the End of Dialing and then routes the call as per the Destination Port Selection method configured.

Dial Plan will be applied on the—Mobile Port and SIP Trunk—when,

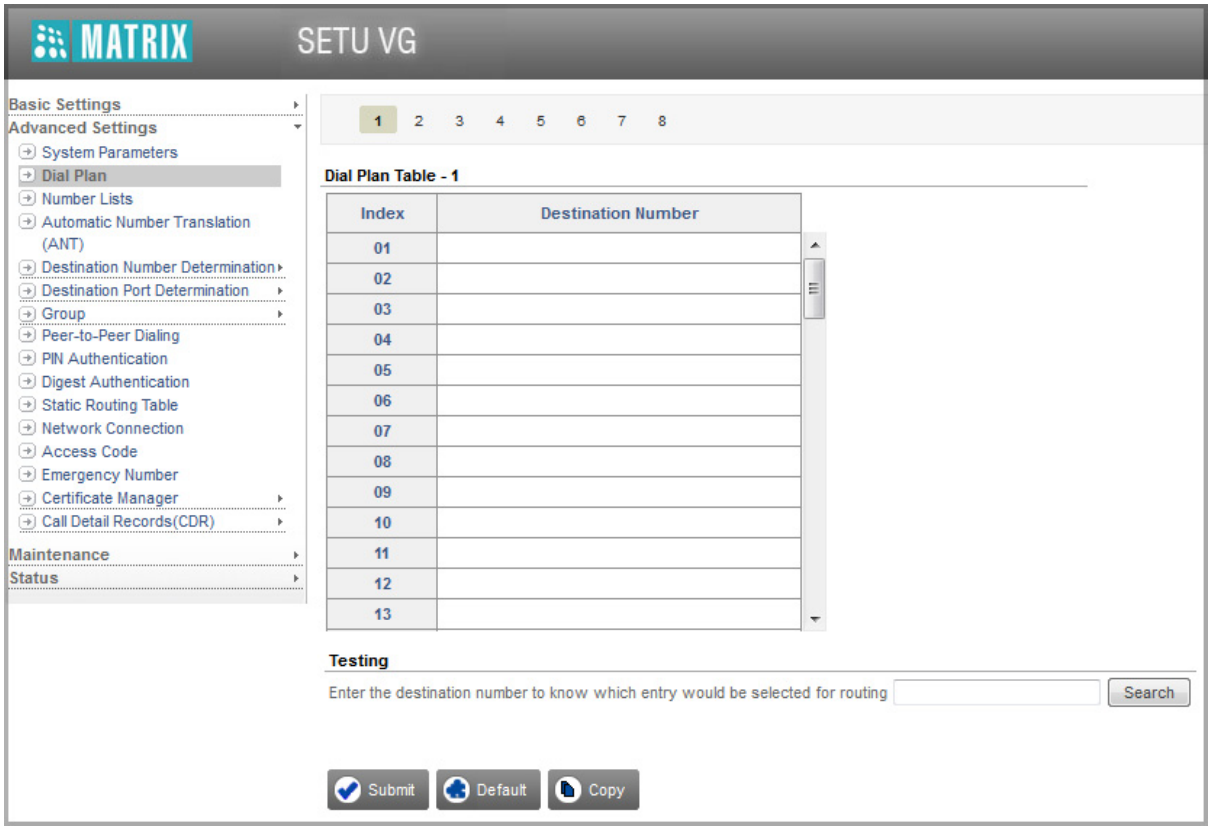
- the Destination Number Selection method used for routing the call is **Answering the call and collecting the digits**.

  and

- the Destination Port Selection method is either **Fixed** or **Calling Number Based**.

## Configuring Dial Plan Table

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Dial Plan** link.



The Dial Plan Table allows you to configure up to 64 entries. Each entry is stored against an Index number.

For each entry,

- In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters: 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^ ]. Default: Blank.
- Click **Submit** to save.

*If there are multiple entries in the Dial Plan table, to search a particular entry in the table, under Testing enter the desired number in the* ***Enter the destination number to know which entry would be selected for routing*** *search box.*

## Wildcard Characters

SETU VG supports following characters.

| Character | Description |
|---|---|
| **X** (letter X) | X represents any single digit from 0 to 9. |
| **#** | When # is configured in a number string, it will not be considered as End of Dialing. |
| ***** | When * is configured in a number string, it will not be considered as End of Dialing. |
| **+** | + (plus) can be configured as a first character of the Destination Number string in the *SIP Trunk-Destination Port Determination-Destination Number Based* table only. |
| **[ - ]** | Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket. |
| **[ , ]** | Comma within a bracket is used as a separator between the groups of numbers. |
| **[ ^ ]** | Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret. |
| **T** (letter T) | Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing. |

Refer the following table to understand how a Dial Plan can be configured.

| Dial Plan Entry | Description |
|---|---|
| 1XX | Allows you to dial any number in a range from 100 to 199. |
| [2-5]XX | Allows you to dial any 3 digit number in a range from 200-599. |
| [2,3,8]XX | Allows you to dial any 3 digit number in the range from 200-299, 300-399, 800-899. |
| [2-9]XXXXXX | Allows you to dial any 7 digit number in the range from 2000000-9999999. |
| 23[^2]1 | Allows you to dial a 4 digit number: 2301, 2311, 2331, 2341, 2351, 2361, 2371, 2381, 2391. |
| 2630[500-550] | Allows you to dial a 7 digit number in the range from 2630500-2630550. |
| [^6-7]X | Allows you to dial a 2 digit number in the range from 00 to 99 except the numbers from 60 to 79. |

| | |
|---|---|
| 1234 | Allows you to dial 1234 number only. |
| 011T | Allows you to dial any number starting with 011. The number must be of minimum 3 digits and maximum digits must be as configured for the port. |

# Number Lists

A Number List is a data structure that constitutes digit and character strings which must be configured for the system to support the features described in the following.

SETU VG offers as many as 24 number lists. Each number list can store up to 64 entries of a maximum of 24 characters each.

You need to configure number lists for the features described in the following. By default, each of these features is assigned a particular number list. You may retain the number list assigned by default, or configure another number list and assign this list to the feature.

## Allowed - Denied Logic

You can apply the Allowed-Denied logic on a source port—SIP, Mobile—if you want to allow or restrict the dialing of particular numbers. You can use this feature for Toll Control.

The Allowed-Denied logic makes use of two Number lists:

- **Allowed Number List:** This is the list of numbers that can be dialed out from the source port.

- **Denied Number List:** This list contains the numbers that are to be restricted from being dialed out from the source port.

Both lists must be programmed separately for each port first and then assigned to the respective port.

When Allowed-Denied Logic is enabled on a source port, for each number dialed from the port, SETU VG uses the best-match-found logic to compare the dialed number with the Allowed Number list and the Denied Number list.

The number is allowed to be dialed, if the dialed number:
- matches with both lists.
- matches with Allowed Number list, but not with the Denied Number list.
- matches with neither the Allowed List nor the Denied List.

The number is denied, if it matches with the Denied Number list, but not with the Allowed Number list.

Allowed-Denied Number feature is not applicable in following cases:
- Destination number string matches with any Access Code.
- Destination number string matches with any Emergency Number.
- For Call Forward Number programmed.
- *Route all Incoming Calls (with CLI)* option selected is:
  - Fixed Destination Number
    - or -
  - on basis of Calling Party Number.

To apply this feature,

- you must configure the numbers you want to allow and restrict from being dialed out in the Allowed and Denied Number lists.

By default, the following number lists are assigned for Allowed Denied Logic for each port type:

| Port Type | Default Allowed Numbers List | Default Denied Numbers List |
|---|---|---|
| SIP Trunks | List 07 | List 08 |
| Mobile Ports | List 01 | List 02 |

You may retain these lists or configure any other Number list from 01 to 24.

- enable **Allowed-Denied Logic** on the port type—SIP, Mobile—on which you want to apply this feature.
- configure the numbers you want to allow and the numbers you want to restrict in the default **Allowed Number List** and **Denied Number List** assigned to the port.

  For instructions, see the following topics under *Basic Settings*:
  "Handling of Incoming Calls" on "SIP Trunk"
  "Handling of Incoming Calls" on "Mobile Port"

  If you do not want to use the default Number Lists assigned to the ports, you may select a different List Number and configure it. In this case, you must assign the List Number you configured as the Allowed Number List/Denied Number List for the respective port.

## Black Listed Callers

The Black Listed Callers feature enables you to block incoming calls from specific numbers and addresses on SIP Trunks and Mobile Ports. You can apply this feature on a Source Port only.

To use this feature,

- you must configure the numbers of unwanted callers in a Number List.

*Make sure you have configured the full SIP URI (for example: 12345@abc.com) of the unwanted callers in the Blacklisted Callers Number List.*

- enable the **Reject Calls from Blacklisted Callers** check box on the SIP Trunks and Mobile Ports on which you want to apply this feature.
- select the Number List you configured as **Black Listed Callers List**.

  For instructions, see the following topics under *Basic Settings*:
  "Handling of Incoming Calls" on "SIP Trunk"
  "Handling of Incoming Calls" on "Mobile Port"

Now, whenever there is an incoming call on the SIP Trunk or Mobile Port you have applied this feature, the SETU VG will match the number with the Blacklisted Callers' Number list you have assigned. If the number matches with any of the numbers you have blacklisted, the system will reject the call.

Make a list of numbers that you want to block. Configure these numbers in a Number List. By default, Number List 16 is assigned as the Black Listed Callers List for the Mobile Ports and Number List 11 is assigned as the Black Listed Callers List for the SIP Trunks.

You may retain this list and configure all the numbers that you want to block in this list or you may configure different number lists for different ports and assign the lists to the ports.

*Each number string in the List can have a maximum of 24 characters. If the callers' number exceeds 24 characters, the first 24 characters of the number will be checked. If the first 24 characters of the callers' number match perfectly with any of the numbers programmed in Blacklisted Callers List, the call will be rejected.*

## Call Detail Record Filters

SETU VG enables you to generate reports of Call Detail Records using different filters. You can generate Call Detail Record report of calls made to specific numbers (Called Party Numbers) and calls received from specific numbers (Calling Party Numbers).

When you want to sort calls by Called Party and Calling Party Numbers, you must configure a Number list for each of these.

To generate Call Detail Records using Called Party and Calling Party Numbers as filters,

- make a list of Called Party Numbers and another list of Calling Party Numbers.
- configure a Number List with the Called Party Numbers and another Number List with the Calling Party Numbers.

  By default, Number list 01 is assigned for both Called Party and Calling Party numbers. You may retain this list and configure Called Party and Calling Party numbers in this list, or you may retain this for Called Party Numbers and configure another list number for Calling Party numbers. In which case you must assign the list you configured to the respective filter.
- assign the Called Party Number list you configured to the CDR filter **Called Party Number Matching with Number List**.
- assign the Calling Party Number list you configured to the CDR filter **Calling Party Number Matching with Number List**.

  For instructions, see “Call Detail Record”.

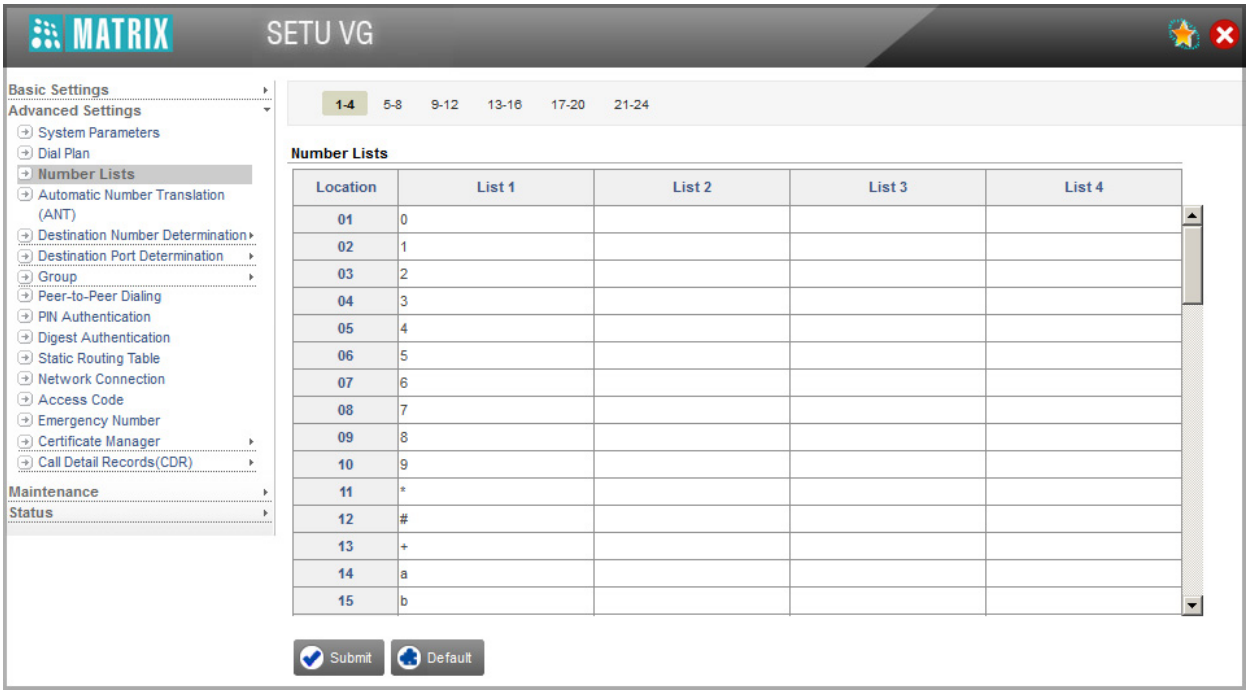
## Configuring Number Lists

You must determine the purpose for which the list is required and accordingly prepare them.

To configure Number lists,

- Log into Jeeves.
- Click the **Advanced Settings** link.

- Click the **Number List** link.




- List 1 to 4 appear on the page. To select another List number, click the tab on the top of the table.
- Select the list number you want to configure.
- Enter the numbers strings in each list.
- Click **Submit** to save entries.
- Assign the list to the respective features for which you configured them on the various port types.

  For example, if you configured Number List 22 with black listed numbers for the Black Listed Callers feature on SIP Trunk 2,

  - Under **Basic Settings**, click **SIP Trunks**.
  - Click the **SIP 2** tab.
  - Under Handling of Incoming Calls, select the **Reject Calls from Blacklisted Callers** check box.
  - In **Blacklisted Callers Number List** field, select **22**.
  - Click **Submit**.

You can also configure Number lists on the respective SIP Trunk and Mobile Ports under the “Basic Settings” link of Jeeves.

# Automatic Number Translation (ANT)

Automatic Number Translation (ANT) is used to modify the number string—entire number or part thereof—into the desired number string as per your requirement. ANT is useful when you need to modify the Called/Calling number, before the system routes the call further.

For example, in India the PSTN requires you to dial the prefix 00 for calling international numbers, whereas the ITSP you have subscribed the SIP Trunk with, restricts the dialing of the prefix 00. If you dial this prefix, your call will be rejected by the ITSP. The ANT Table will enable you to modify the Number string as per your requirement so that the calls routed through the SIP Trunk are not rejected.

The Automatic Number Translation feature can be applied on all the SIP Trunks and the Mobile Ports.

Automatic Number Translation makes use of Automatic Number Translation Table. The ANT Table consists of three columns:

- **Number:** In this column, enter the numbers that you want the system to modify.
- **Strip Digit:** In this column, enter the number of digit(s) to be stripped off by the system from the Called/ Calling number string. If you do not want any digits to be stripped, enter '0'.
- **Add Prefix:** In this column, enter the digit(s) which are to be added as prefix to the Called/Calling number string by the system before routing it further.

To apply this feature on the desired port,

- on a piece of paper make a table, in the first column note down the numbers that need to be modified. In the second column enter the number of digits you want the system to strip off (if required), and in the third column, enter the number you want the system to add as prefix (if required).
- configure the **Automatic Number Translation Table**. You can configure upto 8 different ANT Tables.
- enable **Automatic Number Translation (ANT) for Called Number** and/or **Automatic Number Translation (ANT) for Calling Number** on the respective ports/trunks, on which you want to apply this feature.
- assign the **Automatic Number Translation Table** you configured.
- configure the **Pause Timer**, if applicable.

For instructions, "Handling of Outgoing Calls" under the "SIP Trunk" and "Handling of Outgoing Calls" under the "Mobile Port".

Now, whenever there is a call on/from the Port on which you have applied this feature, SETU VG will match the Called/Calling number with the Number configured in the Automatic Number Translation Table using the best match found logic.

- If a match is found, the system will check whether and how many digits to strip off. It will strip off digits according to the number you have entered in the Strip Digit column. If '0' is configured in the Strip Digit column, it will check the Add Prefix column. If configured, the system will add that prefix. If no prefix is configured, the system will route the same number string further.

If ~ (Wait for Answer) is configured in the Add Prefix column, the system will wait for the call to mature. Similarly, if ^ (Pause) is configured in the Add Prefix column, the system will wait for the Pause timer and then route the call further.

- If no match is found for the Called/Calling number in the ANT Table, the system will route the number string, without modifying it.

*Automatic Number Translation feature will not be applied when Emergency Numbers are dialed.*

Automatic Number Translation also forms the basis of Multi-Stage Dialing. Using of Calling Card for making international calls is the most common example of Multi-Stage Dialing.

While using a Calling Card, you have to dial the digits in the following sequence:

1. Dial the number for using the Calling Card, for example, 160223.
2. After the call is matured, dial the PIN number printed on the Calling Card, for example, 113212.
3. At last, dial the international number you want to call. For example, 0014162357896.

Thus, you will have to dial the Calling Card number and the PIN number every time before dialing the international number. To avoid repetitive dialing of these fixed digits for making a call, you can configure the ANT table as under.

- In **Number**, configure '00', the prefix for international numbers.
- In **Add Prefix**, configure the Calling Card server number and the PIN Number.

  As the system must wait for the Calling Card server to answer before dialing the PIN, you must configure Wait for Answer (**~**) between the Calling Card server number and the PIN number.

  You must also insert a delay by configuring the Pause Timer (**^**) after the PIN number.
- Keep Strip Digit as 00.
- The Automatic Number Translation table would look like this:

| Index | Number | Strip Digit | Add Prefix |
|---|---|---|---|
| 1 | 00 | 00 | 160223**~**113212**^** |
| 2 | | | |
| 3 | | | |
| 4 | | | |
| 5 | | | |
| 6 | | | |
| : | | | |
| 24 | | | |

- When the Automatic Number Translation table is configured, the user must simply dial the destination number, say, 0014125126508.
- The system matches the Called number with the Number configured in the ANT table. The number matches with the entry '00' stored in the table.

- The system dials the Add Prefix number string 160223 (number of the calling card server). It waits for the calling card server to answer the call.

- When the call is matured, i.e. the calling card server has answered the call, the system dials the PIN number 113212 and waits for the Pause Timer before dialing the destination number.

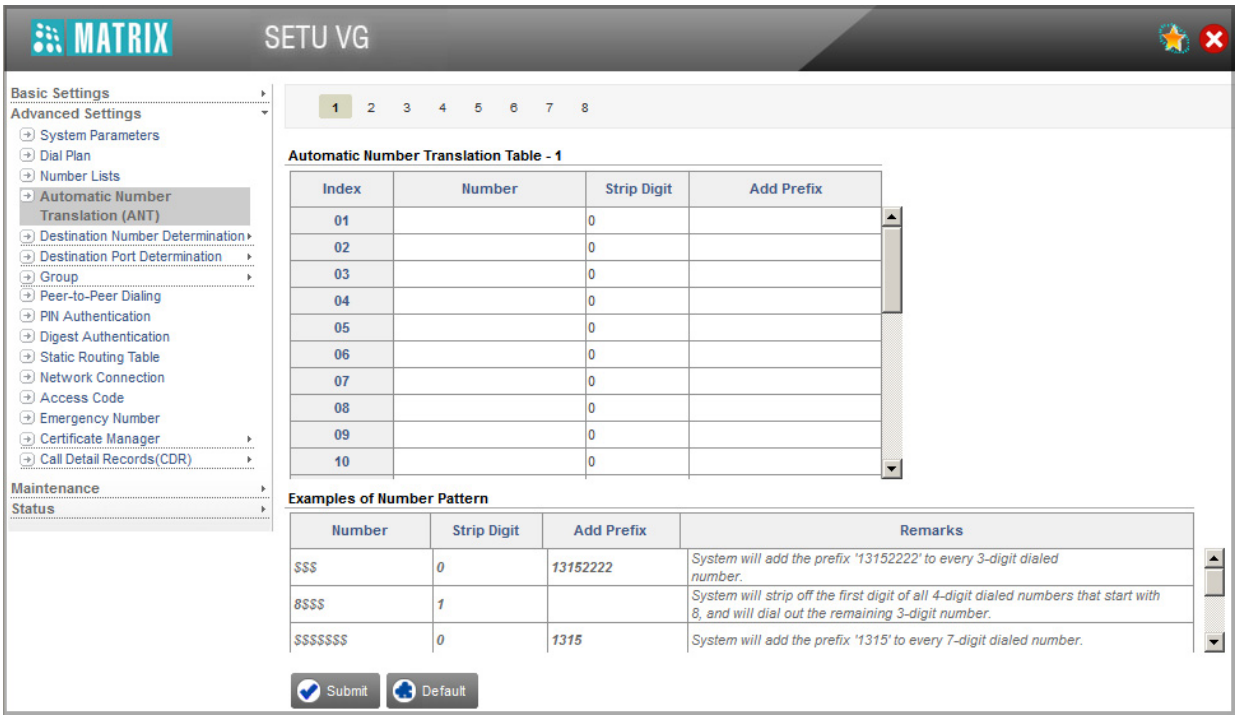
Thus, the user can directly dial the desired destination number and the system dials the rest using the ANT table.

## Configuring Automatic Number Translation Table

- Log into Jeeves.

- Click the **Advanced Settings** link.

- Click the **Automatic Number Translation (ANT)** link.




The Automatic Number Translation Table page will open. In this table, you can store as many as 24 Numbers at Index Numbers 01 to 24.

- In the **Number** column, enter the Called/Calling numbers that need to be modified. You can enter maximum 24 digits. Digits 0-9, #, *, + and $ are allowed. Default: Blank.

  To configure a range of numbers you can use the character **$**. Here, **$** is any number from 0 to 9.

  For example, if you want SETU VG to add prefix ‘1’ to all 10 digit numbers dialed by the user, configure Number as $$$$$$$$$$, Strip Digit as 0 and Add Prefix as 1. Now, when the user dials any number between the range of 0000000000 to 9999999999, say 4161231234, the system will add prefix 1 to it and dials out the number as 14161231234.

- In the **Strip Digit** column, enter the number of digits you want the system to strip off from the Called/ Calling Number. You can configure from 00-24. Default: 00.

- In the **Add Prefix** column, enter the number string(s) that you want the system to add as prefix to the Called/Calling Number. You can enter maximum 24 characters. Characters 0-9, *, #, +, ~ (Wait for Answer), ^ (Pause) are allowed. Default: Blank.

- Click **Submit** to save your entries.

# Destination Number Determination

The process of routing calls originated on Mobile Ports and SIP Trunks to the destination port in SETU VG takes place in two steps:

- Determination of Destination Number
- Determination of Destination Port

SETU VG supports different methods of determining the destination number for the calls originated on Mobile Ports and SIP Trunks.

## Destination Number Determination on SIP Trunks

For SIP Trunks, the system supports the following methods for Destination Number Determination:

- without any Destination Number
- to the Fixed Destination Number
- on the basis of Calling Party Number
- on the basis of DDI Number
- to the Called Party Number
- after Answering the Call and Collecting the Digits

To apply Destination Number Determination **on the basis of Calling Party Number**, you must configure the **Destination Number Determination: SIP-Calling Number Based** table. When there is an incoming call on the SIP Trunk, SETU VG will match the Calling Party Number with the entries of the Calling Party Number Based Table. If a match is found, the call is routed to the destination port.

To apply Destination Number Determination **on the basis of DDI Number**, you must configure the **Destination Number Determination: SIP-DDI Number Based** table. When there is an incoming call on the SIP Trunk, SETU VG will match the DDI Number received in the SIP INVITE message with the entries of the DDI Number Based Table. If a match is found, the call is routed to the destination port.

## Destination Number Determination on Mobile Ports

For Mobile Ports, the system supports the following methods for Destination Number Determination:

- without any Destination Number
- to the Fixed Destination Number
- on the basis of Calling Party Number
- after Answering the Call and Collecting the Digits

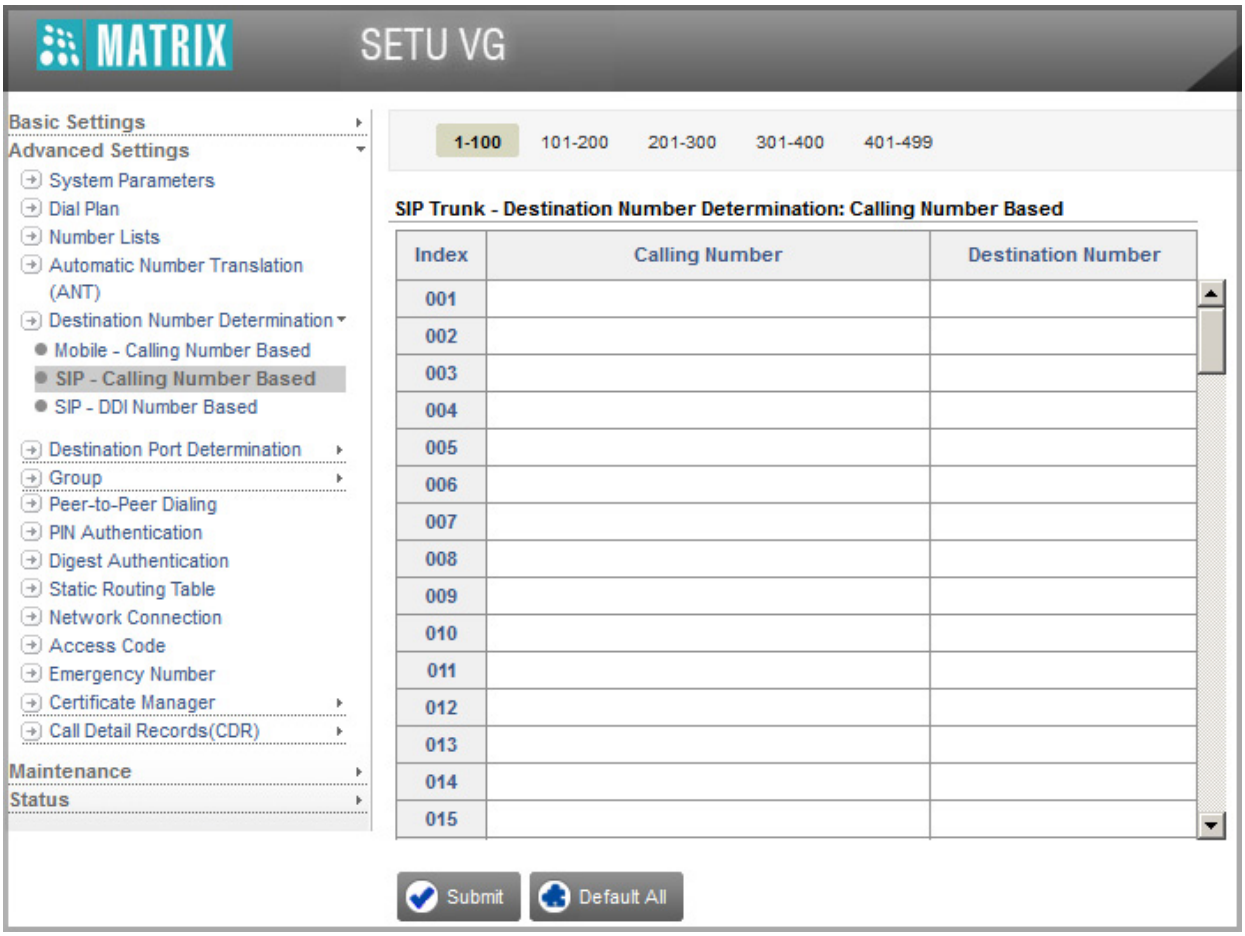
To apply Destination Number Determination **on the basis of Calling Party Number**, you must configure the **Destination Number Determination: Mobile-Calling Number Based** table. When there is an incoming call on the Mobile Port, SETU VG will match the Calling Party Number with the entries of the Calling Party Number Based Table. If a match is found, the call is routed to the destination port.

## Configuring SIP-Calling Number Based Table

- Log into Jeeves.

- Click the **Advanced Settings** link.

- Click the **Destination Number Determination** link.




- To configure the table for the SIP Trunk, click the **SIP-Calling Number Based** link.
- To configure the table for the Mobile Port, click the **Mobile-Calling Number Based** link.

  The Calling Number Based Table page opens.

  - Configure following parameters in this table:

    - Enter the calling party numbers in the column **Calling Numbers**. Calling numbers may consist of a maximum of 24 characters. All ASCII characters are allowed. Default: Blank.

    - For each calling party number, enter a corresponding destination number in the column **Destination Numbers**. Destination numbers may consist of a maximum of 24 characters. Characters 0-9, *, # and dot (.) are allowed. Default: Blank.

    - Select the **Allow Callback** check box, if you want to set callback for a particular calling number. When there is an incoming call from this calling number, the system disconnects the call and will automatically initiate the call to the calling number within 2 to 5 seconds.

***Allow Callback** is applicable only for **Mobile: Calling Number Based** option only.*

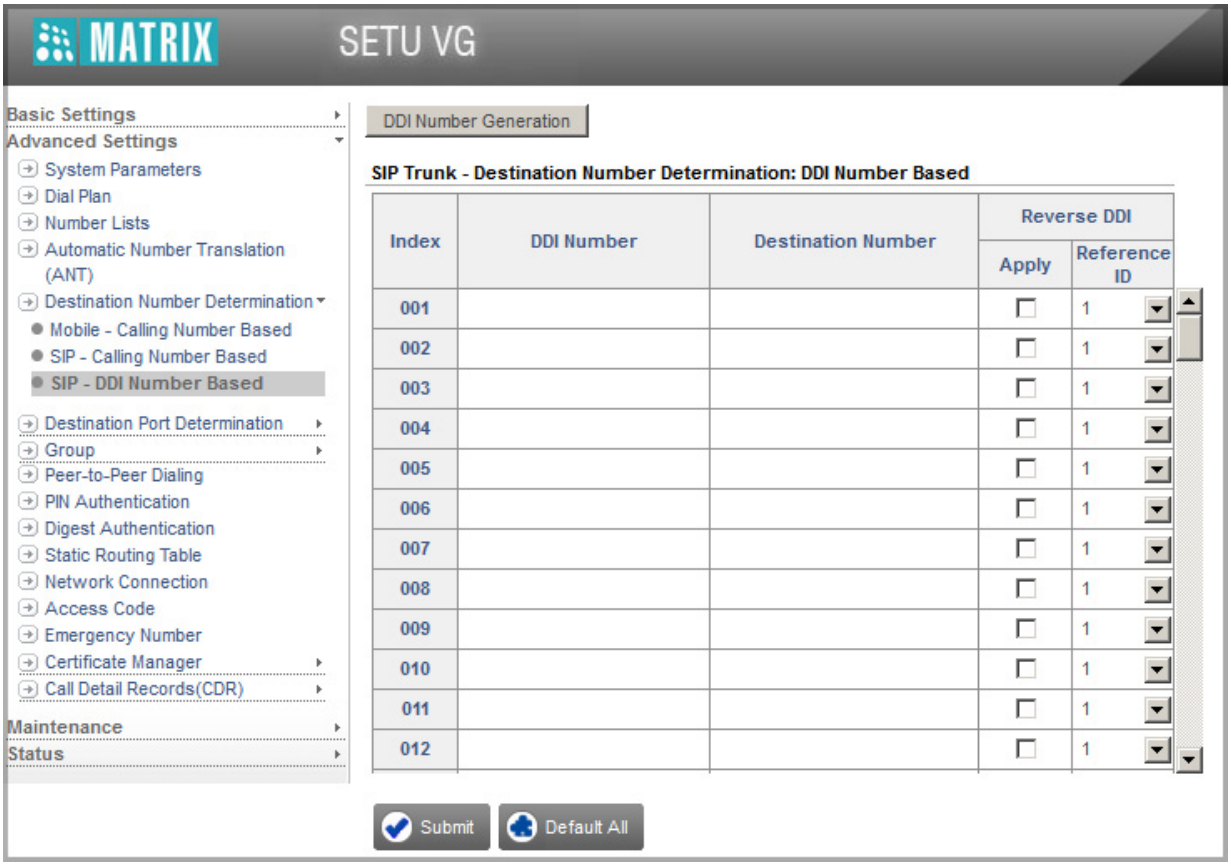
- Click **Submit** to save the entries.
- Click **Default All** to clear all the entries.

## Configuring SIP-DDI Number Based Table

To configure the DDI Number Based Table,

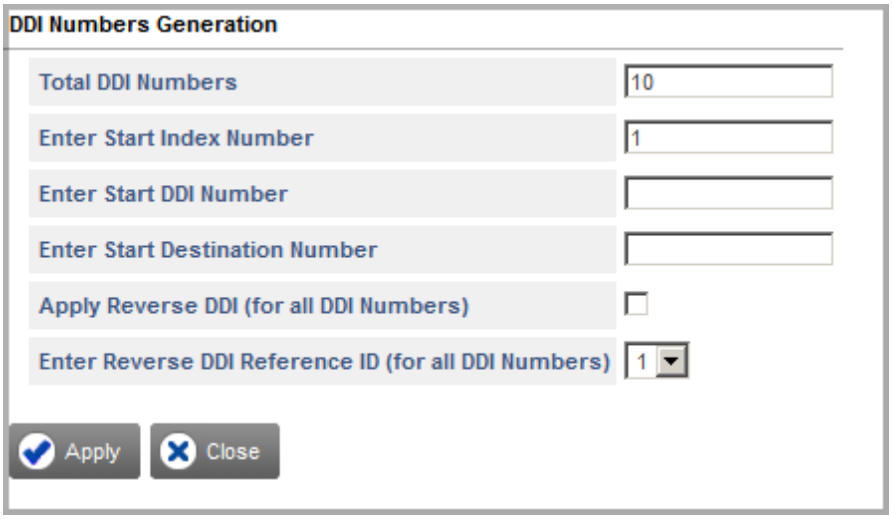
- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Destination Number Determination** link**.**
- Click the **SIP-DDI Number Based** link.

The DDI Number Based Table page opens.



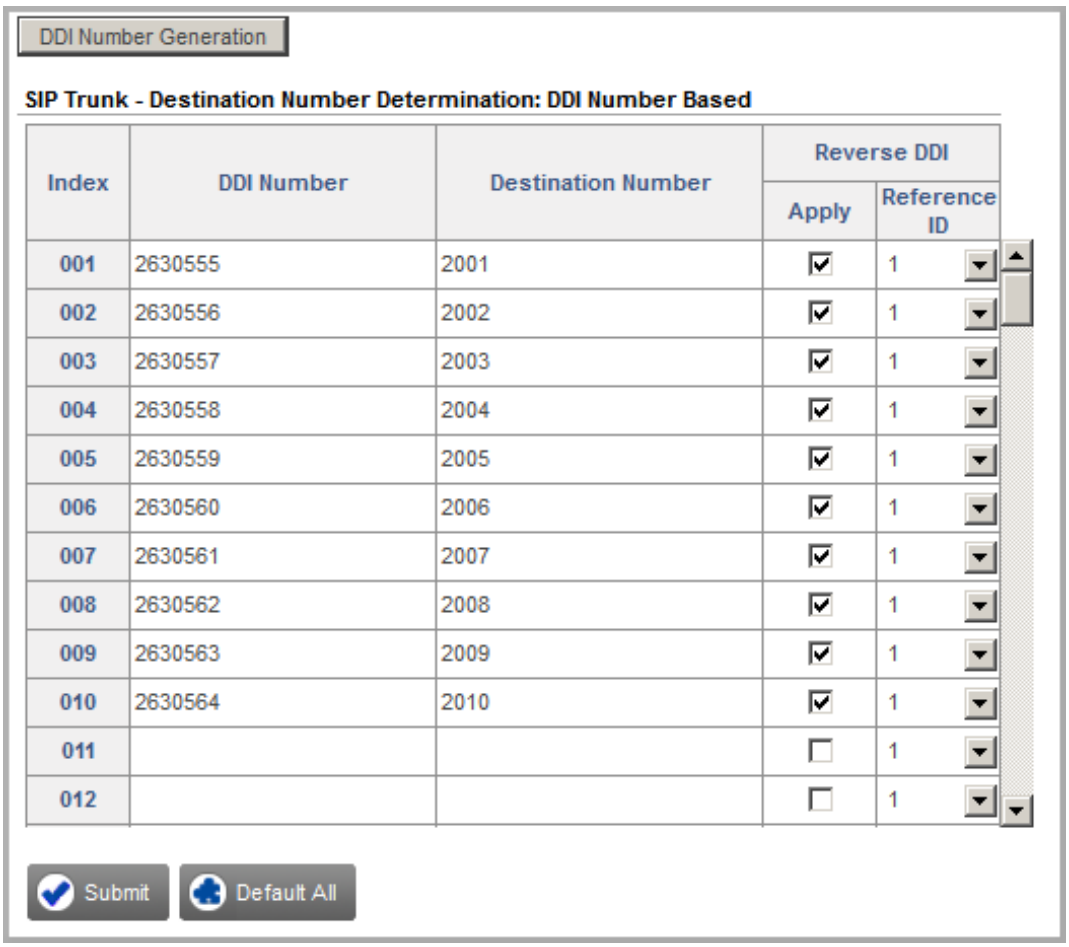

- There are two ways to generate the DDI Numbers:
  - Using the **DDI Number Generation** Button to automatically generate the DDI Number Table.
    ***OR***
  - Entering each DDI Number manually.

- If you want to generate DDI Numbers automatically, click the **DDI Number Generation** button and configure the following parameters:




- **Total DDI Numbers:** The DDI numbers are allotted by the service provider. You must enter the total number of DDI numbers you want to generate in the DDI Number Based table. You can generate upto 100 numbers. Default: 10
- **Enter Start Index Number:** Enter the desired Index Number from where you want to start the DDI Number generation. Default: 1
- **Enter Start DDI Number:** Enter the start DDI Number. DDI Number can be of maximum 24 characters. Characters 0-9, +, * and # are allowed in this field.
- **Enter Start Destination Number:** Each DDI Number can be assigned a corresponding destination number. Enter the Start Destination Number corresponding to the Start DDI Number. Destination Number can be 24 characters long. Characters 0 to 9, # and * are allowed.
- **Apply Reverse DDI (for all DDI Numbers):** When the user makes a call from the assigned DDI number, this number will be displayed to the called party. Select the check box to apply Reverse DDI logic on all DDI Numbers.

- Click **Apply** button to generate the table. The DDI numbers generated will appear in the DDI Number Based Table.




  - You can also edit the generated numbers, if required.

- If you want to generate DDI Numbers manually,

  - Enter each DDI Number and its corresponding Destination Number against the desired Index in the table.

  - To apply **Reverse DDI** logic on the DDI Number, select the **Apply Reverse DDI?** check box.

    The Reverse DDI **Reference ID** for the DDI Number, will be applied on the DDI Number.

    For detailed instruction for generating DDI Numbers manually, see “Route on the basis of DDI Number” under SIP Trunks.

- Click **Submit** to save your entries.

- Click **Default All** to clear all the entries.

# Destination Port Determination

The process of routing calls originated on the Mobile Ports and the SIP Trunks to the destination port in the SETU VG takes place in two steps:

- Determination of Destination Number
- Determination of Destination Port

SETU VG supports different methods of determining the destination port for the calls originated on SIP Trunks and Mobile Ports.

## Destination Port Determination on SIP Trunks

For SIP Trunks, the system supports the following methods for Destination Port Determination:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

To apply Destination Port Determination **on the basis of Calling Party Number**, you must configure the **Destination Port Determination: SIP-Calling Number Based** table.

To apply Destination Port Determination **on the basis of Destination Number**, you must configure the **Destination Port Determination: SIP-Destination Number Based** table.

## Destination Port Determination on Mobile Ports

For Mobile Port, the system supports the following methods for Destination Port Determination:

- Fixed
- On the basis of Destination Number
- On the basis of Calling Party Number

To apply Destination Port Determination **on the basis of Calling Party Number**, you must configure the **Destination Port Determination: Mobile-Calling Number Based** table.

To apply Destination Port Determination **on the basis of Destination Number**, you must configure the **Destination Port Determination: Mobile-Destination Number Based** table.

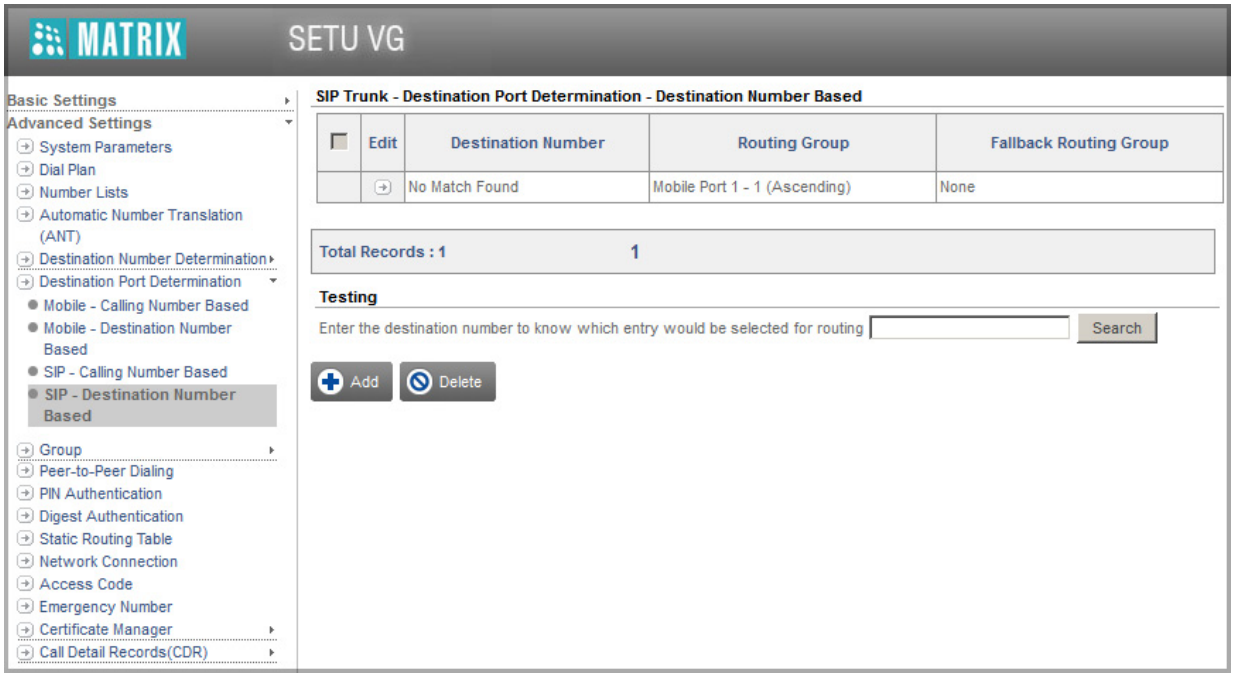
To configure Calling Number based table for SIP/Mobile Ports, see “Configuring Calling Number Based Table for SIP Trunks and Mobile Ports”.

To configure Destination Number based table for SIP/Mobile Ports, see “Configuring Destination Number Based Table for SIP Trunks and Mobile Ports”.

### Configuring Destination Number Based Table for SIP Trunks and Mobile Ports

- Log into Jeeves.
- Click the **Advanced Settings** link.

- Click the **Destination Port Determination** link.




- To configure the table for the SIP Trunk, click the **SIP-Destination Number Based** link.
- To configure the table for the Mobile Port, click the **Mobile-Destination Number Based** link.

  The **Destination Number Based** Table page opens.

- Click **Add** to add an entry. A new window opens.
  - In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters—Digits 0-9 and "Wildcard Characters"—in this field. Default: Blank.

## Wildcard Characters

SETU VG supports following characters.

| Character | Description |
|---|---|
| **X** (letter X) | X represents any single digit from 0 to 9. |
| **#** | When # is configured in a number string, it will not be considered as End of Dialing. |
| ***** | When * is configured in a number string, it will not be considered as End of Dialing. |
| **+** | + (plus) can be configured as a first character of the Destination Number string in the *SIP Trunk-Destination Port Determination-Destination Number Based* table only. |
| **[ - ]** | Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket. |
| **[ , ]** | Comma within a bracket is used as a separator between the groups of numbers. |
| **[ ^ ]** | Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret. |

| | |
|---|---|
| **T** (letter T) | Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing. |

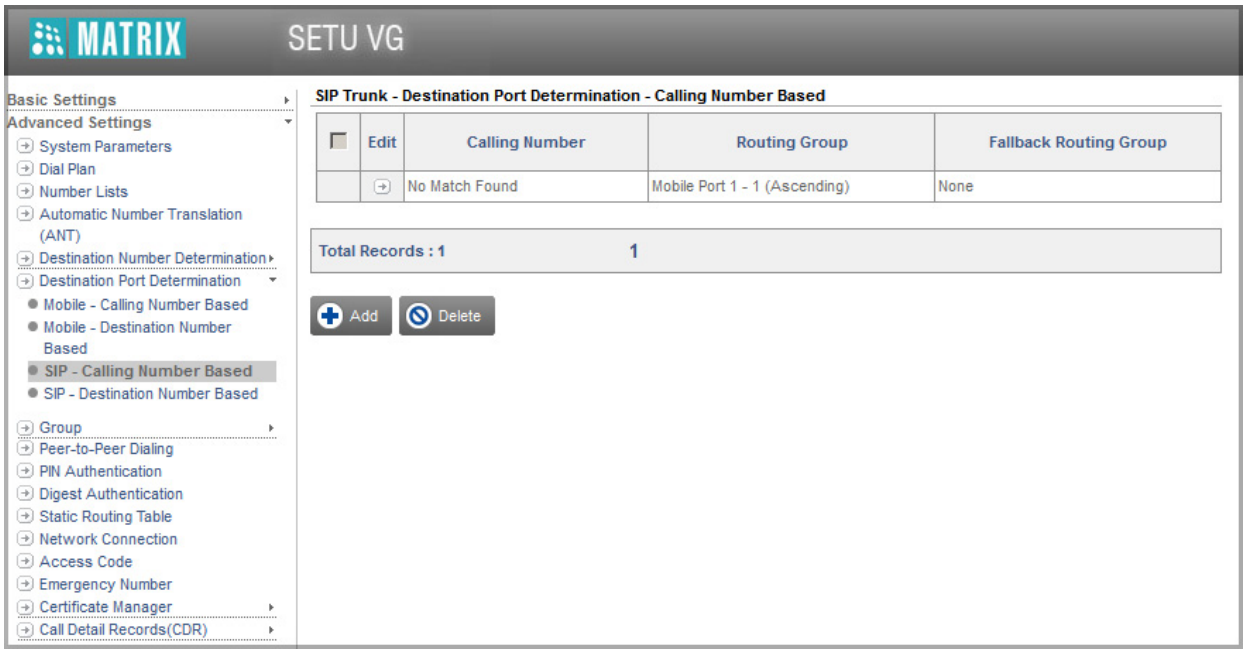
- Create the **Routing Group**.
  - To create a group of *sequential* **Mobile Port** as members,
    - Select the desired **Mobile Port** numbers as members. Default: 1.
    - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

      Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.
  - To create a group of *not-sequential* **Mobile Ports** as members,
    - Select **Mobile Group**.
    - Select the **Mobile Group** number. Default: 1.
    - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See “Group” for detailed instructions.
  - Similarly, you can create group of *sequential* and *not-sequential* SIP Trunks as members.
- You may create the **Fallback Routing Group**. To do this,
  - Select the **Apply** check box.
  - Follow the same instructions given for creating *sequential* and *not-sequential* groups for Mobile Ports.
  - Click **Submit** to save changes. The **Add Entry** window closes.
- The entries you added appear on the screen.
- To change the default Routing Groups assigned for No Match Found numbers entry,
  - For the **No Match Found** entry, under **Edit**, click **Settings** .
  - The **Edit Entry** window opens.
  - Create the **Routing Group** and **Fallback Routing Group**.
  - Click **Submit** and close the window.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.
- Close the window if you have finished adding/editing entries.

*If there are multiple entries in the Destination Number Based table, to search a particular entry in the table, under Testing enter the desired number in the Enter the destination number to know which entry would be selected for routing search box.*

## Configuring Calling Number Based Table for SIP Trunks and Mobile Ports

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Destination Port Determination** link**.**




- To configure the table for the SIP Trunk, click the **SIP-Calling Number Based** link.
- To configure the table for the Mobile Port, click the **Mobile-Calling Number Based** link.

  The **Calling Number Based** Table page opens.

- Click **Add** to add an entry. A new window opens. Configure the following parameters:
  - In the **Calling Number** field, enter numbers (max. 24 characters) from which you expect calls to be received. All ASCII characters are allowed. Default: blank.
  - Create the **Routing Group**.
    - To create a group of *sequential* **Mobile Port** as members,
      - Select the desired **Mobile Port** numbers as members. Default: 1.
      - In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.

- To create a group of *not-sequential* **Mobile Ports** as members,
  - Select **Mobile Group**.
  - Select the **Mobile Group** number. Default: 1.
  - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Port Group. See "Group" for detailed instructions.
- Similarly, you can create group of *sequential* and *not-sequential* SIP Trunks as members.

- You may create the **Fallback Routing Group**. To do this,
  - Select the **Apply** check box.
  - Follow the instructions provided for creating *sequential* and *not-sequential* groups for Mobile Ports.
  - Click **Submit** to save changes. The **Add Entry** window closes.
- The entries you added will appear on the screen.
- To change the default Routing Groups assigned for No Match Found numbers entry,
  - For the **No Match Found** entry, under Edit, click **Settings** .
  - The **Edit Entry** window opens.
  - Create the **Routing Group** and **Fallback Routing Group**.
  - Click **Submit** and close the window.
- Follow the same steps as above to add another entry to this table.
- To delete an entry, select the check box and click the **Delete** button.

# Group

SETU VG supports the following methods of determining the destination port for the calls originated on SIP Trunks and Mobile Ports.

- Fixed
- on the basis of Destination Number
- on the basis of Calling Party Number

A Routing Group may have *sequential* or *not-sequential* ports as members.

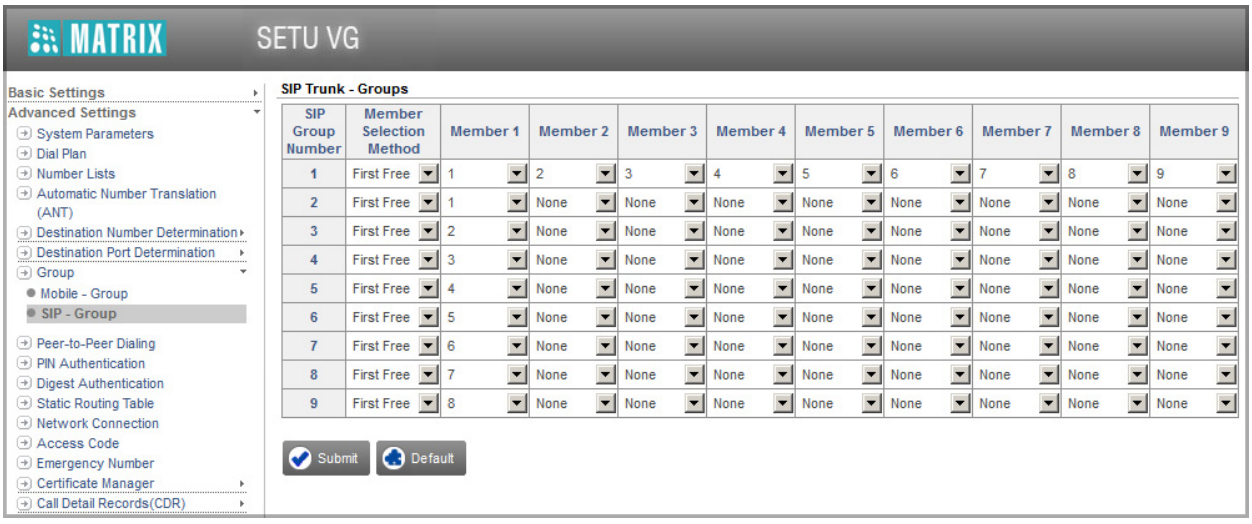
A Routing Group of *sequential* ports is to be formed when you select **SIP Trunk** or **Mobile Port** as the destination port.

A Routing Group of *not-sequential* ports is to be formed when you select **SIP - Group** or **Mobile - Group** as the destination port. The **SIP/Mobile Group** has members of the same port type, but not in a sequence. A SIP Group can have only SIP Trunks as members. Similarly, a Mobile Group can have only Mobile Ports as members.

## Configuring Groups

To create a Group,

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Group** link.




- To create Groups of SIP Trunks, click **SIP Group**. You can create 9 Groups with 9 members in each group.
    - Select a SIP Group Number from **1 to 9.**
    - Configure member ports - **Member 1** to **Member 9**.
        - For each **Member**, select a SIP Trunk number from **1 to 9**.

- If you do not want any more members in a group, select **None**. For example, you want two members in a group, select the SIP Trunk numbers for member 1 and 2, and set the remaining members in the group to None.

- Define the **Member Selection Method**. To route a call, the system checks availability of a free port. There are two options for port selection, namely:

  - **First Free:** The first port which is free will be used for routing the call each time. For example, SIP Group Number 1 has four members SIP Trunk 1 (Member 1), 2(Member 2), 3 (Member 3) and 6 (Member 4). For every incoming call, SETU VG will check the status of Member 1 first. If free, the call will be routed using this port else system will check status of Member 2 and so on.

  - **Rotation:** The first call will be routed through the first member port and the subsequent call through the next member port and so on. For example, SIP Group Number 2 has four members SIP Trunk 6 (Member 1), 7(Member 2), 8 (Member 3) and 9 (Member 4). For the first incoming call, SETU VG will check the status of Member 1 (SIP Trunk 6). If free, the call will be routed using this port else system will check status of Member 2 (SIP Trunk 7) and so on. For the next call, system will check the status of Member 2 (SIP Trunk 7). If free, call will be routed using this port else Member 3 (SIP Trunk 8) will be checked. Similarly, for the subsequent call the system will check the next member port in the group.

    Default: **First Free**.

- Click **Submit** to save the group.

- Similarly, you can create Mobile Groups.

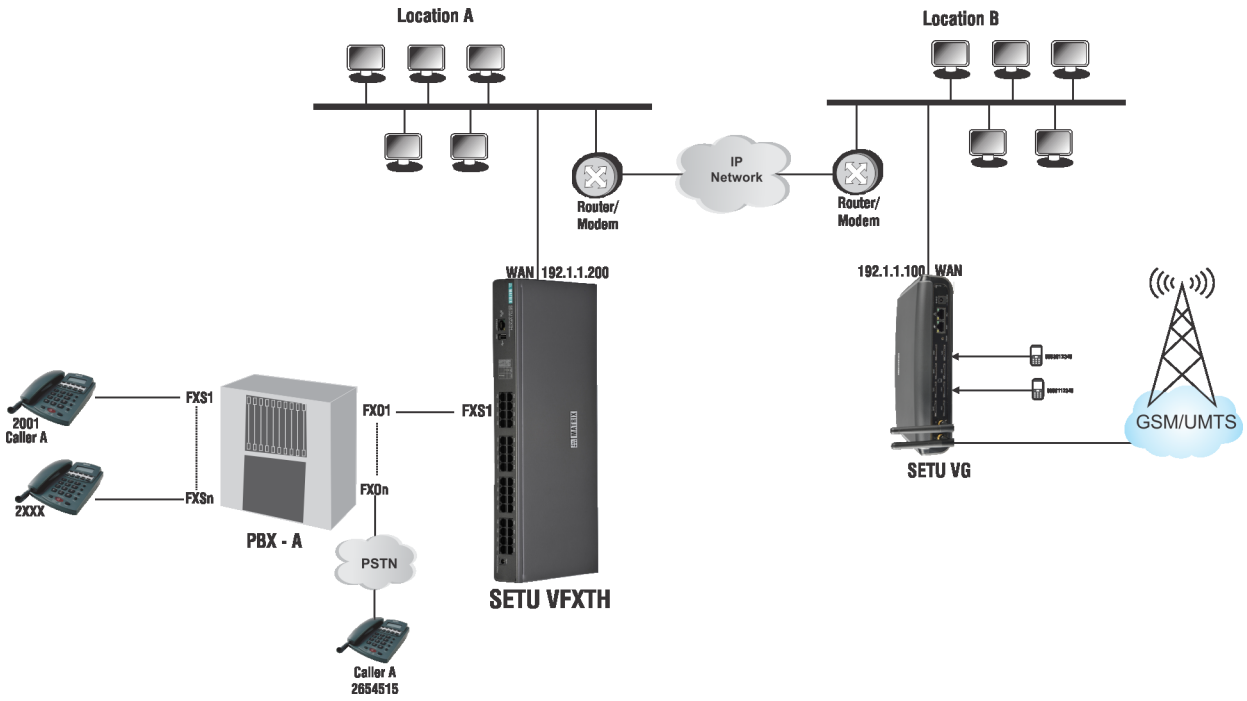
- To create Group of Mobile Ports, click **Mobile Group**.

  SETU VG8 supports 8 Groups with 8 members in each group. SETU VG4 supports 4 Groups with 4 members in each group.

# Peer to Peer Dialing

Making an IP call without the intervention of a proxy server is called Peer-to-Peer Calling. As Peer-to-Peer calling does not require a proxy server, voice communication using this application can be done virtually free of cost. The major cost savings offered by this application makes it a very attractive mode of inter-branch or intra-office voice communication.

Let us understand how to use Peer-to-Peer Calling with the following illustration.




- Two offices are connected to the IP network.
- At Location A, a PBX (PBX A) and a Gateway (SETU VFXTH) is installed as shown above.
- SETU VG is installed at Location B.
- Peer-to-Peer calls can be made between the two locations with suitable configuration of SETU VG and the Gateway (SETU VFXTH).
- **At Location A**, you need to do the following configuration in SETU VFXTH:
  - Select a SIP Trunk to be used for this application and enable it. For example, SIP Trunk 1.
  - Set the **SIP Trunk Mode** of this trunk to **Peer-to-Peer**.
  - Keep the **SIP ID** field of the SIP Trunk **blank**.
  - Under *Handling of Incoming Calls* on the SIP Trunk, set the Incoming Call Routing option as **Route all incoming calls (with CLI) - to the Called Party Number**.
  - For **SIP Trunk 1**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **FXS Port.**

- For **FXS Port**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **SIP Trunk 1** only.

- Now, configure the **Peer-to-Peer Table**.

  The Peer-to-Peer table stores up to 500 entries. Each entry consists of the parameters—Destination Number, Destination Address and Name.

In this example, you would have to configure the Peer-to-Peer table as follows:

- At Location A, in the Number field of the Peer-to-Peer table, enter the Number you want to dial to call the phone at Location B. In this case, 9898012345.

- For the number you entered, in the Destination Address field in the table, enter the IP Address of the WAN Port of VG connected at Location B. In this case, 190.1.1.100

- The Peer-to-Peer table you configure for SETU VFXTH at Location-A would look like this:

| Destination Number | Destination Address | Name |
|---|---|---|
| No Match Found | | |
| 9898012345 | 190.1.1.100 | Location B |
| 9898112345 | 190.1.1.100 | Location B |
| | | |

*Instead of configuring the complete number string, you may configure only the prefix of the number to be dialed as follows, the system will place all calls that start with '9898' to the IP Address 190.1.1.100.*

| Destination Number | Destination Address | Name |
|---|---|---|
| No Match Found | | |
| 9898 | 190.1.1.100 | Location B |
| | | |
| | | |

- **At Location B**, you need to do the following configuration in SETU VG:

  - Select a SIP Trunk to be used for this application and enable it. For example, SIP Trunk 1.

  - Set the **SIP Trunk Mode** of this trunk to **Peer-to-Peer**.

  - Keep the **SIP ID** field of the SIP Trunk **blank**.

  - Under *Handling of Incoming Calls* on the SIP Trunk, set the Incoming Call Routing option as **Route all incoming calls (with CLI) - to the Called Party Number**.

  - For **SIP Trunk 1**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **Mobile Port**.

- For **Mobile Port**, select the **Destination Port for Routing Calls** as **Fixed**, and create **Routing Group** as **SIP Trunk 1** only.

- Now, configure the **Peer-to-Peer Table**.

In this example, you would have to configure the Peer-to-Peer table as follows:

- At Location B, in the Number field of the Peer-to-Peer table, enter the Number you want to dial to call the phone at Location A. In this case, 2001 to 2xxx.

- For the number you entered, in the Destination Address field in the table, enter the IP Address of the WAN Port of VG connected at Location B. In this case, 190.1.1.100

- The Peer-to-Peer table you configure for SETU VG at Location-A would look like this:

| Destination Number | Destination Address | Name |
|---|---|---|
| No Match Found | | |
| 2001 | 190.1.1.200 | Location A |
| : | : | : |
| 2xxx | 190.1.1.200 | Location A |

- Configure PBX at location A such that calls received on the SIP Trunk are routed to respective user, that is, calls to 2001 should be routed to FXS 1 and so on. Similarly, when any FXS Port user dials a number starting with '9898', it should be routed using the SIP Trunk of the Gateway (SETU VFXTH).

  When user 2001 of Location-A calls 9898012345, the call is received on the SIP Trunk of the SETU VG and is placed to the IP address 190.1.1.100, as the system finds a matching entry for the dialed number in the Peer-to-Peer table.

- On receiving a call, the SETU VG at Location-B routes this call through the Mobile Port of the SETU VG to the Mobile user 9898012345.

- Similarly, when the Mobile user 989801245 of Location B calls 2001, the call is received on the SIP Trunk of the SETU VG and is placed to the IP address 190.1.1.200, as the system finds a matching entry for the dialed number in the Peer-to-Peer table and the call is then routed to the extension user 2001.

## How to Configure

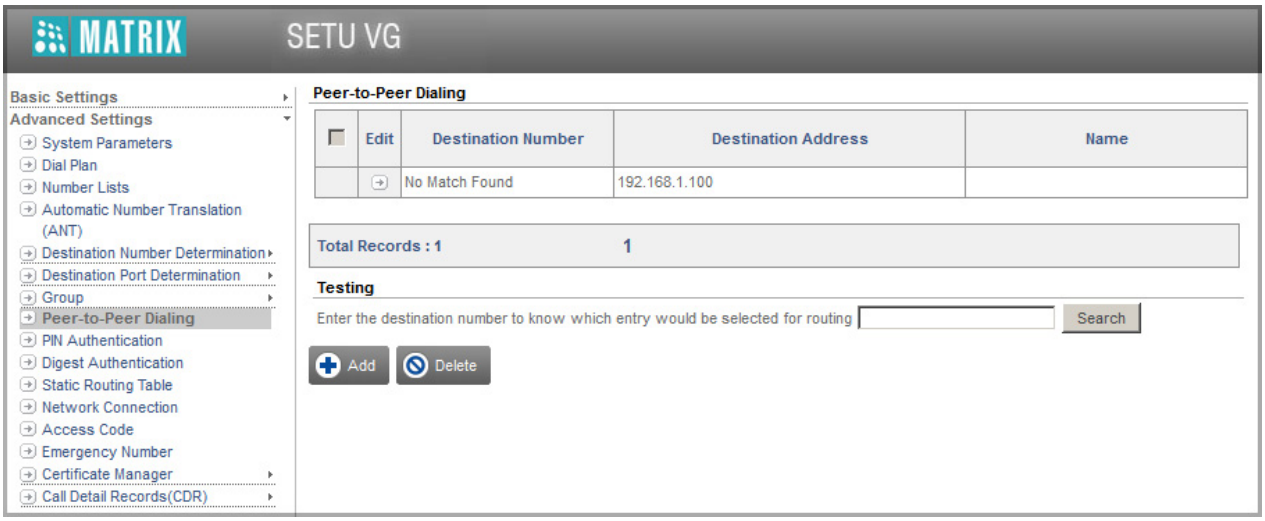
To use Peer-to-Peer calling, you must configure the related SIP Trunk parameters for the Peer-to-Peer application, namely: SIP Trunk Mode, Peer-to-Peer Table, SIP ID, and Handling of Incoming Calls. For instructions, see “SIP Trunk” under *Basic Settings*.

You can also configure the Peer-to-Peer Table from the SIP Trunk page under *Basic Settings*.

To configure the Peer-to-Peer Table,

- Log into Jeeves.

- Click the **Advanced Settings** link.
- Click the **Peer-to-Peer Dialing** link. The Peer-to-Peer table opens.




In the Peer-to-Peer table, the first entry is reserved for No Match Found.

- Click the **Add** button. A new window opens.


- In the **Destination Number** field, enter the number you expect the callers to dial. You may enter upto 64 characters (Digits + "Wildcard Characters") in this field. Valid characters: 0 to 9, *, #, X, T, Comma [,], Hyphen [-], Caret [^]. Default: Blank.

  If the number to be dialed out is <dialednumber@destination address>, for example, 1234@abc.com, you must enter 1234 in this field.

## Wildcard Characters

SETU VG supports following characters.

| Character | Description |
|---|---|
| **X** (letter X) | X represents any single digit from 0 to 9. |
| **#** | When # is configured in a number string, it will not be considered as End of Dialing. |
| ***** | When * is configured in a number string, it will not be considered as End of Dialing. |

| | |
|---|---|
| **+** | + (plus) can be configured as a first character of the Destination Number string in the *SIP Trunk-Destination Port Determination-Destination Number Based* table only. |
| **[ - ]** | Hyphen within the bracket, defines a range. Only digits 0-9 are allowed within a bracket. |
| **[ , ]** | Comma within a bracket is used as a separator between the groups of numbers. |
| **[ ^ ]** | Caret within a bracket is used to deny or restrict the number or range defined after the symbol. Only digits 0-9 are allowed after the caret. |
| **T** (letter T) | Character T can be configured only as a last character in a number string. When configured in a number string, the system waits for End of Dialing. |

- In the **Destination Address** field**,** enter the domain name or IP Address to where the call is to be placed. The Destination Address may consists of up to 40 characters (maximum). Default: 192.168.1.100.

  For example, if the peer-to-peer number to be dialed out is 1234@abc.com, enter abc.com as Destination Address. If the number is 1234@ 192.168.1.197, enter 192.168.1.197 as the Destination Address. The Destination Address can also be in the form of Address: Port number.

- In the **Name** field, enter a name to identify the number string you configured. It may be the name of your contact or any name you wish to assign to the number string. The name may consist of 24 characters (maximum). Default: Blank.

  The name you configure here will not be used in SIP signaling.

- Click **Submit** to save your entries.

*If there are multiple entries in the Peer to Peer table, to search a particular entry in the table, under Testing enter the desired number in the Enter the destination number to know which entry would be selected for routing search box.*

# PIN Authentication

PIN Authentication is a necessary security feature to restrict access to the system and prevent possible misuse of resources.

You can use PIN Authentication on the Source Port to establish the identity of callers before their call is processed by SETU VG.

PIN Authentication can be used on the Source Port only if the incoming call routing for the Source Port is set to ***Route calls After Answering the Call and Collecting the Digits***.

To be able to use PIN Authentication, this feature must be enabled on the Source Port and the PIN Authentication table must be configured.

The PIN Authentication table stores up to 500 PIN Numbers and their corresponding authentication Passwords.

When you enable PIN Authentication on the Source Port, SETU VG answers the incoming call on the port and plays the prompt tone. It waits for the caller to dial the PIN Number and the Password. It collects the digits dialed by the caller and matches them with the PIN Authentication table.

When a match is found in the table, SETU VG authenticates the caller and allows the call to be processed.

If the digits dialed by the caller do not match with any entry in this table, SETU VG allows the caller to make two more attempts to dial a valid PIN Number and Password. If the caller fails to dial the correct PIN and Password in all the attempts, the system disconnects the call.

## Configuring PIN Authentication

To use this feature, you must enable PIN Authentication on the desired SIP Trunks and Mobile Ports and configure the PIN Authentication Table.

To configure PIN Authentication table,

- Log into Jeeves.
- Click the **Advanced Settings** link.

- Click the **PIN Authentication** link.


- Now, configure the **PIN Authentication** table.

  - In the **PIN Number** column, enter the numbers with which callers will authenticate themselves. Default: Blank. The digits 0 to 9, * and # are allowed in PIN Numbers.

*The length of the PIN Number must not exceed four digits. If you enter a PIN Number that is less than 4 digits, the system will add leading zeros. The caller must also dial the PIN Number with the leading zeros to authenticate.*

  - For each PIN Number you store, enter an authenticating password in the **PIN Password** field. The password can be of a maximum of four digits. The digits 0 to 9, * and # allowed. Default: Blank.

- Click **Submit** to save the entries.

- Now, enable PIN Authentication on the desired SIP Trunks and Mobile Ports on which you have selected the incoming call routing option **After Answering the Call and Collecting the Digits** under *Handling of Incoming Calls*. Enable **Prompt caller to enter PIN** on the port.

  Under "Basic Settings", see "SIP Trunk" and "Mobile Port" for instructions.

  You can enable PIN Authentication and configure the PIN Authentication Table also on the SIP Trunk and Mobile Port pages under *Basic Settings*.

# Digest Authentication

Digest Authentication is a challenge-based authentication service of SIP to authenticate the identity of the originator of SIP request in the INVITE message. The recipient of the request can ascertain whether or not the originator of the request is authorised to make the request. When the digest credentials of the originator, namely, User Name and Password, in the INVITE message are authenticated and accepted by the recipient, the originator and the recipient are connected.

SETU VG supports Digest Authentication. The Digest Authentication feature works on the basis of the Digest Authentication Table, in which the credentials, the User Name and Passwords of trusted/authorised calling party SIP devices, are stored. You must configure this table.

When you enable this feature on a SIP Trunk, for all incoming calls (SIP requests),

- SETU VG will challenge the identity of the calling party, that is, the SIP device initiating the request to send its digest credentials.
- When the calling party sends its credentials, SETU VG authenticates the credentials by matching it with its Digest Authentication Table.
- If a match is found, the calling party will be authenticated and the call will be allowed on the SIP Trunk.
- If no match is found, SETU VG will consider it as invalid authentication information and reject the call.

You may use Digest Authentication to:
- restrict access to SETU VG to specific callers.
- prevent unwanted or malicious calls.

## Configuring Digest Authentication

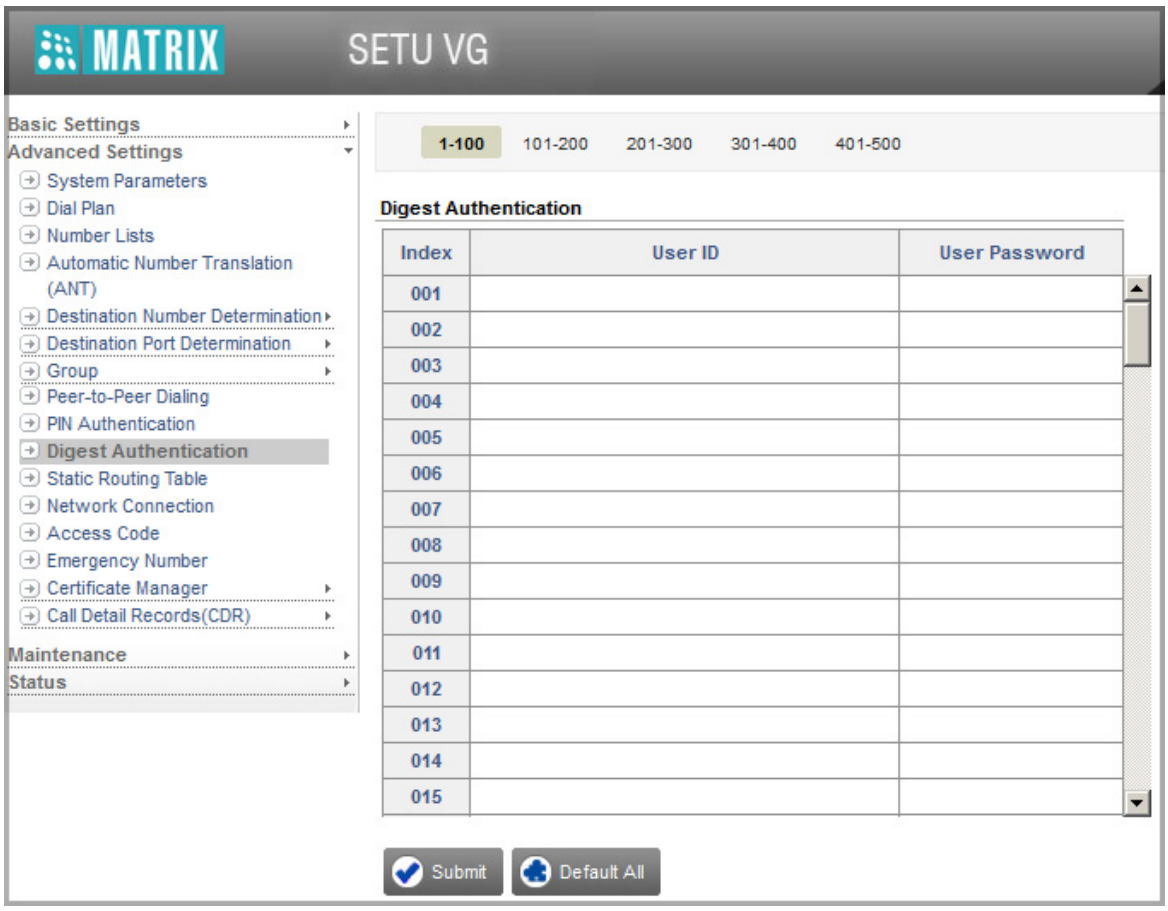
To use this feature, you must enable **Digest Authentication** on the desired SIP Trunk and configure the Digest Authentication Table.

You can configure the Digest Authentication Table also from the SIP Trunk parameters page of Jeeves.

To configure Digest Authentication table,

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Digest Authentication** link.

The **Digest Authentication** Table page opens. You can configure up to 500 entries in this table. This Table is common for all SIP Trunks.




- Enter the user name assigned to the caller/calling device in the **User ID** field. SETU VG will use this User ID to match the digest credentials sent by the caller/calling devices when challenged.

  Make sure the User ID you enter here and the User ID assigned at the *calling end* are the same. The User ID can be up to 40 characters long. Default: Blank.

- Enter the password to authenticate the user ID in the **User Password** field. The password may consist of a maximum of 24 characters. Default: Blank.

  Make sure the User Password you enter here and the User Password assigned at the calling end are the same.

- Click **Submit** to save the entries.

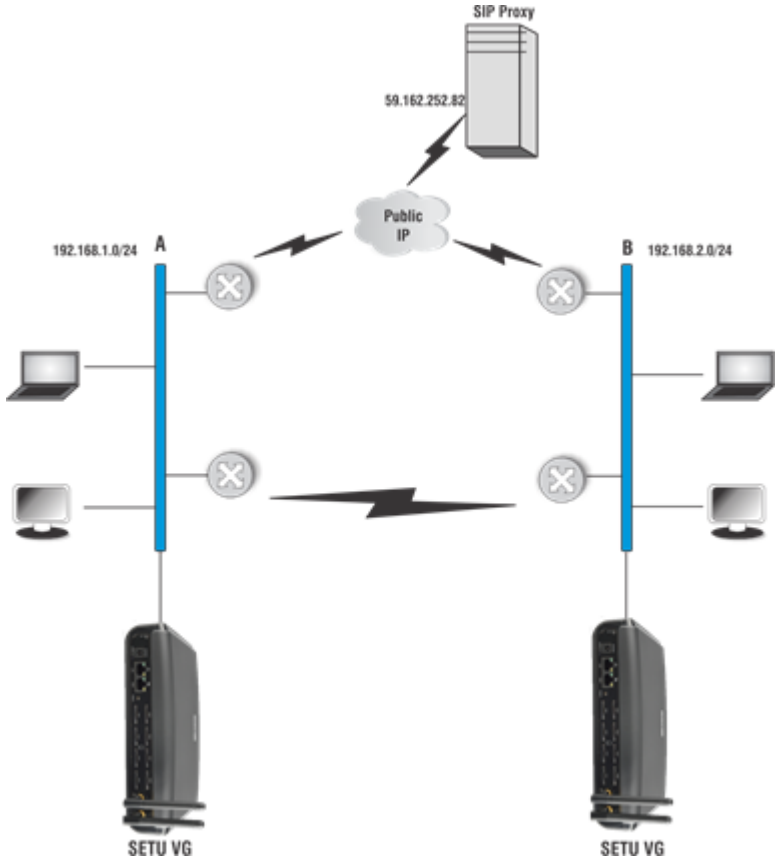
- Make sure you also enable Digest Authentication on the desired SIP Trunk. For instructions, see “SIP Trunk” under *Basic Settings*.

# Static Routing

Static Routing Table is required when you have more than one router (gateway) in your network and you want SETU VG to send packets to multiple routers/gateways for different types of calls.

Static Routing Table helps route calls between point to point sites (connected through Multi Protocol Label Switching-MPLS, Frame Relay, etc.) and to public internet at the same time.

For example, two Local Area Networks, Network A and Network B, are connected through Frame Relay/ Multi Protocol Label Switching (MPLS) network to give access to local resources and also to make Peer-to-Peer calls. SETU VG is connected at both sites behind a router.




These sites are also connected to public IP network to:

- give internet access to local hosts.
- access DID service provided by ITSPs to make GSM calls over IP network.

Network A and Network B are in different subnets.

The Static Routing Table makes it possible to route different types of outgoing calls—Peer to Peer or Proxy—made to different subnets through different Gateways.

The Static Routing Table defines the appropriate Gateway Address (or Router's LAN Address) where the IP packets are to be sent.

In the Static Routing Table, you must configure:

- The address of the final Destination where the packets are to be sent.

- The Subnet Mask to be applied on the final destination address.
- The Gateway Address where the IP packets are to be sent.

When SETU VG sends packets, if the final destination IP Address and SETU VG are not in the same Subnet, the system will check the Static Routing Table.

If a perfect match is found, SETU VG will start sending the IP packets to the corresponding Gateway Address configured in the table.

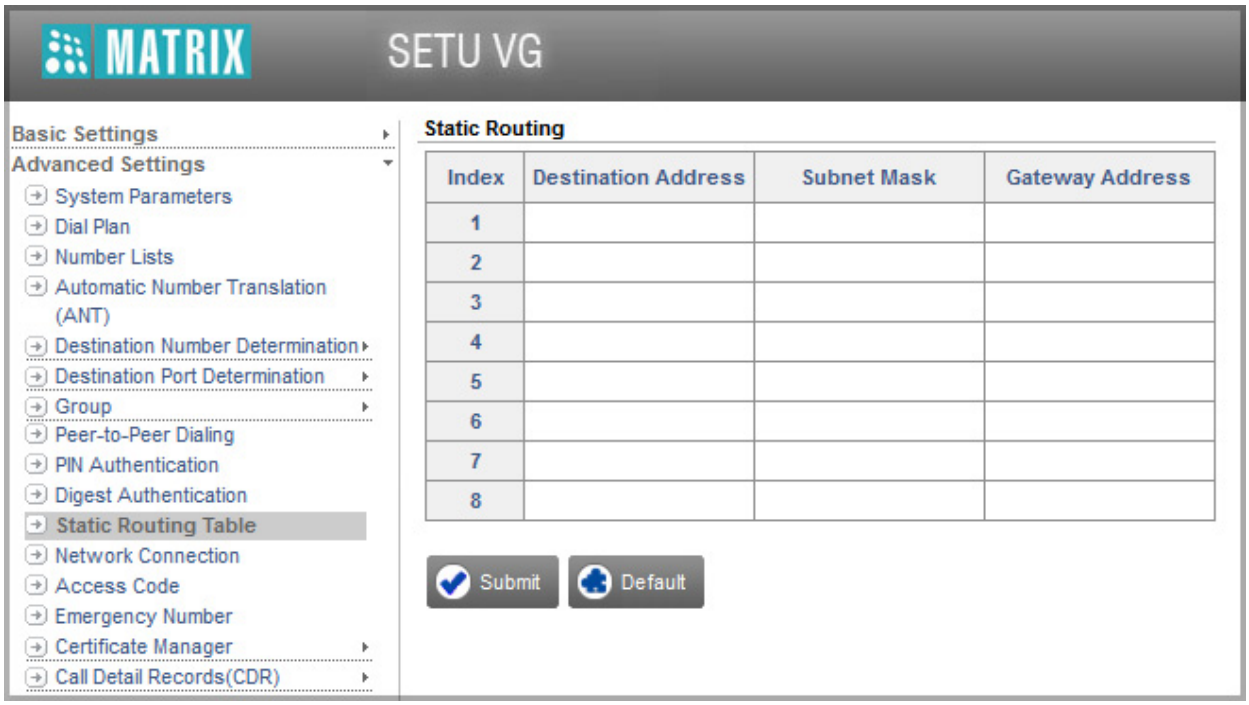
If no match is found, SETU VG will send the IP Packets to the **Default Gateway Address** (Network Connection Type) you configured in "Network" the page.

- *The Static Routing Table is common for all SIP Trunks.*
- *The Static Routing Table is applicable only when the Network Connection is established through WAN.*

## Configuring Static Routing Table

The Static Routing Table must be configured at each location where SETU VG is installed. To configure the Static Routing Table,

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Static Routing** link. The Static Routing Table page opens.




The Static Routing Table allows you to configure up to 8 entries. Each entry is stored against an Index number.

For each entry, you must configure the following fields:

- **Destination Address:** This is the address of the final destination where the call is to be made. This can be a device IP Address or Network Address.

- **Subnet Mask**: This is the mask to be applied on the destination address.

- **Gateway Address**: This is the IP address of the node where the IP packets are to be sent. Generally, it is the IP address of the LAN interface of the Router.

  The Gateway Address must be in the same subnet as SETU VG.

- Click **Submit** to save your entries.

  To take the above example further, the Static Routing Table of SETU VG at Location A should be configured as:

| Index | Destination Address | Subnet Mask | Gateway Address |
|---|---|---|---|
| 1 | 192.168.2.0 | 255.255.255.0 | 192.168.1.1 |
| 2 | | | |
| : | | | |
| 8 | | | |

  - The Destination Address 192.168.2.0 specifies the network address of Location B.

  - The Subnet Mask is the mask to be applied on the Destination address.

  - The Gateway Address 192.168.1.1 specifies the LAN address of the Router A which connects location A and location B.

    The IP address of the LAN interface of the router which connects Location A to the public internet should be configured as Default Gateway in the Network Parameters of SETU VG at Location A.

    With the Static Routing Table configured thus, all calls made by SETU VG to 192.168.2.0/ 24 will be routed through the router which connects Location A to Location B. Whereas, all calls made by SETU VG to addresses other than 192.168.2.0/ 24 will be routed through the Default Gateway.

    Similarly, configure the Static Routing Table in SETU VG at location B to enable calling from Location B to Location A.

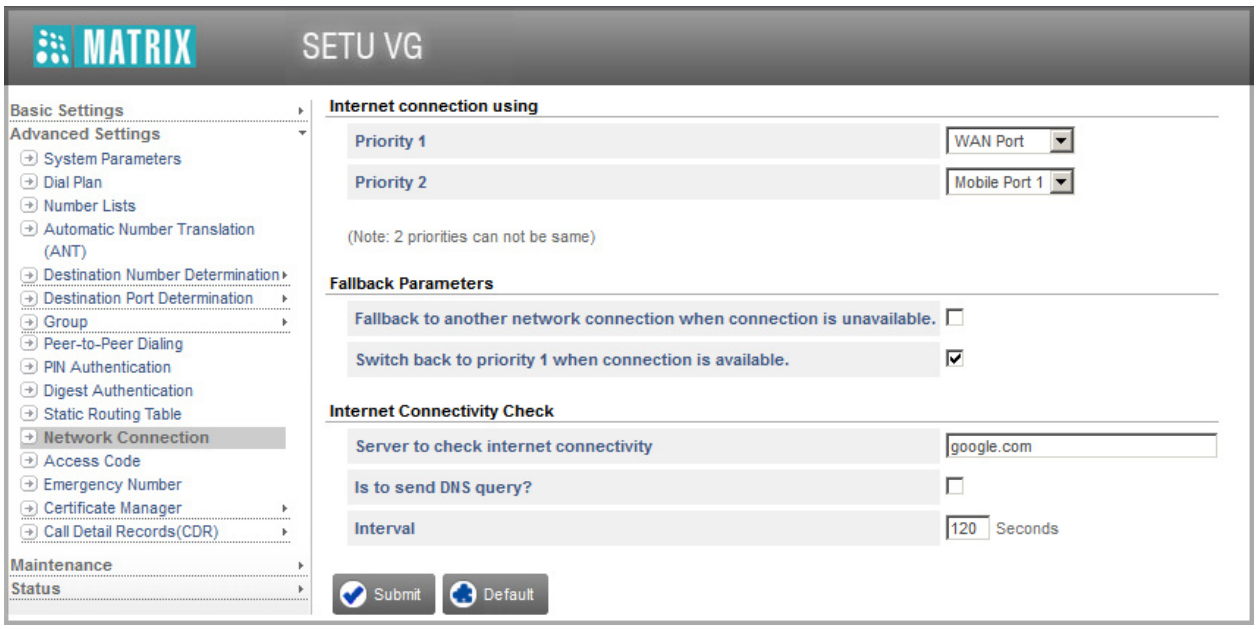
# Network Connection

SETU VG offers connectivity to the IP Network over its WAN Port as well as over the Mobile Wireless WAN (Mobile Port 1).

For uninterrupted connectivity to the IP network and to minimize down time, you can connect SETU VG to the IP network over both WAN and Mobile Port 1. You can set the priority for each internet connection, ensuring that you have a fallback network connection each time one connection is down. You can also set SETU VG to monitor connectivity to the IP network and automatically switch to another, when one link is down.

For this, you need to configure the Network Connection settings.

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Network Connection** link.




- Configure the network connection settings as per your preference and requirement.

## Internet Connection Using

- Under **Internet Connection using** options, by default **WAN Port** is set as **Priority1** and **Mobile Port 1** as **Priority 2**. You can change the **Priority 1** and **2** as per your requirement, from the different connection interfaces:
  - None
  - WAN Port
  - Mobile Port 1

  You cannot select the same option for two priorities except None.

## Fallback Parameters

- Select the **Fallback to another network connection when connection is unavailable** check box, if you want the system to automatically switch over to the next Priority to re-establish the network connection, when the network connection set as Priority 1 fails. Default: Disabled.

- To have the system switch back to Priority 1 when the connection to Priority 1 network is restored, keep the **Switch back to priority 1 when connection is available** check box enabled.

## Internet Connectivity Check

To have the system monitor network connectivity, set Internet Connectivity Check:

- In **Server to check Internet Connectivity**, enter any Public IP Address / Domain Name like 'google.com'.

  The system will ping this programmed address to check internet connectivity regularly at fixed intervals. Default: google.com

- Select the **Is to send DNS query?** check box, if you want the system to check the internet connectivity by sending the DNS query. Default: Disabled.

- In the **Interval** field, define the time interval at which you want the system to ping the Public IP Address / Domain Name to check the Internet Connectivity. Default: 120 seconds.

- Click **Submit** to save the changes.

With these parameters configured, the system pings the server at regular intervals (which you have configured) to monitor the status of the connection, whether the link is up or down.

The system re-establishes the link by selecting the next available connection set as the next Priority for Fallback. Thus, network connectivity is not hampered.

# Access Codes

Access Code is a string of digits dialed to use a feature. SETU VG users can access the following features and facilities by dialing the feature Access Codes.

- Making a New Call
- Disconnect Call

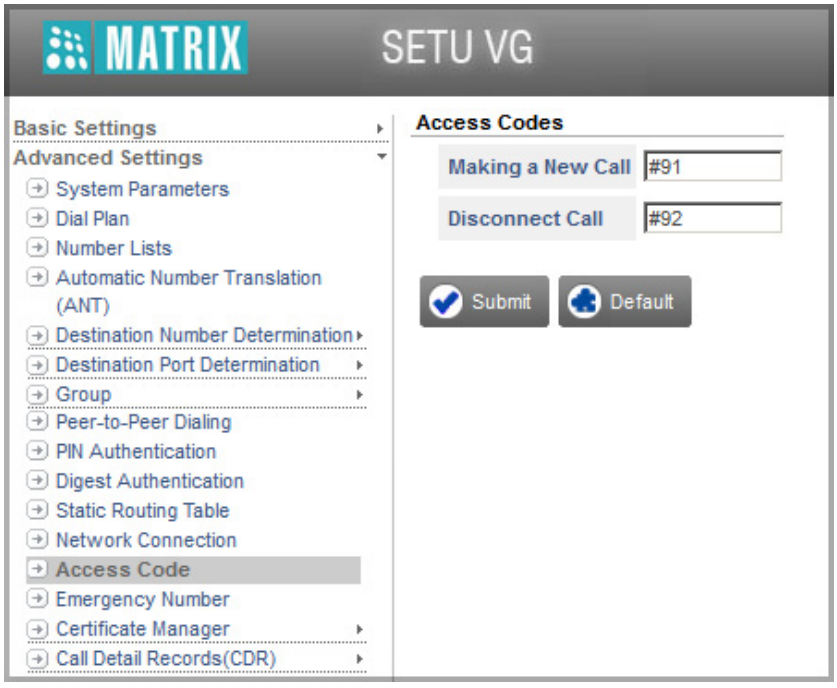
You can change the default access codes assigned to the above features and facilities to suit your requirement.

*Emergency Numbers have priority over Access Codes and Access Codes have priority over the Destination Numbers.*

## Configuring Access Codes

To change the default Access Codes assigned to the features and facilities,

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Access Code** link.




- Change the default access code for the feature/facility, as required. Access Codes can be a maximum of 4 digits and digits 0-9, *, # and ^ are allowed.

*Do not configure Access Codes that may conflict with the Emergency Numbers.*

- Click **Submit** to save changes.

# Emergency Numbers

SETU VG supports the dialing of Emergency Numbers from all ports. Emergency numbers and their respective Routing Groups (through which they are to be routed) must be configured in the Emergency Number Table.

When you select "Region", the system loads the Emergency Numbers used in the country you selected as Region, in the Emergency Number Table.

For each of these numbers loaded, the system assigns a default Routing Group to route the number. You may reassign the Routing Group, as appropriate.

You may also add numbers of emergency services as per your requirement and assign Routing Group for the numbers in the Emergency Number Table.

The Emergency Number Table stores up to 10 numbers, including those loaded by default.

- *For a few Regions, the system may not load default Emergency numbers in the Emergency Table. You may add the numbers as per your requirement.*
- *Emergency number Dialing will not work if Mains power to SETU VG fails.*
- *Emergency Numbers have priority over Destination Number Table, PIN Number and Access Codes.*
- *The system does not apply End-of-Dialing when dialing Emergency Numbers.*
- *The system does not check Allowed-Denied Logic and Automatic Number Translation table when dialing an Emergency Number.*

SETU VG will dial out an emergency number only if the SIP Trunks/Mobile Ports included in the Routing Group for the number are enabled.

SETU VG can dial out the numbers available in the Emergency Number Table even in the following situations:

- When SIM is absent
- When SIM is invalid
- When wrong SIM PIN is entered
- When SIM is blocked
- When GSM module is not registered

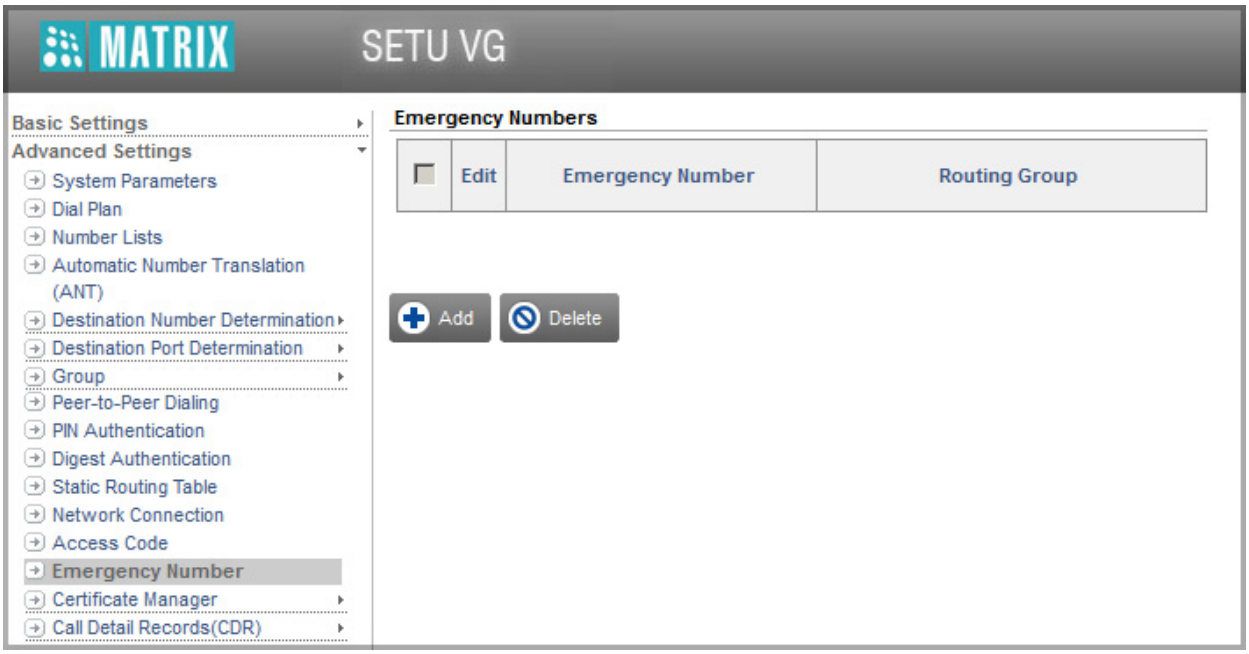
*Some countries do not allow dialing of Emergency Number without SIM. As per TEC standard, India allows dialing of Emergency Number without SIM.*

## Configuring Emergency Numbers

To configure the Emergency Number Table,

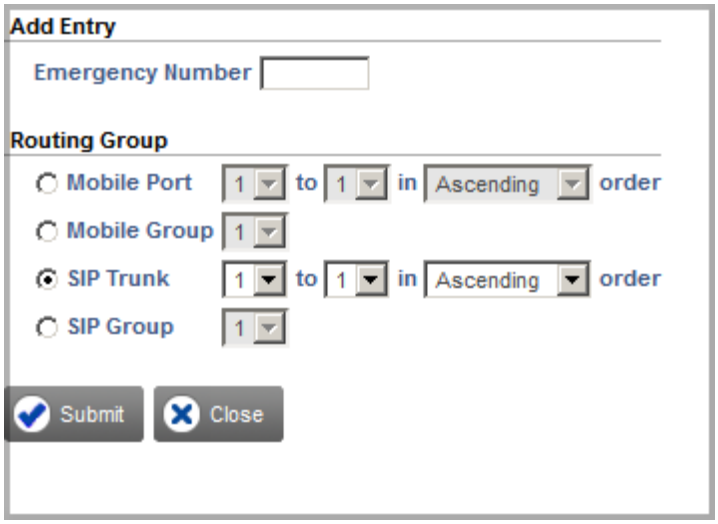
- Log into Jeeves.
- Click the **Advanced Settings** link.

- Click the **Emergency Number** link.




- To **Add** an Emergency Number to the table, click the **Add** button.
- To **Edit** an Emergency Number and or assign a Routing Group, click **Settings** of that number.

  A new window opens, to allow you to add/edit the entry.




- In the **Emergency Number** field, enter the emergency number used in your country/region.

*Make sure that Access Codes you have configured do not conflict with the Emergency Numbers.*

- Create the **Routing Group**.
  - To create a group of *sequential* **Mobile Port** as members,

- Select the desired **Mobile Port** numbers as members. Default: 1.
- In the **in - order** field, select the order in which the system should hunt for a free member Mobile Port to route the call.

  Select **Ascending** to start hunting from the first to the last member Mobile Port. Select **Descending** to start hunting from the last to the first member Mobile Port. Default: Ascending.

- To create a group of *not-sequential* **Mobile Ports** as members,
  - Select **Mobile Group**.
  - Select the **Mobile Group** number. Default:1.
  - Click **Settings** . The **Mobile Groups** window opens. Create the Mobile Group. See “Group” for detailed instructions.
- To create a group of *sequential* **SIP Trunks** as members,
  - Select the desired **SIP Trunk** numbers as members. Default: 1.
  - In the **in - order** field, select the order in which the system should hunt for a free member SIP Trunk to route the call.

    Select **Ascending** to start hunting from the first to the last member SIP Trunk. Select **Descending** to start hunting from the last to the first member SIP Trunk. Default: Ascending.
- To create a group of *not-sequential* **SIP Trunks** as members,
  - Select a **SIP Group**.
  - Select **SIP Group** number. Default:1.
  - Click **Settings** . The **SIP Groups** window opens. Create the SIP Group. See “Group” for detailed instructions.
- Click **Submit** to save. Close the **Add Entry/Edit Entry** window. The entries you added appear on the Emergency Numbers page.

# Certificate Manager

SETU VG supports certification for TLS, Web Server, Firmware Upgrade, Configuration Upgrade and TR-069.

SETU VG supports two types of Certificates: **Self-Signed Certificate** and **CA Signed Certificate.**

## Self-Signed Certificate

A self-signed certificate is created by the clients themselves or by the Servers and then given to their clients. It means that you yourself become the Certificate Authority (CA), create a CA Certificate and sign it. The self-signed certificate is faster to create but is not signed by a trusted CA Organization. The self-signed certificate must be installed in the trusted list of clients that connects over TLS with the Server. Because the certificate has been self-signed, the signature is not likely to be in the clients' trust file, hence, they need to add it.

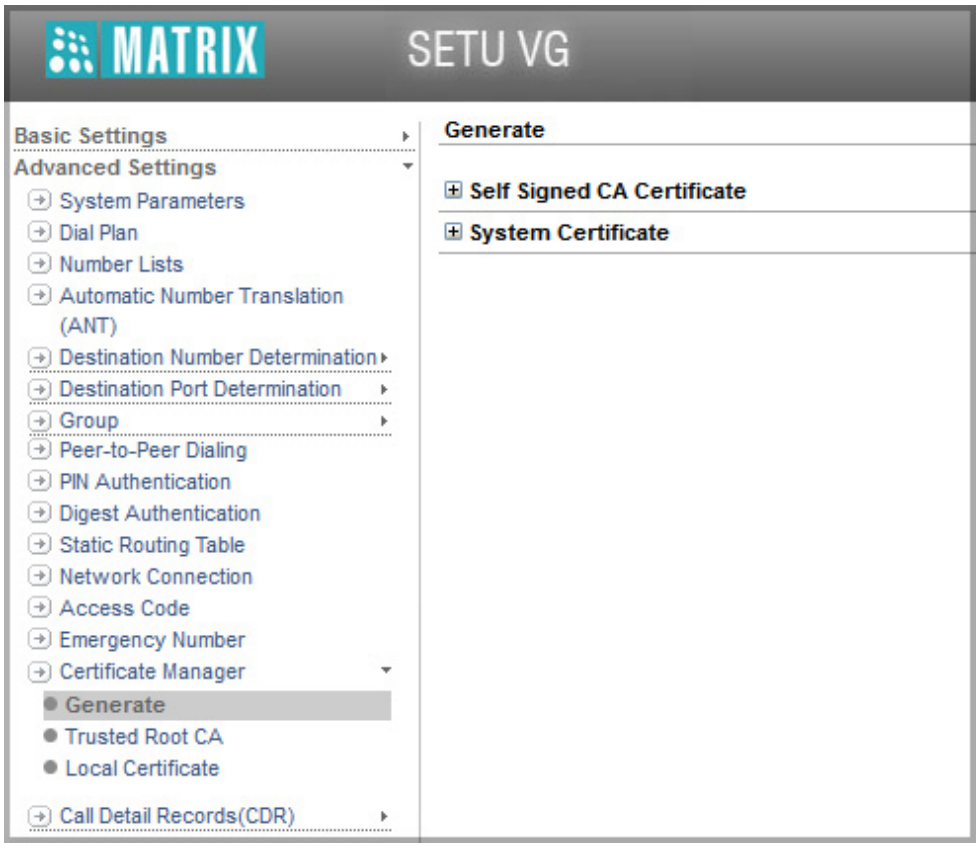
If you select **Self-Signed Certificate**, you need to do the following:

1. Create a Self-Signed CA Certificate.
2. Create a System Certificate (Self-Signed Certificate).

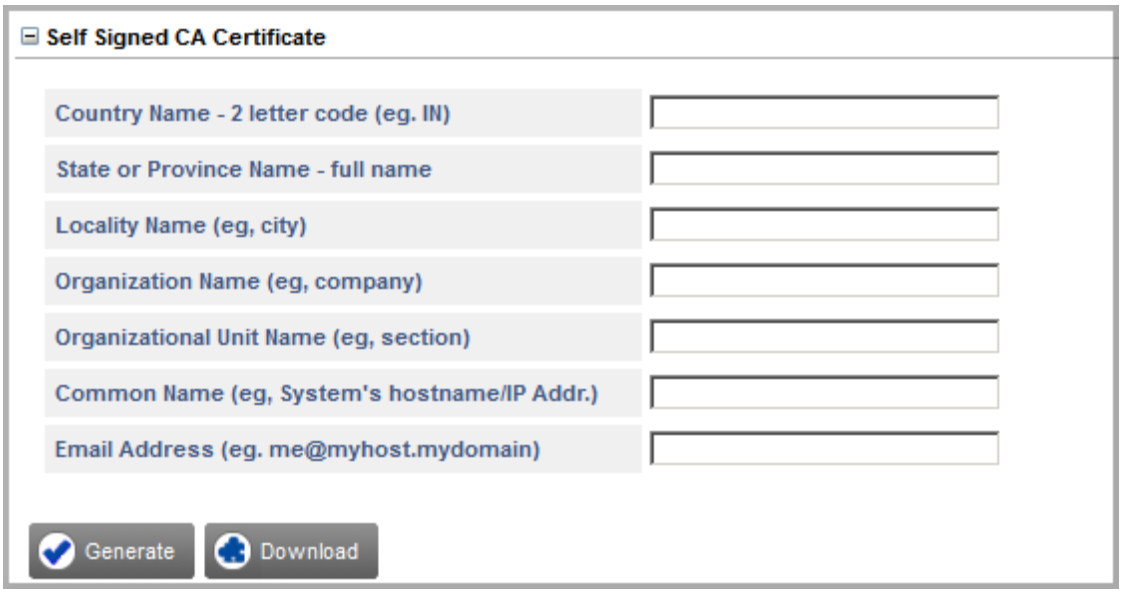
### Generating a Self-Signed CA Certificate

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Certificate Manager** link.

- Click the **Generate** link.




- Click **Self Signed CA Certificate** to expand and configure the following parameters.



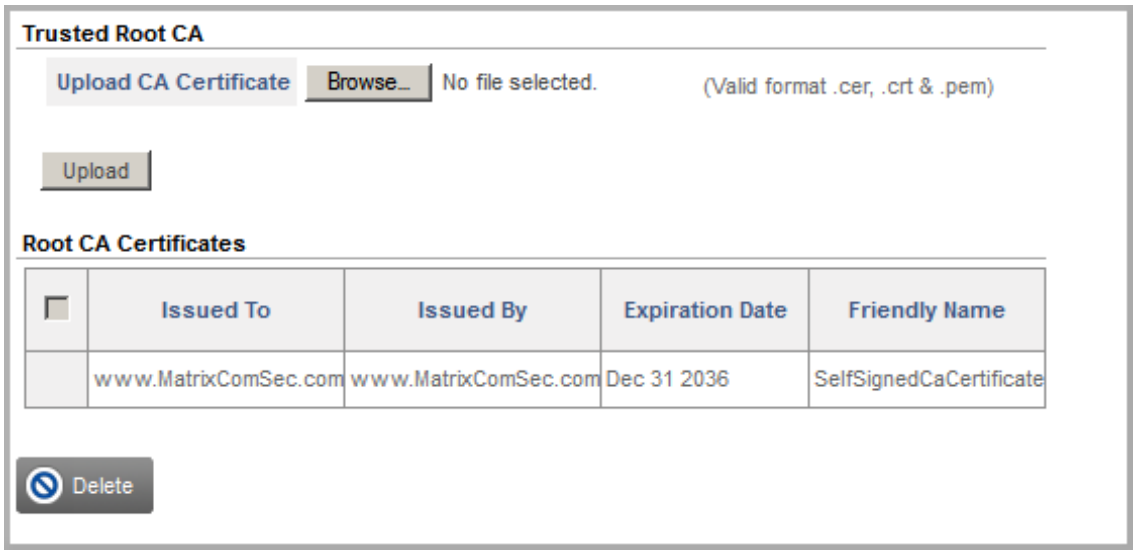

- In **Country Name - 2 letter code (eg. IN)**, enter the name of your country.
- In **State or Province Name - full name**, enter the full name of your state or province.
- In **Locality Name (eg. city)**, enter the name of your city.

- In **Organization Name (eg. company)**, enter the name of your organization where SETU VG is installed.
- In **Organizational Unit Name (eg. section)**, enter the name of the unit or section or domain of your organization, where SETU VG is installed.
- In **Common Name (eg. System's hostname/IP Addr.)**, enter your Server's (SETU VG) host name or IP Address. This Common Name serves as the distinguishing factor.
- In **Email Address (eg. me@myhost.mydomain)**, enter your host's e-mail address.

- Click **Generate**, to generate this self-signed CA Certificate.

Once you generate self-signed certificate, you must send it to your clients so that they install it in their trusted list.

- To do this, click **Download**. Save the file at the desired location.
- Under **Certificate Manager**, click the **Trusted Root CA** link. The CA Certificate you created appears in the **Root CA Certificate** table.




- If you want to upload other CA Certificates, in **Upload CA Certificate** browse the location at which the certificate is saved and click **Upload**. The CA Certificate you uploaded appears in the **Root CA Certificate** table. Valid format are .cer, .crt and .pem.
- To delete a CA Certificate, select the check box of the respective Root CA Certificate and click **Delete**.

A sample Self-Signed CA Certificate is as under:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD.,
OU=R&D, CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
        Validity
            Not Before: Aug 13 13:13:18 2013 GMT
            Not After : Dec 31 13:13:18 2036 GMT
        Subject: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD.,
OU=R&D, CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:da:9e:27:ae:64:58:1d:88:d1:58:10:96:1d:42:
                    cf:7a:cc:ef:07:ef:66:8c:93:1e:66:3b:15:07:60:
                    ea:87:f0:72:a2:93:de:31:05:64:97:92:14:e9:31:
                    47:3e:d2:dd:13:d3:06:d0:19:d4:f9:d6:b9:b6:f3:
                    9a:0c:ec:bb:bd:eb:1e:b5:24:1a:30:a5:53:2f:d5:
                    74:54:a9:10:fa:da:f1:39:05:3d:7d:09:cd:d6:d6:
                    23:37:d1:c4:d7:a4:a7:34:22:70:66:4d:b0:65:f9:
                    3b:bf:06:d0:1a:e8:97:e0:ef:c0:9e:ef:40:f1:c4:
                    c9:e2:a7:7e:03:b6:72:00:fd:8c:02:c5:57:9c:57:
                    fc:99:8c:36:22:9f:e9:7a:32:49:27:a5:11:21:3d:
                    f9:e9:6f:d2:1f:88:65:a9:45:5a:99:e2:1a:51:cb:
                    69:31:b1:dc:06:7b:ef:94:24:2e:c0:f9:f0:bd:25:
                    67:6a:e5:e9:46:f7:e8:d7:6c:f5:5c:ed:dc:cd:7c:
                    82:02:0f:7d:f7:fd:0b:66:d0:ee:24:e1:2b:64:97:
                    58:27:3b:96:bd:dd:b4:ea:3f:51:f7:a5:2c:dd:c7:
                    22:72:b9:3c:09:75:04:df:56:5b:af:f8:3d:fe:f0:
                    50:3f:01:c9:8e:2a:3e:36:66:1f:fe:dd:87:84:99:
                    11:7b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
```

In the above Self-Signed CA Certificate:

- C = Country
- ST = State
- L = Location
- O = Organization
- OU = Organization Unit
- CN = Common Name

- **Issuer** represents the details of the CA issuing the Certificate. Here, the Organization itself is the CA (issuer), hence, the O, OU and CN of both Issuer and Subject is same.

- **Validity** represents the valid period of this certificate.

- **Subject** represents the credentials of the Server / User requesting for certification.
- **Public Key** represents the public key of the certificate.

## Generating a System Certificate (Self-Signed Certificate)

After creating a Self-Signed CA Certificate, you can either,

- generate a System Certificate for your clients. These System Certificates can then be given to the respective clients.

**or**

- the Clients can prepare their own System Certificates. For this you need to send them the CA Certificate created by you.

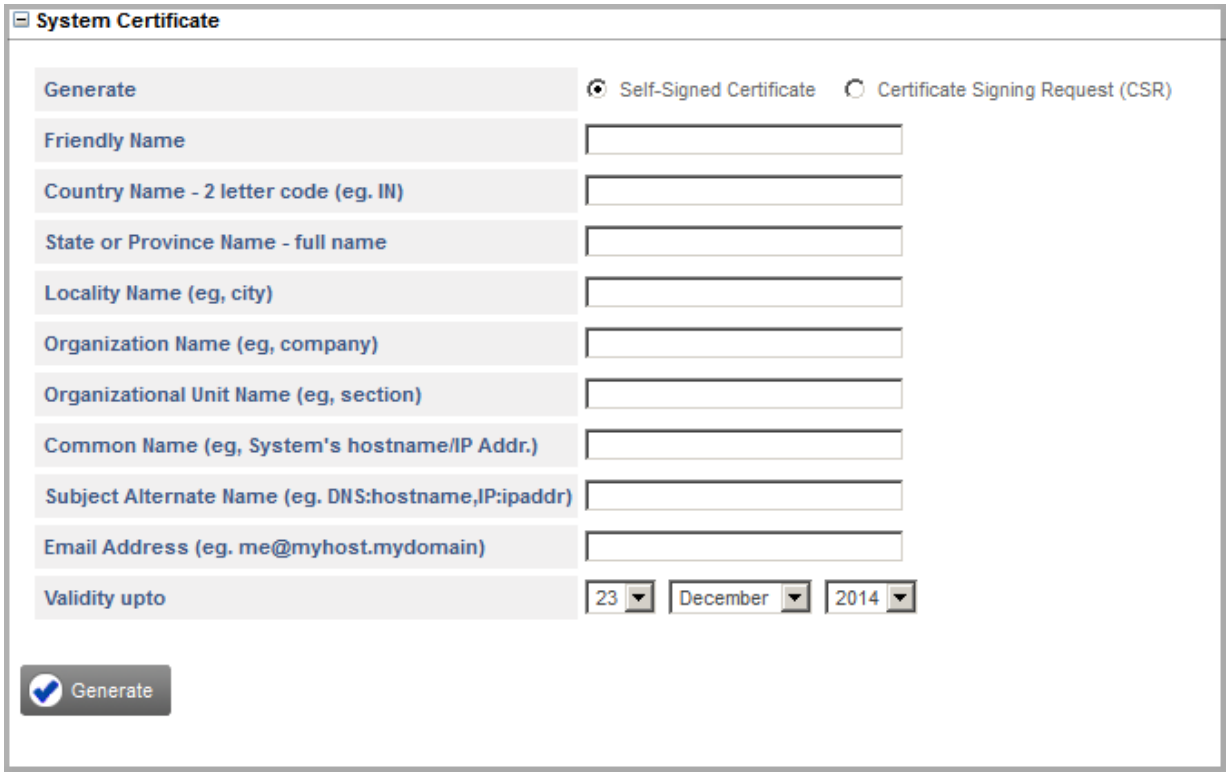
**or**

generate a Certificate Signing Request (CSR), if you want the Certificate to be signed by a third party.

*If the clients prepare their own certificates, you need to send your CA Certificate to all the clients. The clients must upload the same in their system. Similarly, all the clients must send their CA Certificates to you and you must upload the same in your system. To avoid this, it is recommended that you create the Certificates and then provide it to your clients.*

To create the System Certificate,

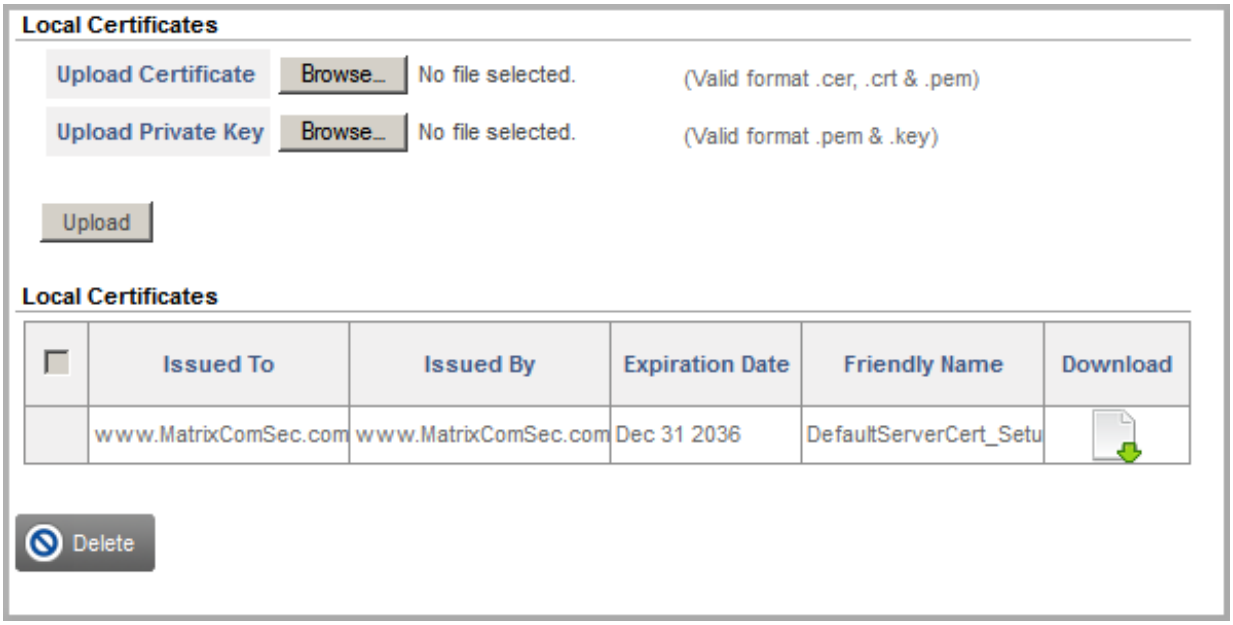
- Click the **Certificate Manager** link.
- Click the **Generate** link.
- Click **System Certificate** to expand and configure the following parameters.




- In **Generate**, select the type of certificate you want to create. You must select **Self-Signed Certificate**.

- In **Friendly Name**, enter the name you want to assign to the certificate.
- In **Country Name - 2 letter code (eg. IN)**, enter the name (two letter code) of your country.
- In **State or Province Name - full name**, enter the full name of your state or province.
- In **Locality Name (eg. city)**, enter the name of your city.
- In **Organization Name (eg. company)**, enter the name of your organization where SETU VG is installed.
- In **Organizational Unit Name (eg. section)**, enter the name of the unit or section or domain of your organization, where SETU VG is installed.
- In **Common Name (eg. System's hostname/IP Addr.)**, enter your Server's (SETU VG) host name or IP Address. This Common Name serves as the distinguishing factor.
- In **Subject Alternate Name (eg. DNS:hostname,IP:ipaddr)**, enter the name of the multiple domain separated by comma (if the same certificate is to be issued for multiple domain of the organization).
- In **Email Address**, enter the your host's e-mail address.
- In **Validity Upto**, select the date till which this certificate will be valid.

- Click **Generate**, to generate this System Certificate.
- Under **Certificate Manager**, click the **Local Certificate** link. The generated certificate appears in the **Local Certificates** table.




- If you want to upload other System Certificates, in **Upload Certificate** browse the location at which the certificate is saved. Along with the certificate you also need to upload the Private Key, in **Upload Private Key** browse the location at which the key is saved and click **Upload**.

The System Certificate you uploaded appears in the **Local Certificates** table. Valid formats for certificate are .cer, .crt and .pem. Valid format for key are .pem and .key (Base64 encoded ASCII file).

- To delete a System Certificate, select the check box of the respective Certificate and click **Delete**.
- To download the System Certificate, click **Download**  .

A sample Self-Signed System Certificate is as under:

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 2 (0x2)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD., OU=R&D,
CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
    Validity
      Not Before: Aug 13 13:14:57 2013 GMT
      Not After : Dec 31 13:14:57 2036 GMT
    Subject: C=IN, ST=Gujarat, L=Vadodara, O=MATRIX COMSEC PVT. LTD., OU=R&D,
CN=www.MatrixComSec.com/emailAddress=Support@MatrixComSec.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          00:b5:29:61:26:35:db:d7:a8:fd:05:4d:ac:2d:6c:
          65:70:4d:42:fb:f6:1e:c8:18:bd:1c:c7:5a:92:b3:
          28:52:48:66:7c:0f:c8:35:6f:13:46:62:1e:23:44:
          b3:27:28:f5:8e:43:1a:e3:f6:7e:d5:8f:a9:73:8a:
          2c:34:1e:35:d0:c8:0c:b2:68:12:dc:1a:23:da:fe:
          02:af:88:4e:a1:7a:7f:a0:2b:ca:b9:72:5d:ac:3a:
          e3:9b:fd:0d:ab:0f:c3:57:a9:99:cd:2e:be:02:9c:
          60:0e:83:e8:69:2d:0f:95:79:52:87:66:9f:4a:10:
          09:db:4e:41:e2:f2:b4:86:cd:42:a9:55:6d:33:a3:
          60:67:fd:1d:3d:0e:8d:6a:53:77:e0:07:78:c9:c8:
          34:23:df:3d:94:02:41:e9:c4:2b:c8:04:10:ba:69:
          dc:d3:4c:85:39:09:a6:df:c4:1d:2d:80:2b:d8:f6:
          88:0a:c6:98:3f:85:34:19:c0:a5:fe:d9:f8:96:39:
          ec:cb:b7:c5:fa:84:e1:93:6d:82:7c:12:70:cf:67:
          5d:95:15:e9:1a:71:18:ad:f7:3f:09:1b:f5:0f:80:
          fb:9e:e9:96:54:91:59:39:6b:dd:5f:02:22:b9:c6:
          2a:60:e8:76:61:88:84:f1:e1:74:a1:17:12:66:98:
          6a:93
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints:
```

In the above Self-Signed System Certificate,

- **Issuer** represents the details of the CA issuing the Certificate. Here, the Organization itself is the CA (issuer), hence, the O and CN of both Issuer and Subject is same.

- **Validity** represents the valid period of this certificate.
- **Subject** represents the credentials of the Server / User requesting for certification. Here, OU=R&D i.e. for whom the certificate is signed.
- **Public Key** represents the public key of the certificate.

## CA Signed Certificate

Certificate Authority (CA) is a trusted organization which creates and sells TLS Certificates to websites. *CA Signed Certificates* are the TLS Certificates which are created by such trusted CAs, signed and sold to any applicant. These certificates contains a public key and the identity of the owner; and it is upto the CA to verify the owner's (applicant's) credentials. CAs issue a TLS Certificate to the organizations/websites after verifying their credentials. Generally, one TLS Certificate is issued for a particular server/website domain and it is valid for a certain period of time.

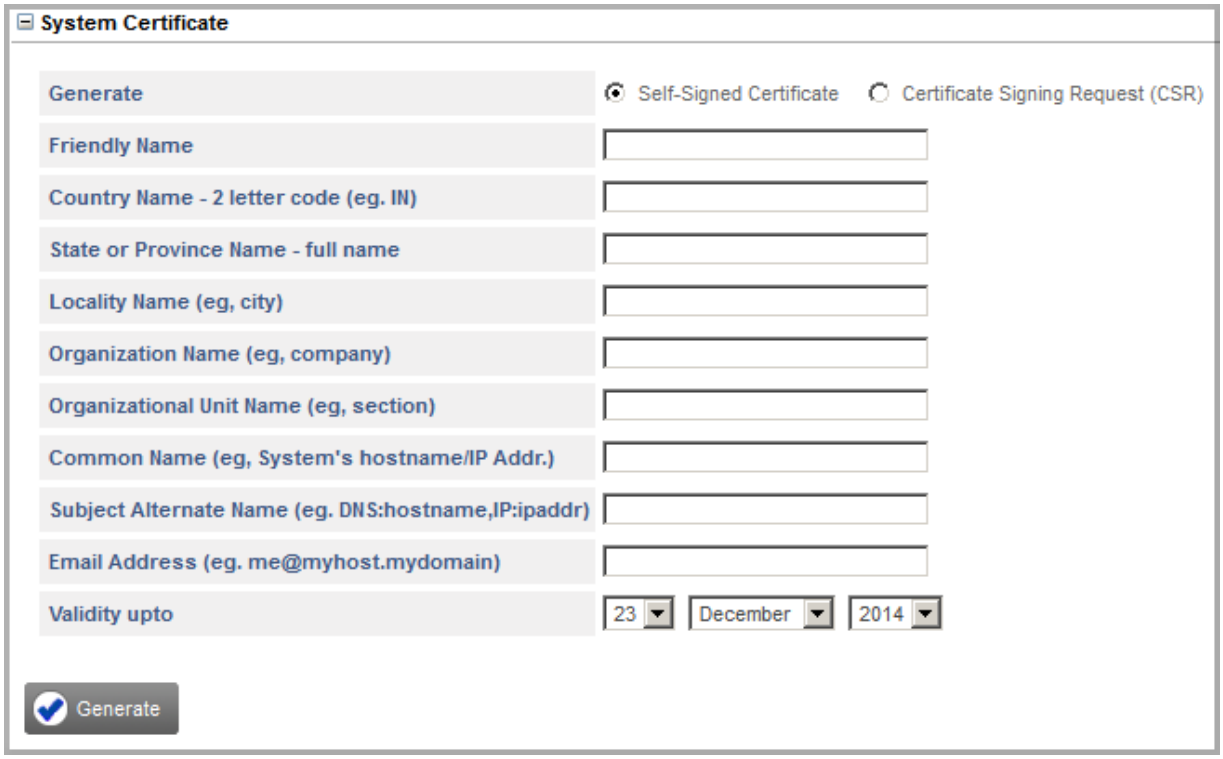
If you want to get a **CA Signed Certificate**, you need to do the following:

1. Generate and enroll the Certificate Signing Request (CSR).
2. Get the Certificate Signing Request (CSR) verified and signed by the Certified Authority (CA).

### Generating the Certificate Signing Request

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Certificate Manager** link.
- Click the **Generate** link.

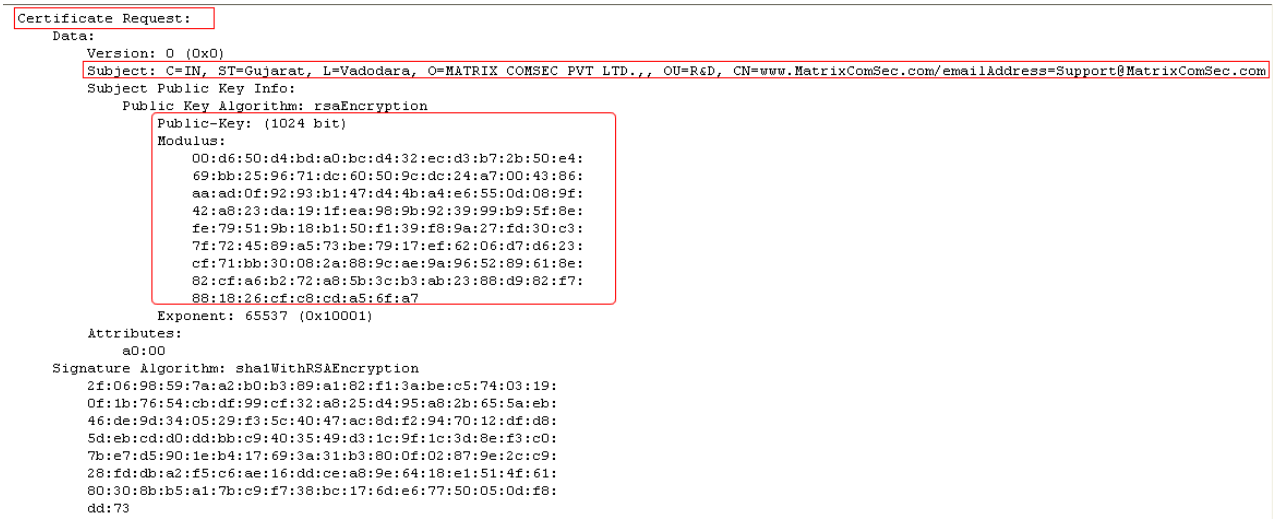
- Click **System Certificate** to expand and configure the following parameters.




  - In **Generate**, select the type of certificate you want to create. You must select **Certificate Signing Request (CSR)**.
  - In **Friendly Name**, enter the name you want to assign to the certificate.
  - In **Country Name - 2 letter code (eg. IN)**, enter the name (two letter code) of your country.
  - In **State or Province Name - full name**, enter the full name of your state or province.
  - In **Locality Name (eg. city)**, enter the name of your city.
  - In **Organization Name (eg. company)**, enter the name of your organization where SETU VG is installed.
  - In **Organizational Unit Name (eg. section)**, enter the name of the unit or section or domain of your organization, where your SETU VG is installed.
  - In **Common Name (eg. System's hostname/IP Addr.)**, enter your Server's (SETU VG) host name or IP Address. This Common Name serves as the distinguishing factor.
  - In **Subject Alternate Name (eg. DNS:hostname,IP:ipaddr)**, enter the name of the multiple domain separated by comma (if the same certificate is to be issued for multiple domain of the organization).
  - In **Email Address (eg. me@myhost.mydomain)**, enter your host's e-mail address.
- Click **Generate**, to generate this System Certificate.

- To send the certificate to the signing authority, click **Download CSR**. The Certificate and the Key downloads.

The Certificate Signing Request (CSR) to be sent to any trusted CA, appears as under:




As shown above, the credentials of the Organization (Server/User) requesting for Certification represents:

- C = Country
- ST = State
- L = Location
- O = Organization
- OU = Organization Unit
- CN = Common Name

- **Subject** represents the credentials of the Server / User requesting for certification. Here, OU= R&D.

- **Public Key** represents the public key of the certificate.

## Enrolling the Certificate Signing Request with CA

Enrollment is a process of obtaining a certificate from any trusted third party (CA). After you have generated the Certificate Signing Request (CSR), you must contact any authorized third party that issues TLS Certificates to companies or web owners, such as Thawte, VeriSign, etc. and enroll the Certificate Signing Request (CSR) with them. These third parties Certificate Authorities (CA) have their charges to sign and validate the Certificate Signing Request (CSR) for a year. After the Certificate Signing Request (CSR) has been validated and signed by the CA, it becomes the CA Signed Certificate.

## *Verification and Signing of the* Certificate Signing Request *by CA*

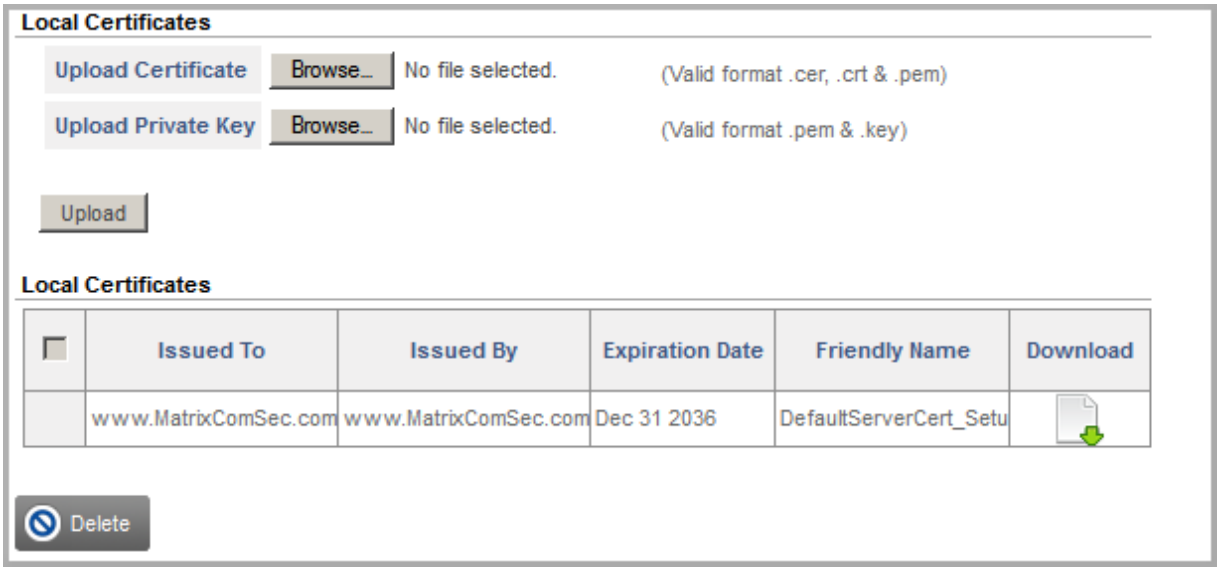
On receiving the Certificate Signing Request (CSR), the CA verifies the Server's / User's credentials. After successful verification, the CA signs and sends the signed certificate.

After you receive the signed certificate, you must:

- Log into Jeeves.

- Click the **Certificate Manager** link.

- Click the **Local Certificate** link.




- In **Upload Certificate** browse the location at which the certificate is saved. Along with the certificate you also need to upload the Private Key, in **Upload Private Key** browse the location at which the key is saved and click **Upload**.

  The System Certificate you uploaded appears in the **Local Certificates** table. Valid formats for certificate are .cer, .crt and .pem. Valid format for key are .pem and .key (Base64 encoded ASCII file).

  To delete a System Certificate, select the check box of the respective Certificate and click **Delete**.

  To download the System Certificate, click **Download**  .

# Call Detail Record

SETU VG enables you to generate reports of Call Detail Records of calls using various filters such as:

- The port from which the calls originate (Source Port)
- The port on which the calls terminate (Destination Port)
- Calls made on particular dates
- Calls made at a particular time
- Calls of a certain duration
- Calls of certain Called Party Numbers
- Calls of certain Calling Party Numbers
- Calls made with PIN Authentication
- Calls made without PIN Authentication

You can set the different filters as required and generate Call Detail Record Report. The reports can be used for analyzing the call records for different purposes like cost savings, productivity enhancement, security and privacy.

The system stores records of matured calls only and it generates reports only of filters that are set. For example, if you have not enabled the filter for *Calls Originated from SIP Trunks*, the system will not generate report for calls originated from SIP Trunks.

SETU VG supports up to 2000 call record entries and these entries are stored using the First In First Out (FIFO) method. Call records remain stored even when the system is set to default and/or the firmware version is changed.

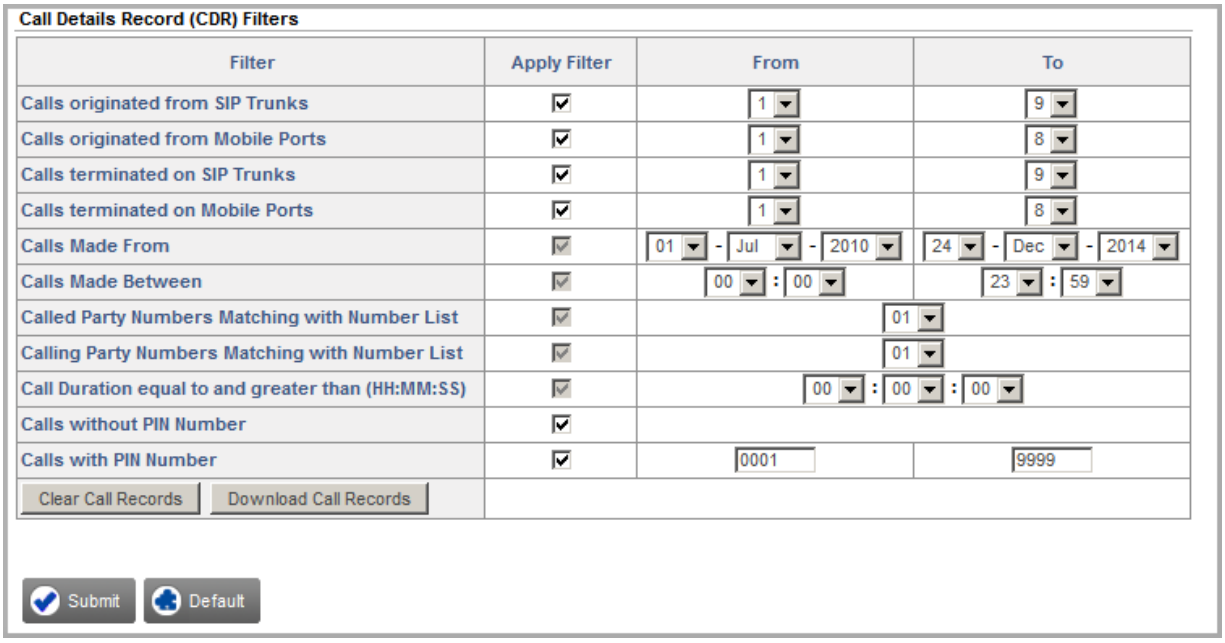
Call records can be cleared manually at any time.

## Configuring Call Detail Record Filters

- Log into Jeeves.
- Click the **Advanced Settings** link.
- Click the **Call Detail Record (CDR)** link.

## Setting Filters

- To set filters, click the **Filters** link under Call Detail Record.




By default, all the filters are enabled. You may disable the filter you do not want to use by clearing the related **Apply Filter** check box.

Some of these filters are enabled by default, you cannot disable them, but you can set them.

- Set the following filters as required:

*The filters you set are not applied on the downloaded report. The CSV and TXT files will contain all the records, without filters.*

- **Calls originated from SIP Trunks:** The system will generate report of calls that were received on the SIP Trunks of SETU VG for further routing. To generate report using this filter for a range of SIP Trunks, select the range of the SIP Trunks in the **From** and **To** fields.

  You can also generate report for a single trunk, by setting the same trunk number in the **From** and **To** fields.

- **Calls originated from Mobile Ports:** The system will generate report of calls that originated from the Mobile Ports. Set the range of the Mobile Ports in the **From** and **To** fields.

  You can generate report for a single Mobile Port by setting the same port number in the **From** and **To** fields.

- **Calls terminated on SIP Trunks:** The system will generate report of calls terminated on the SIP Trunks. To generate report using this filter for a range of SIP Trunks, set the range of the SIP Trunks in the **From** and **To** fields.

  To generate report for calls terminated on a single SIP Trunk, set the same trunk number in both fields.

- **Calls terminated on Mobile Ports:** The system will generate report of calls that terminated on the Mobile Ports. Set the range of ports in the **From** and **To** fields. Set the same port number in both fields, if you want to generate report for calls terminated on a particular Mobile Port.

- **Calls made from:** The system will generate report of calls made between particular dates. Enter the start date and end date in the corresponding **From** and **To** fields.

- **Calls made between:** The system will generate report of calls made between a particular time period. Enter the start time and end time in the corresponding **From** and **To** fields.

- **Called Party Number Matching with Number List:** Select the Number List you want to assign to this filter. Make sure that you also configure this Number List with the Called Party Numbers which you want the system to match. See "Number Lists" for instructions.

- **Calling Party Numbers Matching with Number List:** The system generates report for calls received from specific numbers.

  Select a Number List you want to assign to this filter. Make sure that you also configure this Number List with the Calling Party Numbers which you want the system to match. See "Number Lists" for instructions.

- **Call Duration equal to and greater than (HH: MM: SS):** The system generates report for calls of a specific time duration. Select the call duration in HH: MM: SS format.

- **Calls without PIN Number:** The system will generate report for calls without PIN Authentication.

- **Calls with PIN Number:** The system will generate a report for calls that were made using PIN Authentication. You can generate report of calls of specific PIN Numbers.

  Enter the range of PIN Numbers in the **From** and **To** fields. PIN Numbers can be in the range of 0000 to 9999. The system will generate Report of all calls having PIN Numbers within the range you have set and display them under the 'PIN Numbers' column of the report.

  If you want to generate report of a particular PIN Number, enter the same PIN Number in the **From** and **To** fields.

- Click **Submit** to save the settings.

## Clear Call Records

- You can clear the call detail records any time you want by clicking the **Clear Call Records** button**.**

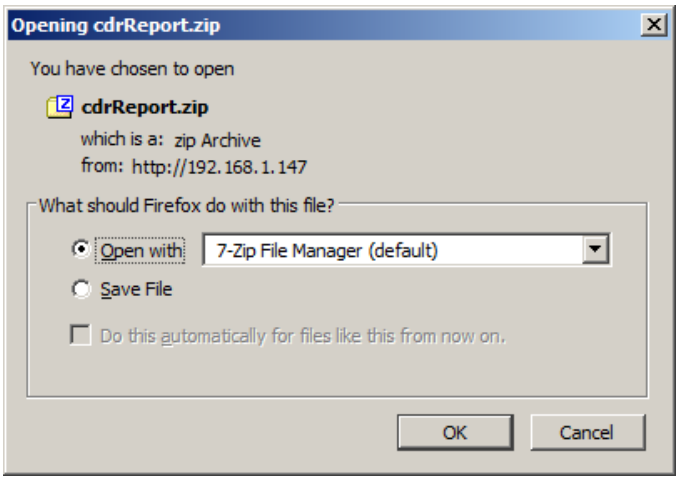
  When call records are cleared, the **From** field of the filter **Calls Made Between** will change to the date of clearing of the records.

## Download Call Records

- If you want to open/ save Call Detail Record Report on your computer, click the **Download Call Records** button.

*If you are using Mozilla Firefox (version 3.5 recommended), set the Downloads option of your browser as* ***Always ask me where to save the files****.*

- You will get a prompt with the option to open the **cdrReport.zip** file or save the file to a location. Save the file on the local disk.




- Open the cdrReport.zip file from the location you saved. The zip file contains the CDR report in Excel and Text format.

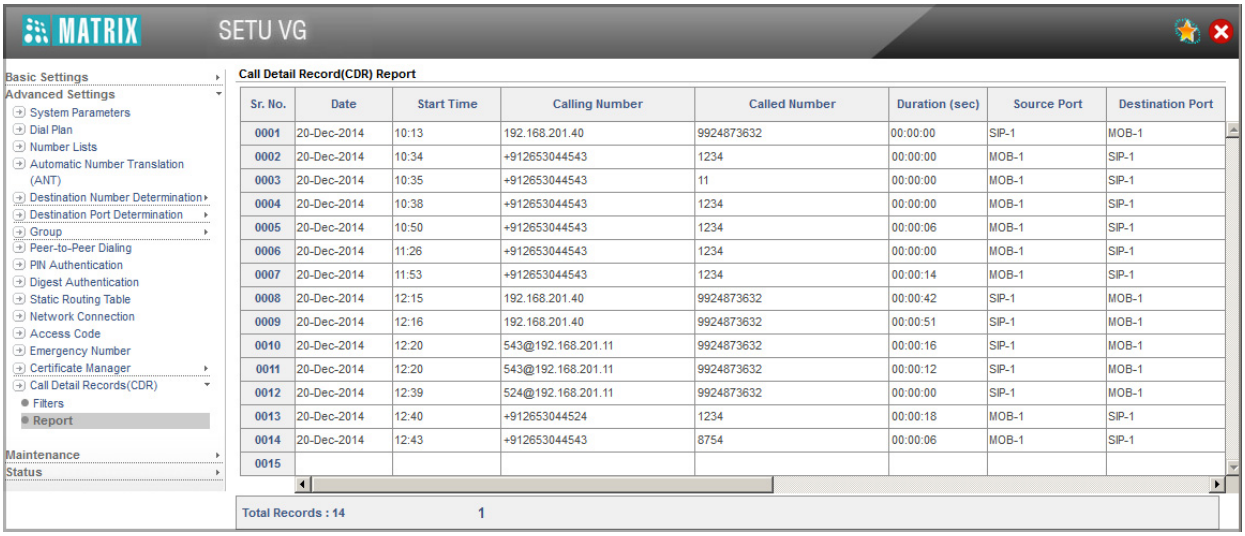
## Printing Call Detail Record Report

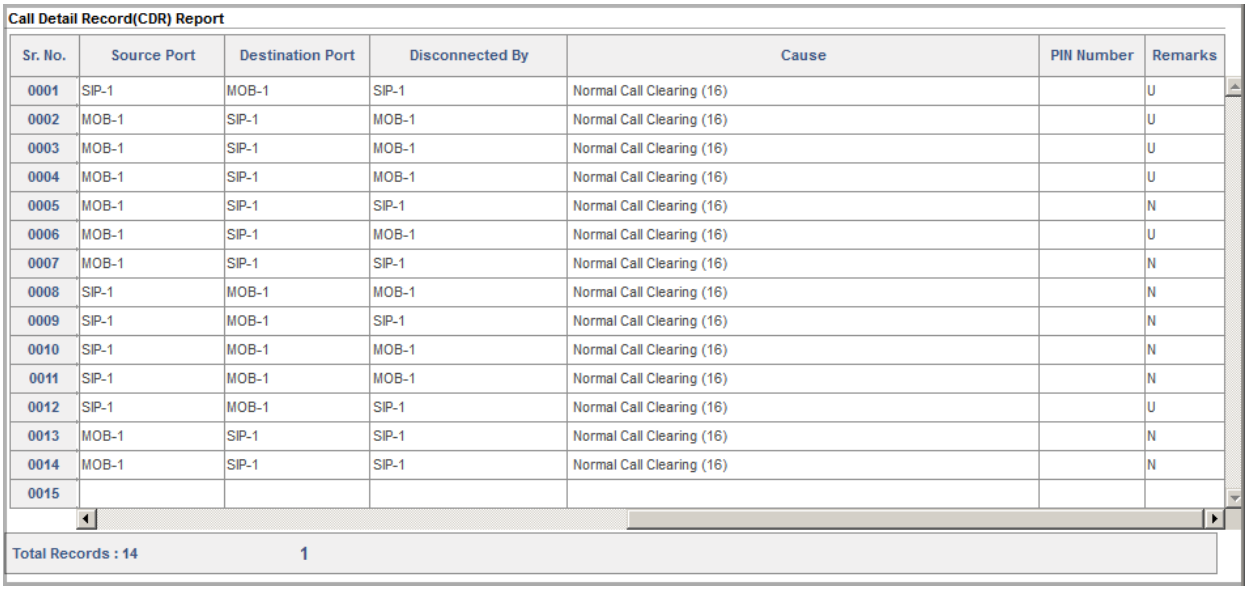
- You can also print the Call Detail Record Report, if required.
  - To print the CDR report in Excel format, open the file **CdrReport.csv**
  - To print the CDR report in text format, open the file **CdrReport.txt**
  - Print the file you opened. You may change the formatting of the text in the files before printing.

*The filters you set are not applied on the downloaded report. The CSV and TXT files will contain all the records, without filters.*

## Viewing Call Detail Report

- To view the report generated by the system for the filters you have set, click the **Report** link under Call Detail Record.




- Call Detail Record Report generated as per the filters you set will appear in the following columns:

  - **Date:** Calls made between particular dates.
  - **Start Time**: Calls made during a particular time period.
  - **Calling Number:** Calls received from specific numbers.
  - **Called Number:** Calls made to specific numbers.
  - **Duration (sec)**: Calls of a specific time duration.
  - **Source Port**: Calls originated from the SIP Trunks/Mobile Ports.
  - **Destination Port**: Calls terminated on the SIP Trunks/Mobile Ports.
  - **Disconnected By**: The port that disconnected the call.
  - **Cause**:The cause for disconnection.
  - **PIN Number**: Calls made using PIN Authentication, the PIN Number dialed by the caller.
  - **Remarks**: The type of call. A for Anonymous, U for Unanswered and N-Normal.

The total number of records is displayed below the table.

On each page, 15 records are displayed. Click the page number at the bottom of the report to view the next 15 records.

The Alert message **No Calls to Display** will appear, if there are no records to be displayed.

CHAPTER 6

# Features

SETU VG offers users the following features and facilities, which they can access by dialing Access Codes.

You can change the default access codes assigned to these features and facilities as per your requirement. See “Access Codes”.

## Making a New Call using Access Code

This feature enables callers to disconnect the current call and make a new call using SETU VG without getting disconnected from the system.

This feature is useful when you want to allow users to make multiple calls without getting disconnected each time their call ends.

This feature is applicable only on the Source Port and only when ***After Answering the Call and Collecting the Digits*** is selected as the Destination Number Determination Method.

To provide this feature to users,

- you must enable **Allow making New Call using Access code** on the SIP Trunks and Mobile Ports. For instructions, under *Basic Settings*, see “Mobile Port” and “SIP Trunk”.

*If you have enabled **Connect Source Port when number is outdialed** on the Mobile Ports or have enabled **Connect Source Port when 183(Session Progress) is received on SIP** on the SIP Trunk, you will not be able to provide this feature to users.*

To Make a New Call using Access Code,

- While you are in speech, dial **#91**.
- The current call will be disconnected.
- Dial the new number you want to call.
- To make another call, while in speech, dial **#91** again.

## Disconnecting a Call using Access Code

SETU VG enables users to disconnect a call using an access code. When the call disconnect access code is dialed, SETU VG releases the port engaged in the call.

To provide this feature to users,

- you must enable **Allow Call Disconnection using Access code** on the SIP Trunks and Mobile Ports. For instructions, under *Basic Settings*, see “Mobile Port” and “SIP Trunk”.

*If you have enabled **Connect Source Port when number is outdialed** on the Mobile Port or have enabled **Connect Source Port when 183(Session Progress) is received on SIP** on the SIP Trunk, you will not be able to provide this feature to users.*

To Disconnect a Call using Access Code, dial **#92**.

# IP Dialing

SETU VG supports direct dialing of IP Addresses from the source port. To provide IP Dialing facility to the users, you must configure a SIP Trunk or a SIP Group for IP Dialing.

When a number is dialed out from the source port, SETU VG routes the call to the desired destination as per the routing mechanism configured for that port. However, when an IP Address is dialed from the source port, SETU VG does not check the Destination Port Determination method you have configured for that port, instead it routes the dialed IP Address through the SIP Trunk or SIP Group you configured for IP Dialing.

When dialing an IP Address, users must press * key (star/asterisk) in place of . (dot/period) in the IP Address.

For example, to call the IP Address **192.167.100.1**, users must dial **192*167*100*1** or **192*167*100*001**

SETU VG interprets the * dialed as a '.' (dot/period).

To provide this feature to users,

- you need to select a **SIP Trunk** or a **SIP Group** through which the dialed IP Addresses are to be routed.

  If you want to use a SIP Trunk group for IP Dialing, you must configure a SIP Group first. This Group is common for all port types. See “Group” for instructions.

  When you assign a SIP Trunk, make sure it is enabled and has the necessary configuration done. See “SIP Trunk” under *Basic Settings* for instructions.

- assign the SIP Trunk you selected or the SIP Group you configured to **SIP Trunk for IP Dialing** in the System Parameters. See “System Parameters”under *Advanced Settings* for instructions. By default, SIP Group 1 is selected for IP Dialing in the System Parameters.

CHAPTER 7 **Maintenance**

# Firmware Upgrade

You can upgrade Firmware of SETU VG:

1. From a Provisioning Server
2. From a Personal Computer

## Firmware Upgrade from Provisioning Server

### Auto Firmware Upgrade

Using Auto-Firmware Upgrade, SETU VG can automatically upgrade its firmware by downloading the firmware files stored at a central location: HTTP Server or HTTPS Server or Provisioning Server.

This feature is useful for ITSPs that have Provisioning Servers to store the firmware files. ITSPs can update the firmware of SETU VG provided to their customers from a centralized location without physically visiting the customer premises.

*For the **Auto Firmware Upgrade File** contact Matrix Support Team.*

To perform Auto-Firmware Upgrade,

1. ITSPs must store the following Auto Firmware Upgrade files of SETU VG on the Provisioning Server.
   - matrix_firmware.html file
   - SETU VG_VwRx.y.z.Zip file

2. The following parameters must be configured in the SETU VG.
   - IP Address of the Provisioning Server.
   - Path of the Folder (containing the firmware files) on the Provisioning Server.
   - The protocol to be used: HTTP, HTTPS.

3. When SETU VG installed at a customer site gets connected to the ITSP network, it will automatically compare its current firmware with the firmware files stored on the Provisioning Server.

   The matrix_firmware.html file helps SETU VG decide which firmware it should upgrade to.

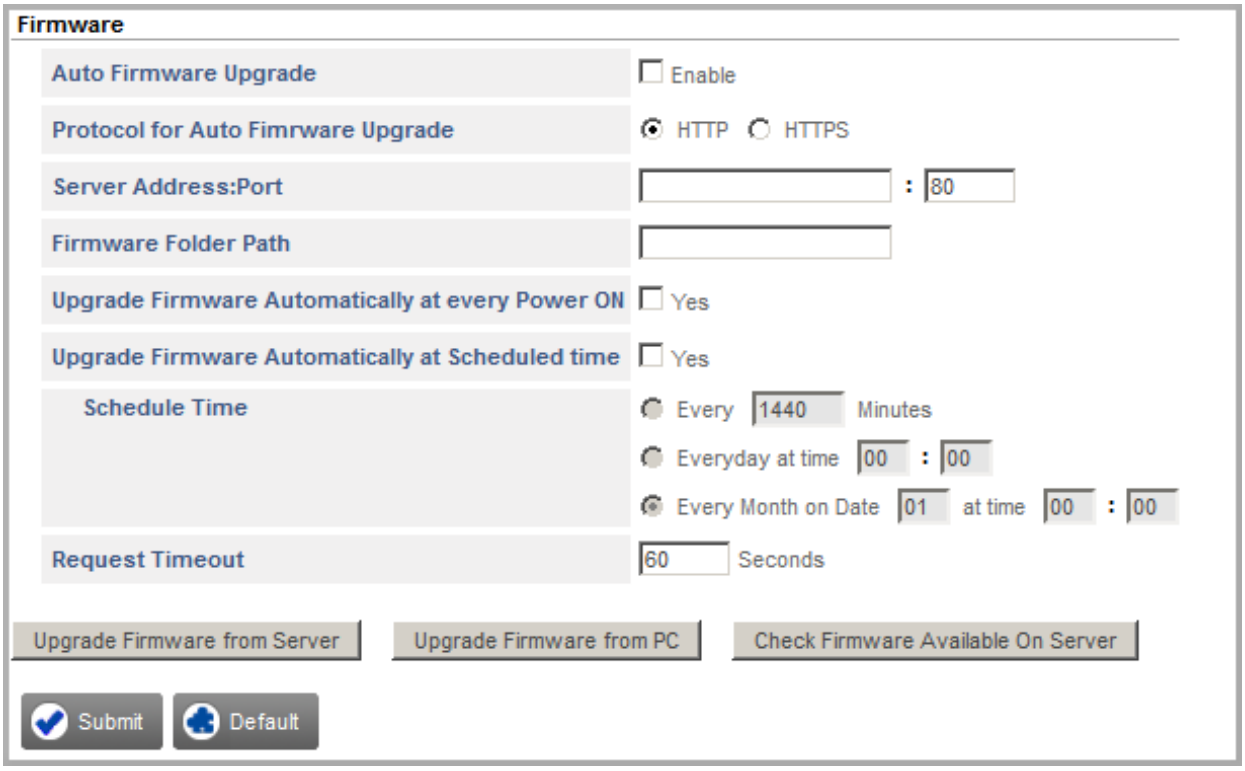
4. After SETU VG decides the Firmware Version/Revision to upgrade to, it will send the request for the firmware files to the Provisioning Server. Once the respective firmware files are received, SETU VG will upgrade its current firmware with the new firmware without the intervention or assistance of a technician.

The table below describes a few possible cases and the corresponding action taken by SETU VG.

| Version-Revision of your SETU VG | Version- Revision in the matrix_firmware.html file received from the Provisioning Server | Action Taken by SETU VG |
|---|---|---|
| V1R5.1.0 | V1R4.1.0 | SETU VG will downgrade its current firmware with V1R4.1.0 |
| | V1R5.1.0 | SETU VG will discard the upgrade process as same Version/Revision is found. |
| | V1R6.1.0 and V1R7.1.0 | SETU VG will upgrade its current firmware with V1R7.1.0 |
| | V1R4.1.0 and V1R5.1.1 | SETU VG will upgrade its current firmware with V1R5.1.1 |
| | V2R2.1.0_V2R1.1.0, V2R1.1.0 and V1R8.1.0 | Highest Version/Revision available is V2R2.1.0, however, V2R2.1.0 has a benchmark of V2R1.1.0. Therefore, SETU VG will first upgrade with V2R1.1.0 and then with V2R2.1.0. |

To configure Auto Firmware Upgrade parameters,

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **Firmware** link.




- Select the **Auto Firmware Upgrade** check box. Default: Disabled.

- Select the **Protocol for Auto Firmware Upgrade** to be used by the Provisioning Server to upgrade the firmware of SETU VG. SETU VG generates file transfer request to the server according to the protocol you select. You may select **HTTP** or **HTTPS**. Default: HTTP.

- **Server Address: Port:** Enter the IP Address/Domain and Port of the Provisioning Server on which the firmware files of SETU VG are stored.

  The Provisioning Server Address can also be obtained by SETU VG using DHCP (using Option 224). To fetch Provisioning Server Address using DHCP, keep the Server Address: Port field blank.

  Make sure that you also set the *Connection Type* on the "Network" page to *DHCP*.

  The default Port differs as per the protocol you select. For HTTP, the Default Port is 80 and for HTTPS, the Default Port is 443. You can also change the port as per your requirement. Valid Port Range: 80, 443, 1031 to 65534.

- **Firmware Folder Path:** Specify the path of the folder on the Provisioning Server where the firmware files are stored. Default: Blank.

- **Upgrade Firmware Automatically at Every Power ON:** Enable this check box, if you want SETU VG to check for updates in the firmware at each power ON.

- *At Power ON, if both Auto-Firmware upgrade and Auto-Configuration upgrade is enabled, Auto-Firmware upgrade has priority over Auto-Configuration upgrade.*

- *While upgrading itself, if SETU VG has to upgrade itself with the benchmark firmware first then it is recommended that you select* ***Upgrade Firmware Automatically at Every Power ON.***

- **Upgrade Firmware Automatically at Scheduled Time:** Enable this check box, if you want SETU VG to check for updates in the firmware at a scheduled time. You may select any one of the following schedule options:

  - **Every XX minutes:** The minutes after which SETU VG should check for firmware updates.

  - **Everyday at HH:MM:** The time in **Hours(00-23)** and **Minutes(00-59)** when SETU VG should check for firmware updates everyday.

  - **Every Month on DD at HH:MM:** The **Date (01-31)** and Time in **Hours (00-23)** and **Minutes(00-59)** when SETU VG should check for firmware updates every month.

*If SETU VG has to upgrade itself with the benchmark firmware and you have selected* ***Upgrade Firmware Automatically at Scheduled Time****, SETU VG will first upgrade itself with the benchmark firmware. At the subsequent scheduled time, it will upgrade itself with the final firmware.*

- **Request Timeout:** Request Timeout is used when SETU VG tries to connect to the Provisioning Server for TCP/TLS binding. This timer specifies for how long SETU VG should wait for successful TCP/TLS binding.

  Enter the required time in seconds. The range of Request Timeout is 01-99 seconds. Default: 60 seconds.

If SETU VG fails to connect to the Provisioning Server, it will make 10 attempts at a regular interval of 10 seconds between each attempt to establish the binding. Even then, if it is unable to establish the binding, it will abort the Auto upgrade process.

- Click **Submit** to save.
- To view the status of Auto-Firmware Upgrade from Jeeves, see "Firmware" under "Status" Chapter.

### Manual Firmware Upgrade

You can manually upgrade Firmware of SETU VG, whenever you want.

To manually upgrade firmware of SETU VG from server,

- Click the **Upgrade Firmware from Server** button on the Firmware page. SETU VG will automatically upgrade its firmware with the latest firmware available on the server.

## Checking Firmware Availability

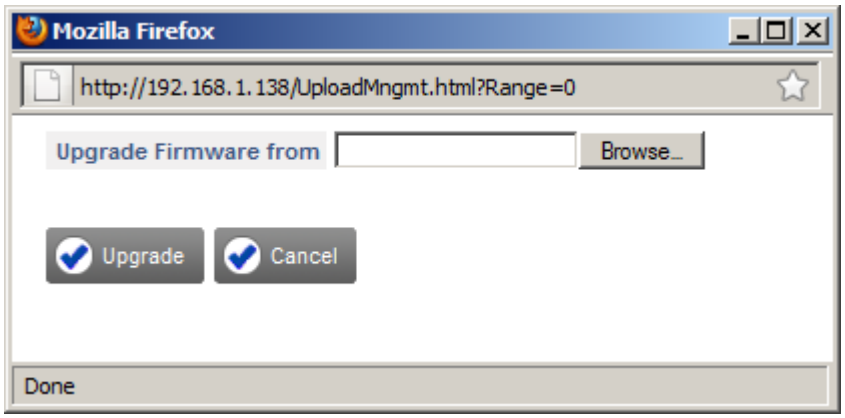
You can check the firmware files available on the server and then decide whether you want to upgrade SETU VG. Before upgrading Firmware from server, you can also choose the firmware with which you want to upgrade your SETU VG.

- To view the firmware files available on the Server, click the **Check Firmware Available on Server** button.
- A list of Firmware files available on the server appears in a new window.
- If you want to upgrade SETU VG with the desired Firmware, select the Firmware and click the **Submit** button.
- SETU VG will upgrade itself with the firmware you select.

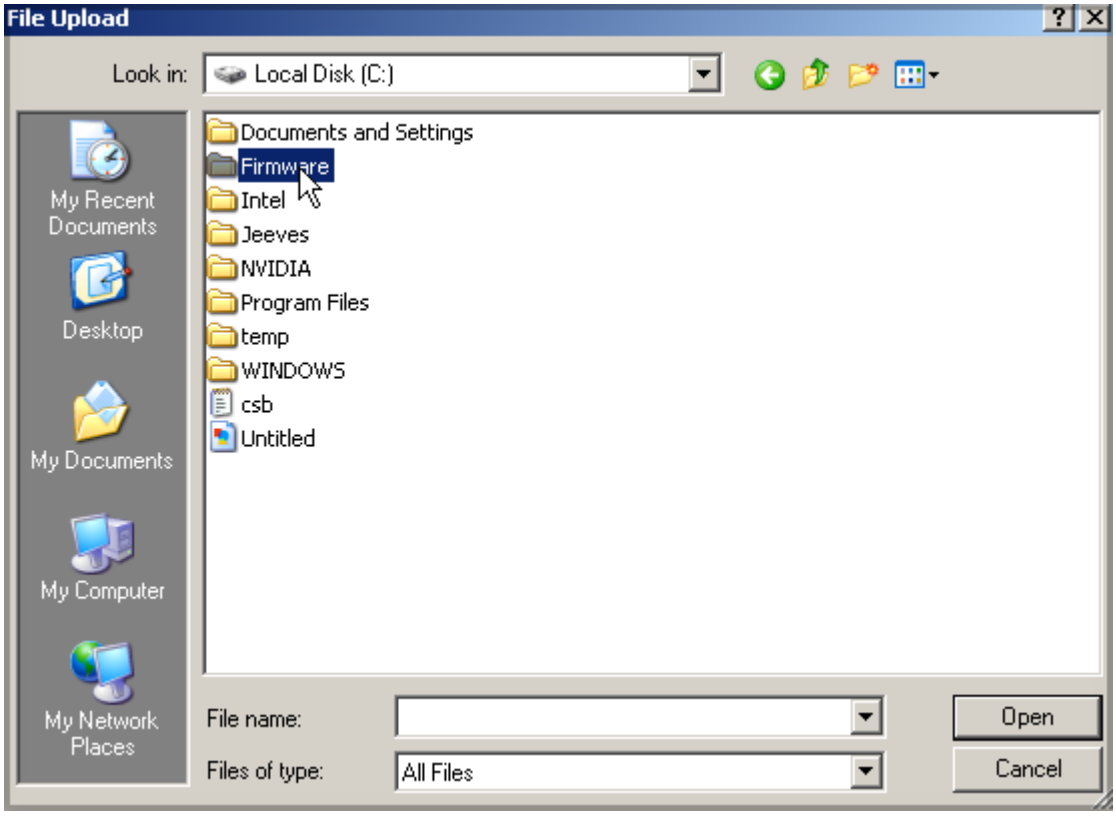
## Firmware Upgrade from Personal Computer

You can also upgrade firmware of SETU VG with the firmware files stored on your computer. To do so,

- Click the **Upgrade Firmware from PC** button. A new window - **Firmware Upgrade From** opens.
  - Click the **Browse** button to reach the location on the local disk on which the firmware files are stored.



- Select the required firmware files from the location on the local disk.




- The path to the file will appear in the **Firmware Upgrade From** box. Click the **Upgrade** button.

# Configuration Upgrade

You can upgrade Configuration of SETU VG:

1. From the Auto Configuration Server
2. From a Personal Computer

## Upgrading Configuration from the Auto Configuration Server

### Auto Configuration Upgrade

Using Auto-Configuration, SETU VG can automatically download the configuration files stored at a central location: Auto Configuration Server (ACS).

This feature is useful for ITSPs that have deployed a large number of SETU VG. ITSPs can store the configuration files of each SETU VG that they have provided to their customers on the Auto Configuration Server (ACS).

*For the **Auto Configuration File** contact Matrix Support Team.*

To perform Auto Configuration,

1. Make sure that the configuration file of SETU VG is stored on the Auto-Configuration Server (ACS).

2. To ensure security, ITSP can encrypt the configuration file stored on the ACS. If the ITSP has encrypted the configuration file, the password to decrypt the file must be provided to you.

3. The following parameters must be configured in the SETU VG.
   - IP Address of the Auto Configuration Server (ACS).
   - Path of the Folder (containing the configuration file) on the Auto Configuration Server.
   - Password to decrypt the configuration file (if encryption is used).
   - The protocol to be used: TFTP, HTTP, HTTPS.

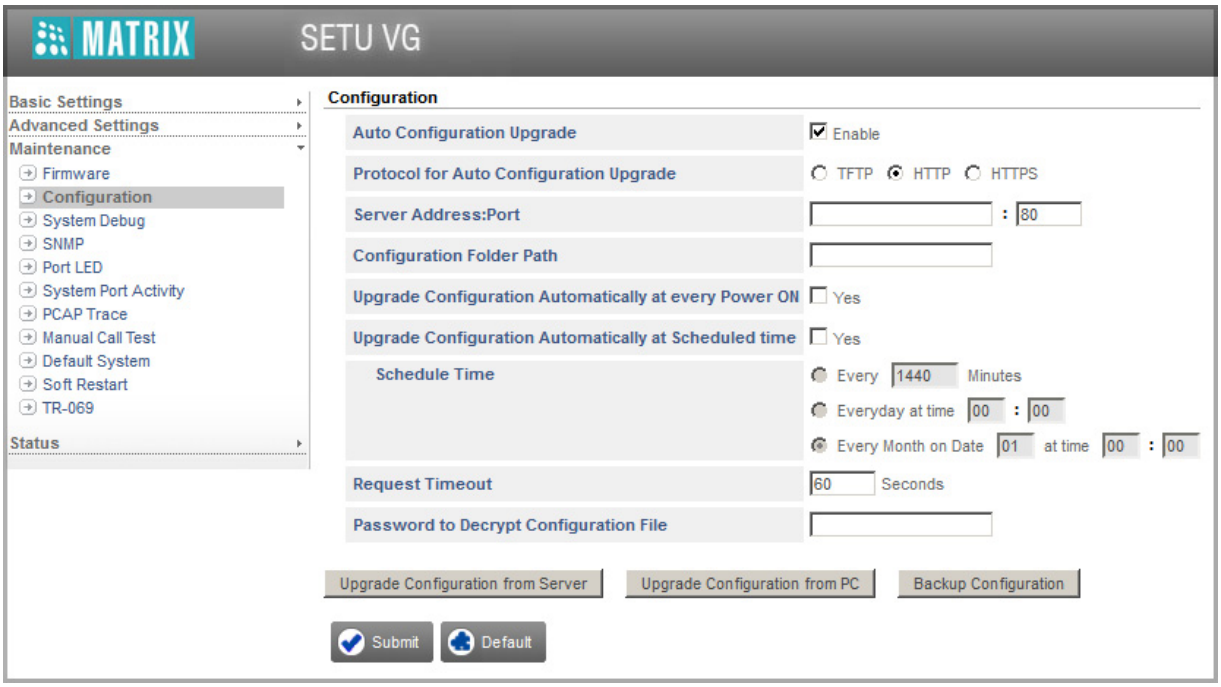
4. When SETU VG installed at a customer site connects to the ITSP network, it will automatically download its configuration file stored on the Auto-Configuration Server (ACS), without the intervention or assistance of a technician.

To configure Auto Configuration parameters,

- Log into Jeeves.

- Click the **Maintenance** link.

- Click the **Configuration** link.




- By default, **Auto Configuration Upgrade** check box is enabled. You may clear this check box, if required.

- **Protocol for Auto Configuration Upgrade:** Select the protocol used by the Auto Configuration Server to upgrade the configuration. SETU VG generates file transfer request to the Auto-Configuration Server according to the protocol you select. You may select **TFTP**, **HTTP** or **HTTPS**. Default: HTTP.

- **Server Address: Port:** Enter the IP Address/Domain and the Port of the Auto Configuration Server on which the configuration files of SETU VG are stored.

  The Auto Configuration Server Address can also be obtained by SETU VG using DHCP (using Option 224). To fetch Auto Configuration Server Address using DHCP, keep the Server Address: Port field blank.

  Make sure that you also set the *Connection Type* on the "Network" page to *DHCP*.

  The default Port differs as per the protocol you select. For TFTP, the Default Port is 69. For HTTP, the Default Port is 80. For HTTPS, the Default Port is 443. You can change the port as per your requirement. Valid Port Range: 69, 80, 443, 1031 to 65534.

- **Configuration Folder Path:** Specify the path of the folder on the Auto Configuration Server where the configuration file is stored. Default: Blank.

- **Upgrade Configuration Automatically at Every Power ON:** Enable this check box, if you want SETU VG to check for updates in the configuration file at each Power ON.

*At Power ON, if both Auto-Firmware upgrade and Auto-Configuration upgrade is enabled, Auto-Firmware upgrade has priority over Auto-Configuration upgrade.*

- **Upgrade Configuration Automatically at Scheduled Time:** Enable this check box, if you want SETU VG to check for updates in the configuration at a scheduled time. You may select any one of the following schedule options:

  - **Every XX minutes:** The minutes after which SETU VG should check for configuration updates.

  - **Everyday at HH:MM:** The time in **Hours(00-23)** and **Minutes(00-59)** when SETU VG should check for configuration updates everyday.

  - **Every Month on DD at HH:MM:** The **Date (01-31)** and Time in **Hours (00-23)** and **Minutes(00-59)** when SETU VG should check for configuration updates every month.

- **Request Timeout:** Request Timeout is the time for which SETU VG will try to connect to the Auto Configuration Server for TCP/TLS binding using HTTP or HTTPS. This timer specifies for how long SETU VG should wait for successful TCP/TLS binding.

  Enter the required time in seconds. The range of Request Timeout is 01-99 seconds. Default: 60 seconds.

  If SETU VG fails to connect to the Auto-Configuration Server, it will make 10 attempts at a regular interval of 10 seconds to establish the binding. Even then, if it is unable to establish the binding, it will stop retry and wait for next event of Auto-Configuration upgrade.

- **Password to Decrypt Configuration File**: Enter the Password as provided by your ITSP to decrypt the configuration file. During Auto-Configuration, if SETU VG receives an encrypted configuration file, it will decrypt the file using this password.

  The password may consist of 40 characters (maximum). Default: Blank.

*The password is case-sensitive, make sure you enter the password in the same format as given to you by your ITSP.*

- Click **Submit** to save.

- To view the status of Auto-Configuration upgrade from Jeeves, see “Configuration” under “Status” Chapter.

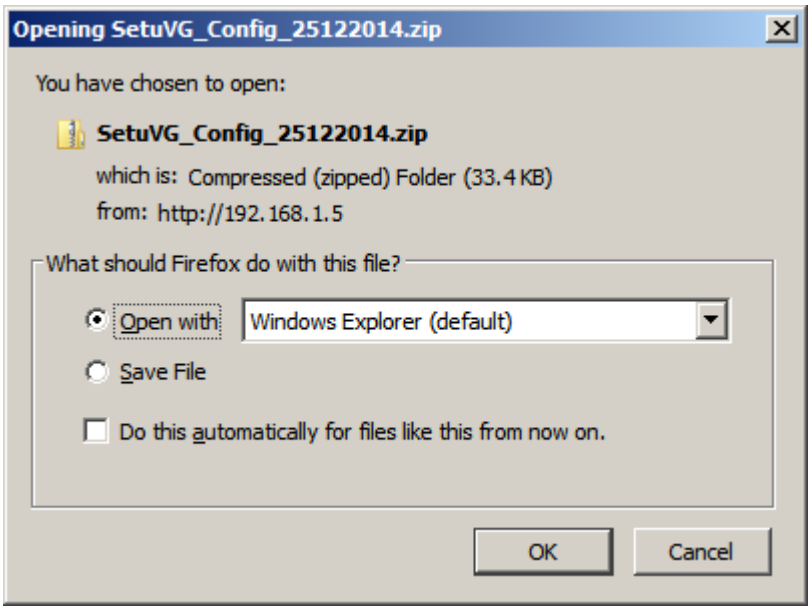
## Manual Configuration Upgrade

To manually upgrade configuration of SETU VG, click the **Upgrade Configuration from Server** button.

## Backup Configuration

- To save the existing configuration files as backup, click the **Backup Configuration** button.

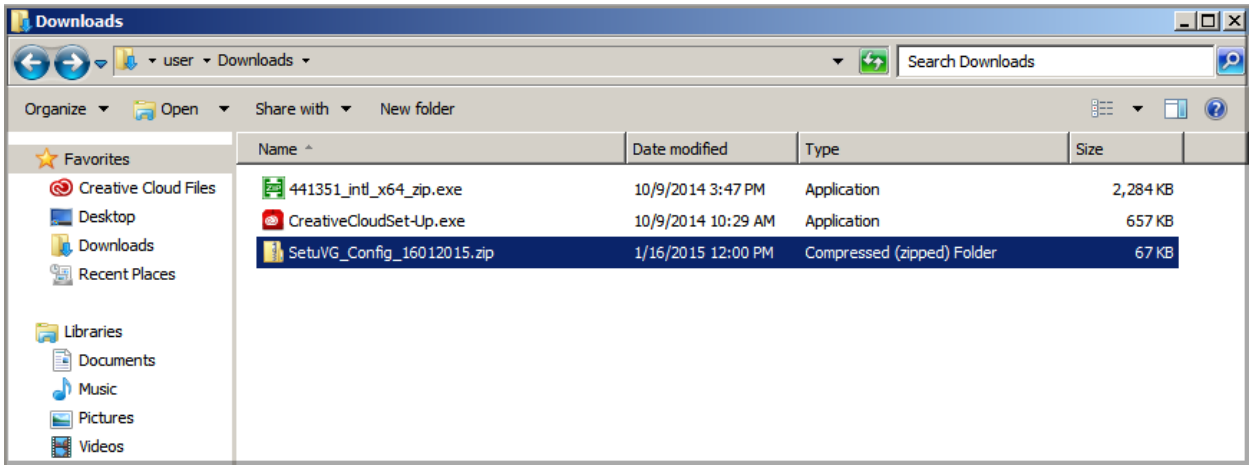
A **Opening config.zip** window will open.




- You can either open the **config.zip** file or save the file to a location.

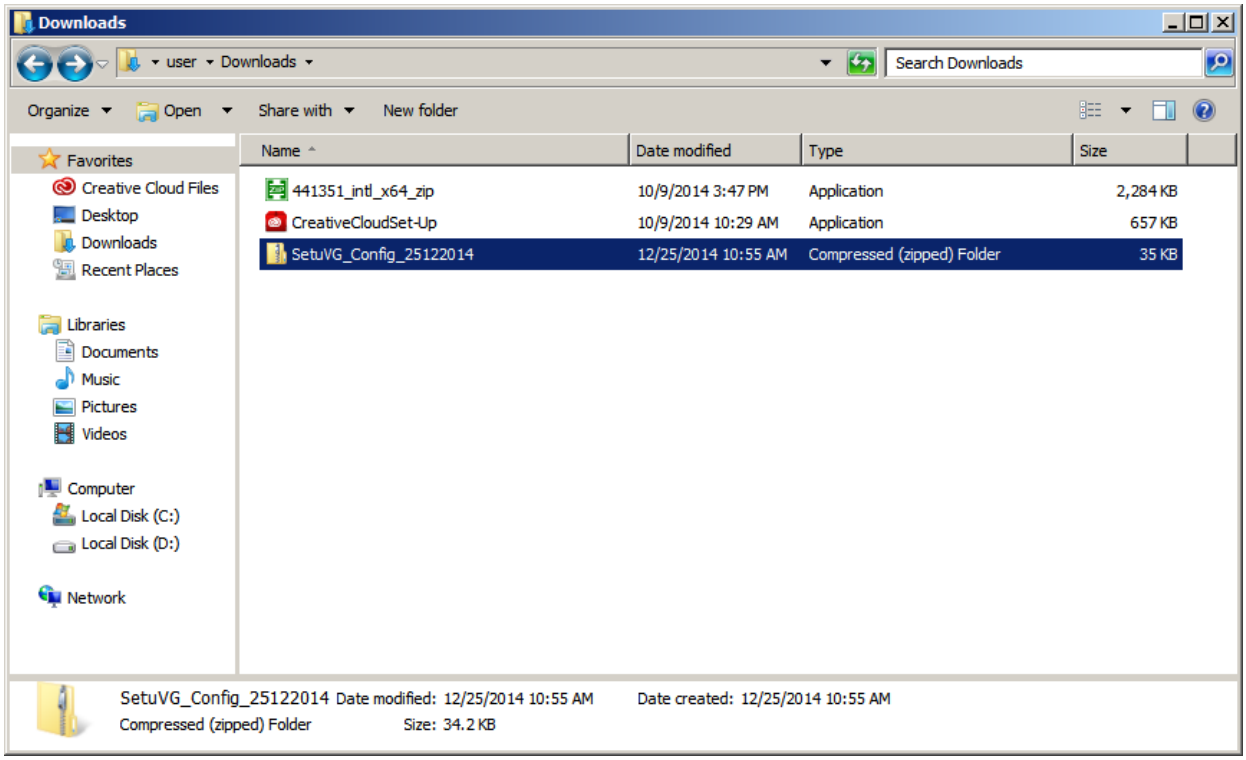
*If you are using Mozilla Firefox (version 3.5 recommended), before you save the configuration files, set the **Downloads** option of your browser as **Always ask me where to save the files**.*

- Save the file on the local disk.

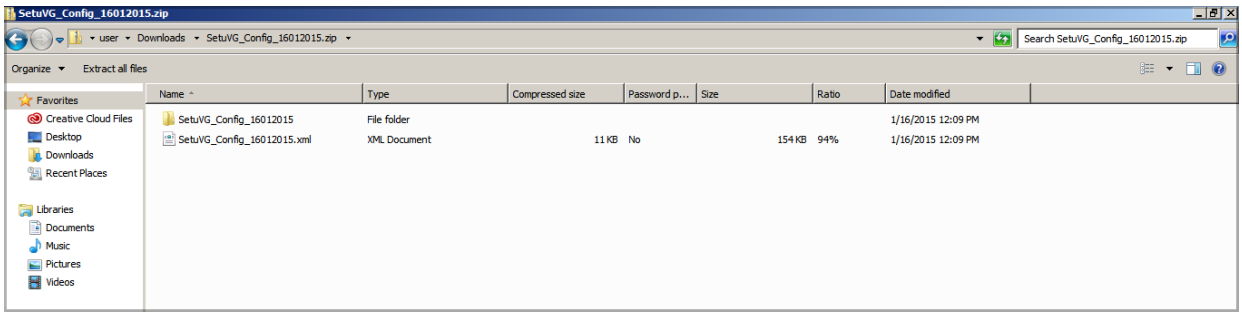



*Save the back up configuration files by tagging the file name with the Version-Revision of the Firmware and tag the name of the backup folder on your computer with the date. This will help you at the time of restoring the back up configuration files.*

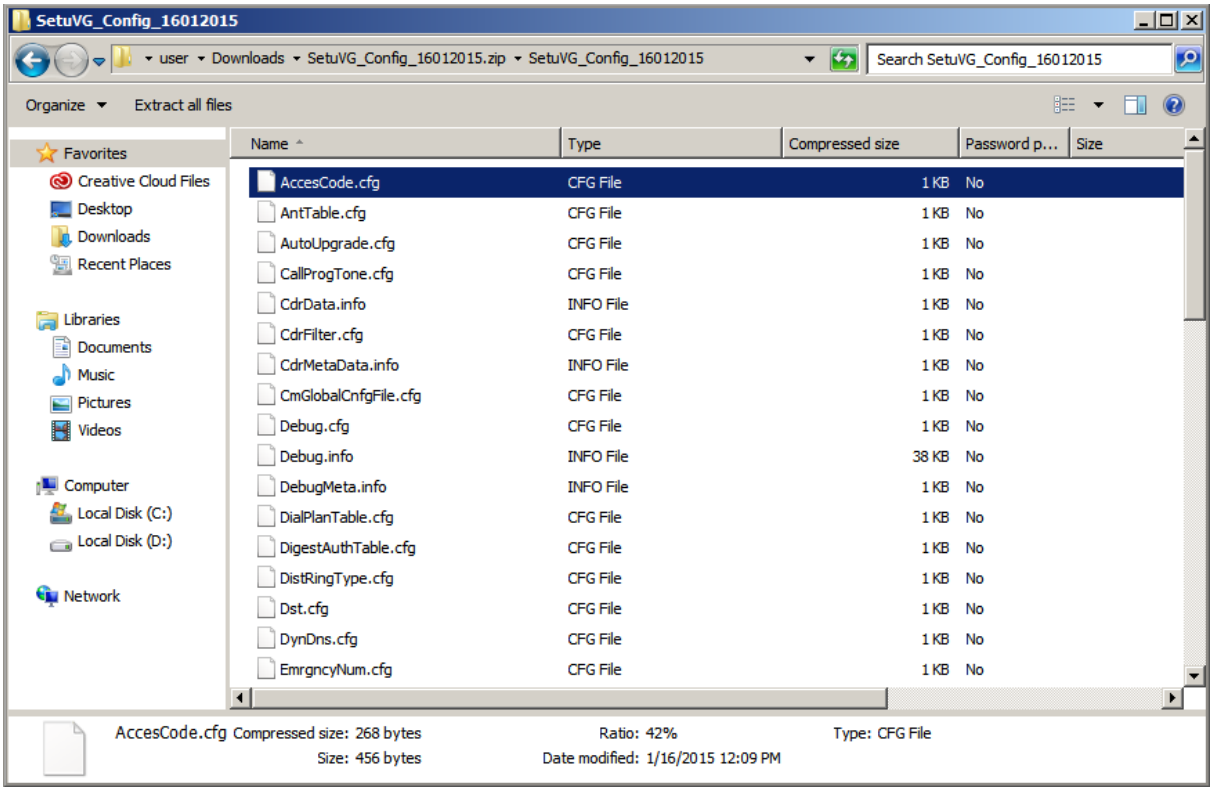
- Open the configuration file (.zip) from the location you saved.




- The zip file contains all the system configuration files in .cfg format and xml format. You cannot edit the configuration files in .cfg format, however you can edit the configuration files in xml format and then upgrade the system with it.



- Open the SETU VG_Config_16012015 folder to view the configuration files.

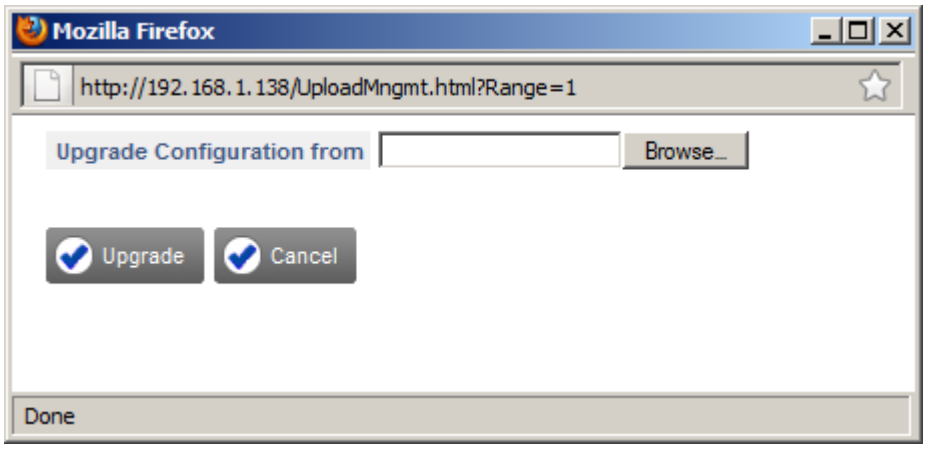



- Keep the Configuration folder as a backup. In case there is a problem with the system configuration files these backup files can be restored back in the system.

## Upgrading Configuration from a Personal Computer

You can upgrade configuration of SETU VG with the configuration files—.cfg format or xml format— stored on your computer. To do so,

- Click the **Upgrade Configuration from PC** button. A new window - **Upgrade Configuration From** opens.




- Click the **Browse** button to reach the location on the local disk on which the configuration file is stored.
- Select the required configuration files from the location on the local disk.

- The path to the file will appear in the **Configuration Upgrade From** box.
- Click the **Upgrade** button.

*At a time, you can upgrade configuration either manually or automatically from Auto Configuration Server or manually from a Personal Computer.*

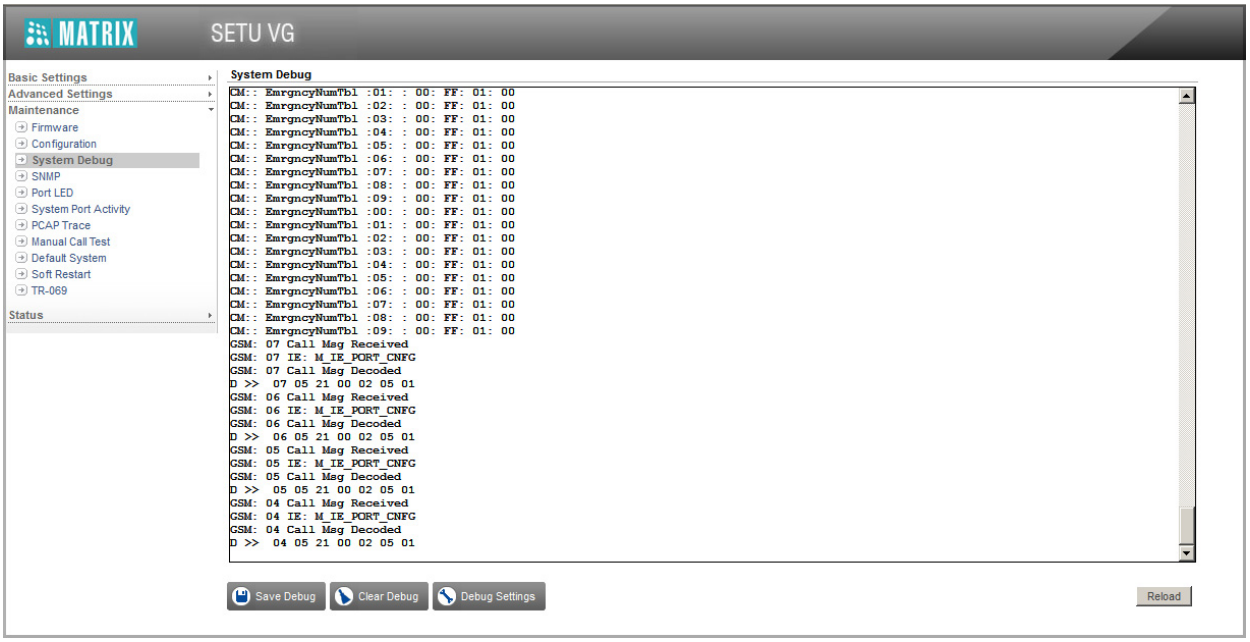
# System Debug

Debugging is a method used for recording actions and events of the system. Debugs are the primary record keepers of the system and network activity. Debugging has several benefits which include troubleshooting, security and system administration.

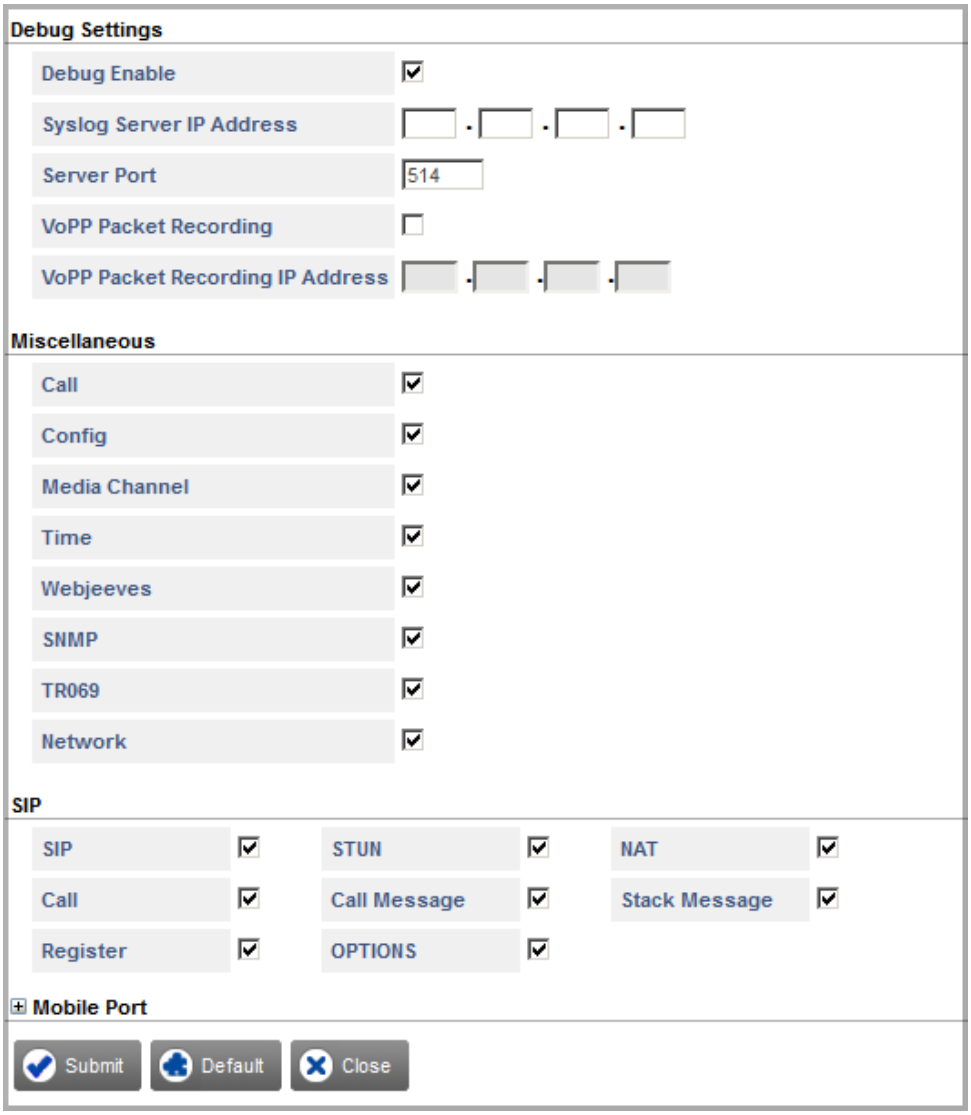
SETU VG supports Syslog Client for sending debug messages to the remote syslog server on the IP network.

## Configuring System Debug

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **System Debug** link.



- To configure the debug settings, click the **Debug Settings** button.




- Select the **Debug Enable** check box to enable system debug. Default: Disabled.
- In the **Syslog Server IP Address**, enter the remote Syslog Server IP Address. Default: Blank.
- In the Syslog **Server Port**, enter the port number. The range of the server port is 514, 1024 to 65535. Default: 514.
- If you have enabled **VoPP Packet Recording**, configure the **VoPP Packet Recording IP Address**.
- For **System Debug**, select the desired debug level:
  - Call
  - Config
  - Media Channel
  - Time
  - Webjeeves
  - SNMP
  - TR069
  - Network

Default: All debug levels, are enabled. To disable a debug level, clear the respective check box.

- For **SIP Port**, select the desired debug level:
  - SIP
  - STUN
  - NAT
  - Call
  - Call Message
  - Stack Message
  - Register
  - OPTIONS

  Default: all are enabled.

- To debug the **Mobile Port 1** to **8**, keep the respective check boxes enabled.

- Click **Submit** to save changes.

*If debug is enabled, atleast one debug level should be selected. If no debug level is selected, SETU VG will prompt you to select a debug level.*

- The window closes, and you return to the System Debug page.

- All the Debug events appear on the screen.

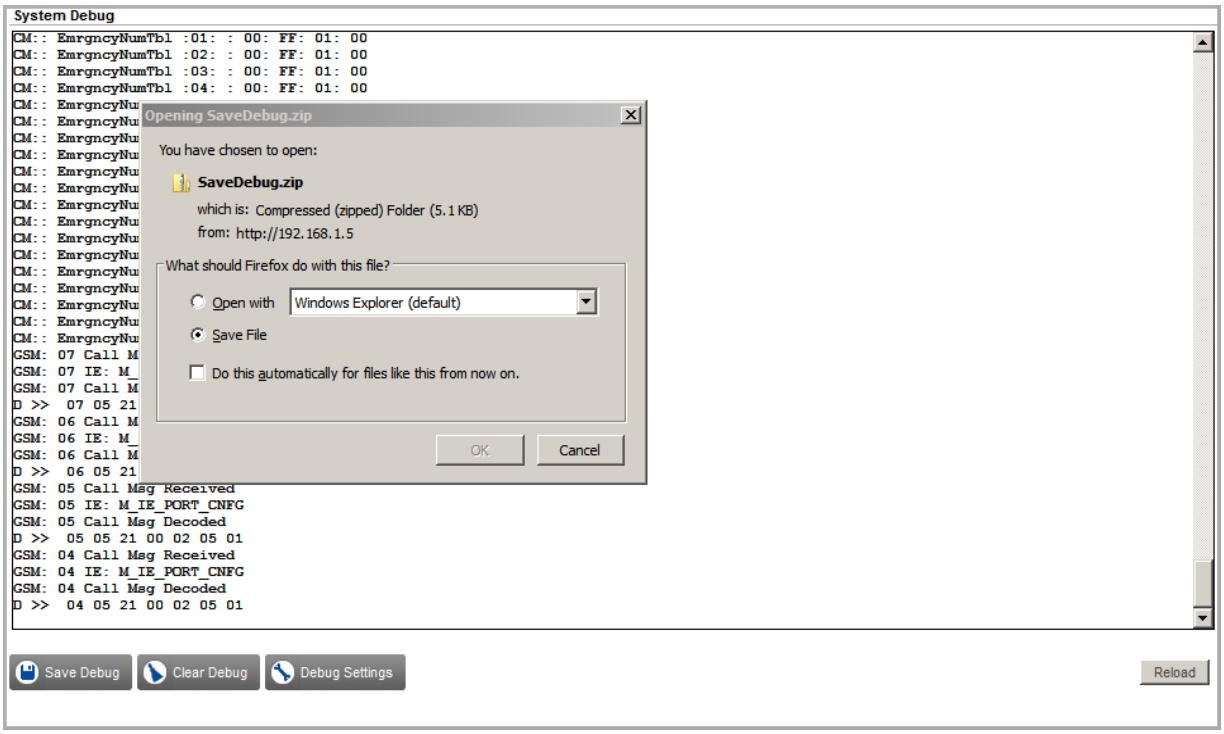
*Events will be displayed only if you enable Debug.*

- Whenever you want the system to fetch an updated debug report, click the **Reload** button on the System Debug page.

- If you want to delete all the events, click the **Clear Debug** button.

- You may also save the Debug file, if required. Click the **Save Debug** button.

- You will get a prompt with the option to open the **debug.zip** file or save the file to a location.




  - Save the file on the local disk.
  - Open the **debug.zip** file from the location you saved. The zip file contains the system debug file **debug.txt**.

- Once you have enabled Debug and set the filters, you can view the debug event log at any time on the **System Debug** page.
- You may log out of Jeeves.

# Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is an application-layer protocol used for exchanging management information between network devices. Using SNMP, you can manage and monitor network elements, audit network usage, detect network faults or inappropriate network access.

The SNMP architecture consists of:

- An **SNMP Agent** is a program that is bundled within the managed device. SNMP agent allows a managed device to collect the Management Information Base from the device and make it available to the SNMP Manager on request. It receives SNMP requests and generates SNMP responses or notifications (traps/informs). The SNMP Agents are SNMP Servers.

- **SNMP Manager**, usually the Network Management Station. The manager communicates with multiple SNMP Agents implemented in the network. It generates SNMP requests and receives SNMP responses and notifications (traps/informs). The SNMP Manager is an SNMP Client.

- **Managed device** or the network element is a part of the network that requires some form of monitoring and management. For example, switch, routers, servers.

- **Management Information Base** is the commonly shared database between the Agent and the Manager.

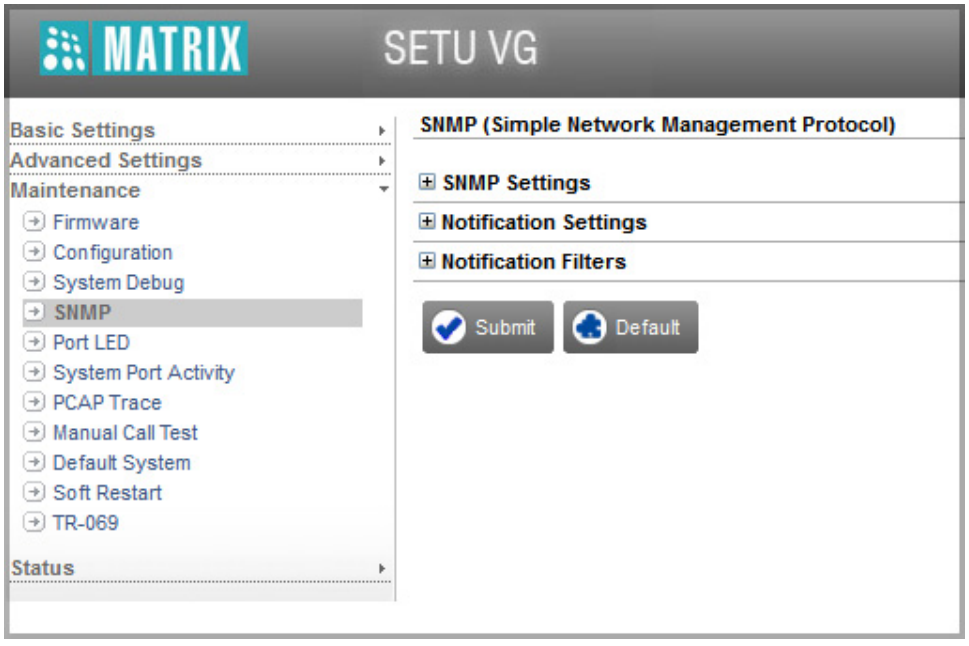
SNMP uses UDP (User Datagram Protocol) as the transport protocol for passing information between Managers and Agents. The Agent listens on UDP port 161 for requests from Manager and the Manager listens on UDP port 162 for notification from Agent.

To configure SNMP parameters,

- Log into Jeeves.

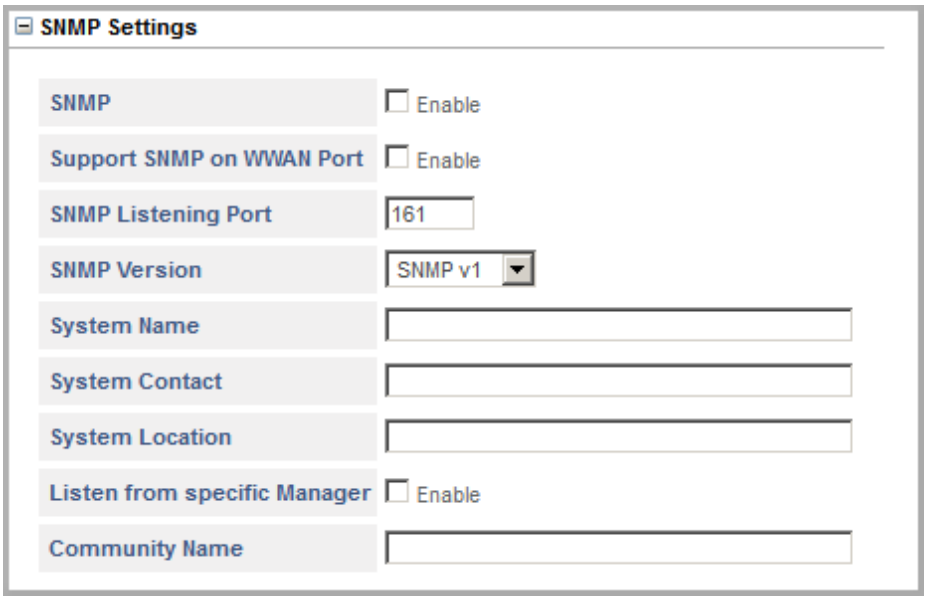
- Click the **Maintenance** link.

- Click the **SNMP** link.



## SNMP Settings

- Click **SNMP Settings** to expand.




- Select the **Enable SNMP?** check box. Default: Disabled.
- Configure the **SNMP Listening Port**. Valid Range:161, 1031-65535. Default: 161.
- Select the **SNMP Version** as supported by your SNMP Manager. You can select from:
  - SNMPv1
  - SNMPv2c
  - SNMPv3

  For enhanced security, you must select SNMPv3.
- Configure the **System Name**. When there are multiple devices connected in the same network, the name configured helps to identify the SNMP Agent within the network. The System Name can be a maximum of 40 characters. Default: Blank.
- Configure the **System Contact**. It is the name and number of the person to be contacted, in case of notification. The System Contact can be of a maximum of 40 characters. Default: Blank.
- Configure the **System Location**. This is the physical location of SETU VG. This information is helpful to the administrator. The System Location may consist of a maximum of 40 characters. Default: Blank.
- Select the **Listen from Specific Manager** check box, if you want the system to listen to the incoming SNMP messages from a specific manager. Default: Disabled.
  - If you have enabled **Listen from Specific Manager** check box, you must configure the specific **Manager's Address.**

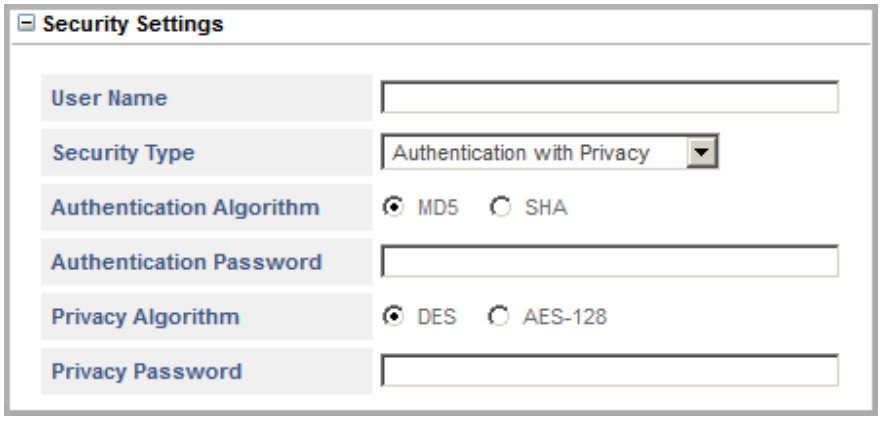
    The Manager's Address can be a Domain Name or an IP Address. It can be a maximum of 64 characters. Default: Blank.
- If SNMP version is set as **SNMPv1** or **SNMPv2c,** configure **Community Name**.

Community Name identifies the SNMP community in which the sender and recipient of the message are located. It enables communication between SETU VG and the Manager. The Community Name can be a maximum of 40 characters. Default: Blank.

- If SNMP version is set as **SNMPv3,** the **System's Engine ID** is displayed in this field. This is a unique identification of the system. It is a hexadecimal field with length of 22 characters. The ID consists of:
  - Enterprise Number (800086df03 which is fixed)
  - MAC Address of the system (MAC address of Network port)

## Security Settings

- If SNMP version is set as **SNMPv3**, click **Security Settings** to expand and configure the following.




- Enter the **User Name**. The User Name can be a maximum of 40 characters. User Name will be used for authentication and privacy in SNMPv3.

- Select the appropriate **Security Type** as per your requirement. Security Type defines the level of security.

  - When Authentication and Privacy are not required, select **No Authentication-No Privacy**

  - When only Authentication is required, select **Authentication without Privacy**. Incoming SNMP Messages will require authentication.

    If you select this method, select the **Authentication Algorithm** as **MD5** or **SHA**. Default: MD5.

    In the **Authentication Password**, enter a password of your choice as Authentication Password for the User Name you have assigned.The Authentication Password must be a minimum of 8 characters and may have upto 24 characters. Default: Blank.

  - When both Authentication and Privacy are required, select **Authentication with Privacy**. Incoming SNMP Message will require authentication and these messages will be encrypted, which will be decrypted at the receivers end only.

    If you select this method,

    - Select the **Authentication Algorithm** as **MD5** or **SHA**. Default: MD5.

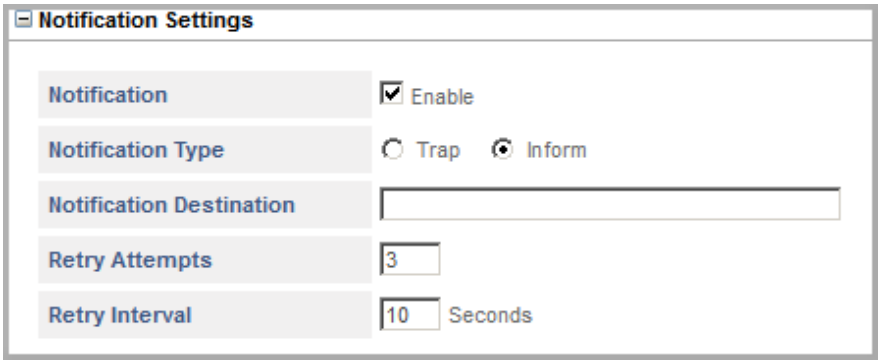
- Enter **Authentication Password** for the User Name you have assigned. The Authentication Password must be a minimum of 8 characters and may have upto 24 characters. Default: Blank.

- Select the **Privacy Algorithm** as **DES** or **AES-128**. Default: DES.

- Enter the **Privacy Password** of your choice.The Privacy Password must be a minimum of 8 characters and may have upto 24 characters. Default: Blank.

## Notification Settings

- Click **Notification Settings** to expand.




If SNMP version is set as **SNMPv1**, configure the following parameters.

- If you want SETU VG to generate Trap message for an error, select the **Enable Trap?** check box. Default: Disabled.

  - You must configure the **Notification Destination**, if you have enabled **Trap**. SETU VG will send the notification (error message) to the destination configured.

    The Notification Destination can be an IP Address or a Domain Name and the Port of the Manager or of any other device where you want to receive the trap messages. IP Address/Domain Name can be a maximum of 64 characters. Valid range of the port is 0-65535. Default port is 162.

- Click **Submit** button to save the settings.

If SNMP version is set as **SNMPv2c or SNMPv3**, configure the following parameters.

- Select **Notification Enable** check box, if you want SETU VG to generate Trap or Inform message for an error.

- Select the **Notification Type**. You may select **Trap** or **Inform**.

  If you want the system to send notification message without acknowledgement, select **Trap**.

  If you want the system to send notification message with acknowledgement, select **Inform**.

  - If you select **Inform** as the *Notification Type*, you must configure Retry Attempts and Retry Interval.

If acknowledgement is not received from the Manager for the notification sent, the system will keep retransmitting the message for the number of attempts you have configured as the **Retry Attempts**. Default: 3.

The system will retransmit the messages at regular time intervals you have configured as **Retry Interval**. Default: 10 seconds.

- Configure the **Notification Destination**. SETU VG will send the notification (error message) to the destination configured.

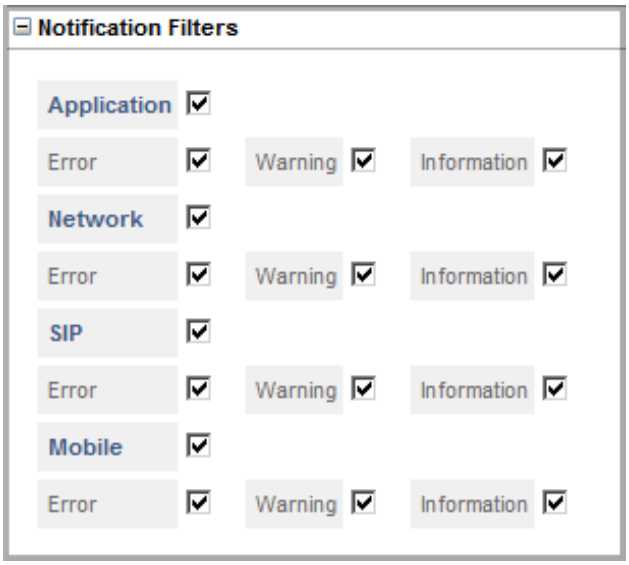
  The Notification Destination can be an IP Address or a Domain Name and the Port of the Manager or of any other device where you want to receive the trap messages. IP Address/Domain Name can be a maximum of 64 characters. Valid range of the port is 0-65535. Default port is 162.

- Click **Submit** button to save the settings.

## Notification Filters

By default, you get error notifications, information and warnings for events related to the Application, Network and all Port Types. See table at the end of this topic for the event list. You can choose the type of notification you want by setting the notification filters.

To set filters, click **Notification Filters** link to expand.




To disable any filter, clear the respective check box.

*You must upload MIB file shipped with the documents of SETU VG in your SNMP Manager to get the status and notifications for SNMP.*

The List of Events for which you will receive notification is presented in the following table.

## Application

| Error | Warning | Information |
|---|---|---|
| | System Reboot/Gateway Restarted | System boot/initialized |
| | Web Login - Authentication failure | Web JEEVES Login/Logout status |
| | CDR Buffer full | Password change |
| | | System Config set to default |
| | | Page config set to default |

## Network

| Error | Warning | Information |
|---|---|---|
| | LAN Link Down | LAN Link Up |
| | WAN Link Down | WAN Link UP |
| | | IP Address of the Gateway |
| | | New IP Address of Gateway |
| | | MAC Address of Gateway |
| | | DNS address of Gateway |
| | | DynDNS status |

## SIP

| Error | Warning | Information |
|---|---|---|
| SIP Stack construction error | DHCP Error | SIP Trunk registering to registrar/ OB Proxy |
| VOPP Download failed | PPPoE Error | SIP Trunk gets active. |
| SIP Trunk Registration failed | STUN Error | Network Connection Disable |
| | SIP Trunk disabled | |

## Mobile

| Error | Warning | Information |
|---|---|---|
| | SIM PUK Required | SIM Absent |
| | SIM PIN Required | SIM Present |
| | SIM PIN Wrong | Network Absent |
| | Call Budget consumed | Network Present |

| Error | Warning | Information |
|---|---|---|
| | | Current balance in the SIM/Mobile Port |

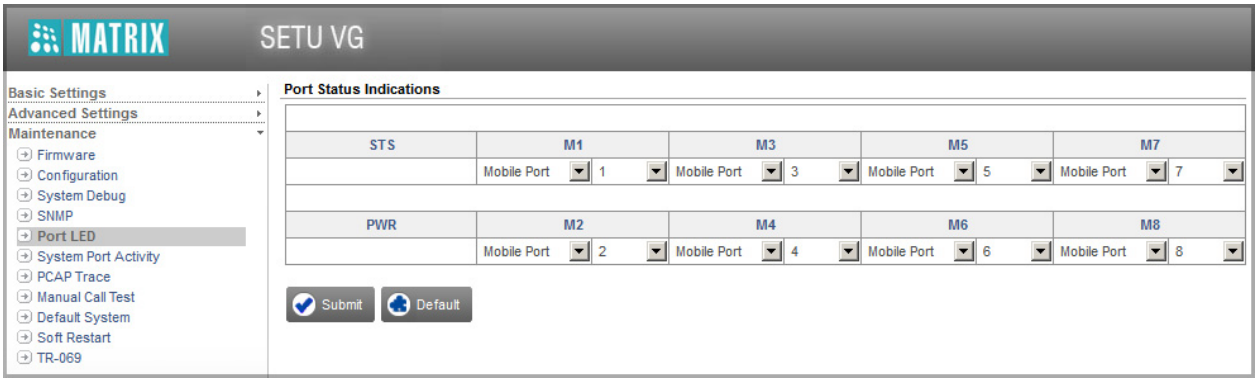
# Port LED

SETU VG8 has eight LEDs for port status indication. SETU VG4 has four LEDs for port status indication. By default, all port LEDs show the status of the Mobile Ports. It is possible to reassign these LEDs to SIP Trunk, if required. These LEDs indicate various events occurring on the ports and error conditions.

By default all Port LEDs are assigned to the Mobile Ports. You may re-assign these LEDs to the SIP Trunks.

To do so in the SETU VG8,

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **Port LED** link.



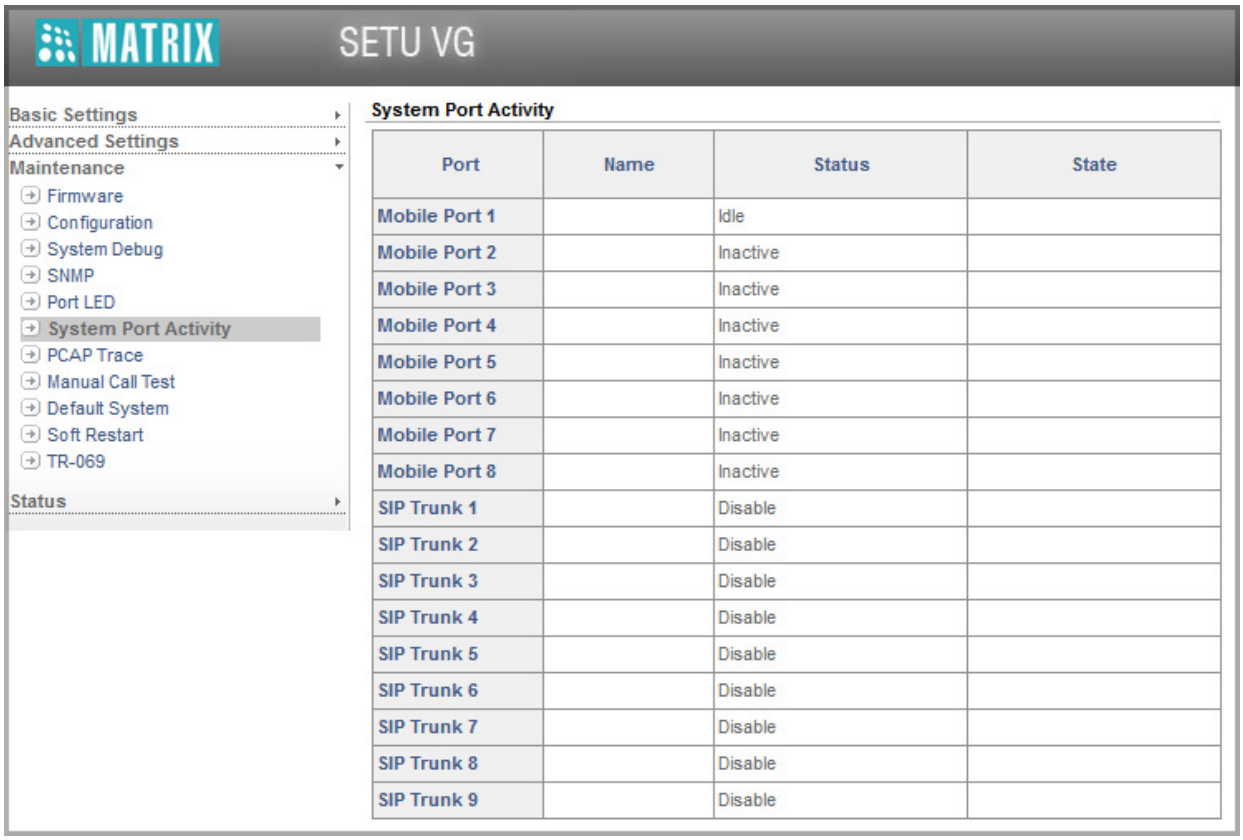

- For each LED labeled **M1**, **M2**, **M3**, **M4, M5, M6, M7, M8**:
  - Select the port type—**Mobile Port** or **SIP Trunk**—which you want to assign to these LEDs from the respective list.
  - For each port type you selected, select the number of the port Mobile/SIP Trunk that you want to assign to the LED from the list.
- Click **Submit** to save.
- You may log out of Jeeves.

  Similarly, you may re-assign port LEDs in SETU VG4.

# System Port Activity

You can view the state and activity of each Port of SETU VG.

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **System Port Activity** link.
- The port states and activity on each Port appear on this page.




| Port | Name | Status | State |
|---|---|---|---|
| Mobile Port 1 | | Idle | |
| Mobile Port 2 | | Inactive | |
| Mobile Port 3 | | Inactive | |
| Mobile Port 4 | | Inactive | |
| Mobile Port 5 | | Inactive | |
| Mobile Port 6 | | Inactive | |
| Mobile Port 7 | | Inactive | |
| Mobile Port 8 | | Inactive | |
| SIP Trunk 1 | | Disable | |
| SIP Trunk 2 | | Disable | |
| SIP Trunk 3 | | Disable | |
| SIP Trunk 4 | | Disable | |
| SIP Trunk 5 | | Disable | |
| SIP Trunk 6 | | Disable | |
| SIP Trunk 7 | | Disable | |
| SIP Trunk 8 | | Disable | |
| SIP Trunk 9 | | Disable | |

- The **Port** column displays all the Ports present in the system.
- In the **Name** column, the names assigned to the ports on their respective Port Parameters page appear.
- In the **Status** column, the port status is displayed as:
  - **Disable**, when the port is disabled
  - **Inactive**, when the port is enabled, but is unable to route calls or accept calls due to any reason.
  - **Idle**, when the port is enabled and is currently in use, but there is no call present currently on this port.
  - **Active**, when the port is enabled, in use and a call is present on the port.
- In the **State** column, the state of **Active** ports is displayed as:

- **Dial**, when the port is in Dial state, i.e. the call has been answered by the system but no called party number is received.
- **Call in Progress**, when the destination Number is outdialed on the destination port.
- **Speech**, when source port and destination port are in speech.
- **Incoming Call Proceeding**, when Ring event is detected on Mobile Port or SIP Trunk.
- **Remote Held**, when Hold message is received on SIP Trunk.
- **Error,** when the other party disconnects the call.
- **Sending SMS**, when the Mobile Port is sending an SMS.
- **Processing Balance Inquiry**, when Mobile Port is processing a Balance Inquiry request.
- **Processing Balance Recharge**, when Mobile Port is processing a Balance Recharge request.

As multiple calls are supported on SIP Trunks, the status and state of each call will appear.

- You may log out of Jeeves.

# PCAP Trace

PCAP or packet capture consists of intercepting and logging the traffic passing over a digital network or a part of a network. PCAP intercepts each packet in the data streams that flow across the network, and can decode and analyze its contents.

PCAP can be used, among others, to monitor the network, analyze network problems, debug client/server communications, debug network protocol implementations.

SETU VG supports PCAP Trace, which you can use to detect and diagnose network related problems; for example, when the SIP account is not getting registered, or a SIP related feature is not functioning.

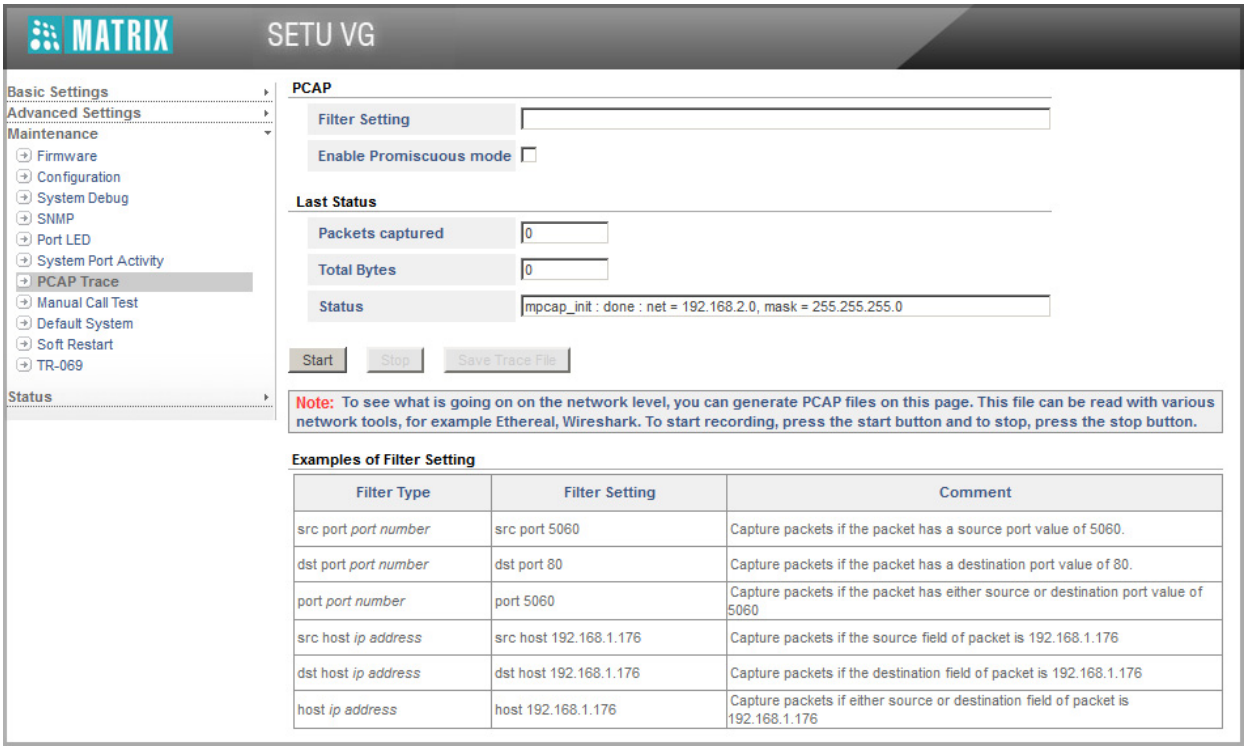
Packets traveling over a network are captured and saved in the system. You can save these trace files (packets captured by the system) on a computer and open these trace files using a graphical packet capture and protocol analysis tool such as Wireshark or Ethereal.

A maximum of 2 MB of packets can be captured and stored in the system.

SETU VG also supports Filters and Promiscuous mode for capturing packets, which you can use to specify the types of data packets to be captured.

To use PCAP Trace,

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **PCAP** link.



- Decide the type of packets to be captured and set the Filter accordingly. The Filter Settings parameter must be within 60 characters. By default, this field is blank. So, all packets will be captured.

  You may view examples of Filter Settings on this page.

*It is not mandatory to set Filters. When the Filter Settings field is left blank, the system will capture all packets.*

- You may enable **Promiscuous Mode** by selecting the check box. Default: Disabled.

  When you enable Promiscuous Mode, the SETU VG will capture all network traffic. However, this will work only in a non-switched environment.

  When Promiscuous Mode is disabled, the system will capture only traffic that is directly related to it. Only traffic to, from or routed through the SETU VG will be picked up by the PCAP Trace.

*'Filter Settings' and 'Promiscuous Mode' (enabled) will not be cleared during power down.*

- Click the **Start** button to begin the capturing of the packets.
- Click the **Stop** button to stop packet capture.

  OR

  Wait for the system to stop packet capturing. The system stops packet capturing once the maximum allotted memory of 2 MB (RAM) is utilized.

  The Number of Packets and bytes captured as per the filter setting will be displayed in the fields **Packets Captured** and **Total Bytes** respectively.

  The **Status** field displays the current activity of packet capturing.

*Capturing of packets will not stop if you open any other page of Jeeves. So, you may continue using Jeeves for any other purpose while PCAP Trace is being used.*

- When the packet capturing is stopped (by you or the system), click the **Save Trace File** button to save the files on your computer or on another computer.

  A dialog box opens. You can select the path for saving the trace file.

*The current packets captured will not be deleted after you have saved the trace file. The current packets will be deleted when you start the PCAP capture again.*

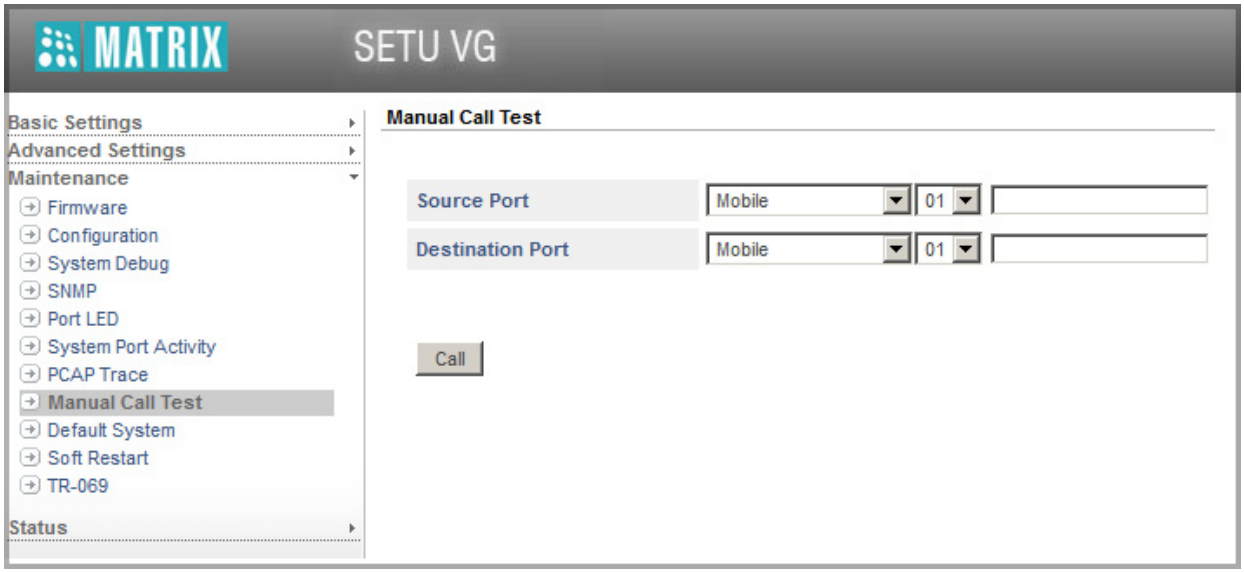
- You may log out of Jeeves.
- Now, you can open the trace files using Wireshark/Ethereal or any other software which supports opening of trace files.

# Manual Call Test

Manual Call Test enables you to check the quality of Speech between two ports—Source Port and Destination Port—of SETU VG without altering the existing call routing configuration.

To conduct Manual Call Test,

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **Manual Call Test** link.




In **Source Port**,

- Select the **Port Type** you want to test from the list.
- Select the **Port Number** you want to test from the list.
- Enter the **Phone Number** in the corresponding field**.** The phone number can be of maximum 16 characters. Valid characters are 0-9, *, #, + and dot (.).

In **Destination Port**,

- Select the **Port Type** you want to test from the list.
- Select the **Port Number** you want to test from the list.
- Enter the **Phone Number** in the corresponding field**.** The phone number must be a valid number that the system can outdial. It can be of maximum 16 characters. Valid characters are 0-9, *, #, + and dot (.).

- Click the **Call** button. SETU VG will out dial the phone number you entered to make a test call between the Source Port and the Destination Port.
- As soon as the test call is made, the **System Port Activity** page will open. You can view the call states and status of the ports you are testing on this page.

  For more information on Call States and Port Status, see “System Port Activity”.

# Default System

You can restore the system configuration to default values:

- using the Web Jeeves.
- using the Reset button.

## Restoring Default Settings using Web Jeeves

When you restore default settings using the Web Jeeves, all the parameters will be assigned default values **except** the following:

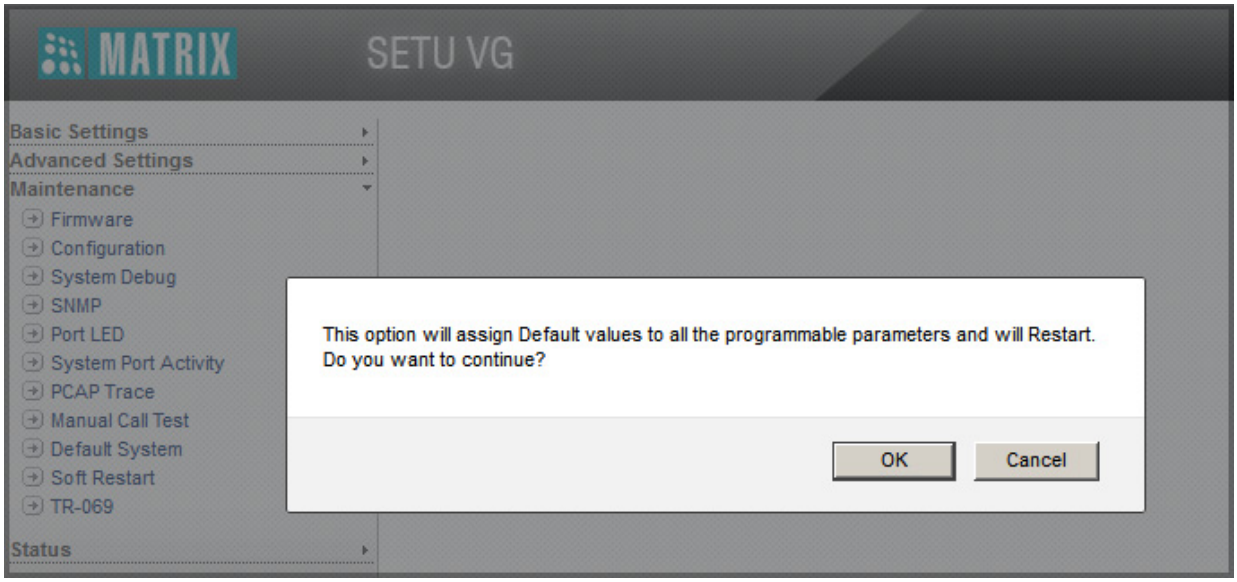
- Real Time Clock
- Call Detail Records
- Region
- Language
- Network
  - Connection Type
  - DNS Settings
  - DYN DNS
- System Parameters - NAT
  - Route Public IP Address
  - STUN Server Address
  - STUN Server Port
- System Parameters - Server Ports
  - HTTP Web Server Port
  - HTTPS Web Server Port
  - FTP Server Port
  - Telnet Server Port
- SIP Trunk
  - White List Parameters (IP / Subnet)
  - NAT Type
- Mobile Port
  - SIM PIN
- Firmware Parameters
- Configuration Parameters
- Login Password

To restore the default settings using the Web Jeeves,

- Log into Jeeves.

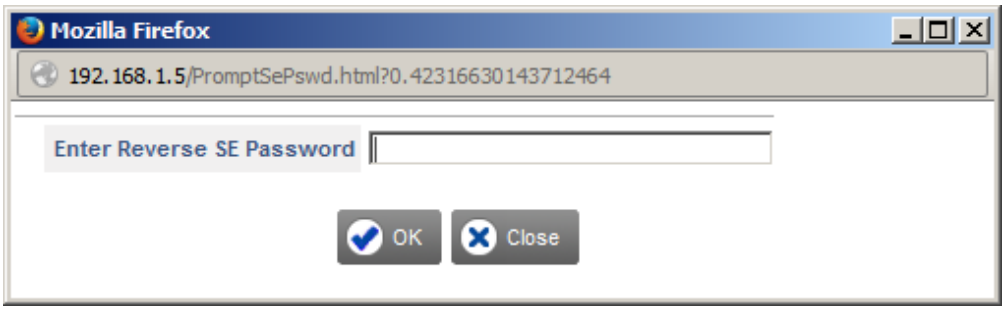
- Click the **Maintenance** link.

- Click the **Default System** link.




- An alert message will appear, "**This option will assign Default values to all the programmable parameters and will Restart. Do you want to continue?"**.

- Click **OK**.




- You will be prompted to enter the reverse SE password. Enter the current SE password backwards. For example, if your password is 5699, enter 9965. Click **OK**. The system will restart.

## Restoring Default Settings using the Reset button

Using Reset button, you can restore the following parameters to default values:

- SE Password
- LAN Port Parameters
  - IP Address
  - Subnet Mask
- System Parameters - Server Ports
  - HTTP Web Server Port
  - HTTPS Web Server Port
  - FTP Server Port
  - Telnet Server Port

To restore the default settings using the Reset button,

- Press the Reset button for more than four seconds.
- Release the Reset button.

*If you press the Reset button for less than four seconds, SETU VG will restart.*

# Soft Restart

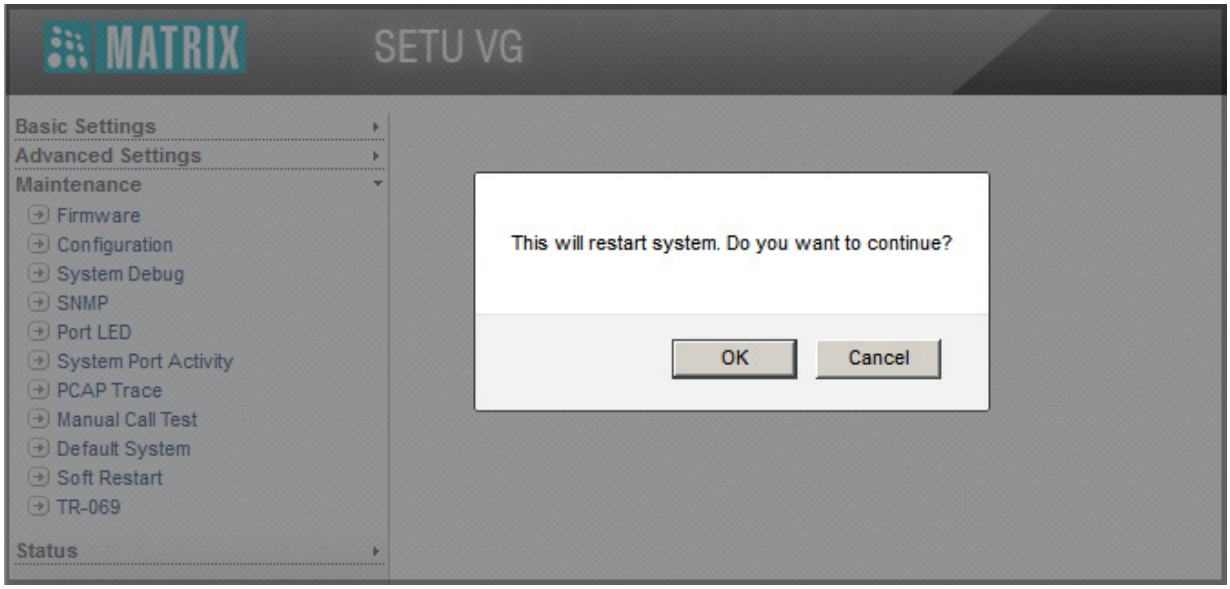
If you need to restart SETU VG, you may do it by

- pressing the Reset button.
  or
- use *Soft Restart* from Jeeves.

When you restart the system, all active calls will be disconnected and the ports in use will be released. The system configuration however, will remain unaffected.

To use Soft Restart,

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **Soft Restart** link.




- An alert message will appear, “**This will Restart System. Do you want to continue?”**
- Click **OK** to restart the system.

To restart the system using the Reset button,

- Use a blunt pin to press and release the Reset button.
- Press the Reset button for less than 4 seconds, the system will restart.

# TR-069

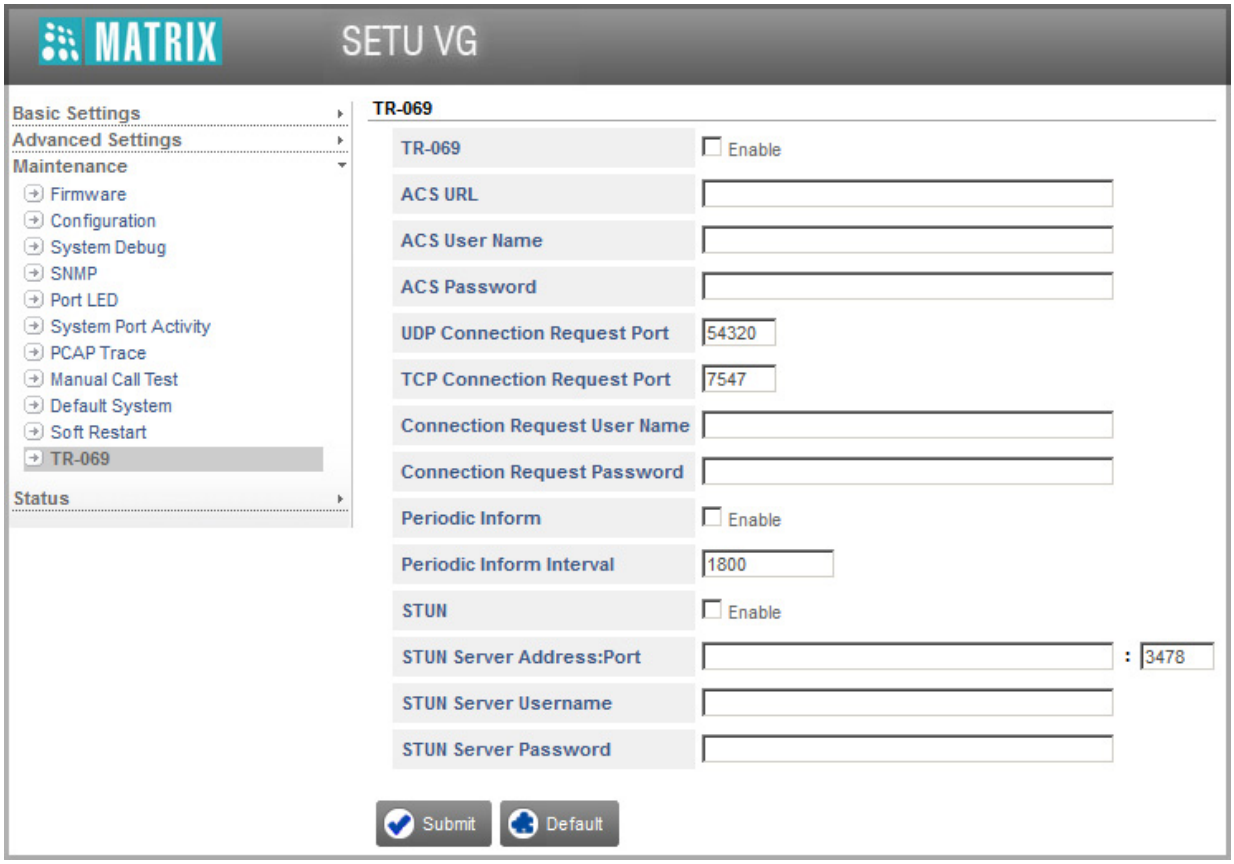
TR-069, also known as CPE WAN Management Protocol (CWMP), is a remote management protocol used for secure communication between the Customer Premises Equipment (CPE) and an Auto-Configuration Server (ACS) for various functionalities such as:

- Auto-configuration and dynamic service provisioning
- Firmware Management
- Status and performance monitoring
- Diagnostics

SETU VG supports TR-069. Using TR-069, service providers can manage SETU VG remotely for the functions described above.

To configure TR-069 parameters,

- Log into Jeeves.
- Click the **Maintenance** link.
- Click the **TR-069** link.




- Select the **TR-069 Enable** check box to use TR-069. Default: Disabled.
- In the **ACS URL** field, enter the URL of the ACS. SETU VG will connect and send message to this server address. Default: Blank.

- In the **ACS Username** field, enter the username used by SETU VG for HTTP authentication. Default: Blank.
- In the **ACS Password** field, enter the password used by SETU VG for HTTP authentication. Default: Blank.
- In the **UDP Connection Request Port** field, enter the port on which the ACS will make a connection request to SETU VG using UDP connection. The valid Port range is from 1031-65535. Default: 54320.
- In the **TCP Connection Request Port** field, enter the port on which the ACS will make a connection request to SETU VG using TCP connection. The valid Port range is from 1031-65535. Default: 7547.
- In the **Connection Request Username** field, enter the username used by SETU VG to authenticate the incoming connection request made by ACS. Default: Blank.
- In the **Connection Request Password** field, enter the password used by SETU VG to authenticate the incoming connection request made by ACS. Default: Blank.
- Select the **Periodic Inform** check box, if you want SETU VG to check updates available on ACS periodically. Default: Disabled.
- In the **Periodic Inform Interval** field, enter the time in seconds after which SETU VG must attempt to connect with the ACS to check for updates. Default: 1800.
- Select the **STUN Enable** check box, if your SETU VG is located behind the NAT Router and SIP messages need to be forwarded to the public network. Default: Disabled.

  STUN specifies the mechanism required for NAT traversal in SIP messages.

*STUN server facilitates traversing through most NATs, except symmetric NATs. If your router has symmetric NAT, do not enable STUN.*

- In the **STUN Server Address: Port** field, enter the STUN Server Address and the Listening Port of the STUN Server.

  The STUN Server Address can be a maximum of 256 characters. All ASCII characters are allowed. The valid range of the STUN Server Port is from 1025–65535. Default: 3478.
- In the **STUN Server Username** field, enter the username provided by the STUN server to authenticate the STUN Request. Default: Blank.
- In the **STUN Server Password** field, enter the password provided by the STUN Server to authenticate the STUN Request. Default: Blank.

- Click **Submit** to save changes.
- You may log out of Jeeves.

CHAPTER 8 Status

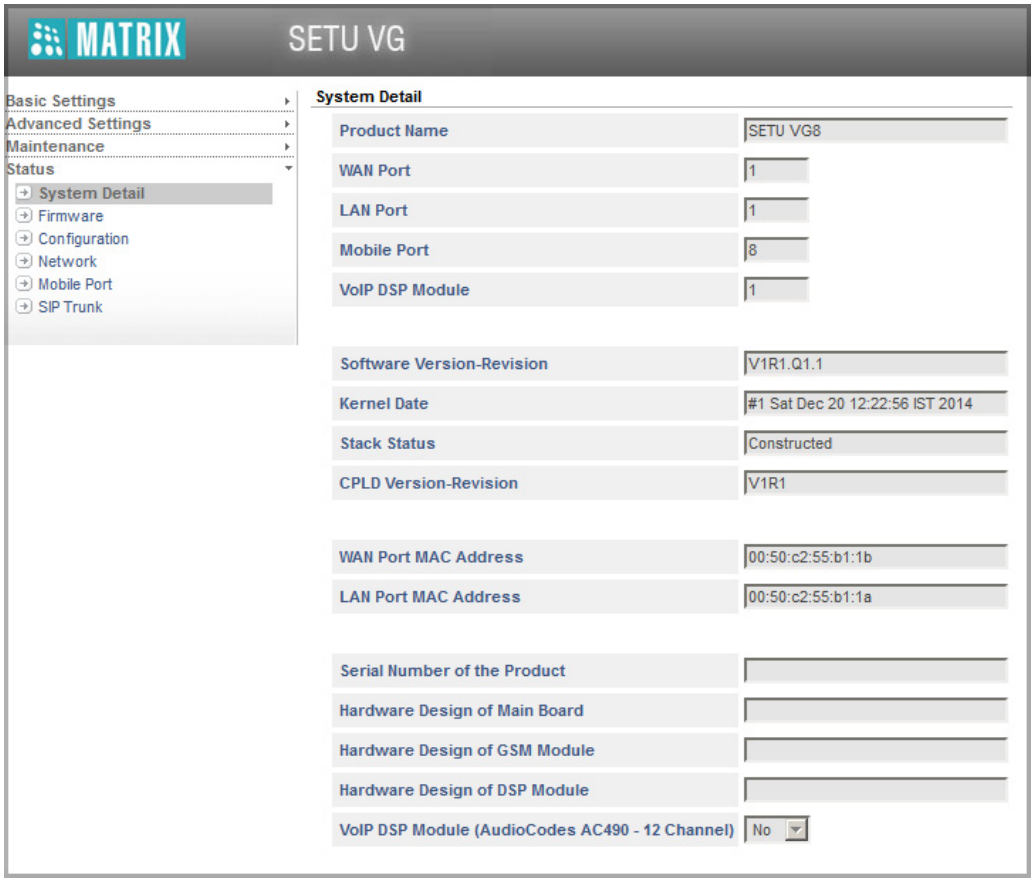
You can view the System Details and the status of Auto-Firmware upgrade, Auto-Configuration upgrade, the LAN Port, the WAN (Ethernet) Port, the SIP Trunks, the Mobile Ports from Jeeves.

To view status,

- Log into Jeeves.
- Click the **Status** link.

# System Details

- Click the **System Detail** link.



The following System Details will be displayed on this page.

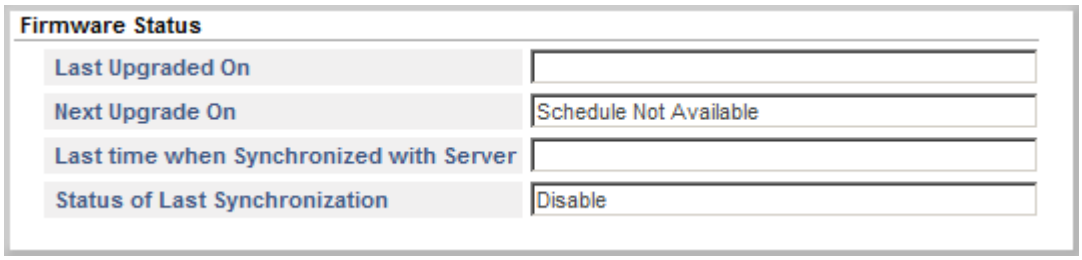
- **Product Name:** This field displays the name of the product.
- **WAN Port:** This field displays the number of WAN Port in the system.
- **LAN Port:** This field displays the number of LAN Port in the system.
- **Mobile Port:** This field displays the number of Mobile Ports in the system.
- **VoIP DSP Module:** This field displays the number of VoIP DSP Modules present in the system.
- **Software Version-Revision:** This field displays the current version and revision of the firmware of SETU VG.
- **Kernel Date:** This field displays the Kernel compilation date.
- **Stack Status:** This field displays the SIP Stack Status.
- **CPLD Version Revision:** This field displays the CPLD version revision.
- **WAN Port MAC Address:** This field displays the factory set MAC Address of the WAN (Ethernet) Port.

*If you have cloned the MAC Address of the WAN (Ethernet) Port, you can view it in Network Status.*

- **LAN Port MAC Address:** This field displays the factory set MAC Address of the LAN Port.
- **Serial Number of the Product:** This field displays the Serial Number of the product.
- **Hardware Design of Main Board:** This field displays the Hardware Design of the Main Board.
- **Hardware Design of GSM Module:** This field displays the Hardware Design of the GSM Module.
- **Hardware Design of DSP Module:** This field displays the Hardware Design of the DSP Module.
- **VoIP DSP Module (AudioCodes AC490 - 12 Channel):** This field displays the VoIP DSP Module present in the system.

# Firmware

- Click the **Firmware** link.




The following information related to Auto-Firmware upgrade will appear on your screen.

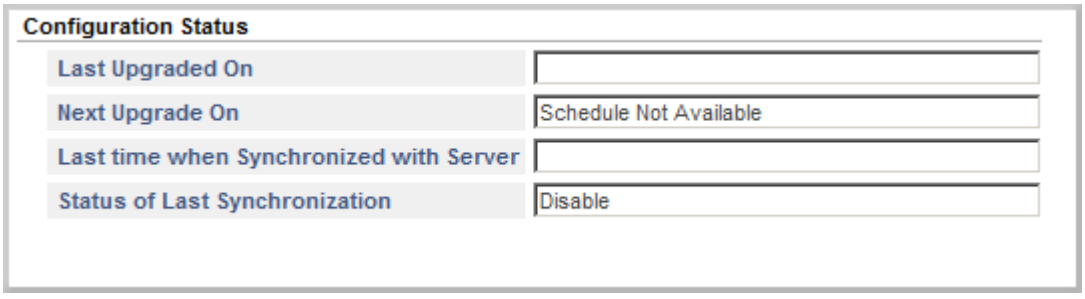
- **Last Upgraded On:** This field displays the firmware with which SETU VG last upgraded itself through the provisioning server, along with the date (DD:MM:YYYY) and time (HH:MM) of the upgradation.
- **Next Upgrade On:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VG will again check for new firmware updates on the server.
- **Last time when Synchronized with Server:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VG last synchronized with the server for new firmware updates.
- **Status of Last Synchronization:** This field displays the status of last synchronization. The possible status messages that may appear are listed in the table below.

| Possible Responses | Event |
|---|---|
| Invalid Parameters | When parameters are not valid. |
| Local Failure | When internal error occurs, like Thread Creation failed. |
| Resolving Server Address | When IP Address is not found using DNS query. |
| Server Not Found | When server is not connected after the expiry of Retry Timer and Retry Counter. |
| Send Request Failed | When there is Curl Internal Error |
| Connecting to Server | When system is establishing TCP connection with server until the expiry of Retry Timer and Retry Counter. |
| TCP Connection Failed | When no response is received for TCP connection until expiry of Retry Timer and Retry Counter. |
| Connection Failed | When no response is received for TCP connection after expiry of Retry Timer and Retry Counter. |
| | When there is an open SSL error.<br><br>When the maximum file size is exceeded.<br><br>When there are too many Redirect or illegal operation from curl response. |
| Permission Denied | When access is denied.<br><br>When there is permission problem on the server.<br><br>When login fails. |
| Downloading Firmware Index File | When the system is retrieving Firmware Index file. |
| Downloading Firmware | When the system is retrieving Firmware zip file. |
| File Not Found | When the remote file is not found. |
| Waiting for Firmware File Name | When *Check Firmware Available on Server* button is clicked manually and the list of available firmware is presented. |

| Possible Responses | Event |
|---|---|
| No File Found for Up-gradation | When selected firmware benchmark is not found.<br><br>When user does not select the firmware name manually.<br><br>When matrix_firmware.html file is received but current product name is not found from this file.<br><br>Single firmware name is received in matrix_firmware.html but this benchmark file does not match with current firmware benchmark.<br><br>Multiple firmware names are received but all files are below the current firmware. |
| Firmware Version Below | When the received firmware version is below the current firmware version. |
| Firmware Version Same | When the received firmware version is same as the current firmware version. |
| Firmware Decryption Failed | When the firmware zip file decryption has failed.<br><br>When the firmware file name does not match or benchmark is less than the current firmware version-revision in the text file. |
| Auto Upgrade stop due to parameter change | When Auto Upgrade is in process and the Firmware parameters are changed. |
| Auto Upgrade stop by system | When Auto Upgrade process is stopped due to network restart. |
| Auto Upgrade Stop on User request | When Firmware upgrade process is started manually but user clicks Cancel button after display of list of firmware files. |
| Successfully Updated | When firmware is updated successfully. |

# Configuration

- Click the **Configuration** link.




The following information related to Auto-Configuration upgrade will appear on your screen.

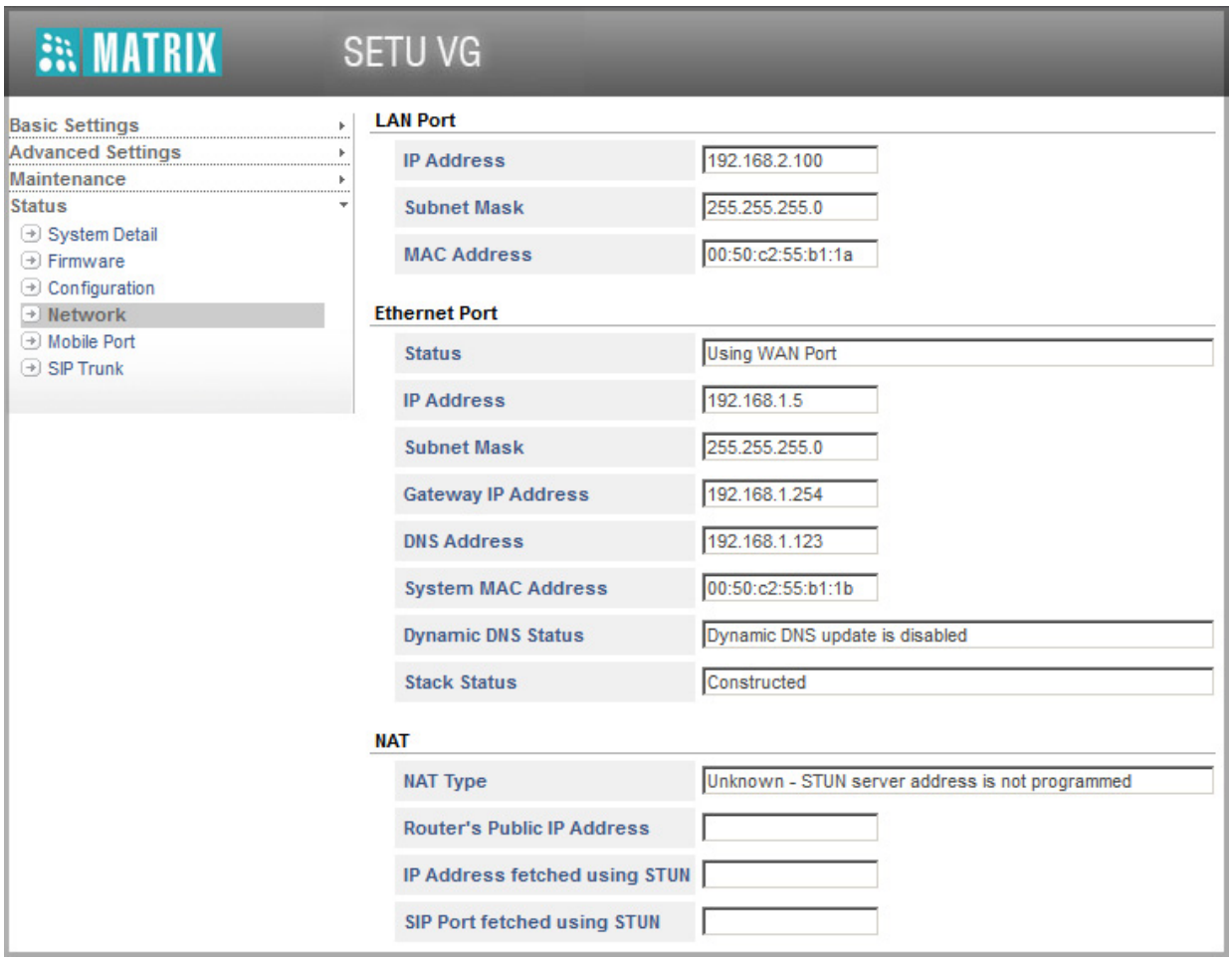
- **Last Upgraded On:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VG last upgraded its configuration through the server.

- **Next Upgrade On:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VG will again check for new configuration on the server.
- **Last time when Synchronized with Server:** This field displays the date (DD:MM:YYYY) and time (HH:MM), when SETU VG last resynchronized with the server for new configuration.
- **Status of Last Synchronization:** This field displays the status of last synchronization. The possible status messages that may appear are listed in the table below.

| Possible Responses | Event |
|---|---|
| Invalid Parameters | When parameters are not valid. |
| Local Failure | When internal error occurs, like Thread Creation failed. |
| Resolving Server Address | When IP Address is not found using DNS query. |
| Server Not Found | When server is not connected after the expiry of Retry Timer and Retry Counter. |
| Send Request Failed | When there is Curl Internal Error |
| Connecting to Server | When system is establishing TCP connection with server until the expiry of Retry Timer and Retry Counter. |
| TCP/TFTP Connection Failed | When no response is received for TCP/TFTP connection until expiry of Retry Timer and Retry Counter. |
| Connection Failed | When no response is received for TCP connection after expiry of Retry Timer and Retry Counter.<br><br>When there is an open SSL error.<br><br>When the maximum file size is exceeded.<br><br>When there are too many Redirect or illegal operation from curl response. |
| Permission Denied | When access is denied.<br><br>When there is permission problem on the server.<br><br>When login fails. |
| Downloading Config File | When the system is retrieving config file. |
| File Not Found | When the remote file is not found. |
| Config Decryption Failed | When the config decryption has failed. |
| Config Parsing Failed | When the file parsing has failed.<br><br>When the root tag is not found. |
| Successfully Updated | When configuration is updated successfully. |

# Network

- Click the **Network** link.




The current values of the following parameters will appear on your screen:

## LAN Port

- **IP Address:** This field displays the current IP address assigned to the LAN Port of SETU VG.
- **Subnet Mask:** This field displays current Subnet Mask assigned to the LAN Port of SETU VG.
- **MAC Address:** This field displays the MAC Address assigned to the LAN Port of SETU VG.

## WAN (Ethernet) Port

- **Status:** This field displays the status of the Ethernet Port of SETU VG.
- **IP Address:** This field displays the IP address assigned to the Ethernet Port of SETU VG.
- **Subnet Mask:** This field displays the Subnet Mask assigned to the Ethernet Port of SETU VG.
- **Gateway IP Address:** This field displays the Gateway Address assigned to the Ethernet Port of SETU VG.

- **DNS Address:** This field displays the DNS address.

- **System MAC Address:** This field displays the MAC Address assigned to the Ethernet Port of SETU VG.

*If you have cloned the MAC Address, this field will display the cloned MAC Address. You can view the factory set MAC Address in System Detail.*

- **Dynamic DNS Status:** This field displays the response received from DDNS server while sending the IP Address update request to the server. Any of the following responses can appear in this field:

| Possible Responses | Event |
|---|---|
| Please Wait….!! | When system is waiting for error/ successful response from DDNS server |
| Updated Successfully - IP Address | IP Address updated successfully in DDNS server |
| Host has been blocked | When 'abuse' is received |
| Authentication Fail | When authentication check is failed either problem in user id or password |
| No such host in the system | When 'no host' is received |
| Invalid hostname format | When 'notfqdn' is received |
| Host not in this account | When '!Yours' is received |
| DNS error encountered | When 'dnserr' is received |
| Server goes under schedule maintenance | When '911' is received |
| No Response | No response is received from DDNS server due to any reason |
| DDNS Failed | For all remaining cases |
| In all remaining cases, the default messages supported by DDNS client will appear in this field. | |

- **Stack Status:** This field displays the SIP Stack Status.

## NAT

- **NAT Type:** This field displays the NAT Type, if STUN is enabled in SETU VG. The commonly used NAT types are:
  - Unknown
  - Open
  - Conenat
  - Restrictednat
  - Portrestrictednat
  - Symmetricnat
  - Symmetricfirewall
  - Blocked

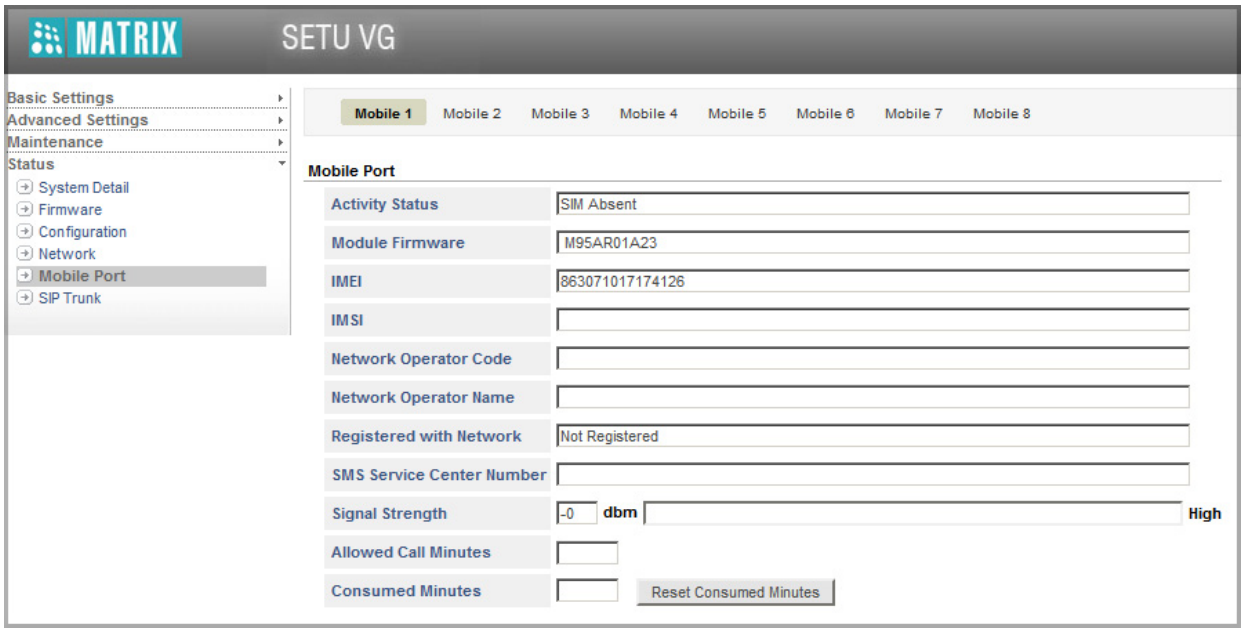
- **Router's Public IP Address:** This field displays the Router's Public IP address programmed in the System Parameters. See “NAT” under *System Parameters.*

- **IP Address fetched using STUN:** This field displays the IP address fetched using STUN, if STUN server address is programmed in the system.

- **SIP Port fetched using STUN:** This field displays the SIP Port fetched using STUN, if STUN server address is programmed in the system.

# Mobile Port

- Click the **Mobile Port** link.




The following parameters will be displayed for Mobile Ports 1, 2, 3 and 4.

- **Activity Status:** This field displays port activity status listed below:
  - Module Initialization
  - SIM PUK Required
  - SIM PIN Wrong
  - SIM Absent
  - SIM Present
  - Network Absent
  - Network Present

- **Module Firmware:** This field displays the current version-revision of the engine's firmware.

- **IMEI:** This field displays the International Mobile Equipment Identity (IMEI) Number, the unique identity number of the GSM engine.

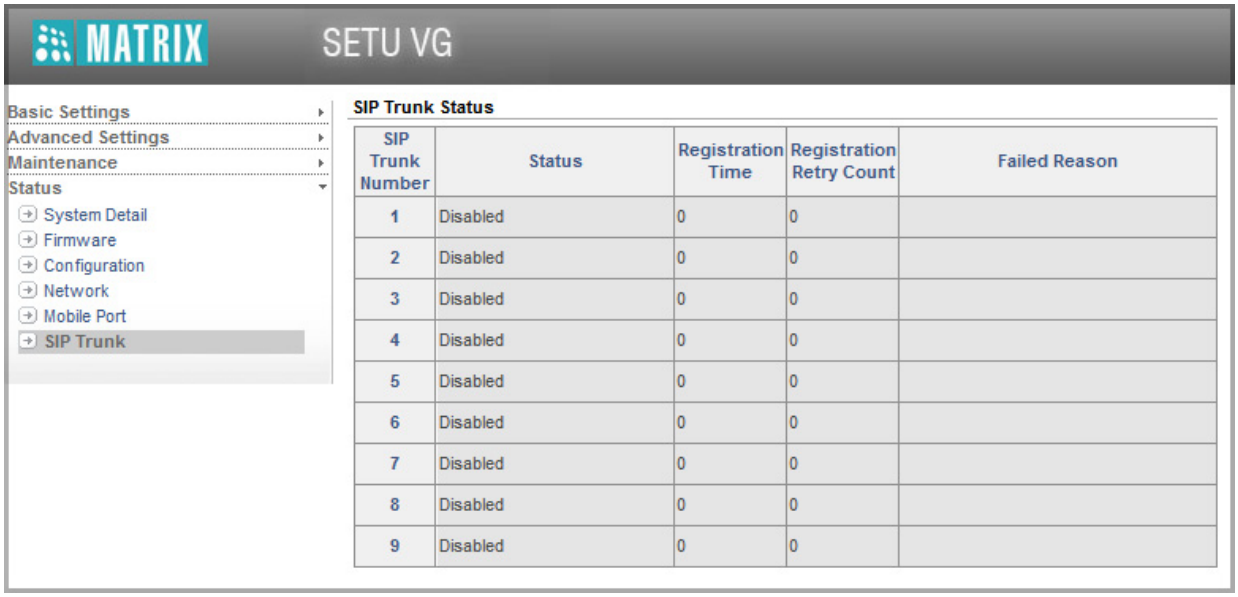
- **IMSI**: This field displays the International Mobile Subscriber Identity (IMSI), the unique identity number of the SIM Card present in the Mobile Port.

- **Network Operator Code:** This field displays the code of the network with which the Mobile Port is registered.

- **Network Operator Name:** This field displays the name of the network with which the Mobile Port is registered.
- **Registered with Network:** This field displays the type of network with which the SIM is registered, that is GSM, UMTS, 3G, 2G. If the SIM is not registered this field displays the status as Not Registered.
- **SMS Service Center Number:** This field displays the Number of the SMS Service Center of the Service Provider.
- **Signal Strength:** This field displays the current signal strength.
- **Allowed Call Minutes:** This field displays the Call Minutes allowed to the Mobile Port. To know more about this feature, see “Call Minutes”.
- **Consumed Minutes:** This field displays the Call Minutes used up by the Mobile Port. You can reset the consumed minutes by clicking the **Reset Consumed Minutes** button. To know more, see “Call Minutes”.

# SIP Trunk

- Click the **SIP Trunk** link.




The following status indications will appear for the SIP Trunks.

- **SIP Trunk Number:** The number of the SIP Trunk.
- **Status:** The possible status indications that will be displayed in this column for the respective SIP Trunk numbers are described in the table below.

| Status Message | Meaning |
|---|---|
| Disable | The SIP Trunk is disabled. |
| Registering | The SIP Trunk is enabled and is waiting for response from the SIP server. |

| Status Message | Meaning |
|---|---|
| Active | The SIP Trunk is registered with the SIP server. |
| Failed | Some error has occurred in the SIP Trunk and no calls can be made using the SIP Trunk (applicable only if the SIP Trunk mode is configured as 'Proxy'). |
| Network Connection Disable | The SIP Trunk is enabled but the active *Network Connection* does not match the option selected for *Use SIP Trunk for Network Connection* parameter. |
| Inactive | The Proxy Server is unavailable (no response is received from the server). |

- **Registration Time:** The SIP Trunk is registered with the Registrar Server for a particular time period, after which it has to be re-registered. The registrar server indicates the time remaining for re-registration of the SIP Trunk. The same is displayed in this field as Registration Time.

- **Registration Retry Count:** This field displays the total number of register messages which are sent to the registrar server for registering the SIP Trunk.

- **Failed Reason:** This field displays the reason for failure of SIP Trunk registration with the registrar server. The different reasons for registration failure that may appear in this field are:

| Failure Message | Description |
|---|---|
| Message send fail | This reason is displayed when registration request sent to registrar server fails. |
| Failed to create Register client | This reason is displayed when SIP stack has memory constraints, or resource limitation or the number of SIP clients to register is greater than the number programmed in the stack. |
| Failed to detach register client | This reason is displayed when SIP stack has memory constraint/ resource limitation/ the number of SIP clients to register is greater than the number programmed in the stack. |
| Failed to send request | This reason is displayed when DNS server is not programmed. |
| Local Failure | This reason is displayed when DNS query fails. |
| Response timeout | This reason is displayed on the expiry of the General Request Timer. |
| Error Response- 4xx to 6xx | This is the error response code. |
| No contact header in 2xx | This reason is displayed when no contact address is received in the 2xx response from the SIP server. |
| Authentication Failed | This reason is displayed when the SIP server does not authenticate the client. |
| STUN address is not programmed | This reason is displayed when STUN is enabled but address is not configured. |
| STUN query fail | This reason is displayed when a query to the STUN server fails. |
| Outbound address is not programmed | This reason is displayed when Outbound is enabled but Outbound address is not configured. |

| Failure Message | Description |
|---|---|
| Router's IP address is not programmed | This reason is displayed when Router's IP Address is to be used in signaling but the address is not programmed. |

*If for a SIP Trunk, you have enabled **Fallback Server** and **Registration Behavior** is set to **Register with all Servers**, the SIP Trunk Status page will display status of all the servers for that SIP Trunk as shown below.*

**SIP Trunk Status**

| SIP Trunk Number | Status | Registration Time | Registration Retry Count | Failed Reason |
|---|---|---|---|---|
| 1 | Registering | 0 | 2 | Response timeout |
| | Registering | 0 | 2 | Response timeout |
| | Registering | 0 | 2 | Response timeout |
| 2 | Disabled | 0 | 0 | |
| 3 | Disabled | 0 | 0 | |
| 4 | Disabled | 0 | 0 | |
| 5 | Disabled | 0 | 0 | |
| 6 | Disabled | 0 | 0 | |
| 7 | Disabled | 0 | 0 | |
| 8 | Disabled | 0 | 0 | |
| 9 | Disabled | 0 | 0 | |

# Appendix

## Acronyms

| | |
|---|---|
| ***ACS*** | Auto Configuration Server |
| ***ASCII*** | American Standard Code for Information Technology |
| ***ANT*** | Automatic Number Translation |
| ***CA*** | Certificate Authority |
| ***CDR*** | Call Detail Record |
| ***CLI*** | Caller Line Identification |
| ***CLIP*** | Caller Line Identification and Presentation |
| ***CLIR*** | Calling Line Identification Restriction |
| ***COS*** | Class of Service |
| ***CPT*** | Call Progress Tone |
| ***DDI*** | Direct Dialing In |
| ***DHCP*** | Dynamic Host Control Protocol |
| ***DNS*** | Domain Name Service |
| ***DTMF*** | Dual Tone Multi-Frequency |
| ***FIFO*** | First In First Out |
| ***FoIP*** | Fax over IP |
| ***FSK*** | Frequency Shift Keying |
| ***FTP*** | File Transfer Protocol |
| ***GMT*** | Greenwich Mean Time |
| ***GSM*** | Global Systems for Mobile Communications |
| ***HTTP*** | Hypertext Transfer Protocol |
| ***ICMP*** | Internet Control Message Protocol |
| ***IMEI*** | International Mobile Equipment Identity |
| ***IP*** | Internet Protocol |
| ***ITSP*** | Internet Telephony Service Provider |
| ***LAN*** | Local Area Network |
| ***LED*** | Light Emitting Diode |
| ***MAC*** | Media Access Control |
| ***MCC*** | Mobile Country Code |
| ***MNC*** | Mobile Network Code |
| ***MS*** | Mobile Station |
| ***NAT*** | Network Address Translation |
| ***PBX*** | Private Branch Exchange |
| ***PIN*** | Personal Identification Number |

| | |
|---|---|
| ***PPPoE*** | Point-to-Point Protocol over Ethernet |
| ***PSTN*** | Public Switched Telephone Network |
| ***PUK*** | Personal Unlock Key |
| ***PWR*** | Power |
| ***QoS*** | Quality of Service |
| ***RTC*** | Real Time Clock |
| ***RTP*** | Real Time Protocol |
| ***SE*** | System Engineer |
| ***SIM*** | Subscriber Identification Module |
| ***SIP*** | Session Initiation Protocol |
| ***SNMP*** | Simple Network Management Protocol |
| ***SNTP*** | Simple Network Time Protocol |
| ***STUN*** | Simple Traversal of UDP over NAT |
| ***TLS*** | Transport Layer Security |
| ***UDP*** | User Datagram Protocol |
| ***URI*** | Uniform Resource Identifier |
| ***URL*** | Universal Reference/Resource Locator |
| ***VoIP*** | Voice over IP |
| ***WAN*** | Wide Area Network |
| ***WWAN*** | Wireless WAN |

# Default Region Table

The country-specific default settings of various parameters that will be loaded on changing the **Region** are presented in the table below.

| Region Code | Country/ Region | Default Language | Default Time Zone | Default DST Type | Default CPTG | Country Code | Companding Type |
|---|---|---|---|---|---|---|---|
| 1 | Afghanistan | English | GMT+04:30 | | | 93 | |
| 2 | Algeria | English | GMT+01:00 | | | 213 | A-law |
| 3 | Antigua and Barbuda | English | GMT-04:00 | | | 1 268 | |
| 4 | Argentina | Spanish | GMT-03:00 | | 4 | 54 | A-law |
| 5 | Australia (Perth) | English | GMT+08:00 | 2 | 5 | 61 | |
| 6 | Australia (Adelaide) | English | GMT+09:30 | 2 | 5 | 61 | |
| 7 | Australia (Brisbane, Canberra, Melbourne, Sydney) | English | GMT+10:00 | | 5 | 61 | |
| 8 | Austria | German | GMT+01:00 | 1 | | 43 | |
| 9 | Bahamas | English | GMT-05:00 | | | 1 242 | |
| 10 | Bahrain | English | GMT+03:00 | 3 | | 973 | |
| 11 | Bangladesh | English | GMT+06:00 | | | 880 | |
| 12 | Belarus | English | GMT+02:00 | | | 375 | |
| 13 | Belgium | French | GMT+01:00 | 2 | 39 | 32 | A-law |
| 14 | Bhutan | English | GMT+06:00 | | | 975 | |
| 15 | Bolivia | Spanish | GMT-04:00 | | | 591 | |
| 16 | Bosnia and Herzegovina | English | GMT+01:00 | | | 387 | |
| 17 | Botswana | English | GMT+02:00 | | | 267 | |
| 18 | Brunei | English | GMT+08:00 | | | 673 | |
| 19 | Brazil (Fernando De Noronha) | Portuguese | GMT-02:00 | | 6 | 55 | A-law |
| 20 | Brazil (Brasilia, Rio de Janeiro, Sao Paulo) | Portuguese | GMT-03:00 | 4 | 6 | 55 | A-law |
| 21 | Brazil (Manaus) | Portuguese | GMT-04:00 | | 6 | 55 | A-law |
| 22 | Brazil (Acre) | Portuguese | GMT-05:00 | | 6 | 55 | A-law |
| 23 | Bulgaria | English | GMT+02:00 | | | 359 | |
| 24 | Cambodia | English | GMT+07:00 | | | 855 | |
| 25 | Cameroon | English | GMT+01:00 | | | 237 | |
| 26 | Canada (St. John's) | English | GMT-03:30 | 5 | 7 | 1 | U-law |
| 27 | Canada (Halifax) | English | GMT-04:00 | 5 | 7 | 1 | U-law |
| 28 | Canada (Montreal, Ottawa, Toronto) | English | GMT-05:00 | 5 | 7 | 1 | U-law |
| 29 | Canada (Winnipeg) | English | GMT-06:00 | 5 | 7 | 1 | U-law |
| 30 | Canada (Calgary) | English | GMT-07:00 | 5 | 7 | 1 | U-law |
| 31 | Canada (Vancouver) | English | GMT-08:00 | 5 | 7 | 1 | U-law |
| 32 | Chile | Spanish | GMT-04:00 | 6 | | 56 | |
| 33 | China | English | GMT+08:00 | | 8 | 86 | A-law |
| 34 | Colombia | Spanish | GMT-05:00 | | | 57 | |
| 35 | Costa Rica | Spanish | GMT-06:00 | | | 506 | |
| 36 | Croatia | English | GMT+01:00 | | | 385 | |
| 37 | Cuba | Spanish | GMT-05:00 | 18 | | 53 | A-law |
| 38 | Cyprus | English | GMT+02:00 | | | 357 | |
| 39 | Czech Republic | English | GMT+01:00 | | | 420 | |
| 40 | Denmark | English | GMT+01:00 | 7 | | 45 | A-law |
| 41 | Egypt | English | GMT+02:00 | 11 | 9 | 20 | A-law |
| 42 | Fiji | English | GMT+12:00 | | | 679 | |
| 43 | Finland | English | GMT+02:00 | 8 | | 358 | A-law |
| 44 | France | French | GMT+01:00 | 2 | 10 | 33 | A-law |
| 45 | Germany | German | GMT+01:00 | 2 | 11 | 49 | A-law |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 46 | Greece | English | GMT+02:00 | 2 | 12 | 30 | |
| 47 | Guyana | English | GMT-04:00 | | | 592 | |
| 48 | Hong Kong | English | GMT+08:00 | | | 852 | |
| 49 | Hungary | English | GMT+02:00 | 2 | | 36 | |
| 50 | India | English | GMT+05:30 | | 13 | 91 | A-law |
| 51 | Indonesia | English | GMT+07:00 | | 14 | 62 | |
| 52 | Iran | English | GMT+03:30 | | 15 | 98 | |
| 53 | Iraq | English | GMT+03:00 | 9 | 16 | 964 | |
| 54 | Ireland | English | GMT | 7 | | 353 | |
| 55 | Israel | English | GMT+02:00 | | 17 | 972 | |
| 56 | Italy | Italian | GMT+01:00 | 2 | 18 | 39 | |
| 57 | Japan | English | GMT+09:00 | | 19 | 81 | U-law |
| 58 | Jordan | English | GMT+02:00 | | | 962 | A-law |
| 59 | Kazakhstan | English | GMT+06:00 | | | 7 | |
| 60 | Kenya | English | GMT+03:00 | | 20 | 254 | |
| 61 | Korea – North | English | GMT+09:00 | | 21 | 850 | |
| 62 | Korea – South | English | GMT+09:00 | | 21 | | |
| 63 | Kuwait | English | GMT+03:00 | | | 965 | |
| 64 | Kyrgyzstan | English | GMT+06:00 | 10 | | 996 | |
| 65 | Lebanon | English | GMT+02:00 | 12 | | 961 | |
| 66 | Libya | English | GMT+02:00 | | | 218 | |
| 67 | Malaysia | English | GMT+08:00 | | 22 | 60 | |
| 68 | Maldives | English | GMT+05:00 | | | 960 | |
| 69 | Mauritius | English | GMT+04:00 | | | 230 | |
| 70 | Mexico (Mexico City) | Spanish | GMT-06:00 | 3 | 23 | 52 | A-law |
| 71 | Mexico (Chihuahua) | Spanish | GMT-07:00 | 3 | 23 | 52 | A-law |
| 72 | Mexico (Tijuana) | Spanish | GMT-08:00 | 3 | 23 | 52 | A-law |
| 73 | Mongolia | English | GMT+08:00 | | | 976 | |
| 74 | Mozambique | Portuguese | GMT+02:00 | | | 258 | |
| 75 | Myanmar | English | GMT+06:30 | | | 95 | |
| 76 | Namibia | English | GMT+01:00 | 13 | | 264 | |
| 77 | Nepal | English | GMT+05:45 | | | 977 | |
| 78 | Netherlands | English | GMT+01:00 | | | 31 | A-law |
| 79 | New Zealand | English | GMT+12:00 | 14 | 24 | 64 | |
| 80 | Nigeria | English | GMT+01:00 | | | 234 | |
| 81 | Norway | English | GMT+01:00 | 15 | | 47 | A-law |
| 82 | Oman | English | GMT+04:00 | | | 968 | |
| 83 | Pakistan | English | GMT+05:00 | | | 92 | |
| 84 | Paraguay | Spanish | GMT-04:00 | 16 | | 595 | |
| 85 | Peru | Spanish | GMT-05:00 | | | 51 | |
| 86 | Philippines | English | GMT+08:00 | | 25 | 63 | A-law |
| 87 | Poland | English | GMT+01:00 | 1 | 26 | 48 | |
| 88 | Portugal | Portuguese | GMT | 7 | 27 | 351 | |
| 89 | Qatar | English | GMT+03:00 | | | 974 | |
| 90 | Romania | English | GMT+02:00 | | | 40 | |
| 91 | Russia (Moscow, St. Petersburg) | English | GMT+03:00 | 1 | 28 | 7 | |
| 92 | Russia (Novosibirsk) | English | GMT+06:00 | 1 | 28 | 7 | |
| 93 | Russia (Vladivostok) | English | GMT+10:00 | 1 | 28 | 7 | |
| 94 | Singapore | English | GMT+08:00 | | 30 | 65 | A-law |
| 95 | Slovakia | English | GMT+01:00 | | | 421 | |
| 96 | South Africa | English | GMT+02:00 | | 31 | 27 | |
| 97 | Spain | Spanish | GMT+01:00 | 1 | 32 | 34 | A-law |
| 98 | Sri Lanka | English | GMT+05:30 | | | 94 | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 99 | Sudan | English | GMT+03:00 | | | 249 | |
| 100 | Sweden | English | GMT+01:00 | 2 | | 46 | A-law |
| 101 | Switzerland | German | GMT+01:00 | 2 | | 41 | |
| 102 | Syria | English | GMT+02:00 | 17 | | 963 | |
| 103 | Taiwan | English | GMT+08:00 | | | 886 | |
| 104 | Tajikistan | English | GMT+05:00 | | | 992 | |
| 105 | Thailand | English | GMT+07:00 | | 33 | 66 | A-law |
| 106 | Turkey | English | GMT+02:00 | | 34 | 90 | |
| 107 | Uganda | English | GMT+03:00 | | | 256 | |
| 108 | Ukraine | English | GMT+02:00 | | | 380 | |
| 109 | United Arab Emirates | English | GMT+04:00 | | 35 | 971 | A-law |
| 110 | United Kingdom | English | GMT | 7 | 36 | 44 | A-law |
| 111 | United States (Atlanta, Augusta, Boston, Charlotte, Columbus, Detroit, Indiapolis, Miami, NY, Philadelphia, Washington) | English | GMT-05:00 | 3 | 37 | 1 | U-law |
| 112 | United States (Chicago, Dallas, Des Moines, Memphis, Minneapolis, New Orleans, Oklahoma, Omaha, St. Louis) | English | GMT-06:00 | 3 | 37 | 1 | U-law |
| 113 | United States (Albuquerque, Boise, Cheyenne, Denver, Salt Lake City) | English | GMT-07:00 | 3 | 37 | 1 | U-law |
| 114 | United States (Las Vegas, Los Angeles, Phoenix, San Francisco, Seattle) | English | GMT-08:00 | 3 | 37 | 1 | U-law |
| 115 | United States (Juneau) | English | GMT-09:00 | 3 | 37 | 1 | U-law |
| 116 | United States (Hawaii) | English | GMT-10:00 | | 37 | 1 | U-law |
| 117 | Uzbekistan | English | GMT+05:00 | | | 998 | |
| 118 | Venezuela | Spanish | GMT-04:30 | | | 58 | |
| 119 | Vietnam | English | GMT+07:00 | | | 84 | |
| 120 | Yemen | English | GMT+03:00 | | | 967 | |
| 121 | Yugoslavia | English | GMT+02:00 | | | 381 | |
| 122 | Zambia | English | GMT+02:00 | | | 260 | |
| 123 | Zimbabwe | English | GMT+02:00 | | | 263 | |

# Call Progress Tones

Call Progress Tones (CPT) are audible tones sent by switching systems such as PSTN or PBX, to calling parties to show the status of the phone call.

Each CPT has a distinctive tone frequency and cadence assigned to it, for which some standards have been established by the ETSI.

On the basis of specific frequency, modulating frequency and cadence, the CPTs generated by SETU VG are categorized as:

- Dial Tone
- Ring Back Tone
- Busy Tone
- Error Tone 1
- Confirmation Tone
- Feature Tone/ Programming Tone
- Intrusion Tone
- Error Tone 2
- Routing Tone

CPT standards are applied differently in different situations and in different countries.You can match call progress tones of SETU VG to that of the country standard where it is installed.

See the table for the **CPTG Type** (frequency and cadence of the different tones) supported by SETU VG. The table shows the CPTG Types supported for different countries.

When you select **Region**, the Call Progress Tones matching the country standards of the selected Region/Country will be loaded automatically. However, you may select a different CPTG Type, if required.

**CPTG Types (as per ETSI standard) supported by SETU VG**

| CPTG Type | Country | Dial tone | | Ring Back Tone | | Busy Tone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 1 | Type1 | 440 | Continuous | 350+440 | 0.4on 0.2off 0.4on 2.0off | 440 | 0.75on 0.75off |
| 2 | Type2 | 400 | Continuous | 400 | 0.6on 0.2off 0.2on 2.0off | 400 | 0.5on 0.5off |
| 3 | Type3 | 350+440 | Continuous | 440+480 | 2.0on 4.0off | 480+620 | 0.5on 0.5off |
| 4 | Argentina | 425 | Continuous | 425 | 1.0on 4.0 off | 425 | 0.3on 0.2off |
| 5 | Australia | 425*25 | Continuous | 400*25 | .4on .2off .4on 2.0off | 425 | 0.375on 0.375off |
| 6 | Brazil | 425 | Continuous | 425 | 1.0on 4.0 off | 425 | 0.25on 0.25off |
| 7 | Canada | 350+440 | Continuous | 440+480 | 2.0on 4.0off | 480+620 | 0.5on 0.5off |
| 8 | China | 450 | Continuous | 450 | 1.0on 4.0off | 450 | 0.35 on 0.36off |
| 9 | Egypt | 425*50 | Continuous | 425*50 | 2.0on 1.0off | 425*50 | 1.0on 4.0off |

| CPTG Type | Country | Dial tone | | Ring Back Tone | | Busy Tone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 10 | France | 440 | Continuous | 440 | 1.5on 3.5off | 440 | 0.5on 0.5off |
| 11 | Germany | 425 | Continuous | 425 | 1.0on 4.0off | 425 | 0.48on 0.48off |
| 12 | Greece | 425 | 0.2on 0.3off 0.7on 0.8off | 425 | 1.0on 4.0off | 425 | 0.3on 0.3off |
| 13 | India | 400*25 | Continuous | 400*25 | .4on .2off .4on 2.0off | 400 | 0.75on 0.75off |
| 14 | Indonesia | 425 | Continuous | 425 | 1.0on 4.0off | 425 | 0.5on 0.5off |
| 15 | Iran | 425 | Continuous | 425 | 1.0on 4.0off | 425 | 0.5on 0.5off |
| 16 | Iraq | 400 | 0.4on 0.2off 0.4on 1.5off | 400 | Continuous | 400 | 1.0on 1.0off |
| 17 | Israel | 400 | Continuous | 400 | 1.0on 3.0off | 400 | 0.5on 0.5off |
| 18 | Italy | 425 | Continuous | 425 | 1.0on 4.0off | 425 | 0.5on 0.5off |
| 19 | Japan | 400 | Continuous | 400*25 | 1.0on 2.0off | 400 | .5on .5off |
| 20 | Kenya | 425 | Continuous | 425 | 0.67on 3.0off 1.5on 5.0off | 425 | 0.2on 0.6off 0.2on 0.6off |
| 21 | Korea | 350+440 | Continuous | 440+480 | 1.0on 2.0off | 480+620 | 0.5on 0.5off |
| 22 | Malaysia | 425 | Continuous | 425 | 0.4on 0.2off 0.4on 2.0off | 425 | 0.5on 0.5off |
| 23 | Mexico | 425 | Continuous | 425 | 1.0on 4.0off | 425 | 0.25on 0.25off |
| 24 | New Zealand | 400 | Continuous | 400+450 | 0.4on 0.2off 0.4on 2.0off | 400 | 0.5on 0.5off |
| 25 | Phillippines | 425 | Continuous | 425+480 | 1.0on 4.0off | 480+620 | 0.5on 0.5off |
| 26 | Poland | 425 | Continuous | 425 | 1.0on 4.0off | 425 | 0.5on 0.5off |
| 27 | Portugal | 425 | Continuous | 425 | 1.0on 5.0off | 425 | 0.5on 0.5off |
| 28 | Russia | 425 | Continuous | 425 | 0.8on 3.2off | 425 | 0.4on 0.4off |
| 29 | Saudi Arabia | 425 | Continuous | 425 | 1.2on 4.6off | 425 | 0.5on 0.5off |
| 30 | Singapore | 425 | Continuous | 425*24 | 0.4on 0.2off 0.4on 2.0off | 425 | .75on .75off |
| 31 | South Africa | 400*33 | Continuous | 400*33 | 0.4on 0.2off 0.4on 2.0off | 400 | .5on .5off |
| 32 | Spain | 425 | Continuous | 425 | 1.5on 3.0off | 425 | 0.2on 0.2off |
| 33 | Thailand | 400*50 | Continuous | 400 | 1.0on 4.0off | 400 | 0.5on 0.5off |
| 34 | Turkey | 450 | Continuous | 450 | 2.0on 4.0off | 450 | 0.5on 0.5off |

| CPTG Type | Country | Dial tone | | Ring Back Tone | | Busy Tone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 35 | UAE | 350+440 | Continuous | 400+450 | 0.4on 0.2off 0.4on 2.0off | 400 | 0.375on 0.375off |
| 36 | UK | 350+440 | Continuous | 400+450 | 0.4on 0.2off 0.4on 2.0off | 400 | 0.375on 0.375off |
| 37 | USA | 350+440 | Continuous | 440+480 | 2.0on 4.0off | 480+620 | 0.5on 0.5off |
| 38 | Type4 | 400 | Continuous | 400 | 1.0on 2.0off | 400 | 0.5on 0.5off |
| 39 | Belgium | 425 | Continuous | 425 | 1.0on 3.0off | 425 | 0.5on 0.5off |
| 40 | Type5 | 350+440 | Continuous | 350+440 | 0.4on 0.2off 0.4on 2.0off | 400 | 0.75on 0.75off |

| CPTG Type | Country | Error Tone 1 | | Error Tone 2 | | Confirmation Tone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 1 | Type1 | 440 | 0.25on 0.25 off | 440 | 1on 1off | 350+440 | 0.1on 0.1off |
| 2 | Type2 | 400 | 0.25on 0.25 off | 400 | 1on 1off | 400 | 0.1on 0.1off |
| 3 | Type3 | 440 | 0.25on 0.25 off | 440 | 1on 1off | 350+440 | 0.1on 0.1off |
| 4 | Argentina | 425 | 0.3on 0.4off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 5 | Australia | 425 | 0.375on 0.375off | 425 | 1on 1off | 425*25 | 0.1on 0.1off |
| 6 | Brazil | 425 | 0.25on 0.25 off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 7 | Canada | 480+620 | 0.25on 0.25off | 480+620 | 1on 1off | 350+440 | 0.1on 0.1off |
| 8 | China | 450 | 0.7on 0.7off | 450 | 1on 1off | 450 | 0.1on 0.1off |
| 9 | Egypt | 450 | 0.5on 0.5off | 450 | 1on 1off | 425*50 | 0.1on 0.1off |
| 10 | France | 440 | 0.25on 0.25off | 440 | 1on 1off | 440 | 0.1on 0.1off |
| 11 | Germany | 440 | 0.20on 0.48off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 12 | Greece | 425 | 0.15on 0.15off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 13 | India | 400 | 0.25on 0.25off | 400 | 1on 1off | 400 | 0.1on 0.1off |
| 14 | Indonesia | 425 | 0.25on 0.25off | 425 | 1on 1off | 425 | 0.1on 0.1off |

| CPTG Type | Country | Error Tone 1 | | Error Tone 2 | | Confirmation Tone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 15 | Iran | 425 | 0.25on 0.25off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 16 | Iraq | 400 | 0.25on 0.25off | 400 | 1on 1off | 400 | 0.1on 0.1off |
| 17 | Israel | 400 | 0.25on 0.25off | 400 | 1on 1off | 400 | 0.1on 0.1off |
| 18 | Italy | 425 | 0.2on 0.2off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 19 | Japan | 400 | 0.25on 0.25off | 400 | 1on 1off | 400 | 0.1on 0.1off |
| 20 | Kenya | 425 | 0.2on 0.6off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 21 | Korea | 480+620 | 0.3on 0.2off | 480+620 | 1on 1off | 350+440 | 0.1on 0.1off |
| 22 | Malaysia | 425 | 2.5on 0.5off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 23 | Mexico | 425 | 0.25on 0.25off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 24 | New Zealand | 400 | 0.25on 0.25off | 400 | 1on 1off | 400 | 0.1on 0.1off |
| 25 | Phillippines | 480+620 | 0.25on 0.25off | 480+620 | 1on 1off | 425 | 0.1on 0.1off |
| 26 | Poland | 425 | 0.5on 0.5off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 27 | Portugal | 450 | 0.33on 1.0off | 450 | 1on 1off | 425 | 0.1on 0.1off |
| 28 | Russia | 425 | 0.25on 0.25off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 29 | Saudi Arabia | 425 | 0.25on 0.25off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 30 | Singapore | 425 | 0.25on 0.25off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 31 | South Africa | 400 | 0.25on 0.25off | 400 | 1on 1off | 400*33 | 0.1on 0.1off |
| 32 | Spain | 425 | 0.25on 0.25off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 33 | Thailand | 400 | 0.3on 0.3off | 400 | 1on 1off | 400*50 | 0.1on 0.1off |
| 34 | Turkey | 450 | 0.2on 0.2off .6on .2off | 450 | 1on 1off | 450 | 0.1on 0.1off |
| 35 | UAE | 400 | 0.4on 0.35off 0.225on 0.525off | 400 | 1on 1off | 350+440 | 0.1on 0.1off |

| CPTG Type | Country | Error Tone 1 | | Error Tone 2 | | Confirmation Tone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 36 | UK | 400 | 0.4on 0.35off 0.225on 0.525off | 400 | 1on 1off | 350+440 | 0.1on 0.1off |
| 37 | USA | 480+620 | 0.25on 0.25off | 480+620 | 1on 1off | 350+440 | 0.1on 0.1off |
| 38 | Type4 | 400 | 0.25on 0.25 off | 400 | 1on 1off | 400 | 0.1on 0.1off |
| 39 | Belgium | 425 | 0.167on 0.167 off | 425 | 1on 1off | 425 | 0.1on 0.1off |
| 40 | Type5 | 400 | 0.25on 0.25 off | 400 | 1on 1off | 350+440 | 0.1on 0.1off |

| CPTG Type | Country | Feature / Programming / Prompt Tone | | Routing Tone | | IntrusionTone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 1 | Type1 | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 440 | 0.1on 2.9off |
| 2 | Type2 | 400 | 1.5on 0.1off | 400 | 0.1on 1.9off | 400 | 0.2on 4.8off |
| 3 | Type3 | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 440 | 0.1on 2.9off |
| 4 | Argentina | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 5 | Australia | 425*25 | 0.1on 0.9off | 425*25 | 0.1on 1.9off | 425 | Continuous |
| 6 | Brazil | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 7 | Canada | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 480+620 | 0.5on 0.5off |
| 8 | China | 450 | 0.1on 0.9off | 450 | 0.1on 1.9off | 450 | 0.2on 0.2off 0.2on 0.6off |
| 9 | Egypt | 425*50 | 0.1on 0.9off | 425*50 | 0.1on 1.9off | 450 | 0.5on 0.5off |
| 10 | France | 440 | 0.1on 0.9off | 440 | 0.1on 1.9off | 440 | 0.1on 2.9off |
| 11 | Germany | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 12 | Greece | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.15on 0.25off 0.15on 1.45off |
| 13 | India | 400*25 | 0.1on 0.9off | 400*25 | 0.1on 1.9off | 400 | 0.15on 4.85off |
| 14 | Indonesia | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 15 | Iran | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 16 | Iraq | 400 | 0.1on 0.9off | 400 | 0.1on 1.9off | 400 | 0.1on 2.9off |

| CPTG Type | Country | Feature / Programming / Prompt Tone | | Routing Tone | | IntrusionTone | |
|---|---|---|---|---|---|---|---|
| | | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) | Freq.(Hz) | Cadence (Seconds) |
| 17 | Israel | 400 | 0.1on 0.9off | 400 | 0.1on 1.9off | 400 | 0.1on 2.9off |
| 18 | Italy | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 19 | Japan | 400 | 0.1on 0.9off | 400 | 0.1on 1.9off | 400*25 | 0.1on 2.9off |
| 20 | Kenya | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 21 | Korea | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 350+440 | 0.1on 2.9off |
| 22 | Malaysia | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 23 | Mexico | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 24 | New Zealand | 400 | 0.1on 0.9off | 400 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 25 | Phillippines | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 440 | 0.1on 2.9off |
| 26 | Poland | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 27 | Portugal | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.2on 1.4off |
| 28 | Russia | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 29 | Saudi Arabia | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 30 | Singapore | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.25on 2.0off |
| 31 | South Africa | 400*33 | 0.1on 0.9off | 400*33 | 0.1on 1.9off | 400 | 0.15on 0.25off 0.15on 1.45off |
| 32 | Spain | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 425 | 0.1on 2.9off |
| 33 | Thailand | 400*50 | 0.1on 0.9off | 400*50 | 0.1on 1.9off | 400 | 0.1on 2.9off |
| 34 | Turkey | 450 | 0.1on 0.9off | 450 | 0.1on 1.9off | 450 | 0.1on 2.9off |
| 35 | UAE | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 350+440 | 0.1on 2.9off |
| 36 | UK | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 400 | 0.2on 4.8off |
| 37 | USA | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 480+620 | 0.5on 0.5off |
| 38 | Type4 | 400 | 1.75on 0.1off | 400 | 0.1on 1.9off | 400 | 0.2on 0.2off 0.2on 2.5off |
| 39 | Belgium | 425 | 0.1on 0.9off | 425 | 0.1on 1.9off | 440 | 0.1on 2.9off |
| 40 | Type5 | 350+440 | 0.1on 0.9off | 350+440 | 0.1on 1.9off | 350+440 | 0.5on 0.5off 1.0on 5.0off |

# Product Specifications

## Port Description

| Description | Application | Qty. |
|---|---|---|
| Maximum SIP Trunks | To connect to Internet Network for VoIP | 9 |
| Maximum Mobile Ports | GSM/UMTS Network Connectivity | 8 |
| Antenna Port | Antenna Connection | 2 |
| LAN Port | Computer Connectivity | 1 |
| WAN Port | VoIP Connectivity | 1 |

## Different Configurations supported in the SETU VG

| Sr. No. | Configuration | VoIP Channels | SIP Trunks | WAN Port | LAN Port | Mobile Ports |
|---|---|---|---|---|---|---|
| 1 | SETU VG4 | 8 | 9 | 1 | 1 | 4 |
| 2 | SETU VG8 | 12 | 9 | 1 | 1 | 8 |

## GSM Parameters

| | 2G | 3G |
|---|---|---|
| GSM Frequency Band | GSM: 850/900/1800/1900 | GSM: 850/900/1800/1900<br>UMTS: 800/850/900/1900/2100 |
| SIM Card | One SIM per GSM Port | One SIM per GSM Port |
| SIM Interface | 1.8V, 3V | 1.8V, 3V |
| Transmission Power | Class 4 (2W) at EGSM900 and GSM850 MHz band<br>Class 1 (1W) at DCS1800 and PCS1900 MHz band | Class 4 (33dBm±2dB) for GSM850 and EGSM900<br>Class 1 (30dBm±2dB) for DCS1800 and PCS1900<br>Class E2 (27dBm±3dB) for GSM850 and EGSM900 8-PSK<br>Class E2 (26dBm+3/-4dB) for DCS1800 and PCS1900 8-PSK<br>Class 3 (24dBm+1/-3dB) for UMTS800/850/900/1900/2100 |

## Antenna

| | 2G | 3G |
|---|---|---|
| Type of Antenna | One Antenna per 4 GSM Ports, Fixed Omni Directional Swivel Antenna | One Antenna per 4 GSM Ports, Fixed Omni Directional Swivel Antenna |
| Antenna Gain | 1.8dBi | 2.0dBi |
| Antenna Connector | SMA (Male), 50Ω Impedance | SMA (Male), 50Ω Impedance |

## VoIP Parameters

| | |
|---|---|
| Connector | RJ45 |
| VoIP Protocols | SIP v2, SDP, RTP (RFC 2833), SRTP |
| Network Protocols | IPv4, TCP, UDP, DHCP, PPPoE, SNTP, NAT, STUN, HTTP, TLS, DynDNS |
| SIP | 9 SIP Trunks with Out Bound Proxy Support |
| NAT | STUN and NAT Keep Alive |
| Voice Codec's | G.711 (a-Law and mu-Law), G.729, G.723, GSM FR |
| Line Echo Cancellation | G.168 with 128ms Tail Length |
| Call Progress Tones | Dial Tone, Ring Back Tone, Busy Tone, Error Tone |
| Voice | Dynamic Jitter Buffer (Adaptive), Comfort Noise Generation and Voice Activity Detection |
| Fax | T.38(UDPTL), T.38(RTP) and Pass Through |
| Quality of Service | Layer 3 Diffserv and TOS |
| Data Network | 2 Ports Auto MDIX 10/100 Base-T (RJ-45) |
| Security | Password Protected Administration |

## Time Settings

Synchronizing with specific Time Server

## Provisioning, Administration and Maintenance

- Auto Firmware and Configuration Upgrade
- Programmable using Web Jeeves

## LED Indication (Total 10 LEDs)

- Power = 1
- Status = 1
- Port = 8

## Packing

- **Dimension (W x H x D):** 231 x 162.5 x 55 mm
- **Unit Weight:** 720 Gms
- **Shipping Weight:** 1.60 Kgs
- **Mounting:** Wall Mounting and Table-Top

## Power Supply

- **External Adaptor:** 12V DC @ 2A
- **Power Consumption:** 15W Typical
- **Connector:** DC Power Jack

## Environmental

- **Operating Temperature:** 0°C to 45°C
- **Storage Temperature:** -20°C to 70°C
- **Operating Humidity:** 5-95% RH (Non-Condensing)
- **Storage Humidity:** Max. 0-95% RH (Non-Condensing)

# Warranty Statement

Matrix warrants that its products will be free from defects in material and workmanship, under normal use and service for a period of twelve (12) months from the date of installation.

Matrix warranties the replacement or repair of any product or component(s) found to be defective during the applicable period and return the same, or grant a reimbursement credit with respect to the product or component. Parts repaired or replaced will be under warranty throughout the remainder of the original warranty period only. In case of software program design defect(s) that prevents the program from performing the specified functionality, affecting service and beneficial use of the product, Matrix reserves the right to incorporate solutions in its new release of the software and make it available to the customer within a reasonable period of time. The above said with regard to the software design defect, constitutes the sole obligation of Matrix and its authorized installer with respect to the product.

Matrix does not, however, affirm or stand for that the functions or features contained in the system will satisfy its end-user's particular purpose and /or requirements or that the operation of the program will be uninterrupted or error free.

This warranty is voidable by Matrix:

1. If the product is used other than under normal use and is not properly serviced and maintained by qualified technicians.
2. If the product is not maintained under proper environmental conditions.
3. If the product is subjected to abuse, damage, misuse, neglect, fire, power flow, acts of God, accident.
4. If the product is installed or used in combination or in assembly with the products that are not supplied or authorized by Matrix or are of inferior quality or design than Matrix supplied products, which may cause reduction or degradation in functionality.
5. If the product is operated outside the product's specifications or used without designated protections.
6. If the completely filled warranty cards have not been received by Matrix within 15 days of the installation.

In no event will Matrix be liable for any damages, including lost profits, lost business, lost savings, downtime or delay, labor, repair or material cost, injury to person, property or other incidental or consequential damages arising out of use of or inability to use such product, even if Matrix has been advised of the possibility of such damages or losses or for any claim by any other party.

Except for the obligations specifically set forth in this Warranty Policy Statement, in no event shall Matrix be liable for any direct, indirect, special, incidental or consequential damages, whether based on contract or any other legal theory, and where advised of the possibility of such damages.

Neither Matrix nor any of its channel partners makes any other warranty of any kind, whether expressed or implied, with respect to Matrix products. Matrix and its distributors, dealers or sub-dealers specifically disclaim the implied warranties of merchantability and fitness for a particular purpose.

This warranty is not transferable and applies only to the original user of the Product. All legal course of action subjected to Vadodara (Gujarat, India) jurisdiction only.

# Disposal of Products/Components after End-Of-Life

**Main components of Matrix products are given below:**

- **Soldered Boards:** At the end-of-life of the product, the soldered boards must be disposed through e-waste recyclers. If there is any legal obligation for disposal, you must check with the local authorities to locate approved e-waste recyclers in your area. It is recommended not to dispose-off soldered boards along with other waste or municipal solid waste.

- **Batteries:** At the end-of-life of the product, batteries must be disposed through battery recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved batteries recyclers in your area. It is recommended not to dispose off batteries along with other waste or municipal solid waste.

- **Metal Components:** At the end-of-life of the product, Metal Components like Aluminum or MS enclosures and copper cables may be retained for some other suitable use or it may be given away as scrap to metal industries.

- **Plastic Components:** At the end-of-life of the product, plastic components must be disposed through plastic recyclers. If there is any legal obligation for disposal, you may check with local authorities to locate approved plastic recyclers in your area.

After end-of-life of the Matrix products, if you are unable to dispose-off the products or unable to locate e-waste recyclers, you may return the products to Matrix Return Material Authorization (RMA) department.

Make sure these are returned with:
- proper documentation and RMA number
- proper packing
- pre-payment of the freight and logistic costs.

Such products will be disposed-off by Matrix.

**“SAVE ENVIRONMENT SAVE EARTH”**

# E-Waste Management and Handling Rules

E-waste is a popular, informal name for electronic products nearing the end of their useful life. E-wastes are considered dangerous, as certain components of some electronic products contain materials that are hazardous, depending on their condition and density. The hazardous content of these materials pose a threat to human health and environment. Discarded electronics products such as circuit boards, batteries, wires and other electronic accessories if improperly disposed can leach lead and other substances into soil and groundwater. Many of electronic products can be reused, refurbished or recycled in an environmentally sound manner so that they are less harmful to the ecosystem.

## Benefits of E-waste Recycling leach

**Electronics Recycling Conserves Natural Resources**

There are many materials that can be recovered from old electronic products. These materials can be used to make new products, thus reducing the need for the new raw materials. For instance, various metals can be recovered from circuit boards and other electronics can be recycled.

**Electronics Recycling Supports the Community**

Donating your old electronics plays an important role in the provision of refurbished products which can be of great help to certain industries, small organizations and non-profitable organizations. It also helps individuals gain access to technology that they could not have otherwise afforded.

**Electronics Recycling Creates Employment Locally**

Considering that around 90 percent of electronic equipment is recyclable, electronics recycling can play a significant role in creating employment. This is because new firms dealing with electronics recycling will form and existing firms will look to employ more people to recover recyclable materials. This can be triggered by the increase in the demand for electronics recycling.

**Electronics Recycling Helps Protect Public Health and the Environment**

Many electronics have toxic or hazardous materials such as mercury and lead, which can be harmful to the environment if disposed in trashcans. Reusing and recycling electronics safely helps in keeping the hazardous materials from harming humans or the environment. For example, certain electronic components and batteries are hazardous since they have lead in them. Printed circuit boards contain harmful materials such as cadmium, lead, mercury and chromium.

Instead of keeping old electronics or dumping them in landfills, recycling or reusing them is an appropriate option that should be supported by individuals and organizations. Considering the benefits of electronics recycling, it is very important that people in various parts around the world embrace this concept.

**Creates Jobs**

E-waste recycling creates new jobs for professional recyclers and creates a second market for the recycled materials.

## Do's & Don'ts

Do's:

- Always look for information on the catalogue with your product for end-of-life equipment handling.
- Ensure that only Authorized Recyclers/Dismantler handle your electronic products.
- Always call at our toll-free No's to Dispose products that have reached end-of life.
- Always drop your used electronic products, batteries or any accessories, when they reach the end of their life at your nearest Authorized E-Waste Collection Points.
- Always disconnect the battery from product and ensure any glass surface is protected against breakage.

Don'ts:

- Do not dismantle your electronic Products on your own.
- Do not throw electronics in bins having "Do not Dispose" sign.
- Do not give e-waste to informal and unorganized sectors like Local Scrap Dealer/ Rag Pickers.
- Do not dispose your product in garbage bins along with municipal waste that ultimately reaches landfills.

## E-Waste Management Plan

**M/s. MATRIX COMSEC PVT LTD** has partnered with **E-Waste Recyclers India (EWRI)** to comply with the new India E-Waste management and handling rules in providing drop-of centers and environmentally sound management of end of life electronics.

EWRI has obtained authorizations from the appropriate governmental agency for their processing facilities. EWRI will receive and recycle customer returned equipment, including all the e-waste. Customers can drop their e-waste in the drop-box provided at various collection centers of EWRI.

A list of collection centers along with the address is mentioned below.

The customers can also call on the following toll free number (1800-102-5679) from Monday to Friday between 10:00 AM to 5:30 PM to get details about the collection centers.

## Collection Centers:

| State/ City | Location | Logistic | Address | Toll-Free Number |
|---|---|---|---|---|
| Delhi | Rangpuri | Professional Logistics | Rangpuri, Milakpur Kohi Rangpuri, Rangpuri, New Delhi - 110037 | 1800-102-5679 |
| Gurugram | Gurugram | Professional Logistics | 295, LIG Colony, Sector 31, Gurugram, Haryana - 122022 | 1800-102-5679 |
| Jharkhand | Dhanbad | Professional Logistics | Sardar Patel Nagar, Dhanbad, Jharkhand - 826004 | 1800-102-5679 |
| Noida | Salarpur Khadar | Professional Logistics | 2, Gejha Rd, Goyal Colony, Salarpur Khadar, Sector 102, Noida, Uttar Pradesh - 201304 | 1800-102-5679 |
| Mumbai | Vashi | Professional Logistics | Plot-92,gala no 01,Sector 19C Vashi Navi, Mumbai - 400705 | 1800-102-5679 |

| State/ City | Location | Logistic | Address | Toll-Free Number |
|---|---|---|---|---|
| Pune | Vallabh Nagar | Professional Logistics | No.3/20,Near Ashok Sah Bank, Vallabh Nagar, S.T.Stand Road, Pimpri, Pune - 302021 | 1800-102-5679 |
| Odisha | Cuttack | Professional Logistics | Cuttack, Odisha | 1800-102-5679 |
| Hyderabad | Secunderabad | Professional Logistics | 4,Block-3,4th Shatter at 179, MPR Estates Near Old Check Post Old Bowaenpally Secunderabad, Hyderabad - 500011 | 1800-102-5679 |
| Bangalore | Yeshwanthpur | Professional Logistics | No.44 1st floor 2nd main D.D.U.T.T.L. Yeshwanthpur, Bangalore - 560022 | 1800-102-5679 |
| Mangalore | Bhathery Road Boloor | Professional Logistics | Opp. Hindustan Lever Ltd, Sulthan, Bhathery Road Boloor, Mangalore (KA) - 575003 | 1800-102-5679 |
| Jharkhand | Ranchi | Professional Logistics | Ranchi, Jharkhand | 1800-102-5679 |
| Chennai | Sennerkuppam | Professional Logistics | 27,Sakthi Nagar Phase-II, Sennerkuppam, Near Bisleri Water Plant, Chennai - 600056 | 1800-102-5679 |
| Rajasthan | Jaipur | Professional Logistics | A-81, 200 ft. By Pass, Heerapura, Jaipur, Rajasthan - 302021 | 1800-102-5679 |
| Bokaro | Odisha | Professional Logistics | Cuttack, Odisha, India | 1800-102-5679 |
| Guwahati | Kundil | Professional Logistics | HN-34, Kundil Nagar Basistha Chariali, Near Parbhat Apartment, Guwahati - 781029 | 1800-102-5679 |
| Lucknow | Kanpur Road | Professional Logistics | S-175,Ist Floor Transport Nagar Near RTO Kanpur Road Lucknow - 226004 | 1800-102-5679 |
| Madhya Pradesh | Indore | Professional Logistics | 284 AS-3 Scheme No.-78,Vijay Nagar, Indore, Madhya Pradesh | 1800-102-5679 |
| Ahmedabad | Pushp Penament | Professional Logistics | Shop No D-18, Pushp Penament, Behind Mony Hotel, Isanpur, Ahmedabad | 1800-102-5679 |
| Patna | Malyanil buddha | Professional Logistics | Dr. A.K Pandey (IPS) Malyanil buddha Colony, Patna (Bihar) - 800001 | 1800-102-5679 |
| Andhra Pradesh | Vishakapatnam | Professional Logistics | Shop No.8, New Gajuwaka, Opp. High School Road, Vishakapatnam, Andhra Pradesh - 530026 | 1800-102-5679 |
| Chandigarh | Pharbhat Road | Professional Logistics | Shop no:-19, Pharbhat Road, Opp:- Tennis Academy, Zirakpur, Chandigarh, Punjab | 1800-102-5679 |

| State/ City | Location | Logistic | Address | Toll-Free Number |
|---|---|---|---|---|
| Kolkata | B.T. ROAD DUNLOP | Professional Logistics | 156A/73, Northern Park, B.T. Road Dunlop, Kolkata -700108 | 1800-102-5679 |
| Odisha | Bhubaneswar | Professional Logistics | Acharya Vihar - jaydev Vihar Rd, Bhubaneswar, Odisha | 1800-102-5679 |
| West Bengal | Asansol | Professional Logistics | Shop No-4 Asansol Station Bus Stand Road, Munshi Bazar, Asansol, West Bengal - 713301 | 1800-102-5679 |

# Regulatory Information

## Federal Communications Commission Statement

### Part 15: Class B Information

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

# CE and ROHS Certificate

MATRIX
TELECOM | SECURITY

## Declaration of Conformity

| | |
|---|---|
| Manufacturer's Name: | Matrix Comsec Pvt. Ltd. |
| Manufacturer's Address : | 15 &19-GIDC, Waghodia,<br>Dist: Vadodara 391760<br>Gujarat, India |
| Declares that the product/s<br>Product: | Multi-Port VoIP to GSM Gateway |
| Model Type: | SETU VG |
| Variants/Type: | SETU VG4 & SETU VG8 |
| Trade Name: | MATRIX |
| Product Options: | This declaration covers all options of the above product, conforms to the following product specifications: |

**EMI/EMC Standards:**

EN 55022 : 2010 + AC:2011
EN 61000-3-2 : 2014 (Edition 4.0)
EN 61000-3-3 : 2013 (Edition 3.0)
EN 55024 : 2010 (Edition 3.0)
IEC 61000-4-2 : 2008 (Edition 2.0)
IEC 61000-4-3 : 2010 (Edition 3.0)
IEC 61000-4-4 : 2012 (Edition 3.0)
IEC 61000-4-5 : 2014 (Edition 3.0)
IEC 61000-4-6 : 2013 (Edition 4.0)
IEC 61000-4-8 : 2009 (Edition 2.0)
IEC 61000-4-11 : 2004 (Edition 2.0)

**SAFETY Standard:**

IEC 60950-1 : 2005 (2nd Edition) + A1:2009 + A2:2013

Supplementary Informations:
The Product herewith complies with the following directives :

| | |
|---|---|
| EMC | 2014/30/EU |
| Low Voltage Directive | 2014/35/EU |
| RoHS Recast (RoHS 2) | 2011/65/EU (as per standard EN 50581:2012) |

**Mr. Ganesh Jivani**
**Director**
Date: 17.07.2017

Matrix Comsec Pvt. Ltd. MATRIX Vadodara

CE

**MATRIX COMSEC PVT. LTD.**
**Registered/Head Office:** 394-GIDC, Makarpura, Vadodara-390 010, India. Ph: +91 265 2630555, Email: Inquiry@MatrixComSec.com • www.MatrixComSec.com
**Manufacturing Unit:** 15 & 19-GIDC, Waghodia, Dist. Vadodara-391 760, India. Ph: +91 2668 263172/73 • **CIN:** U72200GJ1998PTC034047

# Open Source Licensing Terms and Condition

- The firmware of this product also includes some of the Open-Source software released under GNU General Public License (GPL) Version 2 and SNMP License. Terms of these licenses are printed in full below.

- The source of the open source software used in this product is available on CD, upon written request from:
  R&D Team
  Matrix Comsec Pvt Ltd
  394, Makarpura GIDC,
  Vadodara - 390 010
  Gujarat
  India.
  Customer shall bear the shipping and handling charges.

## GPL Version 2

```
  GNU GENERAL PUBLIC LICENSE
       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.,
 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

    Preamble

  The licenses for most software are designed to take away your
freedom to share and change it.  By contrast, the GNU General Public
License is intended to guarantee your freedom to share and change free
software--to make sure the software is free for all its users.  This
General Public License applies to most of the Free Software
Foundation's software and to any other program whose authors commit to
using it.  (Some other Free Software Foundation software is covered by
the GNU Lesser General Public License instead.)  You can apply it to
your programs, too.

  When we speak of free software, we are referring to freedom, not
price.  Our General Public Licenses are designed to make sure that you
have the freedom to distribute copies of free software (and charge for
this service if you wish), that you receive source code or can get it
if you want it, that you can change the software or use pieces of it
in new free programs; and that you know you can do these things.

  To protect your rights, we need to make restrictions that forbid
anyone to deny you these rights or to ask you to surrender the rights.
These restrictions translate to certain responsibilities for you if you
distribute copies of the software, or if you modify it.

  For example, if you distribute copies of such a program, whether
gratis or for a fee, you must give the recipients all the rights that
```

you have.  You must make sure that they, too, receive or can get the source code.  And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software.  If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents.  We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary.  To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License.  The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language.  (Hereinafter, translation is included without limitation in the term "modification".)  Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope.  The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and

you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to

this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,

```
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License along
    with this program; if not, write to the Free Software Foundation, Inc.,
    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts
of the General Public License.  Of course, the commands you use may be called
something other than `show w' and `show c'; they could even be mouse-clicks or
menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary.  Here is a sample; alter the names:

 Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.
```

## The SNMP License

```
Various copyrights apply to this package, listed in various separate
parts below.  Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

       Copyright 1989, 1991, 1992 by Carnegie Mellon University

  Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

 All Rights Reserved
```

Permission to use, copy, modify and distribute this software and its
documentation for any purpose and without fee is hereby granted,
provided that the above copyright notice appears in all copies and
that both that copyright notice and this permission notice appear in
supporting documentation, and that the name of CMU and The Regents of
the University of California not be used in advertising or publicity
pertaining to distribution of the software without specific written
permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL
WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS.  IN NO EVENT SHALL CMU OR
THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL,
INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING
FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF
CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN
CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the
  names of its contributors may be used to endorse or promote
  products derived from this software without specific prior written
  permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS
IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
  notice, this list of conditions and the following disclaimer in the
  documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or
  promote products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY
EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT HOLDER BE
LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright B) 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,
California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered
trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
    this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright
    notice, this list of conditions and the following disclaimer in the
    documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the
    names of its contributors may be used to endorse or promote

products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003
oss@fabasoft.com
Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR

BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----
Copyright (c) 2009, ScienceLogic, LLC
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived

# Index


**MATRIX COMSEC**

**Head Office**
394-GIDC, Makarpura, Vadodara - 390010, India.
Ph: (+91)1800-258-7747
E-mail: Customer.Care@MatrixComSec.com

www.MatrixTeleSol.com

*Version 1, August 2019*