



HipLink[®] Software Installation and Administration Guide

HipLink® Software Installation and Administration Guide

HipLink Software Copyright

The *HipLink Software Installation and Administration Guide* is for use by Licensed Users only. This document contains proprietary information owned by HipLink Software and is protected by copyright law and international treaties. It may not be copied, published or used, in whole or in part, for any purposes other than as expressly authorized by HipLink Software. Any unauthorized copying, distribution or disclosure of information in any manner without the prior written consent of HipLink Software is a violation of copyright laws and will be prosecuted to the maximum extent possible under law.

Trademarks and Copyright

- HipLink® is a registered trademark of Semotus, Inc., DBA HipLink Software.
- Apache® is a registered trademark of Apache Software Foundation.
- ©Minicom: Copyright 1991, 1992, 1993, 1994, 1995, 1996. Miquel van Smoorenburg.
- All other trademarks and copyrights are the property of their respective owners.

Disclaimer

HipLink Software has made every effort to ensure the accuracy of information contained within this document. However, HipLink Software makes no warranties with respect to this document and disclaims any implied warranties of merchantability or fitness for a particular purpose. All screen images used in this document are for illustrative purposes and are only intended to provide an example of the screen. Screens may vary dependent upon the service provided. Information in this document is subject to change without notice.

Please carefully read the instructions provided in this guide before installing and administering HipLink Software. Retain these instructions for future use. If you do not agree with the terms of this license agreement, do not install, copy, or use this software.

For technical assistance, contact HipLink Technical Support:

Phone: 408-399-0001

Email: support@hiplink.com

HipLink Software Offices
718 University Ave, Suite 110
Los Gatos, California 95032
Tel: (408) 399-6120
Fax: (408) 395-5404
Web: www.hiplink.com

Table of Contents

Welcome to HipLink	7
Customer Support	7
About this Guide	7
HipLink Terminology	7
HipLink Software Installation	9
Windows Installation	9
Installing HipLink	10
Installation Scenarios.....	10
Installation Steps	10
Troubleshooting.....	12
Verifying Installation	13
Upgrading HipLink.....	13
Uninstalling HipLink.....	13
UNIX Installation	14
Installation Steps for UNIX.....	15
HTTP Secure Mode.....	17
Verifying Installation	17
Startup Scripts	17
Location.....	18
Script Names	18
Permissions.....	18
Uninstalling HipLink	18
Upgrading HipLink	20
CLI Installation	20
HipLink Fax Module Installation	21
Prerequisites	21
Installation Steps	21
Verifying Installation	22
HipLink Voice Module Installation	23
Prerequisites	23
Installation Steps	23
Installing the HipLink Voice Service.....	25
Upgrade Steps.....	27
HipLink Installation for IIS 7 Guide	29
Upgrading from HipLink 4.6 and earlier	35
HipLink Installation for IIS on Windows Server 2008	35
Pre-Installation Steps.....	36
Post-Installation Steps	41
Basic System Configuration	45
Initial Log in	45
Change Password	45
Enter License Key	45
Directory Settings	45
Multiple Queues.....	47
Define Departments.....	48
Department Members	48

Department Guests.....	48
Editing Department Members	49
Departments Panel	49
User Group Permissions.....	51
Default User Groups	52
Department Permission Settings.....	53
User Group Permission Settings.....	54
Create Login Users.....	55
Define Messengers.....	58
Standard Protocols – SNPP ~ WCTP ~ SMTP.....	59
DTMF & TDD/TTY Protocol	60
GSM Protocol	61
Facebook Protocol.....	62
HNP Protocol.....	63
OAI Protocol	63
SMPP Protocol	64
TAP Dial-Up Protocol.....	64
TAP-Leased Protocol.....	64
Twitter Protocol.....	65
UCP/Dial-Up Protocol	65
XMPP Protocol	65
Create Carriers.....	66
BES Carrier	69
CAP Carrier	69
DTMF & TDD/TTY Carrier.....	70
Facebook Carrier and Receiver Set-up.....	70
Generic Delivery Protocol	78
GSM Carrier.....	79
HNP Carrier	79
HTTP Carrier	80
MHTTP Carrier	81
OAI Carrier	82
SMPP Carrier.....	83
SMTP Carrier.....	83
SNPP Carrier.....	84
TAP Dial-Up Carrier.....	84
TAP-Leased Carrier.....	85
Twitter Carrier and Receiver Setup.....	85
UCP/Dial-Up Carrier	96
UCP/TCP Carrier	96
VOIP Carrier	97
WCTP Carrier	98
WAP Carrier.....	98
XMPP Carrier.....	99
Automatic Carrier Update.....	100
Receivers - Create and Manage.....	105
Add a Receiver	106
Modify a Receiver	110
Change Device Status	111
Delete a Receiver(s)	111
Receiver Schedule.....	111

System Attendant Configuration	113
Global Settings Configuration	115
Display Settings	117
Common Settings	118
Message Sending	118
Receiver	118
Recipient User	119
Department Settings	120
Report Export Settings	120
Cleanup Settings	120
Session Settings	121
Email Server Settings	121
HTTP Proxy Settings	122
Redundancy Settings	122
Automatic User Disable Settings	122
Message Campaign Settings	124
Other Settings	124
Starting HipLink and Services Menu	124
Advanced Configuration & Administration Tools	127
Session Manager	127
Advanced Messaging Module	127
Blackberry App Setup	128
Control Panel	128
HNP Manager	132
Activation	135
Groups	137
Broadcast Groups	137
On-Duty Groups	141
Escalation Groups	151
Rotate Groups	156
Follow-Me Groups	158
Viewing Group Parent & Members	169
Queue Panel	172
Queue Main Panel	172
To Sort Queue Grid	174
To Filter Queue Grid	174
To Personalize Queue Grid	174
Default Queue	175
Escalation Queue	175
Scheduled Queue	175
Failed Queue	175
Completed Queue	176
Fax Queue	176
Voice Queue	176
Logs Setting Panel	176
Filter Logs	178
Edit Logs	178
Export Logs	178
Change Logging Level	178
Delete Logs	179

Archive Logs.....	179
Upgrade Panel.....	180
Time Zone	180
ODBC Conversion and Configuration	181
DB Configuration	181
Enhanced LDAP configuration.....	182
Single Sign-on Configuration Guide.....	184
Filters	192
Feedback Action Panel.....	193
Dial-Up Modem Settings.....	193
Export/Import Utility	194
Backup Service	211
Set the Backup Service parameters.....	211
Restore from a Backup	211
Special Module Configuration.....	212
HipLink Fax Module	212
HipLink Voice Module	214

Welcome to HipLink

Welcome! And thank you for your interest in HipLink Software. HipLink is a wireless messaging software solution that is about to change the way you communicate. We hope you'll enjoy using HipLink.

Customer Support

HipLink provides installation assistance and technical support for HipLink Software. This assistance is intended to get you up and running with the HipLink messaging system as quickly and easily as possible. HipLink Technical Support will answer any questions you may have before the installation process is initiated as well as any questions regarding post installation issues.

We welcome your suggestions on how we can improve the HipLink product and want to hear about any problems you may experience.

Contact HipLink Technical Support:

Phone: 408-399-0001

Email: support@hiplink.com

About this Guide

This guide is organized to walk you through the process of Installing and Administering the HipLink messaging system with ease. Toward that goal, let's take a glance at each section to help you get acclimated.

The Installation section will help you to plan your installation process. It details separately the Windows and the UNIX installation processes. For each platform, it specifies the system requirements and the prerequisite steps to perform before starting the installation. Then it guides you through the installation steps and shows you how to verify if the installation was successfully completed. Uninstalling and upgrading HipLink topics are addressed in separate sections.

The Administration section will guide you through the configuration steps, providing you with examples of how to customize the settings, and help you get started using HipLink. The differences between Windows and UNIX administration are highlighted where necessary. Please refer to the *HipLink User Guide* for more details about HipLink.

HipLink Terminology

The main functionality of HipLink is to enable Users to send messages to Receivers registered with different Carriers. Each Carrier has one protocol assigned to it. In order to perform its tasks, HipLink uses a System Attendant, a Scheduler, and one or more Messengers. The number of Users, Receivers, and Messengers, type of protocols, and other features are defined by the License Key.

User	Initiates the message(s) or action(s). Each User must belong to a User Group and inherits
-------------	---

	the User Group permissions.
Receiver	<p>The receiver is a device or system that receives a message. This can be a pager, smartphone, computer, fax, an automated alarm or signage, an iPod, or any other device. Any number of Receivers may receive a message, notification, alarm or signal. Each Receiver is assigned to one Carrier.</p> <p>Receivers can be one-way or two-way. A two-way Receiver can respond to a message. The response is retrieved by HipLink and it can be used to trigger a predefined Response Action. The Response Action might be a command to be executed on the HipLink server.</p>
Carrier	Carrier is the service provider that is assigned to a device. Examples of Carriers include AT&T, Sprint, T-Mobile, Verizon, American Messaging, or Cook Paging.
Groups	<p>Groups are used to organize Receivers in HipLink. The Group that a User belongs to designates the permissions for messages to be sent to that Receiver. Receivers can be assigned to simple groups (i.e., Receiver Groups), task oriented groups (i.e., On-Duty Groups, Escalation Groups, Rotate Groups, and Follow-Me Groups), and logical groups (i.e., Departments). All types of Groups can contain other Groups as Members.</p> <ul style="list-style-type: none"> ▪ On-Duty Groups designate the working schedule for each Receiver and messages are sent only to the on-duty Receivers. ▪ Escalation Groups designate Receivers that will get a message one at a time, after a specified delay. The escalation continues if the message confirmation is not received in time and is stopped once the message is acknowledged. ▪ Rotate Groups allow you to send messages to different Receivers in a rotation. ▪ Follow-Me Groups allow you to send messages to different Receivers depending on the time of day. ▪ Departments designate what access Users have to certain Receivers and Groups.
Messenger	A Messenger takes messages from a queue and sends them to Carriers using specific protocols. Each Messenger has one protocol assigned to it. Messengers are services that handle the send message requests. A messenger will check the paging queue for message files, select only those messages that require its protocol, and use it to deliver the message to the Carrier.
System Attendant	The Attendant is a background process within HipLink Software that monitors HipLink Services.

All of the following entities must be configured in a specific order before using HipLink: Users, User Groups, Receivers, Receiver Groups, On-Duty Groups, Escalation Groups, Rotate Groups, Follow-Me Groups, Departments, Response Actions, Carriers, Messengers, and the System Attendant.

The sequence of necessary steps is detailed in the Configure HipLink section of this document. The starting procedure is detailed in the Configure HipLink section.

HipLink Software Installation

While installing HipLink is a straightforward process, it can take some time, patience, and knowledge of your hardware components. Thus, taking some time prior to starting the installation can make things go much more smoothly. The purpose of this section is to help you throughout these important first steps. If it is your first time using HipLink, please read through this entire document before attempting your installation.

The Installation process is different for Windows and for UNIX platforms. Please refer to the section that applies to your case.

Windows Installation

System Requirements

The following components are required to install the HipLink software:

Platforms Supported by HipLink:

- Windows XP Professional
- Windows 2003 Server
- Windows 2008 Server
- Windows 7

Minimum Hardware Requirements

- Intel compatible Dual Core 2.0 GHz or higher system.
- 4 GB of RAM
- High-speed HDD
- High-speed Internet connection (required for the Internet protocols)
- Serial port with modem and analog phone line (required for dial-up protocols)

Prerequisites You Should Perform Prior to Installing HipLink:

You must be either logged in as an administrator, or have administrator privileges for the machine on which you will install HipLink. In order to be able to send messages using HipLink, your machine should have either an Internet connection or modem (or both) installed.

During the HipLink set up, if Apache is selected as a Web server it will be installed on your machine. *If you choose IIS, then it has to be pre-installed separately before you begin your HipLink installation.* You must decide on which port this Web server will be running. The default value is 8000 for Apache and 80 for IIS. If there is any other Web server running on your machine on that port, you must use some other port of your choice (higher than 8000 or 80 recommended).

*The port must be changed in the Registry also; otherwise during future upgrades this will be lost. **Please consult with your IT department or systems administrator before changing the Registry entries in Windows as it could adversely affect the system.***

For IIS installation prerequisites please refer to the IIS Section
Exit all Windows programs before running the Installer.

Installing HipLink

Before you start, please make sure you have all of the resources you will need for the installation. If you have already read through the previous section, Prerequisites, and followed the instructions, you should be ready.

Installation Scenarios

You may choose one of the following installation scenarios:

Install the current HipLink version for the first time. You will need to select the destination folder where HipLink will be installed.

Reinstall the current HipLink version on the same machine. HipLink will be installed in the same folder and will use the same port number as the version that is already installed on your machine. If you want to change the HipLink folder, you must uninstall HipLink first.

Upgrade a previous version of HipLink to the current version. HipLink will be installed in the same folder and will use the same port number as the version that is already installed on your machine. If you want to change the HipLink folder, you must first uninstall HipLink. For more details on upgrading HipLink, please refer below.

Installation Steps

Note: It is strongly recommended that you exit all Windows programs before running the Setup program. If you have not done so yet, please make sure that you stop any existing Web server that is running on the machine on which you are installing HipLink.

How to install HipLink for the first time:

Run the HipLink Installer and please wait while the *InstallShield Wizard™* extracts the necessary files.

This may take a few moments.

The *InstallShield Wizard™* will help install HipLink on your computer. To continue, click Next.

Please read the License Agreement carefully. Press the Page Down key to see the rest of the agreement. Proceed with the installation only if you agree with the terms and conditions stated in the License Agreement. To install HipLink, you must accept this agreement and click Yes. If you do not agree with the terms, do not install the software. Choose No and the Setup will close.

Setup will install HipLink either in the default folder (i.e., C:\Program Files\HipLink Software\HipLink) or in a different folder of your choice. Click Browse and select another folder (i.e., D:\Applications\HipLink). You can choose not to install HipLink by clicking Cancel to exit.

At this step, you will select the HTTP Server that HipLink will use. Please select either Apache or IIS as your Web Server for HipLink and click Next to continue.

Web server settings for Apache. HipLink setup will install an Apache Web server on your computer.

Please enter the port number on which this Web server will be running. The default value is 8000. Make sure that the port you set is not being used by any other application.

Web server settings for IIS. HipLink setup will check if IIS is installed on your computer and then it will set up an IIS website. Please enter the Host value and the port number, on which this website will be running, leaving the host name empty to install it on the default website. The default port number is 80.

The install will set up and start the HipLink System Attendant service. Please enter the following data: administrator email address (e.g., johndoe@company.com), SMTP server address (e.g., mail.company.com), and domain name for the email gateway (e.g., gateway.company.com). All of these settings can be changed later using the HipLink GUI.

Setup has now enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying the files.

Setup Status. Please wait while the *InstallShield Wizard™* installs the necessary files and HipLink is performing the requested operations. This may take a few minutes. Your HipLink installation is complete. You have the option to launch the HipLink console now or later using the URL which is displayed on your screen. (Please remember this URL for future use.) You can also open and read the Read Me file.

Troubleshooting

Apache/IIS Web Server Fails to Start

If the Web server fails to start, it might be that the port number you specified is already being used by another application. Please verify. If in doubt, change the port number and try to start the Apache/IIS Web server manually from the Windows Control Panel Services console.

In order to display all connections and listening ports, use the netstat -a command from a Command Prompt window.

HipLink Does Not Run

It is possible that even though the port number is being used by another application the Apache/IIS Web server is able to start, but then HipLink is not able to run. In this case, verify again the port number and the applications that are running on your machine. If in doubt, stop the Apache/IIS Web server from the Windows Control Panel Services console, change the port number, and start the Apache/IIS service again. Then try to open HipLink.

Change the Port Number

You do not have to reinstall HipLink to change the port number.

Decide which port number you want to use and verify that it is not already used by another application by using the netstat -a command.

Stop the Apache/IIS Web server from the Windows Control Panel Services console.

Edit the file httpd.conf from the \$HipLink_path\Apache\conf directory, change the port number (e.g., replace in the example below Listen 8000 with the port number of your choice), and save the file.

Start the Apache Web server service again.

The httpd.conf file looks something like:

```
ServerRoot C:/Program Files/HipLink Software/HipLink/Apache/PidFile/logs/httpd.pid
```

```
Timeout 300
```

```
KeepAlive On
```

```
MaxKeepAliveRequests 100
```

```
KeepAliveTimeout 15
```

```
<IfModule mpm_winnt.c> ThreadsPerChild 250
```

```
MaxRequestsPerChild 0
```

```
</IfModule>
```

Listen 8000

Note: For more details about the Apache Web server, please refer to the readme.txt file located in the HipLink default folder.

Verifying Installation

You should try to connect to HipLink console URL from your workstation and log in as username admin with password admin. You should also verify the modems, connections, and phone lines.

Upgrading HipLink

If you are currently using a previous version of the HipLink messaging system, you should upgrade to the most recent version available with this installer. You can check the version of the installer by looking in the file properties in the Version tab. When you execute the installer, the current version is displayed on the main page.

Prerequisites

The upgrade process preserves existing configuration and license files.

Note: Upgrading from an older version to 4.X requires a new License Key. Please contact HipLink Technical Support to get your new License Key.

Data: It is advisable to save the existing data, in the event of failed upgrade we have to revert to the old version. Please contact HipLink support desk for steps on how to save the old version.

Upgrading Steps

The upgrade procedure starts out identically to the installation procedure.

Run the HipLink Installer. If the Installer detects an older version of HipLink installed on your machine, you will be directed to choose to upgrade or to uninstall. Select upgrade.

You can only upgrade HipLink at the location where HipLink is already installed on your machine. For example, if HipLink is installed at C:\Program Files\HipLink Software\HipLink\, then the Installer will not allow you to upgrade HipLink to a new location, e.g., D:\Applications\HipLink without uninstalling the old one first.

Uninstalling HipLink

In order to uninstall HipLink, you should either run the Add/Remove Programs application from the Windows Control Panel, or launch the HipLink installer and choose uninstall. The uninstall application will stop and delete all HipLink related services (i.e., the Messengers, System Attendant, Scheduler, Backup service, etc., and the Apache or IIS Web server).

Note: The HipLink Web entry is not deleted from the IIS server. You must delete it manually.

UNIX Installation

System Requirements

The following components are required to install the 4.X HipLink software:

Platforms Supported by HipLink:

- Solaris Sparc 10 or higher
- HP-UX 11.11, 12
- AIX 5.3 to 6
- Linux (Contact HipLink Support for current versions)

Minimum Hardware Requirements

- 4 GB of RAM
- 200 GB of free disk space
- Internet connection (required for the Internet protocols)
- Serial port with modem and analog phone line (required for dial-up protocols)

Prerequisites You Should Perform Prior to Installing HipLink:

You must be logged in as root on the machine on which you will install HipLink. In order to be able to send messages using HipLink, your machine should have either an Internet connection or modem (or both) installed and working.

During the HipLink setup, an Apache Web server will be installed on your machine. You must decide on which port this Web server will be running. The default value is 8000 for Apache. If there is another Web server running on your machine on that port, you must use a different port of your choice (higher than 8000 or 80 recommended).

You need to make sure that the User nobody and group nobody are created on the machine. The Apache Web server uses this account (User + Group) by default. On some platforms the User and group nobody can be nonexistent or removed. On HPUX, the account lp (i.e., line printer account) and the group Users are used instead.

If your HipLink Server has more than one network card (or more than one IP address assigned), you may need to check which IP address to use. The installer resolves the first IP address of the first network card on your server.

Download or copy the installation file HipLinkinstall.sh to the local directory on your UNIX box. The file can be downloaded from the Web or FTP sites.

Change the file permissions to make it executable: `chmod a+x HipLinkinstall.sh`

Installing HipLink on UNIX

Before you start, please make sure you have all of the resources you will need for the installation. If you have already read through the previous section, Prerequisites, and followed the instructions, you should be ready.

Installation Steps for UNIX

Answer all the questions prompted during the installation procedure. It is safe to accept the default values that are indicated with capital letters.

Execute the HipLink Shell script: `./HipLinkinstall.sh`

The installer displays the *End User License Agreement*. Press Enter to read it. The installer prompts: Do you accept all terms of this License Agreement? (Y/N).

Accept the terms by selecting Y to continue the installation, or decline the terms by selecting N which will abort the installation. You can abort the installation at any time by pressing Ctrl+C.

The installer will prompt you to enter the directory where HipLink will be installed. Please enter target directory [/usr/local/hiplink]:

The installer will create the target directory where it will extract the binary file. The installer will not install HipLink into an existing directory. The installer will check that the uncompressed file is OK. If the uncompressed file is corrupted, then the installation process is aborted.

Note that the most frequent reason for having a corrupted file is due to the fact that the installer was not downloaded in binary mode. Make sure that the installer is received in binary mode using the FTP protocol.

Next, the installer will prompt you for the port number (default 8000). The port number will identify the HTTP port for Apache Web server running on your HipLink server. If you do not know how to set it up, use the default value.

The installer prompts: Please enter port number: and after entering the port number, Are you sure you want to use this port? [Y/N]:

Note: This question is asked only if the port number is less than 1024 (i.e., the port numbers reserved by the operating system).

Answer Y and the HipLink installer will start to update the configuration files and set permissions for the executable files.

It will then attempt to start Apache and prompt you: Do you want to start Apache Web server now [Y/N]:

If you answer N, then you will have to start Apache later. If you answer Y, the installer will start Apache. If for some reason the attempt to start the server has failed, it will prompt you, Apache server is not running.

Then you will have the following option: Do you want to set up Apache Web server to start automatically when you reboot [Y/N]:

If you answer Y, then the installer will create startup files for the Apache server.

Example for Linux:

```
/etc/rc.d/rc3.d/S98hiplink_apache  
/etc/rc.d/init.d/hiplink_httpd
```

Example for Solaris:

```
/etc/rc3.d/S98hiplink_httpd  
/etc/init.d/hiplink_httpd
```

The RUNLEVEL (denoted by rc (some number)), depends on the run level and may be different on your system.

The startup scripts for the HipLink System Attendant and scheduler are automatically installed under the /sbin directory. Also, after messengers have been created using the GUI, these will be added in the /sbin directory tree. For example, on HP, the System Attendant startup script is installed in /sbin/init.d/hip_monitor. The file /sbin/rc3.d/S30hip_mon is a link to that script. For more details about startup scripts, see the following section.

Note: The directories for startup scripts may vary on different platforms.

At the end of the installation process, the installer will copy the queue files. If you upgrade from a previous version, it will convert the configuration files. You are now ready to run the HipLink console from your browser. If you have not started Apache, you will need to start it manually by executing: /usr/local/hiplink/apache/bin/apachectl start (This is the default installation directory)

At the end, the installer will display the URL of the HipLink console. For example: URL: http://192.168.39.251:8000. The installer creates a version file, installs the minicom application (useful to test your modems), and prompts, Do you want to view README now [Y/N]:

You can answer Y or N. The installation is finished.

Note: Despite its .sh extension, the installer is a binary file so binary mode has to be used if the FTP protocol is used for transferring the file.

HTTP Secure Mode

The Apache Web server shipped with HipLink can be used in secure mode. The HTTPS protocol enables higher security by using SSL certificates.

Note: SSL has to be configured and installed prior to this. The customer is responsible for purchasing and installing the SSL certificates.

- To start Apache Web server in HTTP mode, use the command:

```
/usr/local/hiplink/apache/bin/apachectl start (This is the default installation directory)
```

- To start Apache Web server in HTTPS mode use the command:

```
usr/local/hiplink/apache/bin/apachectl startssl (This is the default installation directory)
```

When started in HTTPS mode, the HTTP protocol is also supported.

Please note that when using HTTPS mode, the port designation changes. The HipLink URL is no longer `http://123.123.123.123:8000` but `https://123.123.123.123`.

The HTTPS protocol uses the port 443 by default, and it is not recommended to change it.

By default, HipLink starts Apache startup script in HTTP mode.

The Apache Web server ships with a generic 128-bit server certificate. It is a secure certificate. However, all Users that want to use HTTPS are urged to replace it with a certificate issued by a recognized certificate authority of their choice. For example, Verisign (see <http://www.verisign.com/>).

Verifying Installation

Connect to the HipLink console URL from your workstation and log in as User admin with password admin.

Verify the modems, connections, and phone lines.

Startup Scripts

There are startup scripts for all HipLink services:

- Apache Web server
- Messengers
- System Attendant
- Scheduler
- Email Gateway
- Backup Service
- File System Interface

Location

The location of the startup scripts is platform dependent. For each startup script, there is always a defined script (file) and a link pointing to it. If a script needs to be removed, both: script file and a link should be deleted.

1. Solaris

startup scripts: /etc/init.d/
links: /etc/rcRUNLEVEL.d/

2. HP-UX

startup scripts: /etc/rc.d/init.d
links: /etc/rc.d/rcRUNLEVEL.d/

3. Linux RedHat

startup scripts: /sbin/init.d
links: /sbin/rcRUNLEVEL.d/

4. AIX

startup scripts: /etc/rc.d/init.d/
links: /etc/rc.d/rcRUNLEVEL.d

Note: RUNLEVEL is a number. If the server boots in a text mode, RUNLEVEL is set to 3 in most cases.

Script Names

The names of the startup scripts are as follows:

Apache: hiplink_httpd
Messengers: hip_msgrN with N = 1, 2,
System Attendant: hipmon
Scheduler: hipsched
Email Gateway: hipsmtp
Backup Service: hipback
File System Interface: hipfi.

Permissions

All startup scripts should be owned by root and have rwx permissions for the owner, and r permissions for everyone else.

Uninstalling HipLink

In order to uninstall HipLink you should perform the following steps:

Stop all HipLink processes (i.e., messengers and System Attendant) using HipLink GUI.

For Windows:

Open IIS Manager

Right-click the HipLink server and click Stop. For Linux/UNIX:

- a. Stop HipLink Apache Web server:

`/usr/local/hiplink/apache/bin/apachectl stop`. This is the default installation directory

For Windows:

Run the install program and choose to uninstall.

Delete the whole directory tree where HipLink is installed

(e.g., `C:\Program Files\HipLink Software \HipLink`). Here, `C:\` is the default installation directory.

For Linux/UNIX:

Run the install program and choose to uninstall.

Delete the whole directory tree where HipLink is installed

(e.g., `rm -r /usr/local/hiplink`). This is the default installation directory. For example: `rm -r /usr/local/Hiplink`. In case a symbolic link is in use, make sure the target directory is removed.

Startup scripts may have also been installed under the `/etc` director and under the `/sbin` directory. The scripts will be for the System Attendant and the Messengers. If you installed HipLink Apache startup files during the installation process, you will have to delete them too. Their number on the value of the `RUNLEVEL` may be different depending on your installation.

Example for Linux:

```
rm /etc/rc.d/rc3.d/S98hiplink_apache
rm /etc/rc.d/init.d/hiplink_httpd
```

Example for Solaris:

```
rm /etc/init.d/hiplink_httpd
rm /etc/init.d/hip_msgr1
rm /etc/init.d/hip_msgr2
rm /etc/init.d/hip_msgr3
```

```
rm /etc/rc3.d/S98hiplink_httpd
rm /etc/rc3.d/S31hip_msgr
```

```
rm /etc/rc3.d/S32hip_msgr
rm /etc/rc3.d/S33hip_msgr
```

Example for HP:

```
rm /sbin/init.d/hip_monitor
rm /sbin/init.d/hip_msgr1

rm /sbin/rc3.d/S30hip_mon
rm /sbin/rc3.d/S31hip_msgr
```

Upgrading HipLink

If you are currently using a previous version of the HipLink messaging system, you have three choices:

Manually remove the older version and then install the new one. Data will be lost in this case.

Upgrade the existing version. The HipLink installer will automatically detect the older version and will import all your existing settings (i.e., Receivers, Carriers, Users, etc.). The upgrade can be done in a different directory than that where HipLink is already installed.

Keep older version as a backup. Rename the directory `/usr/local/hiplink` to `/usr/local/hiplink_old` for UNIX/Linux and `C:\Program Files\HipLink Software\HipLink` to `C:\Program Files\HipLink Software\HipLink_old` for Windows. The other option is to backup the whole folder to a different location.

Note: Before you do any changes to the older version of HipLink, all HipLink services and Apache Web server must be stopped

CLI Installation

The CLI can be used either from the same machine where the HipLink server is installed or from a different machine.

The CLI comes with the HipLink server installer. Thus, no other CLI installation is required if the CLI is used on HipLink. The executable is located in the `HipLink\bin` directory (i.e., `C:\Program Files\HipLink Software\HipLink\bin\cli.exe` on Windows platforms and `/usr/local/hiplink/bin/cli.exe` on UNIX platforms, considering default installation locations).

If the CLI has to be used remotely as a client from a different machine, then you must copy the CLI on that machine into the directory of your choice and execute it using the URL parameter.

On Windows, you have to copy the following files from the `...\HipLink\bin` directory:

cli.exe
libcurl.dll
libeay32.dll
ssl3.dll
ssleay32.dll

On UNIX, you have to copy only the cli.exe file from the .../hiplink/bin directory.

Note: The directory where the CLI is executed must have write permissions because the CLI needs to generate some temporary files.

For details about HipLink CLI programming and usage, refer to the HipLink Programmer Guide.

If you need to run the CLI on another platform than your HipLink server, contact HipLink Technical Support to get the executable for the respective platform.

A simple zip or tarball agent program (with log and configuration directories) is with required with the dll/library files is provided and allows cross platform communications.

HipLink Fax Module Installation

Prerequisites

The HipLink Fax Console must be installed on a server running Windows 2003 or greater.

It can be installed either on the same machine where the HipLink server is installed, or on a different machine that has access to the HipLink server. This includes the modem.

The Fax Modem and Windows Fax Service must be installed on the system.

HipLink needs to copy files to the Fax Module's Spool Directory and the Fax Module needs to read those files. They must both be able to access the same shared folder.

This folder could be on either machine.

Installation Steps

How to install the HipLink Fax Module:

Run the HipLink Fax Module Installer, HipLinkFaxModule.exe. The *InstallShield Wizard™* will help install the HipLink Fax Module on your computer.

It is strongly recommended that you exit all Windows programs before running this Setup program. If you have not done it yet, click Cancel to quit the Setup and then close any programs you have running. Click Next to continue with the Setup program.

Setup will install the HipLink Fax Module either in the default folder (i.e., C:\Program Files\ HipLink Group\HipLinkXS Fax) or in a different folder of your choice. Click Browse

and select another folder (i.e., D:\Applications\HipLink_FAX). You can choose not to install the HipLink Fax Module by clicking Cancel to exit.

Enter the URL of the HipLink server in the format http://machinename:portnumber. For example, http://robson:8000, where robson is the name of the machine, and 8000 is the port number.

Enter the FAX server name, usually the name of the machine.

Enter the license key provided.

Please wait while the *InstallShield Wizard™* extracts the files needed to install HipLink on your computer. This may take a few moments.

In the target directory, execute HiplinkFax.exe. Here you can modify the directories, connect to the FAX server and activate the phone line(s). If the Fax Module is installed on a different computer than the HipLink server, then you must ensure that the HipLink server will have access to the FAX directories. (Usually this will simply be a shared Windows folder.)

Verifying Installation

After executing the HipLink Fax Module Windows Installer, the following directory structure and files will be created under the path that you chose to install HipLink:

Table 1:

Directory	Description
\HipLink Group\HipLinkXS Fax	
cplopen.bat	
HipLinkFax.exe	The executable
HipLinkFax.ini	The configuration file
Archive\completed	Directory for successful faxes sent
Archive\failed	Directory for failed faxes
\Logs\	Logs directory
\Spool\	Spool directory
\Queue\	Queue directory
\Temp	Temp directory
\Templates	Templates

If something from this package is missing or not working properly, contact HipLink Technical Support.

HipLink Voice Module Installation

The HipLink Voice Module allows a HipLink administrator to receive incoming calls and to send outgoing voice calls. In both cases, the Module creates the interface to allow Users to control telephony IVR (Interactive Voice Response) session flow, and to perform HipLink functions over the phone.

Before installing the HipLink Voice Module, you should install the hardware and software that come with your Dialogic board. Please refer to the Dialogic User Guide and Read Me file for details.

Prerequisites

Hardware Requirements

- Intel® Core™ i5 or Core™ i7 processor
- 2 to 4GB RAM
- High-speed HDD
- Dialogic Voice Board.
- The CTADE run time hardware key (Sentinel System Driver dongle).

Software Requirements

Intel Dialogic System Release v6.0.

The current latest version can be downloaded from the following URL.

http://membersresource.dialogic.com/search/DDL/download/DDLAgreement1.asp?url=_releases/WinSU/SU211/red/red.zip.

NOTE: While installing, select all optional features except SNMP.

Envox CT Application Development Environment v9.2

One of the following Text To Speech (TTS) Engines:

- Microsoft TTS 5.0 (default)
- Nuance RealSpeak Telecom 4.0 (optional, recommended for a best quality)

HipLink Voice Module 4.0.x Installer

The Voice Module can be installed either on the same machine where the HipLink server is installed, or on a different machine that has access to the HipLink server.

The HipLink Voice Module needs to communicate with the HipLink server using TCP/IP and via a Windows shared folder with write access.

Installation Steps

Installing Software and Hardware Prerequisites

Install Windows (Windows Server 2003 recommended).

Insert the Intel Dialogic board into a PCI (or PCIe) extension slot.

Download and install the Dialogic System Release 6.0

After the installation is complete, run the Intel Dialogic Configuration Manager - DCM from the Start menu.

- go to: Start Menu > Programs (or All Programs) > Intel Dialogic System Release 6.0 > Configuration Manager - DCM

When the Intel Dialogic Configuration Manager is started:

- the Dialogic board should be configured automatically
- select the board from the configured device
- go to the menu: Settings > Check System/Device Autostart > Start System
- press the Green Start Arrow button from the menu bar and wait until the service is started
- exit the Configuration Manager

NOTE: A problem might occur with the SR 6.0 Device Configuration Manager. If the service is not starting (freezes the machine) you have to reboot the machine and start DCM: select Settings -> Start Devices Preferences ->

Start Selective (good devices only); press the Green Start Arrow button from the menu bar and wait until the service is started;

Install a Text to Speech Engine

- choose between Microsoft TTS 5.0 and Nuance RealSpeak Telecom 4.0

5.a) Install Microsoft TTS 5.0 (it is part of Windows 2003)

- download the installation package from:

<ftp://ftp.hiplink.com/hiplink/windows/voice/speechsdk51.exe>

- run the speechsdk51.exe

5.b) To install Nuance RealSpeak Telecom 4.0 TTS engine:

- Obtain the installation package RealSpeak v4.0.zip.

Contact HipLink Technical Support for details on how to obtain it.

- Follow the instructions in readmeRealSpeak4.txt

Attach the CT ADE run-time hardware key (the Sentinel System Driver dongle) to the parallel port.

Install the Envoy CT Application Development Environment (CT ADE) v9.2.

Installing the HipLink Voice Service

1. Download the HipLink Voice Module 4.0.1 Installer from:
 2. <ftp://ftp.hiplink.com/hiplink/windows/voice>
 3. Run the HipLink Voice Module 4.0.1 installer. The *InstallShield Wizard™* will help install the HipLink Voice Module on your computer.
 4. Choose the destination location. By default this is: C:\Program Files\Semotus\HipLink Voice Module
 5. Select the program folder. By default this is: HipLink Voice Module
 6. Please read the License Agreement. Press the Page Down key to see the rest of the agreement. To install HipLink Voice Service, you must accept this agreement and click Yes. Proceed with the installation only if you agree with the terms and conditions stated in the License Agreement. If you do not agree with the terms, do not install the software. Choose No and Setup will close.
 7. Enter the License Key that was sent to you when you purchased the HipLink Voice Module.
 8. Enter the URL of the HipLink server in the format using the machine name or IP address: <http://machinename:portnumber/cgi-bin/action.exe>. or: <http://123.123.123.123:portnumber/cgi-bin/action.exe>. (for example, <http://robson:8000/cgi-bin/action.exe>, where robson is the name of the machine, and 8000 is the port number).
 9. Enter the voice messages queue directory. Assuming default HipLink installation location, the default path of voice messages queue is: C:\Program Files\Semotus\HipLink\voice. If the HipLink Voice Module and the HipLink Server are installed on different machines you have to use the machine name when specifying a path (for example: \\machinename\Program Files\Semotus\HipLink\voice).
- NOTE: Write and Delete permissions are a must for this folder. The HipLink Voice Module must also be configured to use an account that has access to the network. By default the service is installed with the local system account.
10. Start copying files. The setup has all the information to start the installation of the HipLink Voice Module files. If you want to review or change any settings, click the Back button. If you are satisfied with the settings, click the Next button. You can choose not to install the HipLink Voice Module and click the Cancel to exit the installer.
 11. Choose the TTS engine that best suits your needs:
 12. Microsoft TTS 5.0 (default)
 13. Nuance RealSpeak Telecom 4.0 (optional, recommended for a best quality)
 14. Please wait while the *InstallShield Wizard™* extracts the files needed to install HipLink on your computer. This may take a few moments.
 15. After the installation is complete, you will be prompted to restart your computer now or later. If you do not have the Microsoft XML Parser 4.0 installed on your computer you should select later. The HipLink Voice Module installer will prompt you to install the Microsoft XML Parser 4.0.

16. press the Yes button if you do not have it yet installed on your PC.
17. press the No button if you already have it installed on your PC, or if you want to do it later.

NOTE: During the installation process select the Install Now and not the Custom installation.

If not done already, then you have to run the Microsoft XML 4.0 installer:

[HipLinkVoiceModuleInstallationFolder]/MSXML4/msxml4.msi

NOTE: During the installation process, select the Install Now and not the Custom installation.

At the end of the installation, reboot the machine.

Attach telephone lines to the Dialogic board.

Before starting the HipLink Voice Module you have to recreate the CT ADE Resource Profile.

from the Start Menu:

Start Menu > Programs (or All Programs) > Envovx CT ADE > Common > Configure CT ADE Profile

go to the menu: File > Recreate Profile

Click on Discard and Recreate button.

For Windows server 2003

Check if two ini files, CTADE.INI and ADX.INI, are in the C:\Windows folder. If they are not, search the C:\Documents and Settings folder (all subdirectories) for these files and copy them into the C:\Windows folder.

HipLink Server and HipLink Voice Module matching settings to be done

In HipLink Server make sure that there is a Non-GUI User with the IP address matching the IP address of the PC where the HipLink Voice Module is running. Remember the Access Code of this User (for example 5555).

In Voice Service

For the following files:

C:\Program Files\Semotus\HipLink Voice Service\templates\t_basic_m.svxml

C:\Program Files\Semotus\HipLink Voice Service\templates\t_basic_a.svxml

C:\Program Files\Semotus\HipLink Voice Service\templates\Exchange Server shutdown.svxml

C:\Program Files\Semotus\HipLink Voice Service\templates\Power Outage.svxml

perform the following actions:

- open the file with a text editor;
- in the line `<var id="AccessCode">1111</var>`; change 1111 to 5555,
- updated line will be `<var id="AccessCode">5555</var>`;
- save file and close

Set up the HipLink Voice Module. Go to:

Start Menu > Settings > Control Panel > Administrative Tools > Services

Select the Voice Module Service, right-click and open the Properties, then go to the Log On tab.

Click the radio button to enable This account (instead of Local system account), and enter the account name and password under which the HipLink Voice Service will be running.

Start the HipLink Voice Module User Interface from the Start Menu:

Start Menu > Program Files (or All Programs) > Semotus > HipLink Voice Service > HipLink Voice Module User Interface

This will start an interface that you can use to configure your voice service.

Right click on the HipLink Voice Module node and select properties to configure Voice Module properties.

Right click on the VM service to Start/Stop the Voice Service.

Expand the lines node to view the currently configured lines.

Right click on any line node and select commands to Start/Stop/Enable/Disable individual lines or set the line properties.

IMPORTANT: Any time when some of the parts of Voice Module has been reinstalled or upgraded or added (including software and hardware) you have to Recreate Resources Profile before running Voice Service. Step 16 above.

If something from this package is missing or not working properly, please contact HipLink Support at support@hiplink.com

Upgrade Steps

This is the readme file for HipLinkVoiceModule4.5_Patch_03.zip.

This HipLink Voice Module patch contains binaries built with CTADE v.10.

Please perform the following steps to apply the patch. It has been assumed that C:\Program Files\Semotus\HipLink Voice Module is the installation path; please replace it with the actual installation path if it is different.

Stop Voice Module Service from Windows Services Panel and exit HipLink Voice Module User Interface if running.

Unregister HiplinkVoiceUI.dll. To do so, go to Start > Run and type the following command:

```
regsvr32 C:\Program Files\Semotus\HipLink Voice Module\HiplinkVoiceUI.dll /u
```

Create a backup folder and move three files VMservice.exe, HiplinkVoiceUI.dll, HiplinkVoiceUI.msc from C:\Program Files\Semotus\HipLink Voice Module to that backup folder

Extract VMservice.exe, HiplinkVoiceUI.dll, HiplinkVoiceUI.msc from HipLinkVoiceModule4.5_Patch_03Sep2010.zip into C:\Program Files\Semotus\HipLink Voice Module.

Register HiplinkVoiceUI.dll. To do so, go to Start > Run and type the following command:

```
regsvr32 C:\Program Files\Semotus\HipLink Voice Module\HiplinkVoiceUI.dll
```

Start Voice Module Service from Windows Services Panel.

Start the HipLink Voice Module User Interface and refresh VMservice, then refresh Lines.

HipLink Installation for IIS 7 Guide

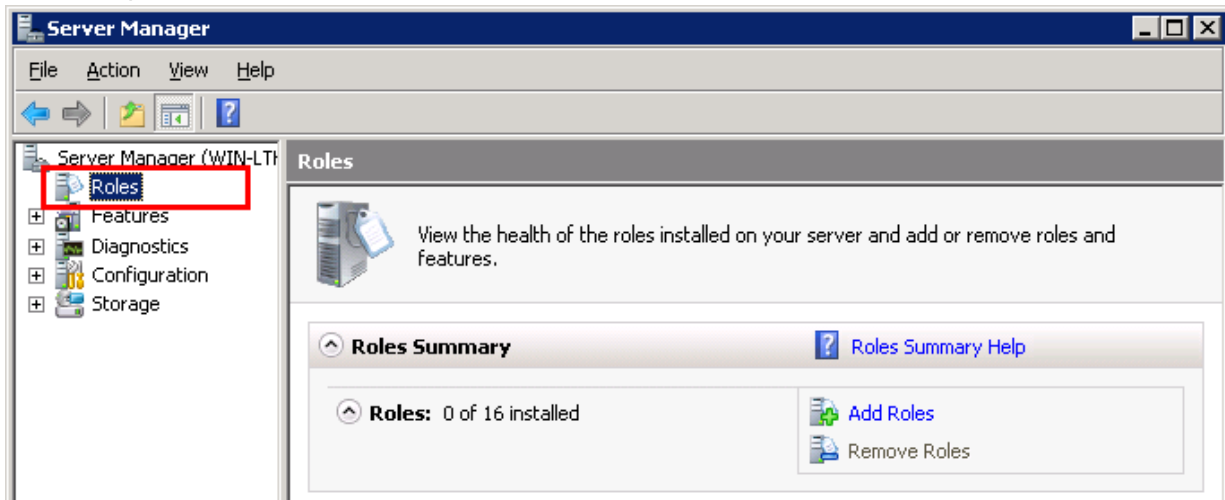
Note: If you are upgrading HipLink from an earlier installed version on the same machine, you may skip this section and proceed to the next section titled Upgrading from HipLink 4.6 and earlier.

With the Internet Information Services (IIS) version 7, the installation of the Web Server has been divided into the main Web Server itself and various components. Many of the components required for HipLink to install and run properly are not enabled by default and need to be enabled before installing HipLink.

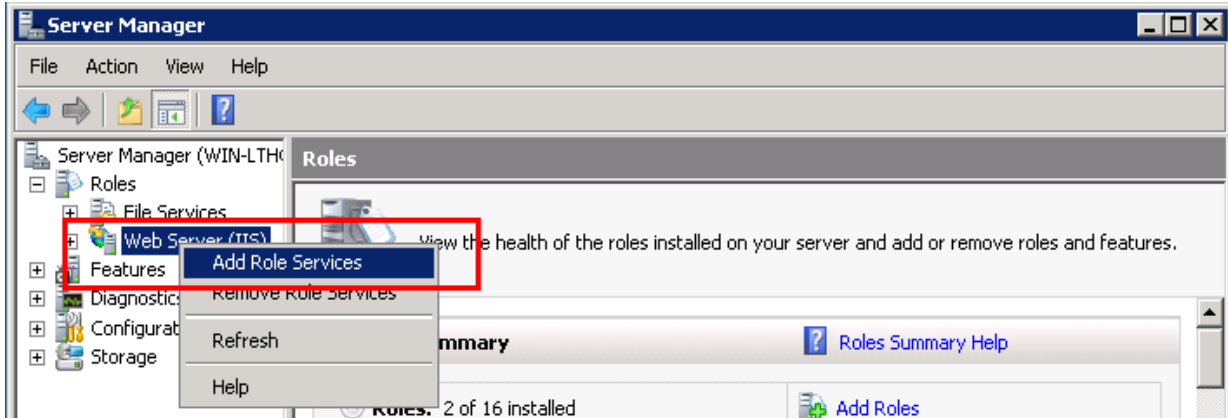
Installing HipLink on IIS has the primary requirement for IIS to be properly installed. Please follow the required pre-installation steps given in this document and then proceed to install HipLink.

Open Server Manager (possibly via Control Panel > Administrative Tools > Server Manager).

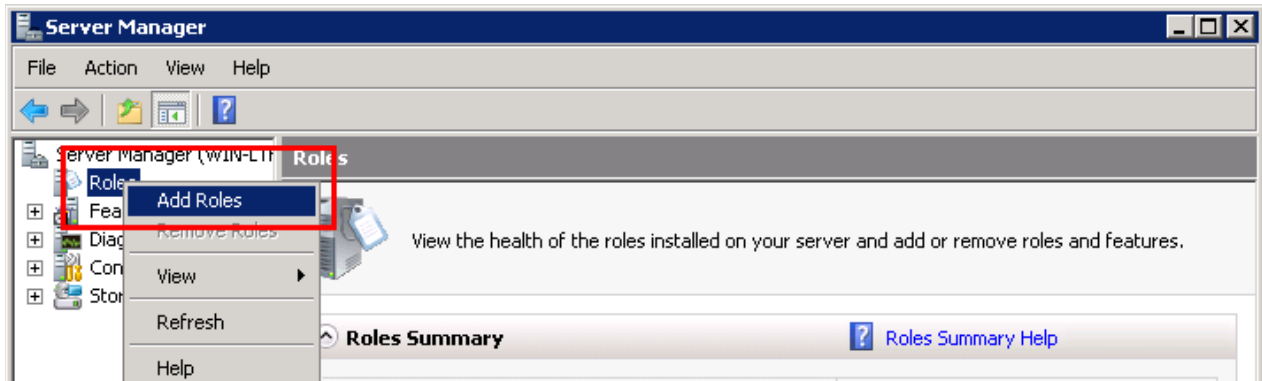
In the left window pane, select option *Roles* (as shown in the screenshot below) and expand it.



If the entry Web Server (IIS) is already there, IIS is already installed on the system. Right-click on it and select Add Role Services menu option (as shown in the screenshot below) to open the Add Role Services wizard where the Select Role Services page would come up. **Skip steps (3) to (7) and proceed to (8).**

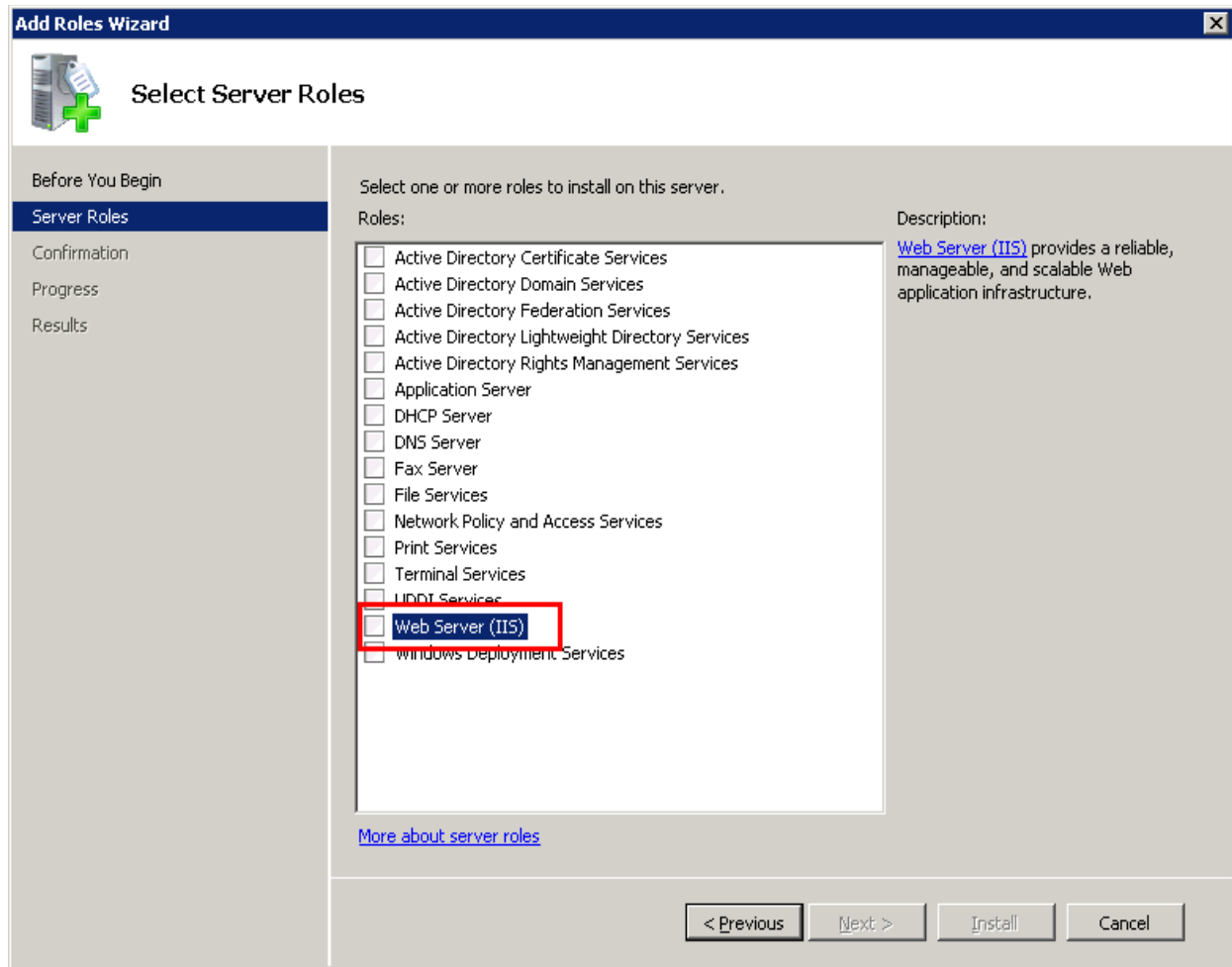


If IIS is not installed on the system, right-click on Roles and select Add Roles option to open the Add Roles Wizard.



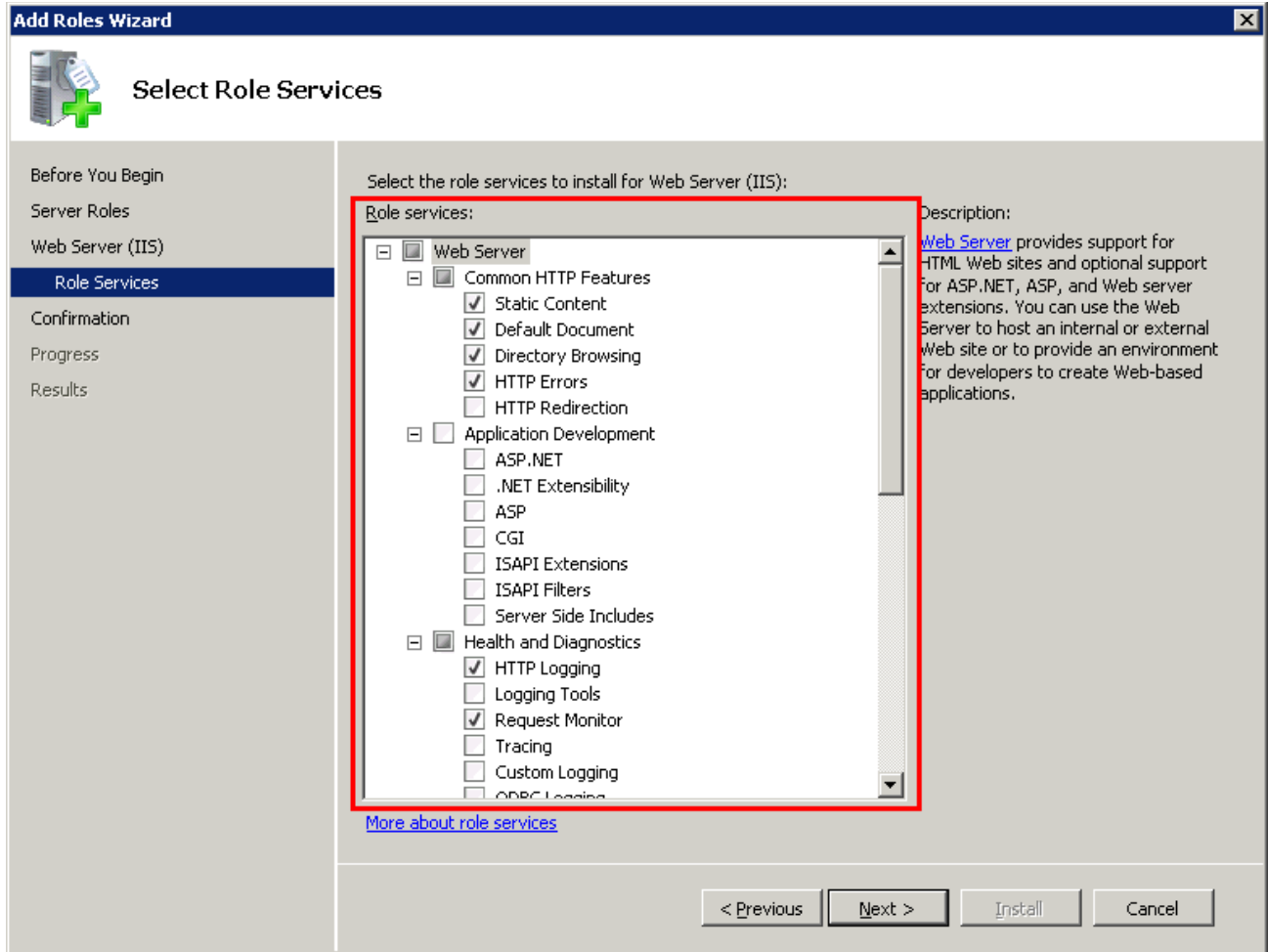
Press the Next button on the first page of the wizard to open the Select Server Roles page.

In the Select Server Roles page, select the Web Server (IIS) check-box. If prompted with the Add Features required for Web Server (IIS)? question, press the Add Required Features button.



Press the Next button on each of the next pages till the Select Role Services page comes up.

On the Select Role Service page, a list of options would be presented (as shown in the screenshot below) with some of the options are selected by default.



In addition to those selected by default, some of the other options are required to be enabled manually for HipLink to install and run properly. Following are those additional options that were required to be manually checked on.

Web Server

Common HTTP Features

HTTP Redirection

Application Development

ASP

CGI

ISAPI Extensions

ISAPI Filters

Security

Windows Authentication

Management Tools

IIS 6 Management Compatibility

IIS 6 Metabase Compatibility

The following screenshot shows the complete list of options that were checked on during our testing.

Add Roles Wizard



Select Role Services

Before You Begin

Server Roles

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Select the role services to install for Web Server (IIS):

Role services:

- Web Server
 - Common HTTP Features
 - Static Content
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - HTTP Redirection
 - Application Development
 - ASP.NET
 - .NET Extensibility
 - ASP
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
 - Server Side Includes
 - Health and Diagnostics
 - HTTP Logging
 - Logging Tools
 - Request Monitor
 - Tracing
 - Custom Logging
 - ODBC Logging
 - Security
 - Basic Authentication
 - Windows Authentication
 - Digest Authentication
 - Client Certificate Mapping Authentication
 - IIS Client Certificate Mapping Authentication
 - URL Authorization
 - Request Filtering
 - IP and Domain Restrictions
 - Performance
 - Static Content Compression
 - Dynamic Content Compression
 - Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service
 - IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting Tools
 - IIS 6 Management Console
 - FTP Publishing Service
 - FTP Server
 - FTP Management Console

Press the Next button on the page and Install button on the next page to finish installing IIS with all of the Role Services required for HipLink to install and run properly.

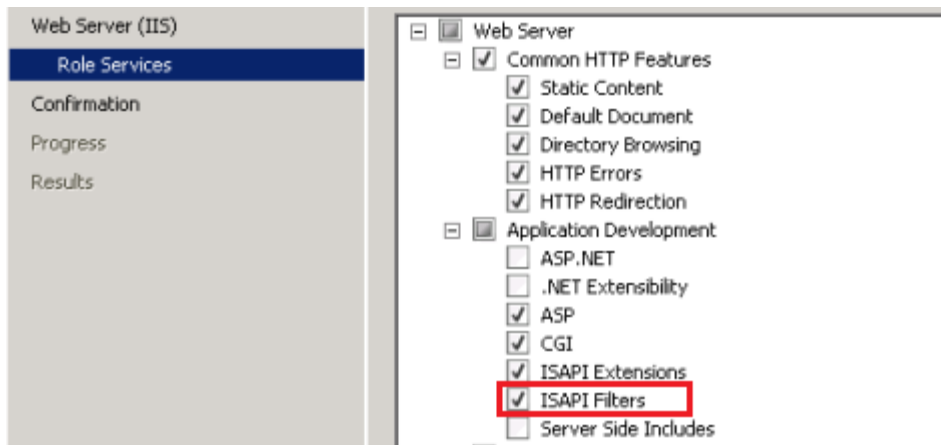
Upgrading from HipLink 4.6 and earlier

If you are upgrading from HipLink 4.6 or earlier version on this same machine, you may have most of the features required by HipLink already enabled.

The option(s) additionally required for some of the new features in HipLink 4.7 are given as follows.

- Web Server
- Application Development
- ISAPI Filters

The following screenshot highlights the additionally required option(s).



You can now proceed to install HipLink.

HipLink Installation for IIS on Windows Server 2008

On Windows Server 2008, installing HipLink on the Internet Information Services (IIS) web server requires some additional pre-installation and post-installation steps for HipLink to install and run properly. Both of these are explained in this document. Please properly follow the required pre-installation steps, then install HipLink and then perform the post-installation steps given in this document.

Pre-Installation Steps

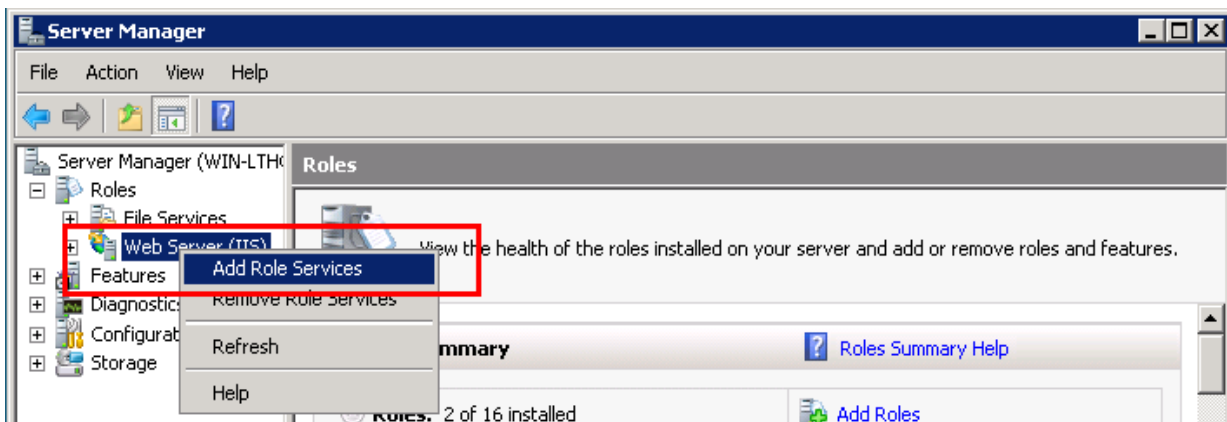
Installing HipLink on IIS has the primary requirement for IIS to be properly installed and configured in the system. Please follow the steps below to install and configure IIS properly.

Open Server Manager (possibly via Control Panel > Administrative Tools > Server Manager).

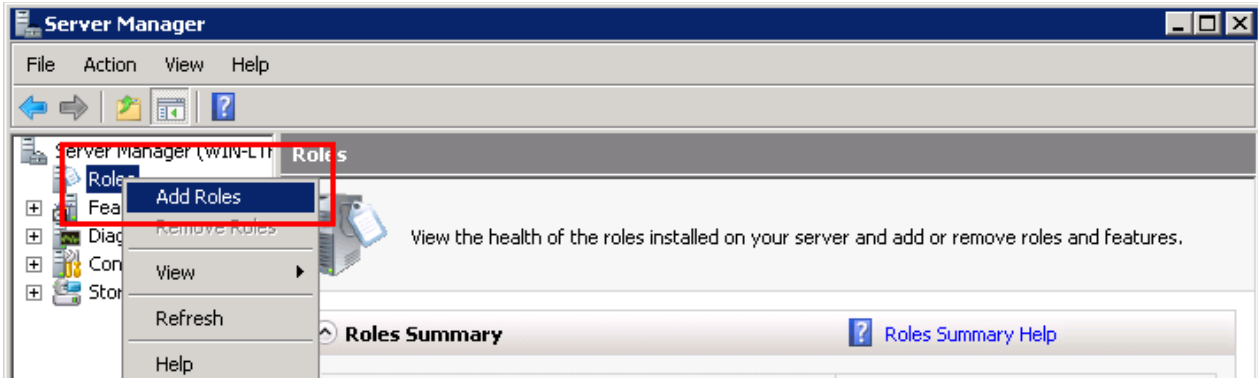
In the left window pane, select option Roles (as shown in the screenshot below) and expand it.



If the entry Web Server (IIS) is there, IIS is already installed on the system. Right-click on it and select Add Role Services menu option (as shown in the screenshot below) to open the Add Role Services wizard where the Select Role Services page would come up. **Skip steps (3) to (7) and proceed to (8).**

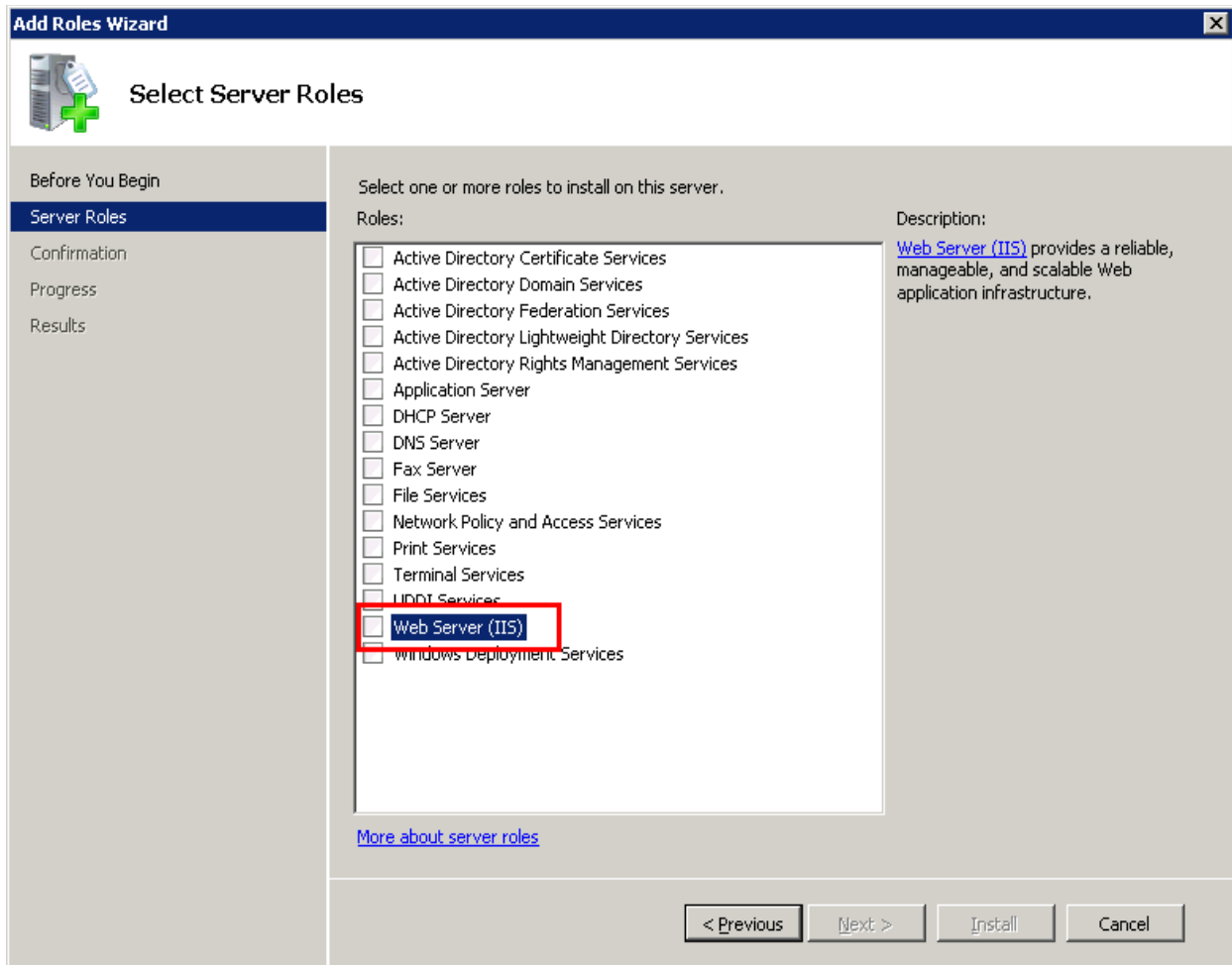


If IIS is not installed on the system, right-click on Roles and select Add Roles option to open the Add Roles Wizard.



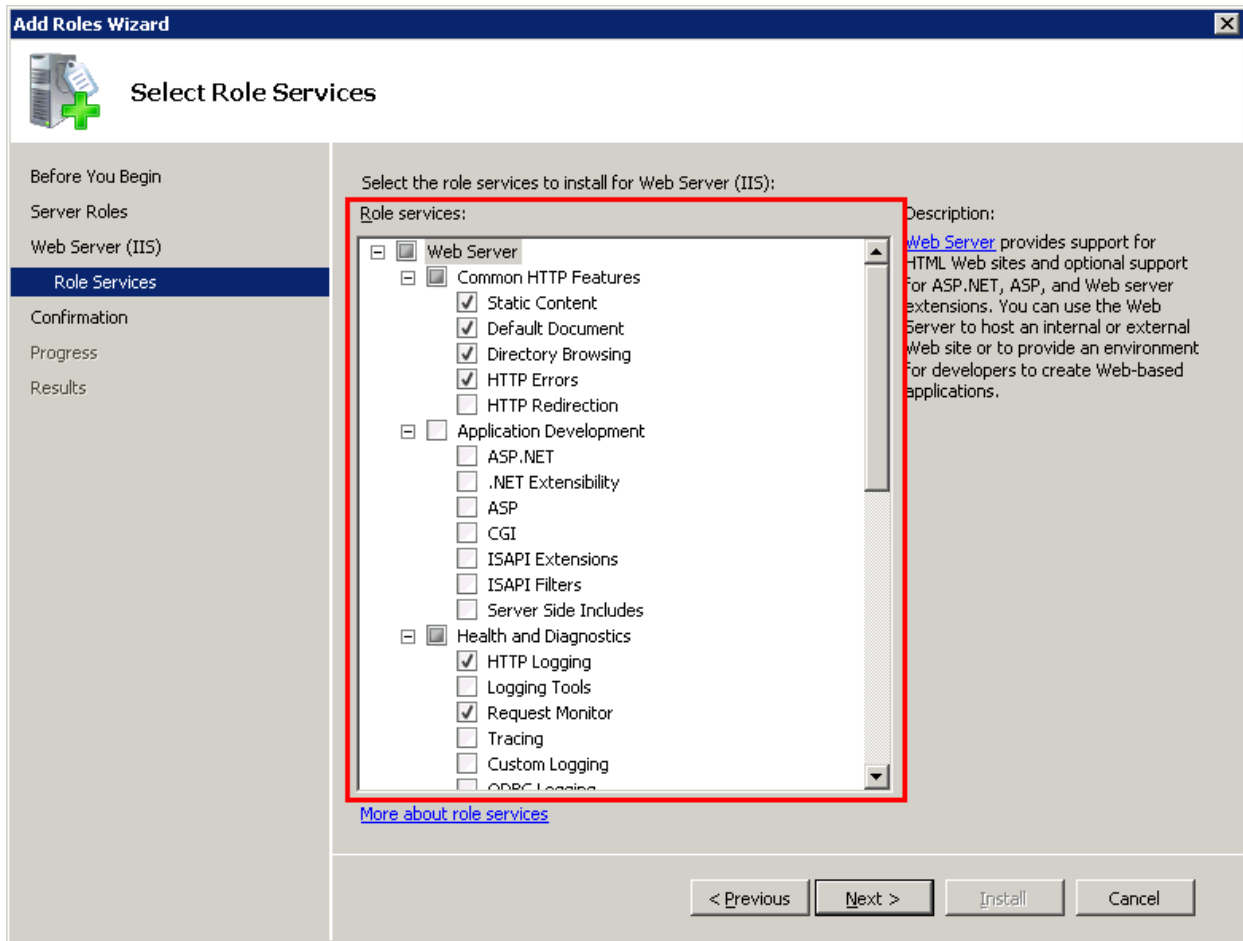
Press the Next button on the first page of the wizard to open the Select Server Roles page.

In the Select Server Roles page, select the Web Server (IIS) check-box. If prompted with the Add Features required for Web Server (IIS)? question, press the Add Required Features button.



Press the Next button on each of the next pages till the Select Role Services page comes up.

On the Select Role Service page, a list of options would be presented (as shown in the screenshot below) with some of the options are selected by default.



In addition to those selected by default, some of the other options are required to be enabled for HipLink to install and run properly. Following are those additional options that were required to be manually checked on.

Web Server

Common HTTP Features

HTTP Redirection

Application Development

ASP

CGI

ISAPI Extensions

Security

Windows Authentication

Management Tools

IIS 6 Management Compatibility

IIS 6 Metabase Compatibility

The following screenshot shows the complete list of options that were checked on during our testing. While most of the options were checked on by default, some of the others (listed above) were manually checked on, as shown in the screenshot below.

Add Roles Wizard



Select Role Services

Before You Begin

Server Roles

Web Server (IIS)

Role Services

Confirmation

Progress

Results

Select the role services to install for Web Server (IIS):

Role services:

- Web Server
 - Common HTTP Features
 - Static Content
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - HTTP Redirection
 - Application Development
 - ASP.NET
 - .NET Extensibility
 - ASP
 - CGI
 - ISAPI Extensions
 - ISAPI Filters
 - Server Side Includes
 - Health and Diagnostics
 - HTTP Logging
 - Logging Tools
 - Request Monitor
 - Tracing
 - Custom Logging
 - ODBC Logging
 - Security
 - Basic Authentication
 - Windows Authentication
 - Digest Authentication
 - Client Certificate Mapping Authentication
 - IIS Client Certificate Mapping Authentication
 - URL Authorization
 - Request Filtering
 - IP and Domain Restrictions
 - Performance
 - Static Content Compression
 - Dynamic Content Compression
- Management Tools
 - IIS Management Console
 - IIS Management Scripts and Tools
 - Management Service
- IIS 6 Management Compatibility
 - IIS 6 Metabase Compatibility
 - IIS 6 WMI Compatibility
 - IIS 6 Scripting Tools
 - IIS 6 Management Console
- FTP Publishing Service
 - FTP Server
 - FTP Management Console

Press the Next button on the page and Install button on the next page to finish installing IIS with all of the Role Services required for HipLink to install and run properly. **You can now proceed to install HipLink.**

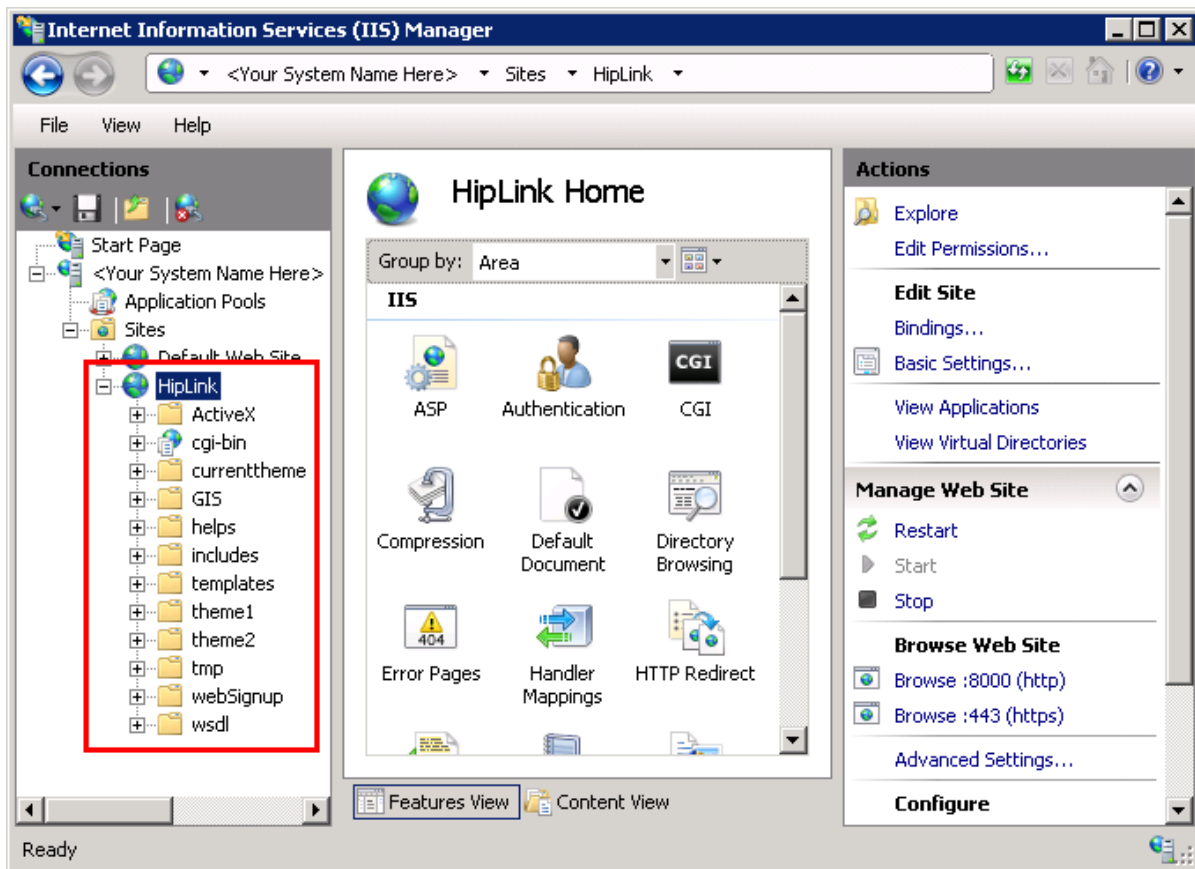
Post-Installation Steps

Once HipLink has been successfully installed on the system, there is one additional manual configuration step required for HipLink to run properly. Please follow the steps given below.

Open Internet Information Services (IIS) Manager (possibly via Control Panel > Administrative Tools > Internet Information Services (IIS) Manager).

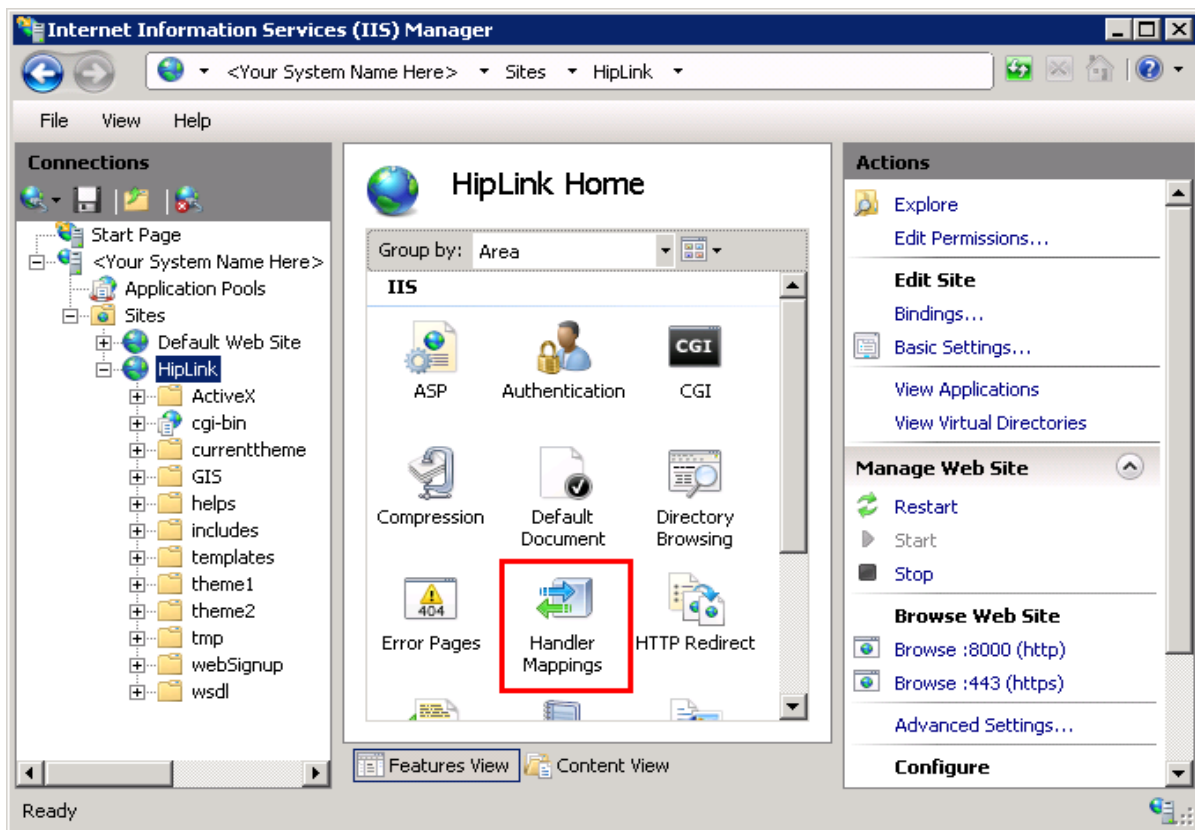
In the left window pane, expand your system name and find the Sites option under it and expand it as well. Under Sites option, find HipLink and select it, as shown in the screenshot below.

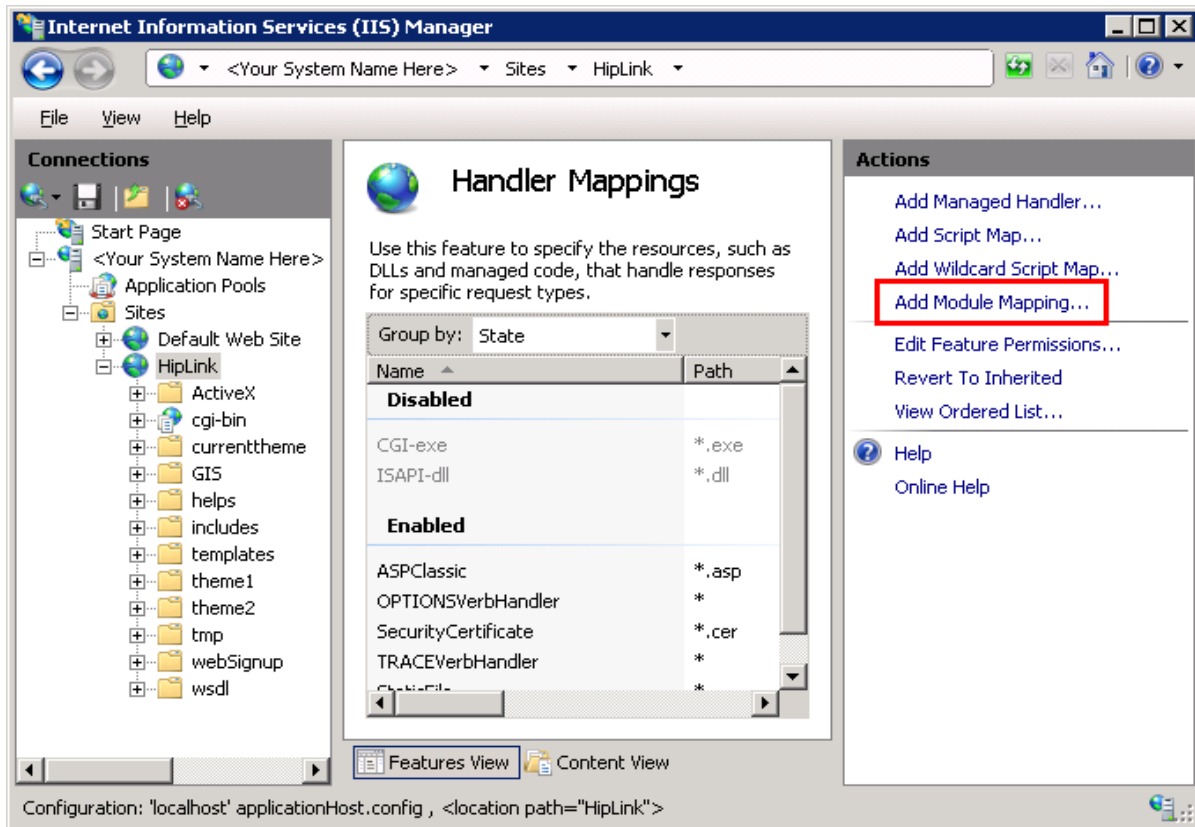
Note: If HipLink is not there and only Default website is there, then HipLink might have been installed as the default website. Just cross-check the contents under the Default website from the screenshot below and select this option instead.



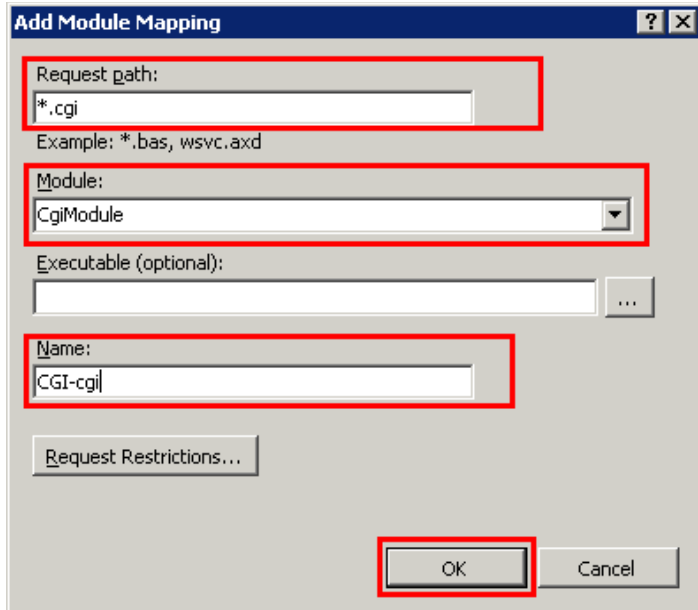
In the center window pane, under the heading *HipLink Home* (or *Default website Home*), find the *Handler Mappings* option (as highlighted in the first screenshot on the next page) and double-click it to go to the *Handler Mappings* page.

On the *Handler Mappings* page, click on the *Add Module Mapping* option in the right window pane (as highlighted in the second screenshot on the next page), which would pop-up the *Add Module Mapping* dialog.





In the Add Module Mapping dialog,
enter the value *.cgi in the *Request Path* field,
select CgiModule from the *Module* drop-down list,
leave the *Executable* field blank,
enter any name (e.g. CGI-cgi) in the *Name* field,
and press the *OK* button to add the module mapping to the HipLink website.



These values should be entered in the dialog.

Close IIS Manager. If prompted with the question *The connection list has changed. Do you want to save changes?*, choose *Yes* to save the changes and close the IIS Manager.

HipLink is now installed configured to run properly.

Basic System Configuration

It is important to initially configure HipLink in the order specified below.

Initial Log in

Launch HipLink and log in as the default administrator (i.e., User: admin with password: admin). From the HipLink GUI main screen, use the horizontal tabs located on the top of the page and the vertical bar located on the left side of the screen to navigate through HipLink.

The entries in the left navigation bar depend on the menu button that is currently selected. From the navigation bar, you can open submenus (here called panels) from where you can perform specific functions. Panels can also be accessed by using the underlined hyperlinks on the menu screens.

Open the Settings menu and perform the following steps.

Change Password

The administrator has permissions to access all HipLink functions. It is strongly recommended that you change your administrator password from admin to something unique.

Enter License Key

When you download a copy of HipLink, it automatically comes with a 15-day trial evaluation license with limited features. If you already have a permanent license, please enter it now before the trial expiration date approaches.

Verify that the HipLink capabilities (i.e., number of messengers, protocols, Users, Receivers, etc.) are those you have specified in the License Key request. If there is any problem, please contact HipLink Technical Support.

To enter a new License Key:

1. From the Settings menu, click License Key on the left navigation bar.
2. On the License Key panel, enter your new License Key in the appropriate field.
3. Click the Save button. Your new parameters will be displayed. Check that the new parameters correspond to your License Key request.

Directory Settings

The Directories panel lists the default locations of the HipLink files: message queues (i.e., Main, Scheduled, Escalation, Failed, Completed, Fax, and Voice queues), Logs, Reports, and Statistics.

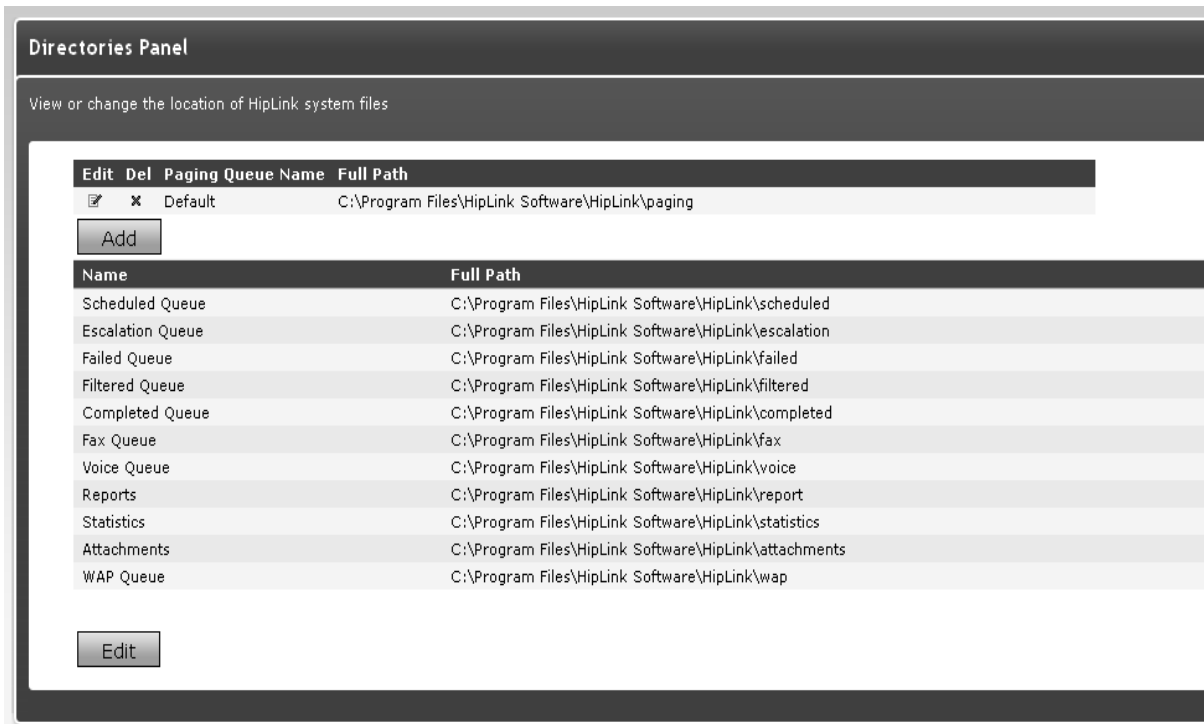
If working with multiple Paging Queues feature is enabled by the License Key then the Main queue is replaced by the Default queue and the User can add more custom Paging Queues up to the number allowed by the License Key.

HipLink uses the following queues to store the messages: Main, Scheduled, Escalation, Failed, and Completed queues. It also lists the default locations for Reports and Statistics.

All directories are mandatory.

IMPORTANT. *It is strongly recommended that you keep the directories in their default locations to avoid message loss. However, if you choose for some reason to change the*

directory locations follow all of the steps below. After changing the location of the directories, it is mandatory to restart the Messengers, System Attendant, and Scheduler from the Services Menu, and move manually all the existing files from the old locations to the new locations.



Modify a Directory

1. From the Settings menu, click Directories on the left navigation bar.
2. On the Directories Panel, click any Edit button to reach the Edit Directories page.
3. Change the path of the directory you want to modify.
4. Click the Save button to submit your changes and return to the Directories Panel, Reset button to fill in the previous values, or Cancel button to return without saving.
5. Restart Messengers, System Attendant, and Scheduler from the Services menu.
6. Move all the files from the old locations to the new locations.

Queue Name	Directory Path	Mandatory
Scheduled Queue	C:\Program Files\HipLink Software\HipLink\scheduled	*
Escalation Queue	C:\Program Files\HipLink Software\HipLink\escalation	*
Failed Queue	C:\Program Files\HipLink Software\HipLink\failed	*
Completed Queue	C:\Program Files\HipLink Software\HipLink\completed	*
Filtered Queue	C:\Program Files\HipLink Software\HipLink\filtered	*
Fax Queue	C:\Program Files\HipLink Software\HipLink\fax	*
Voice Queue	C:\Program Files\HipLink Software\HipLink\voice	*
Reports	C:\Program Files\HipLink Software\HipLink\report	*
Statistics	C:\Program Files\HipLink Software\HipLink\statistics	*
Attachments	C:\Program Files\HipLink Software\HipLink\attachments	*
WAP Queue	C:\Program Files\HipLink Software\HipLink\wap	*

Note: Fields marked with an asterisk "" are mandatory

Note: The Fax Queue and Voice Queue directories will be displayed only if the Fax and Voice services are enabled by the License Key.

Multiple Queues

Please see the Advanced Configuration & Administration Tools section in this Guide for a full description and management of the Queues.

The Multiple Queue feature allows dedicated queues that will be used exclusively by one or more Messengers and Carriers assigned to that queue. There should be at least one Messenger assigned to a given paging queue in order to be able to create a Carrier using the same protocol as that Messenger.

For example if you create a TAP Messages queue dedicated for messages using the TAP Dial-Up protocol, then you must create a TAP Dial-Up Messenger that is assigned to that queue before creating the TAP Dial-Up Carrier.

To add a Paging Queue:

1. From the Settings menu, click Directories on the left navigation bar.
2. On the Directories panel, click the Add button to reach the Manage Queue page.
3. Enter a name for the new paging queue (required).
4. Enter the path of the Directory you want to be used as a paging queue (required).
5. Click the Save button to submit your changes and return to the Directories panel, Reset button to fill in the previous values, or Cancel button to return without saving.

To modify a Paging Queue:

1. From the Settings menu, click Directories on the left navigation bar.
2. On the Directories panel, click the Edit icon.

3. Change the name of the queue or the path of the paging queue.
4. Enter the path of the directory you want to be used as a paging queue (required).
5. Click the Save button to submit your changes and return to the Directories panel, Reset button to fill in the previous values, or Cancel button to return without saving.
6. Restart Messengers, Monitor, and Scheduler from the Services menu.
7. Move all the files from the old locations to the new locations.

Define Departments

The Departments feature is optional and enabled in your License Key. This provides the HipLink administrator with the ability to organize Receivers and different types of Groups into logical segments based on the company organization structure, geographic regions, or any other grouping desired.

Note: *If the Department feature is enabled by the License Key, there is a Default Department already defined in the HipLink database.*

The reason for organizing Receivers and Groups into Departments is that administrators can then control the Departments that individual Users can send messages to and manage (i.e., add, delete, or modify), through the permission settings for each User Group. This is a valuable feature when, for example, the administrator wants to allow a particular User Group to send messages to only one Department (e.g., Tech Support) within the organization.

There are two basic relationships that govern the operation of Departments and characterize both Receivers and Groups. These are membership and visibility.

Department Members

Receivers and Groups can belong to or be a Member of one Department only. A Member of a Department is an entity (a Receiver or a Group) that can be added to other Groups. Users can send messages to a Member that is added to a Recipient List. A Member can also be managed (i.e., modified, moved to another Department, and deleted).

Whenever a new Group is created, the Group as a whole must be assigned to one Department, just as an individual Receiver would be. The Receivers that are Members of a Group can belong to different Departments, but the Group as a whole must be assigned to one Department only. For example, an On-Duty Group called Morning Shift could consist of one Receiver from the Tech Support Department, one from the Engineering Department, and one from the Marketing Department. But the administrator may decide to assign this Morning Shift Group only to the Marketing Department. This means that only permissioned Users would be able to send messages to or manage the Members of the Marketing Department Group.

Note: *Even if your License Key does not support Departments, HipLink uses a Default Department and assigns all created Groups to that Department. This Default Department exists only at the backend.*

Department Guests

Receivers and Groups can be a Member or guest of a Department. Receivers and Groups can be a Member of only one Department but they can be a guest in several Departments.

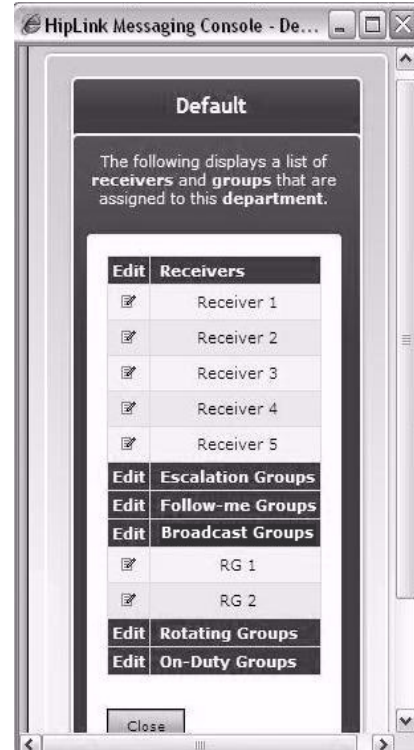
As a Guest in a Department, they can receive messages sent to that Department. But they cannot be modified, edited or deleted by the Users (administrators) of that Department. Users of a Department can modify, edit or delete only entities that are Members of a Department.

When a Receiver or a Group is created, its membership to a Department is assigned. The Guest feature is useful, for example, when an administrator wants a Receiver who is a Member of the Marketing Department to receive messages that are sent to the Sales Department.

Editing Department Members

From the Departments Panel, click on the underlined Department name. This opens up another Web page with a list of Receivers and Groups that are assigned to this Department. The Members that can be managed from here have an edit icon displayed next to their name. Clicking on this takes you directly to the Add/Edit Receiver or Add/Edit Groups page.

On the Departments Panel, click on a Department Name link to see the Receivers or Groups that are assigned to a Department on a separate Web page.



Departments Panel

The Departments button is on the left navigation bar from the Settings menu. The Department Panel is accessible only for Users that are assigned to the sysAdmin User Group and only if the Department feature is licensed.

From the Departments Panel, the HipLink administrator is able to:

- add, modify, or delete Departments,
- have a quick view of the Members assigned to any Department on a separate Web page, and
- assign and remove Members and Guests from the current Department to a selected Department.

Click the Edit icon to reach the Edit Receiver or Edit Group page.

TO ADD A NEW DEPARTMENT:

1. From the Settings menu, click Departments on the left navigation bar.
2. On the Departments Panel, click the Add Department button to reach the Add Department page.
3. Enter a unique name for this Department (mandatory).
4. Enter a description for this Department (optional).
5. Click the Save button and return to the Departments Panel.

TO MODIFY THE DEPARTMENT PARAMETERS:

1. From the Settings menu, click Departments on the left navigation bar.
2. On the Departments Panel, find the Department name you want to modify and click the Members (or Guests) link to reach the Manage Department's Members (or Manage Department's Guest) page.
3. Click the Edit icon to reach the Edit Department page.
4. Edit the Department Parameters.

5. Click the Save button to submit your changes and return to the Manage Department's Members or Manage Department's Guest, Reset button to fill in the previous values, or Cancel button to return without saving.

TO DELETE A DEPARTMENT:

1. From the Settings menu, click Departments on the left navigation bar.
2. On the Departments Panel, find the Department name you want to remove and click the Delete icon.
3. Click the OK button to confirm deletion or click Cancel to revoke this action.

Note: *You cannot delete a Department that still has Receivers or Groups assigned to it. You will first have to remove all the Members and Guests of that Department.*

TO REASSIGN MEMBERS FROM ONE DEPARTMENT TO ANOTHER:

1. From the Settings menu, click Departments on the left navigation bar.
2. On the Departments Panel, find the Department name you want to modify and click the Members link on the same row to reach the Manage Department's Members page.
3. In the Current Department's Members list on the right of the page, all the Receivers and Groups are displayed that are Members of this Department.
4. Select a Department from the dropdown menu and the Receiver and Group Members of this Department will be displayed in the Selected Department's Members list on the left of the page.
5. To change the membership of one or more Members from the Selected Department to the Current Department, select the Members you want to move from the Selected Department's Members list on the left and click the Move >> (to the right) button. The new Members of the Current Department will be displayed in the Current Department's Members list on the right.
6. To change the membership of one or more Members from the Current Department to the Selected Department, select the Members you want to move from the Current Department's Members list on the right and click the << Move (to the left) button. The new Members of the Selected Department will be displayed in the Selected Department's Members list on the left.
7. To select multiple items on a list, click the left mouse button while holding down either the Shift or Ctrl key.
8. Click Done when you are finished.

Note: *Select a Group and click the Show Group Members link to see the Members of that Group on a separate Web page. (This is useful if you want to see who is On-Duty right now.) Move Receivers and Groups as Members from any Department to the Current Department's Member list.*

TO REASSIGN GUESTS FROM ONE DEPARTMENT TO ANOTHER:

1. From the Settings menu, click Departments on the left navigation bar.
2. On the Departments Panel, find the Department name you want to modify and click the Guests link on the same row to reach the Manage Department's Guests page.
3. In the Current Department's Guests list on the right of the page, the Receivers and Groups that are actually Guests of this Department are displayed.
4. Select a Department from the dropdown menu and the Receivers and Groups Members of this Department will be displayed in the Selected Department's Members list on the left of the page.
5. To assign one or more Guests from the Selected Department to the Current Department, select the Members you want to move from the Selected Department's Members list on the left and click the Add >> (to the right) button. The new Guests of the Current Department will be displayed in the Current Department's Guests list on the right.
6. To remove one or more Guests from the Current Department, select the Guests you want to remove from the Current Department's Members list on the right and click the

Remove button. You can remove Guests from any Department, regardless of the Selected Department.

7. To select multiple items on a list, click the left mouse button while holding down either the Shift or Ctrl key.
8. Click Done when you are finished.

Note: Select a Group and click the Show Group Members link to see the Members of that Group on a separate Web page. (This is useful if you want to see who's On-Duty right now.)

The screenshot shows the 'Manage Department's Members' interface. At the top, there is a dark header with the title 'Manage Department's Members'. Below the header is a dark bar with the instruction 'Move Receivers and Groups to and from current Department.'. The main content area has a dark header with 'Edit Department Name Description' and a table with one row: 'Default' (with a checkmark icon) and 'Default department'. Below this is a 'Select Department' section with a dropdown menu showing 'Default'. The interface is split into two columns: 'Select Department's Members' (an empty box) and 'Current Department's Members' (a box containing 'Receiver 1', 'Receiver 2', and '(G) Group1'). Between the columns are two buttons: 'Move >>' and '<< Move'.

(above) Manage Department Members and (below) Manage Department's Guest list.

The screenshot shows the 'Manage Department's Guests' interface. At the top, there is a dark header with the title 'Manage Department's Guests'. Below the header is a dark bar with the instruction 'Assign Receivers and Groups as guests to the current Department.'. The main content area has a dark header with 'Edit Department Name Description' and a table with one row: 'Default' (with a checkmark icon) and 'Default department'. Below this is a 'Select Department' section with a dropdown menu showing 'Default'. The interface is split into two columns: 'Select Department's Members' (an empty box) and 'Current Department's Guests' (an empty box). Between the columns are two buttons: 'Add >>' and 'Remove'.

User Group Permissions

A User Group defines the level of access that a User will have to the HipLink features. Administrators can create new User Groups, in addition to the predefined ones: sysAdmin, sysOper, and usrSend. All the existing User Groups are displayed as entries in the User Group drop-down menu on the Add/Edit User Account page.

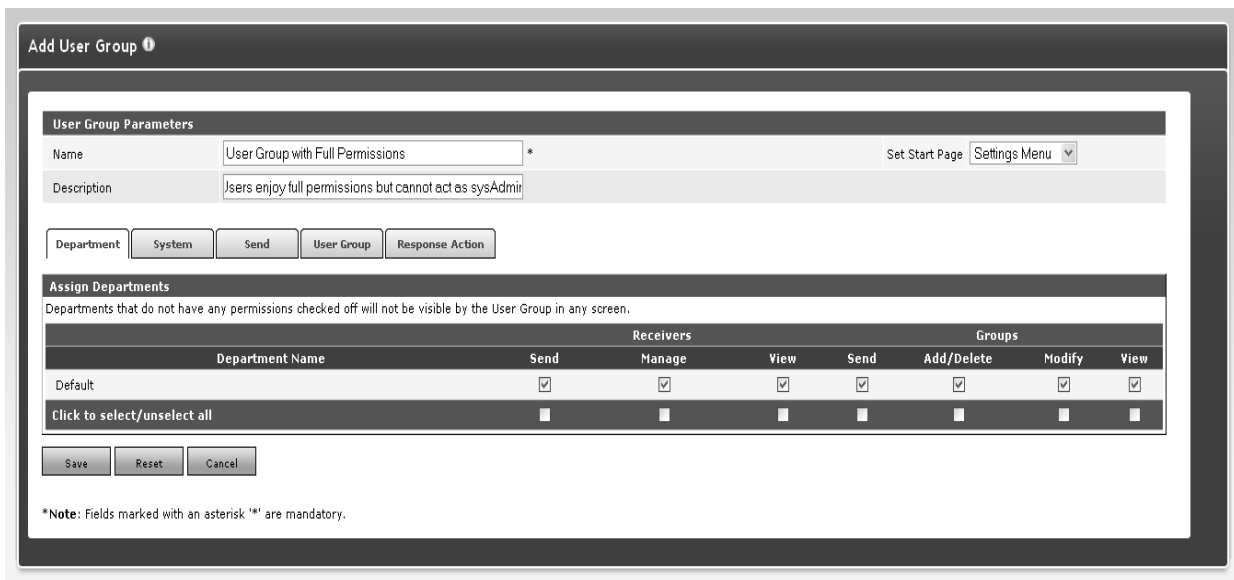
Default User Groups

HipLink comes with the following predefined User Groups:

- The sysAdmin User Group gives system administrators access to all functions in the Settings menu, Stats, and Reports. This group cannot be edited or deleted.
- The sysOper User Group gives system operators access to the Send, Receiver, Groups, Logs, Services, Queues, and Reports from this group.
- The usrSend User Group gives normal Users access to all functions in the Send menu, Reports from this group, and it allows them to change their password in the Settings menu.

ADDING NEW USER GROUP

1. From the Settings menu, click User Groups on the left navigation bar.
2. On the User Group Panel, click the Add Group button to reach the Add User Group page.
3. Enter a unique Name for this User Group (mandatory).
4. Enter a Description for this User Group (optional).
5. Check the permission settings you wish to assign to this User Group. These permissions allow the Users assigned to this User Group to access specific menus and panels, which are used to manage and operate the HipLink application.
6. Specify a Start page for all Users assigned to this User Group (mandatory). After logging in to HipLink, the User is automatically redirected to the start page specified here at the User Group level. Select from the drop-down menu: Standard Send (default), Reports Menu, or Settings Menu.



Add User Group

User Group Parameters

Name: * Set Start Page:

Description:

Department:

Assign Departments

Departments that do not have any permissions checked off will not be visible by the User Group in any screen.

Department Name	Receivers			Groups			
	Send	Manage	View	Send	Add/Delete	Modify	View
Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Click to select/unselect all	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: Fields marked with an asterisk "" are mandatory.

Add a User Group

7. Assign Departments Permissions (see details below).
8. Assign User Group Permissions (see details below).
9. Click the Save button.



Add User Group

User Group Parameters

Name: User Group with Full Permissions * Set Start Page: Settings Menu

Description: Users enjoy full permissions but cannot act as sysAdmin

Department System Send User Group Response Action

Assign User Group Permissions

User Group	Manage User Group	View Report
sysOper	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
usrSend	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Click to select/unselect all	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Save Reset Cancel

Note: Fields marked with an asterisk "" are mandatory.

Check the permissions settings for each User Group.

Note: The Departments, Templates, and Email Gateway features are enabled by the License Key. If the Department feature is enabled there is a Default Department already defined in the HipLink database.

To modify a User Group:

1. From the Settings menu, click User Groups on the left navigation bar.
2. On the User Group Panel, find the User Group name you want to modify and click the Edit icon.
3. On the Edit User Group page, edit the User Group Parameters and/or the Permission Settings.
4. Click the Save button to submit your changes and return to the User Groups Panel, Reset button to fill in the previous values, or Cancel button to return without saving.

To delete a User Group:

1. From the Settings menu, click User Groups on the left navigation bar.
2. On the User Group Panel, select the User Group you want to delete and click the Delete icon. You can also delete multiple User Groups.
3. Click the OK button to confirm deletion or click Cancel to revoke this action.

Note: You cannot delete a User Group that still has Users assigned to it. You have to reassign these Users to other User Groups.

Department Permission Settings

On the Add/Edit User Group page, the HipLink administrator can set permissions that allow a user to view the settings and send messages to the Members and Guests of a Department, and also manage (i.e., add, delete, and modify) the Members of each Department.

The existing Departments are displayed in a table where the permissions can be enabled or disabled using check boxes.

Note: For more details about Department Permission Settings see the Departments/Send and Manage Permissions section.

User Group Permission Settings

On the Add/Edit User Group page, the HipLink administrator can set permissions for the Users of that group to be able to manage (i.e., create, edit, delete) Users assigned to other User Groups, and to view reports of the messages sent by the members of these User Groups.

This feature is aimed to help the HipLink administrator delegate User management functions to other users. The existing User Groups are displayed in a table where the permissions can be enabled or disabled using check boxes.

Note: The All Users radio button from the Reports Menu gives a User access to see the status of messages sent by Users assigned to User Groups for which he/she has the View Report permission enabled.

Note: You can only delete an empty User Group. Any Members of the Group will have to be removed or relocated prior to the Group's deletion.

Example: User Group Parameters

Name	Value	Comment
Name	Value	
Name	SysOper	required
Description	System Operator	optional

Example: Permission Settings

Permission Name	Status	Comment
SSSSSSSSdfdsafdsafdsafdsafdsafdsafds	Status	Comment
send to individual Receivers	No	if Departments are not supported
send to Groups	No	if Departments are not supported
add, modify, or delete Receivers	No	if Departments are not supported
add or delete Groups	No	if Departments are not supported
modify Groups	No	if Departments are not supported
add, modify, or delete Carriers	No	
add, modify, or delete Messengers	No	
access Standard Send panel	No	
access Two-Way Send panel	No	
access Quick Send panel	No	
access Schedule Send panel	No	
access Custom Escalation Send panel	No	
access Fax Send panel	No	
access Voice Send panel	No	
manage Users within this User Group	No	
see User Group Members report	No	
modify System Attendant	No	
modify Email Gateway	No	

modify Directories	No	
start or stop Services	Yes	
view Logs	Yes	
view or modify Queues	Yes	
add, modify, or delete Response Actions	Yes	
add, modify, or delete Templates	No	If Templates are supported
use Templates	Yes	If Templates are supported
modify License Key	No	
start Page	standard Send	standard Send (default), Reports Menu, Settings Menu

Note: The Departments and Templates features depend on the License Key permissions.

Example: Assign Departments

Department Name	Receivers Value			Groups			
	Send	Manage	View	Send	Add/Delete	Modify	View
Default	No	No	No	No	No	No	No

Example: Assign User Group Permissions

User Group Name	Manage User Group Value	View Report
sysOper	No	No
usrSend	No	No
Click to select/unselect all	No	No

Create Login Users

A User accesses HipLink using their User name and password. Different Users have different privileges to HipLink. The privileges of the User Group will determine which menus and panels a User has access to.

User panel displays all the Users of HipLink. This panel allows adding, modifying, deleting, or disabling HipLink Users. It is available to all Users belonging to sysAdmin User Group. For non-sysAdmin Users, the panel is available if the Users have following privileges:

- Manage Users within this User Group: allows a User to manage Users in their own User Group.
- Assign User Group Permissions -> Manage User Group: allows a User to manage Users in other User Groups (except for sysAdmin Group)

The panel contains following columns:

- Edit:** Clicking on this button directs the User to Edit User page for the selected User.
- User Name:** Displays User name.
- Description:** Displays User description.
- User Group:** Displays User Group that the User belongs to.
- Email:** Displays email address of the User.
- Last Login:** Displays last login time for the User.
- Status:** Displays the status of the User. This is described in detail below.

By default, the User records are sorted by User name. The columns on the User Panel can be resized and relocated to suit the User's needs.

The screenshot shows the HipLink User Panel. At the top, there is a navigation bar with 'Settings', 'Web Sign-up', 'Services', 'Send', 'Logs', 'Queues', 'Reports', and 'Statistics'. On the left, a sidebar menu includes 'Accounts' (Users, Recipients), 'System' (Carriers, Messengers, System Attendant, Email Gateway, SNPP Gateway, TAP Gateway, A.N. Gateway, File System Interface, Backup Service, Filters, Feedback, Directories), 'Monitoring', and 'General' (Password, Response Actions, Templates, Schedule Templates, DB Configuration, License Key, Global Settings, LDAP Settings, GIS Settings, Time Zones, Upgrades, About). The main content area is titled 'User Panel' and contains the text 'Setup User accounts and assign them to User Groups.' Below this is an 'Add User' button and a search bar with a 'Find' button. A table displays a list of users with columns: Sel, Edit, User Name, Description, User Group, Email, Last Login, and Status. The table contains six rows of user data. At the bottom of the table area, there are 'Delete', 'Enable', and 'Disable' buttons.

Sel	Edit	User Name	Description	User Group	Email	Last Login	Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	admin		sysAdmin		Wed Apr 28 17:13:20 2010	Enabled
<input type="checkbox"/>	<input checked="" type="checkbox"/>	irfan		sysAdmin	irfank@folio3.com		Enabled
<input type="checkbox"/>	<input checked="" type="checkbox"/>	mushanib		sysAdmin	mraheem@folio3.com		Enabled
<input type="checkbox"/>	<input checked="" type="checkbox"/>	noman		sysAdmin	nbutt@folio3.com		Enabled
<input type="checkbox"/>	<input checked="" type="checkbox"/>	saira		sysAdmin	ssarfraz@folio3.com	Mon Apr 26 15:03:26 2010	Enabled
<input type="checkbox"/>	<input checked="" type="checkbox"/>	shuja		sysAdmin	szaka@folio3.com		Enabled

TO SORT USERS:

1. On the User Panel, click on the button at the top of each column to sort the records in ascending order.
2. Click on the button again to sort in descending order.

TO FILTER USERS:

1. Enter key words in the first box of User Name, Description, or Email columns, or select a value from User Groups or Status columns.
2. Click on Filter link.
3. HipLink will search for Users with this specific text, refresh the page, and display the results.
4. To perform a wildcard search, use an * as a prefix, suffix, or both. For example, entering "Tech*" in the filter box in a particular column may return records with the words Technical, Technician, Tech Service, etc.
5. Click on Clear Filter link to clear filter from the grid and load all the records.
6. To perform filtering on Last Login, select one of the values for the dropdown:
 - a. Within N days: Enter the number of days in the pop-up; select time unit from the dropdown (mins/hours/days). This will display all the Users that have logged in within the given time.
 - b. Before N days: This will display all the Users that have logged in before the given time.
 - c. Exactly N days ago: This will display all the Users that have logged in exactly N days ago.
 - d. Range: Specify the range of days in which Users have logged in. This will display all the Users that have logged-in in the given range.
 - e. Never Logged In: This will display all the Users that have never logged in to HipLink.

- For managing a large number of Users, use either the simple Alphabetical Filtering feature (e.g., by pressing one of the links A, B, C,..., Z, and Others), or the Advanced Search feature to display only the information that you need (e.g., enter a keyword and press the Find button). Select the All link to display all of the available Users.

TO COPY USER RECORDS:

- Select a row by clicking it or select multiple rows by holding down either the Shift or Ctrl key while clicking on the rows.
- Click the Copy Rows link at the top of the data grid. This will copy the data in selected rows on your clipboard.

TO ADD A NEW USER:

- From the Settings menu, click Users on the left navigation bar.
- On the Users Panel, click the Add User button to reach the Add User Account page.
- Enter a unique Name for this User (mandatory).
- Enter a Description for this User (optional).
- Enter a Password for this User (mandatory).
- Retype the Password (mandatory).
- Enter the User's Email address (mandatory).
- Select a User Group from the dropdown menu (mandatory).
- Enter the Access Code for this User (optional but mandatory if the NetIQ User ID was entered). The Access Code is a 4 and up to 10 digit code used for authentication of Users that execute actions or send messages remotely through a 3rd party interface (email or the Voice Module for example). If the Access Code is set, it means that the User has permissions to send messages or execute actions using either a two-way device or another software application.
- Select a User Group from the dropdown menu (mandatory).
- Select the User Type from the dropdown menu: GUI User (default), Non GUI, or both.
- For a User of type Non GUI or both, enter the IP Address of the computer where the external application is running (mandatory).
- Set the Time Zone. Select the Server Time or a different time zone if it was defined. Time Zones are defined in the Settings menu.
- Click the Save button.

HipLink allows Users to be disabled at the time of adding them. Selecting the Disabled check adds the User with login disabled. Such a User would not be able to login using their credentials.

Note: *Users belonging to sysAdmin Group cannot be disabled. For such Users, Disabled checkbox is disabled by default.*

TO MODIFY A USER:

1. From the Settings menu, click User on the left navigation bar.
2. On the User Panel, find the User name you want to modify and click the Edit icon.
3. On the Edit User Account page, edit the Users Parameters.
4. Click the Save button to submit your changes and return to the Users Panel, Reset button to fill in the previous values, or Cancel button to return without saving.

TO DELETE A USER:

1. From the Settings menu, click Users on the left navigation bar.
2. On Users Panel, select the User you want to remove.
3. Click the Delete button.
4. Click OK button to confirm deletion or click Cancel to revoke this action.

TO DISABLE A USER:

1. From the Settings menu, click Users on the left navigation bar.
2. On Users Panel, select the User you want to disable.
3. Click Disable button.
4. Click the OK button to confirm disable or click Cancel to revoke this action.

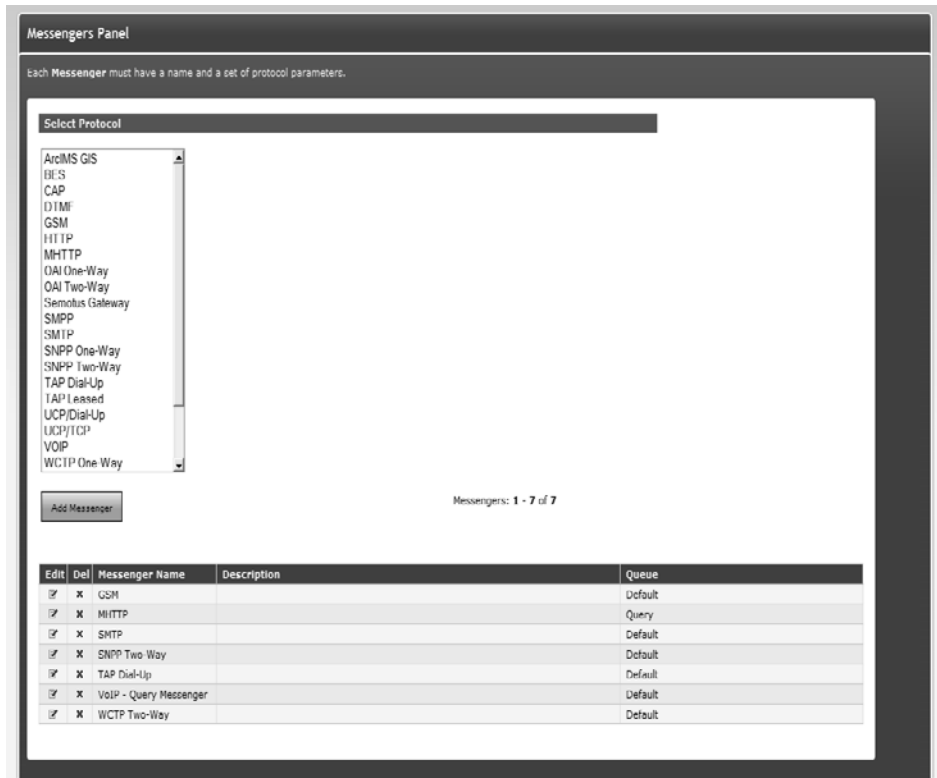
Note: *You can add more than one User with administrator privileges, and you can modify the predefined admin User. However, you cannot delete the pre-defined User, admin. The logged-on Users will be deleted after confirmation. Also, Users with administrative privileges (belonging to sysAdmin Group) cannot be disabled.*

Define Messengers

Messengers are services that handle the send message requests. A messenger will check the paging queue for message files, select only those messages that require its protocol, and use it to deliver the message to the Carrier.

Each Messenger handles one wireless protocol to deliver messages. However, depending on the message volume and redundancy needs of the company, more than one Messenger for one protocol may be required. For example, a company might license the TAP One-Way protocol, but need multiple TAP Messengers to manage the message volume. The maximum number of Messengers that can be added depends upon license key permissions.

The Messengers Panel can be accessed from Settings tab's left navigation bar in the Systems menu, as well as from the main Settings Panel. This panel is available to all sysAdmin Users. For non-sysAdmin Users, the panel is available if add, modify, or delete Messengers permission is assigned in the User Group.



The list of protocols available on the panel displays all the protocols supported by the License Key. To add a Messenger, you need to select a protocol first.

The panel contains the following columns:

1. **Edit:** Clicking on this icon directs the User to the Edit Messenger page for the selected Messenger.
2. **Del:** Clicking on this icon deletes the selected Messenger after User confirmation.
3. **Messenger Name:** Displays Messenger name.
4. **Description:** Displays messenger description.
5. **Queue:** Displays the name of the paging queue assigned to the Messenger.

Standard Protocols – SNPP ~ WCTP ~ SMTP

For many Messengers the Parameters for set up are the same. These include SMTP, SNPP, WCTP, etc. We have given the parameters that need to be defined.

1. On the Messengers panel, select a protocol from the list of protocols.
2. Press the Add Messenger button to reach the Add Messenger page.

Add Messenger

Each **Messenger** must have a name and a set of protocol parameters.

Messenger Parameters

Name: *

Description:

Paging Queue: *

Protocol Parameters

Protocol Type: **SMTP**

Queue Checking Period: * (seconds)

Note: Fields marked with an asterisk "" are mandatory.

There are two sections on the Add Messenger page:

1. **Messenger Parameters (Common to all protocols)**
 - a. Enter a unique Name for the messenger (mandatory).
 - b. Enter a Description for this messenger (optional).
 - c. Select a Paging Queue from the dropdown (displayed and mandatory only if multiple queues are enabled in License Key).

2. **Protocol Parameters (Specific for each protocol)**

There are a few parameters that are common to all protocols. These are defined below:

- a. Select Queue Checking Period from the dropdown. This is the number of seconds to wait before the messenger checks the paging queue (mandatory, 10 seconds by default).

For protocols that require additional details, protocol parameters are defined separately:


DTMF & TDD/TTY Protocol

Protocol Parameters

Protocol Type: **DTMF**

Queue Checking Period: * (seconds)

Serial Port: *

Modem Init Command: *  Help

Modem Dial Command:

Flow Control: Hardware Software

1. Select Serial Port from the dropdown: COM1, COM2, COM3 etc. for Windows Operating Systems. For UNIX, you have to enter the Serial Port name in a text box because the device name will depend on your Operating System (i.e., Solaris, HP, Linux, AIX). An example for a serial port in UNIX is /dev/ttyS0.
2. Enter Modem Initialization Command for the modem (mandatory). Click the Modem List icon to select a modem type from the list. The modem parameters fields will be automatically set with default values. If needed, you can change these settings by entering new values.

Note: The Help button right next to it provides support for modem initialization strings field.

GSM Protocol

HipLink can send and receive SMS messages using a GSM modem or a standard GSM mobile phone connected to a RS232 communication port.

Requirements

The requirements for GSM modems and handsets are the following:

- Support the SMS send/receive AT command set (GSM 07.05 / 07.07),
- Valid SIM card with a GSM operator capable of delivering SMS messages,
- Serial interface connection.

Compatible devices

- Any GSM device that complies with GSM 07.05 and GSM 07.07

Recommended devices

- Merlin G100/G201 GSM/GPRS wireless PC Card Modem from Novatel Wireless (<www.novatel-wireless.com>),
- FastTrack G1200 series GSM/GPRS modem from WaveCom (<<http://www.wavecom.com>>),
- Siemens M20T, MC35T, TC35T (<www.siemens.com/wm>).

Settings

- The modem has to be connected through a serial port to the computer hosting the HipLink server.
- A license key supporting the GSM protocol is required.
- A new Messenger has to be created for the GSM protocol. See the required protocol parameters below.
- A Carrier has to be created for the GSM protocol. There are no specific parameters for the GSM Carrier.

Once the GSM Messenger is started and a GSM Carrier is created, HipLink is capable of one-way or two-way SMS communication with GSM handsets.

ONE-WAY SMS COMMUNICATION

SMS messages can be sent to GSM handsets using HipLink. The sender of the message is the number of the SIM card used by the GSM modem. If message delivery reports are available, the status of the message will be updated in the reports section.

TWO-WAY SMS COMMUNICATION

If HipLink is licensed for two-way communication, messages can be initiated on GSM handsets and sent to HipLink using the number of the SIM card used by the GSM modem.

HipLink comes with a few predefined commands, like confirming and sending messages. Additional custom commands can be implemented by the HipLink administrator in the Response Actions panel. Normally response actions generate a response which is delivered back to the device that initiated the command.

Protocol Parameters	
Protocol Type	GSM
Queue Checking Period	1 * (seconds)
Serial Port	COM9 *
Password	
SMSC Number	923330005150
Baudrate	460800
Stop Bits	1
Data Bits	8
Parity	Even *
Flow Control	<input checked="" type="radio"/> Hardware <input type="radio"/> Software
GSM initial strings	[modem initialization] ATZ AT&F ATE0 ATS0=0 ATX4&C1
Wait Time to Reset Modem	0 (seconds)

GSM Protocol

1. Select Serial Port from the dropdown: COM1, COM2, COM3 etc. for Windows Operating Systems. For UNIX , you have to enter the Serial Port name in a text box because the device name will depend on your Operating System (i.e., Solaris, HP, Linux, AIX). An example for a serial port in UNIX is /dev/ttyS0.
2. Set Password for the SIM card (if any).
3. Enter the SMSC Number (Short Messaging Service Center) for your GSM Carrier (mandatory).
4. Enter the serial port settings: Baud Rate, Parity, Data Bits, and Stop Bits, Flow Control. These settings should be similar to those of your GSM modem.
5. Choose the appropriate modem initialization string from the GSM Initial String edit box or enter a new one. You might delete the strings that are not required. The following example shows how to query a GSM modem and set up the initialization string for it:
at+cnmi=?+CNMI: (0-3),(0,1),(0,2,3),(0,2),(1) // example result. This result shows what numbers are allowed in this setting. Set the AT+CNMI setting to an appropriate value, for example: AT+CNMI=2,1,2,2,1
6. Choose Wait Time to Reset Modem from the dropdown.

Facebook Protocol

To be able to post to a Facebook account you must first have a messenger defined with standard fields and then create the Carrier. The full instructions for Facebook setup are included in the carrier section.

HNP Protocol

Protocol Parameters	
Protocol Type	HNP Two-Way
Queue Checking Period	10 * (seconds)
File Transfer Method	Peer To Peer Bytestream
Host Port	0 *
Packet Size	65 (KBs)
File Transfer Timeout	15 (seconds)

1. Select File Transfer Method from the dropdown.
2. Enter Host Port used at HNP Manager Server (mandatory).
3. Select Packet Size from the dropdown. This is the size of the packet transferred
4. Select File Transfer Timeout from the dropdown. This is the time (in seconds) after which the file transfer will be cancelled.

OAI Protocol

The OAI Messengers are written to communicate with SpectraLink Wireless phones. It communicates with the OAI Gateway (using SpectraLink's Open Application Interface). The protocol supports both 1-way and 2-way communication.

The OAI gateway is installed and configured by SpectraLink at the customer's site. It is configured to talk to the handsets. The OAI gateway can communicate with our Messengers either over a TCIP port or RS- 232 serial port.

Protocols Parameters	
Protocol Type	OAI Two-Way
Queue Checking Period	10 * (seconds)
Communication Type	<input type="radio"/> Serial Port <input checked="" type="radio"/> TCP/IP
Gateway IP	192.168.4.174 *
Port	5456 *

OAI Protocol - Communication Type: TCP/IP

1. Select Communication Type as TCP/IP if HipLink Messenger is communicating with the OAI gateway over the network.
 - a. Provide Gateway IP for OAI gateway.
 - b. Provide Port number over which OAI gateway will communicate (default is 5456). Consult with the SpectraLink administrator for the port number, in case the default is not used.
2. Select Communication Type as Serial Port if OAI gateway is connected to the HipLink System via a serial port. Select appropriate values for Serial Port, Baud rate, Stop Bits, Data Bits and Parity Bits.

Protocols Parameters	
Protocol Type	OAI Two-Way
Queue Checking Period	10 * (seconds)
Communication Type	<input checked="" type="radio"/> Serial Port <input type="radio"/> TCP/IP
Serial Port	COM1
Baudrate	110
Stop Bits	1
Data Bits	5
Parity	Even

OAI Protocol - Communication Type: Serial Port

SMPP Protocol

Set the SMPP Carrier ID. This should match the SMPP Carrier ID defined for the SMPP Carrier.
Note: SMPP protocol requires a Messenger defined for each Carrier.

TAP Dial-Up Protocol

Protocol Parameters	
Protocol Type	TAP Dial-Up
Queue Checking Period	1 * (seconds)
Serial Port	COM1 *
Modem Init Command	AT&F *
Modem Dial Command	ATDT
Flow Control	<input checked="" type="radio"/> Hardware <input type="radio"/> Software

1. Select Serial Port from the dropdown: COM1, COM2, COM3, etc. for Windows Operating Systems. For UNIX , you have to enter the Serial Port name in a text box because the device name will depend on your Operating System (i.e., Solaris, HP, Linux, AIX). An example for a serial port in UNIX is /dev/ttyS0.
2. Enter Modem Initialization Command for the modem (mandatory).
 - a. Click the Modem List icon to select a modem type from the list. The modem parameters fields will be automatically set with default values. If needed, you can change these settings by entering new values.
3. Enter Modem Dial Command line for the modem (optional, ATDT usually works).
4. Select the Flow Control. This should be similar to that of your modem device.

TAP-Leased Protocol

Protocol Parameters	
Protocol Type	TAP Leased
Queue Checking Period	5 * (seconds)
Serial Port	COM10 *
Flow Control	<input checked="" type="radio"/> Hardware <input type="radio"/> Software

1. Select Serial Port from the dropdown: COM1, COM2, COM3, etc. for Windows Operating Systems. For UNIX , you have to enter the Serial Port name in a text box because the device name will depend on your Operating System (i.e., Solaris, HP, Linux, AIX). An example for a serial port in UNIX is /dev/ttyS0.

2. Select the Flow Control. This should be similar to that of your modem device.

Twitter Protocol

To be able to post to a Twitter account you must first have a messenger defined with standard fields and then create the Carrier. The full instructions for Twitter setup are included in the carrier section.

UCP/Dial-Up Protocol

Protocol Parameters	
Protocol Type	UCP/Dial-Up
Queue Checking Period	10 * (seconds)
Serial Port	COM1 *
Modem Init Command	ATZ * Help
Modem Dial Command	ATDT
Flow Control	<input checked="" type="radio"/> Hardware <input type="radio"/> Software

1. Select the Serial Port from the dropdown: COM1, COM2, COM3, etc. for Windows Operating Systems. For UNIX, you have to enter the Serial Port name in a text box because the device name will depend on your Operating System (i.e., Solaris, HP, Linux, AIX). An example for a serial port in UNIX is /dev/ttyS0.
2. Enter Modem Initialization Command for the modem (mandatory).
 - a. Click the Modem List icon to select a modem type from the list. The modem parameters fields will be automatically set with default values. If needed, you can change these settings by entering new values.
3. Enter Modem Dial Command line for the modem (optional, ATDT usually works).
4. Select the Flow Control. This should be similar to that of your modem device.

XMPP Protocol

Protocol Parameters	
Protocol Type	XMPP
Queue Checking Period	3 * (seconds)
File Transfer Timeout	30 (seconds)

1. Select File Transfer Timeout from the dropdown. This is the time (in seconds) after which the file transfer will be cancelled.

TO MODIFY A MESSENGER

1. On the Messengers Panel, find the Messenger name you want to modify and click on Edit icon.
2. On the Edit Messenger page, edit the parameters.
3. Press Save to save the changes made on the panel, Reset to reset the fields, or Cancel to go back to the Messengers Panel without saving the changes.

TO DELETE MESSENGER

1. On the Messengers Panel, find the Messenger name you want to delete and select the Del checkbox.
2. Press the Delete button
3. Press OK to confirm deletion, or Cancel to revoke the action.

Note: A Messenger cannot be deleted if it is running. To delete a Messenger, you first need to stop it from the Services Panel.

Create Carriers

Carrier is a service provider that is used to deliver messages from HipLink to wireless devices. The Carriers panel can be accessed through the Settings tab in System section. This panel is available to all sysAdmin Users. For non-sysAdmin Users, the panel is available if add, modify, or delete Carriers permission is assigned in the User Group.

The screenshot displays the HipLink Carriers Panel. On the left is a sidebar with a tree view containing categories like Accounts, Recipients, System, and General. The main content area is titled 'Carriers Panel' and includes a 'Select Protocol' dropdown menu listing various protocols such as BES, CAP, (D)TMF, GSM, IHTTP, MHTTP, OAI One-Way, OAI Two-Way, Semolus Gateway, SMPP, SMTP, SNPP One-Way, SNPP Two-Way, TAP Dial-Up, TAP Leased, UCP/Dial-Up, UCP/TCP, VOIP, WCTP One-Way, and WCTP Two Way. Below the dropdown is an 'Add Carrier' button. A table below shows a list of carriers with columns for Edit, Del, Disable, Auto Update, Carrier Name, Description, Backup Carrier, Backup Status, and Queue. At the bottom, there is an 'Automatic Carrier Updates' section with a 'Download' button and a note: 'Note: HipLink will display carriers list with the available updates, to allow user selected carriers to be updated.'

Edit	Del	Disable	Auto Update	Carrier Name	Description	Backup Carrier	Backup Status	Queue
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	AT&T Enterprise SNPP	Requires Enterprise Paging Service - Internet Connection			Default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	AT&T Enterprise WCTP	Requires Enterprise Paging Service - Internet Connection			Default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	BES Carrier 1		T-Mobile Email	In Use	Default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	OAI Two-Way Carrier 1				Default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	T-Mobile Email	Requires Network Connection			Default
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	VOIP Carrier 1				Default

The list of protocols available on the panel displays all the protocols supported by the License Key. Carriers use protocols to deliver messages. To add a Carrier, you need to select a protocol first.

Important: *If the multiple Paging Queues feature is enabled in the License Key, then you need to create the respective Messenger before you created a Carrier for any protocol.*

The panel contains the following columns:

1. **Edit:** Clicking on this icon direct User to Edit Carrier page for the selected Carrier.
2. **Del:** Clicking on this icon deletes the selected Carrier after User confirmation.
3. **Disable:** A device with a backup Carrier defined for it can be disabled by selecting this checkbox. To select a backup Carrier, go to the Carrier's Add/Edit page and in the Carrier Parameter section, the User can select up to two different backup Carriers.
4. **Auto Update:** Selecting this checkbox enables an automatic update of the Carrier. This is explained in section 4.3.2.
5. **Carrier Name:** Displays Carrier name.
6. **Description:** Displays Carrier description.
7. **Backup Carrier:** Displays backup Carrier (if any) defined for the Carrier.
8. **Backup Status:** Displays the status of the backup Carrier if the Carrier is disabled.
9. **Queue:** Displays the name of paging queue assigned to the Carrier.

TO ADD A CARRIER:

1. On the Carriers panel, select a protocol from the list of protocols.
2. Press the Add Carrier button to reach the Add Carrier page.

Add SNPP Carrier

Each Carrier must have unique name and a set of protocol parameters.
A Carrier could have a backup carrier assigned to it and a set of message parameter.

Carrier Parameters

Name: AT&T Enterprise SNPP * Carrier List
 Description: Requires Enterprise Pa
 Paging Queue: Default *
 Backup carrier:
 Backup carrier 2:
 Check for Automatic Carrier Updates:

Protocol Parameters

Type: SNPP Two-Way
 SNPP Host Server: snpp.att.net *
 SNPP Port Number: 444 *
 SNPP Server Login Name [Password]:
 2-Way Response Type: Multi-Choice
 Messenger Query Interval: 10 * (seconds)
 Messenger Query Retry: 5 * (times)

Message Parameters

Truncate long message:
 Maximum total length (characters): 320
 Split long message into parts:
 Maximum part length (characters): 160
 Enable Numbering on message parts: Disabled
 Number of retries (times): 0
 PIN template:
 Save Reset Cancel

Note: Fields marked with an asterisk "" are mandatory.

There are three sections on the Add Carrier page:

1. Carrier Parameters: Common to all protocols.
2. Protocol Parameters: Specific for each protocol.
3. Message Parameters: Common to all protocols.

Carrier Parameters:

1. Enter a unique Name for the Carrier (mandatory).
2. Enter a Description for this Carrier (optional).
3. Select a Paging Queue from the dropdown (displayed and mandatory only if multiple queues are enabled in License Key).For each Carrier, the dropdown lists only those queues of which a Messenger for its protocol is assigned.
4. Select a Backup Carrier from the dropdown (optional). In the event that messages cannot be delivered to the primary Carrier after a specified number of retries, HipLink will use the backup Carrier to deliver the messages.
5. Select a Backup Carrier 2 from the dropdown (optional). In the event that messages cannot be delivered to the first backup Carrier either, HipLink will use the second backup Carrier to deliver the messages.

Note: Once a Carrier has been assigned to a backup Carrier, then it can be disabled from the Carriers Panel.

6. Select Check for Automatic Carrier Updates checkbox to enable automatic update of the Carrier.

Protocol Parameters:

Protocol parameters are defined separately for each protocol:

BES Carrier

1. Enter the BES URL (mandatory).
2. Enter the Handheld Application Port (mandatory, default 101).
3. Enter the Handheld Request URI (optional). For example, @skytel.com.
4. Select Skip Content Push to skip content push (optional).

Protocol Parameters	
Type	BES
BES URL	192.168.4.174:8080/push *
Handheld Application Port	101 *
Handheld Request URI	
Skip Content Push	<input type="checkbox"/>

CAP Carrier

Protocol Parameters	
Type	CAP
Host URL	http://generic:generic@t *
Sender	<input checked="" type="checkbox"/> Use Sender's Email

Advanced Settings	
Status	Actual *
Message Type	Alert *
Scope	Public *
Category	Safety *
Event	Tone Devices *
Urgency	Immediate *
Severity	Severe *
Certainty	Likely *

1. **Host URL** (mandatory): URL of the server where WSI application is hosted.
For example: http://<username:password>@<ip>:<port>/cgi-bin/parse_tone.cgi
2. **Sender: Use Sender's Email**: Select this checkbox if you want the User's email address as the Sender. If you want to use a different email address as Sender email, unselect this checkbox and provide an email address in the field displayed.
3. **Advanced Settings**: These settings are configured for outbound CAP message. When delivered to the target recipients, a CAP message has the following fields defined for it:
 - a. **Status**: Sets the status of the message. The status depends on the organization
 - b. **Message Type**: Defines the message type
 - c. **Scope**: Defines the scope of the message
 - d. **Category**: Defines the category of the message
 - e. **Event**: Defines the event for message generation
 - f. **Urgency**: Defines the urgency of the message
 - g. **Severity**: Defines the severity of the message
 - h. **Certainty**: Defines the certainty of the message

DTMF & TDD/TTY Carrier

Protocol Parameters	
Type	DTMF
Use as TDD/TTY Carrier	<input type="checkbox"/>
Baud Rate	2400 *
Parity	Even *
Data Bits	7 *
Stop Bits	1 *
Message Center Phone Number	
First Delay	6 * pause after dial completion (seconds)
Second Delay	0 * pause after PIN submission (seconds)

1. Use as TDD/TTY Carrier: If this option is enabled, then the Message Center Phone Number, First Delay and Second Delay will not be required and they will be hidden.
 - a. Select Baud Rate from the dropdown, specific to your Carrier.
 - b. Select Parity from the dropdown, specific to your Carrier.
 - c. Select Data Bits from the dropdown, specific to your Carrier.
 - d. Select Stop Bits from the dropdown, specific to your Carrier.

Note: TDD/TTY (Telecommunications Device for the Deaf/TeleTypewriter) used for sending messages to the hearing and speech impaired.

2. Unchecked Use as TDD/TTY Carrier: If this option is not checked, then the additional fields: Message Center Phone Number, First Delay and Second Delay will be visible.
 - a. Select Baud Rate from the dropdown, specific to your Carrier.
 - b. Select Parity from the dropdown, specific to your Carrier.
 - c. Select Data Bits from the dropdown, specific to your Carrier.
 - d. Select Stop Bits from the dropdown, specific to your Carrier.
 - e. Enter the Message Center Phone Number for your DTMF Carrier (optional).
 - f. Enter the First Delay (mandatory). This delay represents a pause after the dial completion, necessary to skip the welcome message of the Message Center. The default value of this parameter is six seconds, but it is recommended to adjust the delay manually by trial and error.
 - g. Enter the Second Delay (optional). Sometimes you need to use another pause after the submission of the PIN. If this is the case, it is recommended to adjust this delay manually by trial and error.

Facebook Carrier and Receiver Set-up

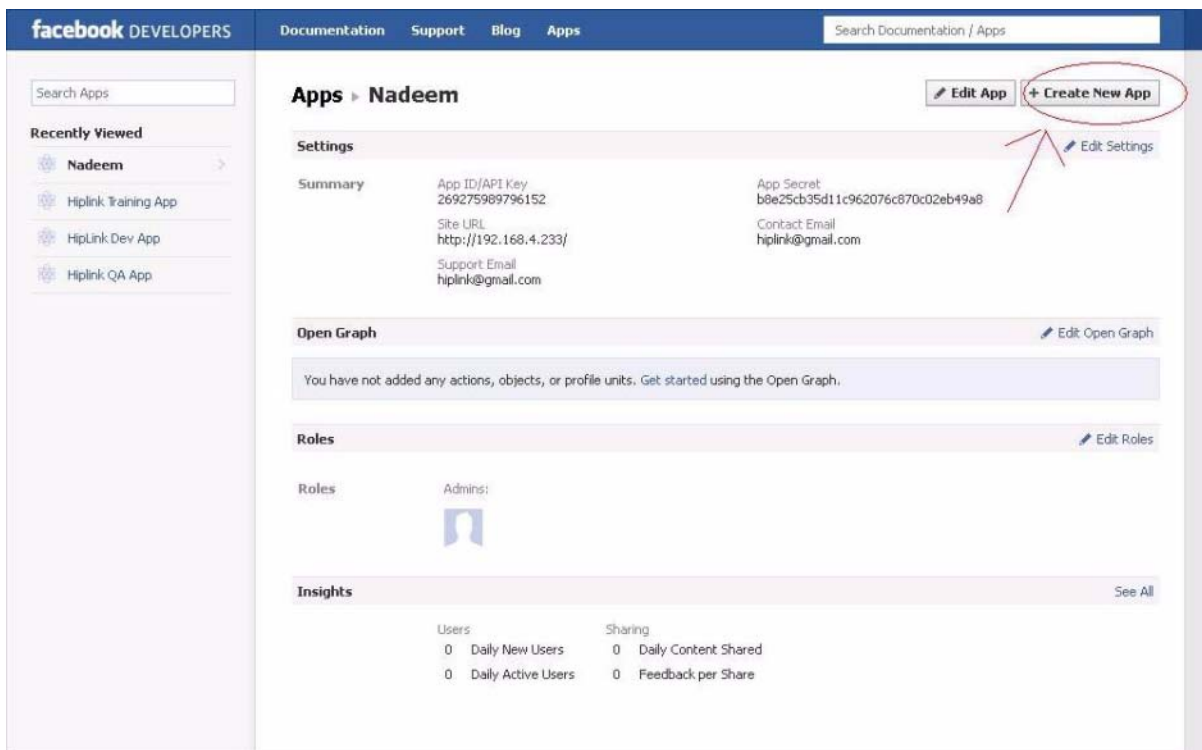
In order to set up a carrier for Facebook you must first go through the process to register HipLink as an approved application for your Facebook account and obtain the proper ID

Step 1:

1. Access Facebook in browser on <http://www.facebook.com>
2. Create a user account on Facebook, if you do not have one.
3. Login to <http://developers.facebook.com/> with this account.
4. Click on Apps tab at the top.



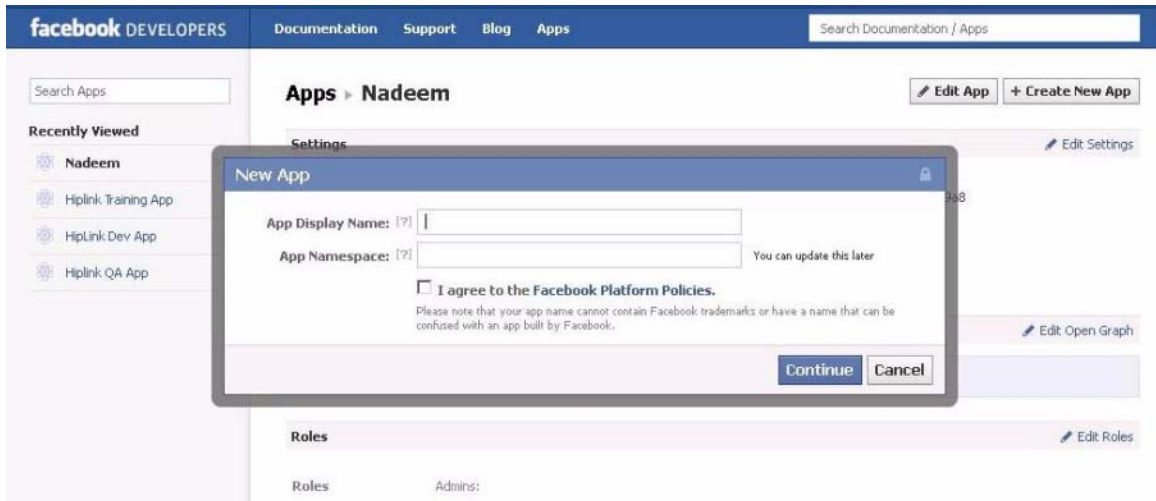
5. Click on Create New App on top right.



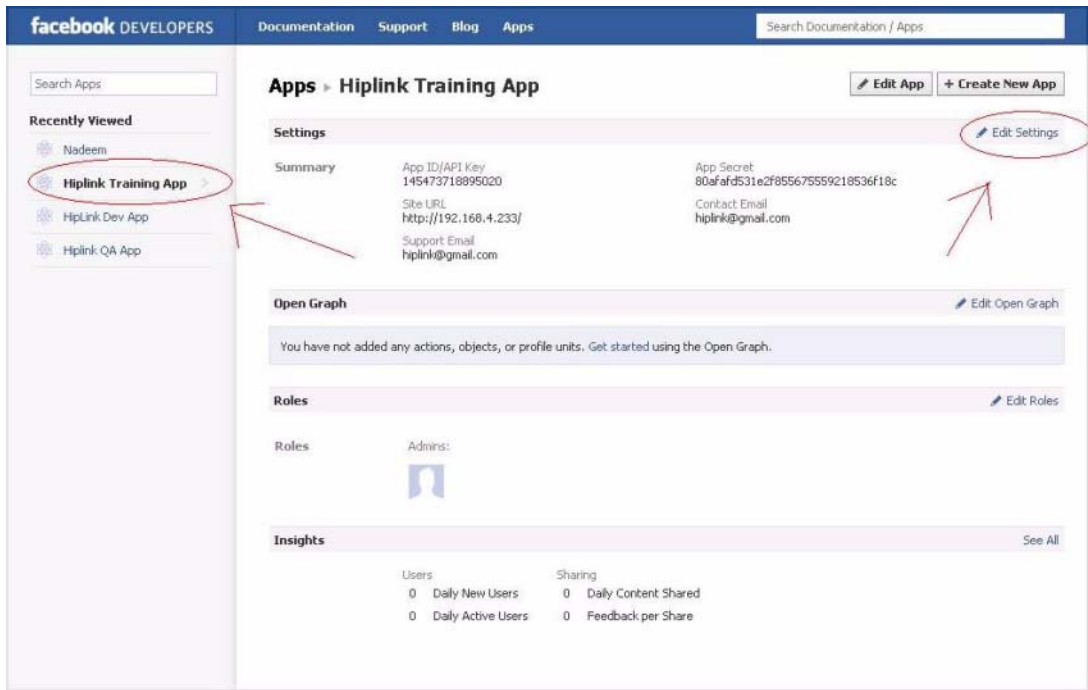
6. In the New App pop-up window, give the app an appropriate name in App Display Name.

7. Leave App Namespace blank.

8. Click on Continue.



9. Once the app is created, navigate to the app main page from the left panel.
10. Click on Edit Settings at top right.



11. In the Website field, enter the URL where HipLink is currently deployed. This would need to be changed if the location of HipLink is changed.

facebook DEVELOPERS Documentation Support Blog Apps Search Documentation / Apps

Related links
 Use Debug Tool
 Use Graph API Explorer
 See App Timeline View
 Promote with an Ad
 Translate your App
 Delete App

App Display Name: [?]


App Namespace: [?]

Contact Email: [?]

App Domain: [?]

Category: [?]

Cloud Services

 **Cloud Services** ×
 Need hosting for your app? We are partnering with the top cloud service providers to make building apps easy.
[Get Started](#) [Learn More](#)

Hosting URL: [?] You have not generated a URL through one of our partners ([Get one](#))

Select how your app integrates with Facebook

Website ×
 Site URL: [?]

App on Facebook I want to build an app on Facebook.com.

Mobile Web I have a mobile web app.

Native iOS App I have a native iOS app.

Native Android App I have a native Android app.

Page Tab I want to build a custom tab for Facebook Pages.

[Save Changes](#)

Step 2:

1. Log into HipLink.
2. Create a Facebook messenger if you have not already done so.
3. Start the messenger service.
4. Create a Facebook carrier.
5. In the Protocol Parameters section, give the Application ID/API Key of the app you just created.

facebook DEVELOPERS Documentation Support Blog Apps Search Documentation / Apps

Search Apps

Recently Viewed

- Hiplink Training App
- Nadeem
- Hiplink Dev App
- Hiplink QA App

Apps > Hiplink Training App

[Edit App](#) [+ Create New App](#)

Settings [Edit Settings](#)

Summary


App ID/API Key 145473718895020	App Secret 80afafd531e2f855675559218536f18c
Site URL http://192.168.4.233/	Contact Email hiplink@gmail.com
Support Email hiplink@gmail.com	

Open Graph [Edit Open Graph](#)

You have not added any actions, objects, or profile units. Get started using the Open Graph.

Roles [Edit Roles](#)

Roles Admins:



Insights [See All](#)

Users	Sharing
0 Daily New Users	0 Daily Content Shared
0 Daily Active Users	0 Feedback per Share

HipLink [Support Email](#) [Help](#) [Logout](#)

[Settings](#) [Web Sign-up](#) [Services](#) [Send](#) [Logs](#) [Queues](#) [Reports](#) [Statistics](#)

Accounts

- Users
- User Groups
- User Search
- Session Manager
- Recipient User

Recipients

- Departments
- Receivers
- Receiver Groups
- On-Duty Groups
- Escalation Groups
- Rotate Groups
- Follow-Me Groups
- Subscription Groups
- Receiver Search
- My Favorites

System

Carriers

- Messengers
- System Attendant
- Email Gateway
- SNPP Gateway
- TAP Gateway
- A.N. Gateway
- File System Interface
- Backup Service
- Filters
- Feedback
- Directories

Monitoring

- SNMP

General

- Response Actions
- Templates
- Schedule Templates
- DB Configuration
- License Key
- Global Settings
- LDAP Settings
- GIS Settings
- Logs Settings
- Time Zones
- Upgrades
- About

Edit Facebook Carrier

Each Carrier must have a unique name and a set of protocol parameters.
A Carrier could have a backup carrier assigned to it, and a set of message parameters.

Carrier Parameters

Name	Facebook Carrier 1 *
Description	
Paging Queue	facebook *
Backup Carrier	
Backup Carrier 2	
Check for Automatic Carrier Updates	<input type="checkbox"/>

Protocol Parameters

Type	Facebook
Application ID	145473718895020 *

Message Parameters

Truncate long message	<input type="checkbox"/>
Maximum total length (characters)	200
Split long message into parts	<input type="checkbox"/>
Maximum part length (characters)	100
Numbering scheme on parts	Disabled
Number of retries (times)	0
PIN template	

[Save](#) [Reset](#) [Cancel](#)

Note: Fields marked with an asterisk "" are mandatory.

Create a receiver with following parameters:

1. Primary Carrier: Facebook carrier
2. Primary PIN: Facebook record ID of the Facebook user.
3. To find out the Facebook user record ID, follow these steps:
4. Access your Facebook profile page by clicking on your name. Your Facebook username would be written in the URL in the format `http://www.facebook.com/<your user name>` e.g `https://www.facebook.com/johndev`



- a. Copy this user name and append it in this form the browser url: `https://graph.facebook.com/<your user name>` (e.g. if your Facebook username was johndev from your URL `https://www.facebook.com/johndev`, then write in the browser url: `https://graph.facebook.com/johndev`.) and press enter
- b. The Facebook user record ID would be displayed on the page. Copy this record ID and use it as the pin for your Facebook receiver.



5. Although a Facebook receiver has been created, messaging to this receiver is still not possible since it is unauthorized.
6. To authorize this receiver, go to the following directory path on HipLink server:
...\\HipLink\\server\\htdocs\\social
7. Edit the file fbhlauth.html in notepad.
8. Append the APP ID and CARRIER ID on top (the carrier ID would be visible in the browser command bar) by editing the respective Facebook carrier. It would be the numeric value written after parameter **rid**. E.g. in the URL `http://192.168.4.74/cgi-bin/hip-link.csx?cmd=Carrier_Add_Edit&uid=3&sid=18&rid=3&pageid=1` the Facebook carrier ID is 3.

The screenshot shows a web browser window with the URL `192.168.4.74/cgi-bin/hiplink.cgi?cmd=Carrier_Add_Edit&uid=38&id=38&sgid=1`. The `id=38` part is circled in red. Below the browser is a Notepad window titled `fbHLAuth.html - Notepad` containing the following JavaScript code:

```

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title[ Hiplink ~ Facebook Integration ]</title>
<link href="style.css" rel="stylesheet" type="text/css" />
</head>
<body>
<script type="text/javascript">
var accessToken = "";
var appID = 278266872191728;
var iCarrierID = 29;
function displayUser(user)
{
    var path = "/cgi-bin/action.exe?";
    var queryParams = ['cmd=updReceiver&accessToken=', 'modid=ivr', 'carrier_id=' + iCarri
        'profile_id=' + user.id,
        accessToken, 'callback=displaystatus'];
    var query = queryParams.join('&');
    var url = path + query;
    // use jsonp to call
    var script = document.createElement('script');
    script.src = url;
    document.body.appendChild(script);
}
function displaystatus(response)
{
    var status = document.getElementById('status');
    var respText = document.createTextNode('Status: '
        + response.status + '.');
    status.appendChild(respText);
}

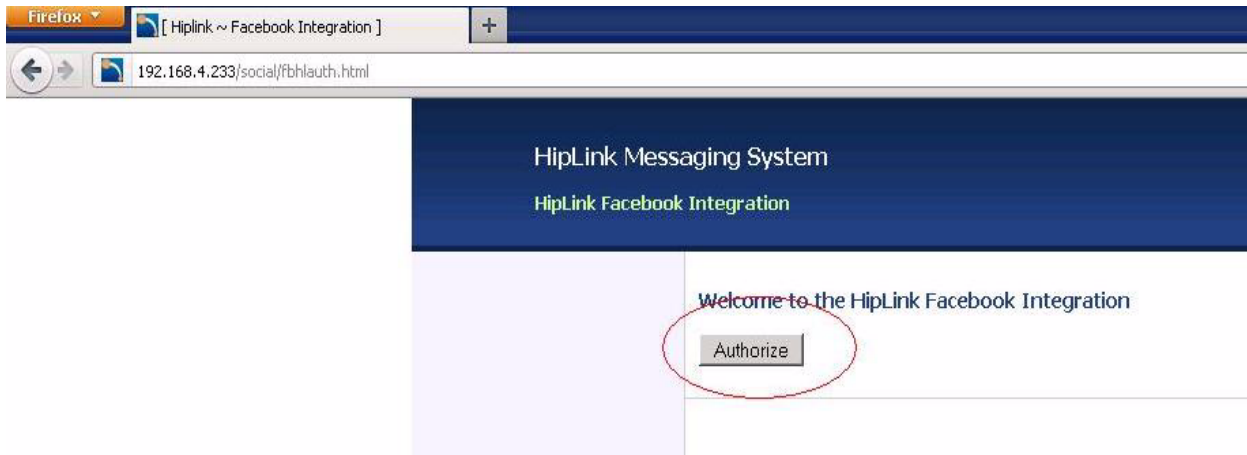
```

The `var iCarrierID = 29;` line is circled in red in the Notepad window.

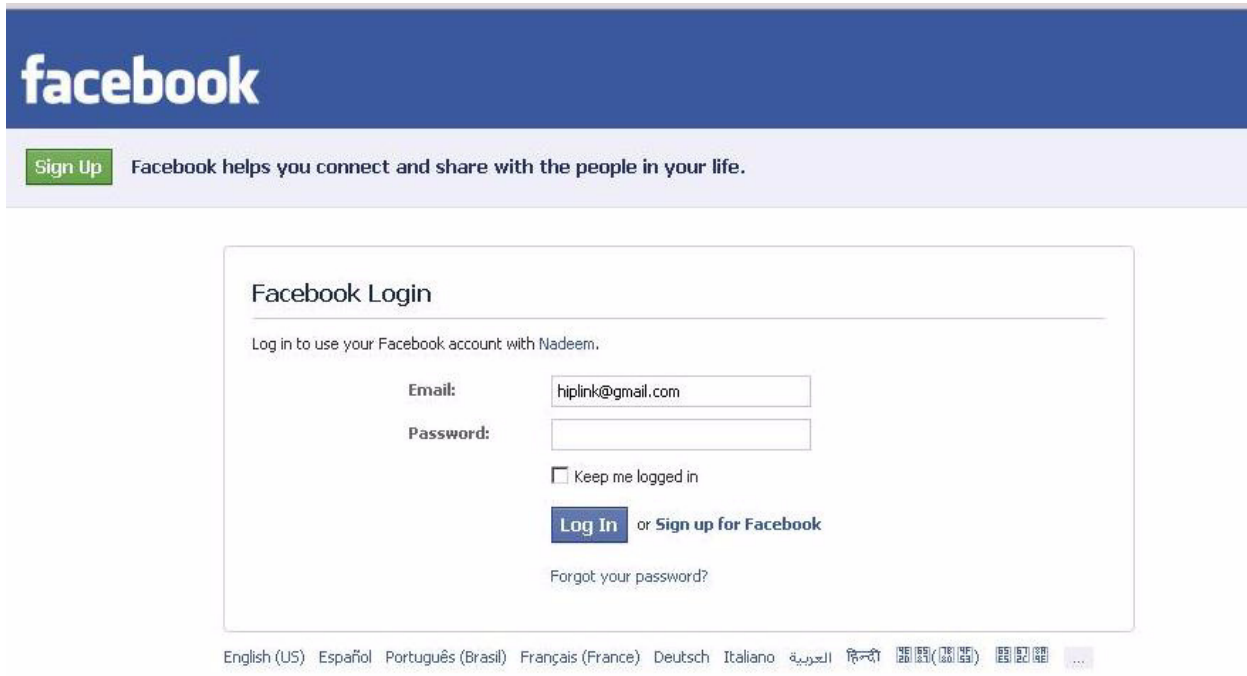
9. Save the changes.

Step 3:

1. Access the following url in the browser: <http://<hiplink-ip:port>/social/fbhlauth.html>
2. Click on the Authorize button.



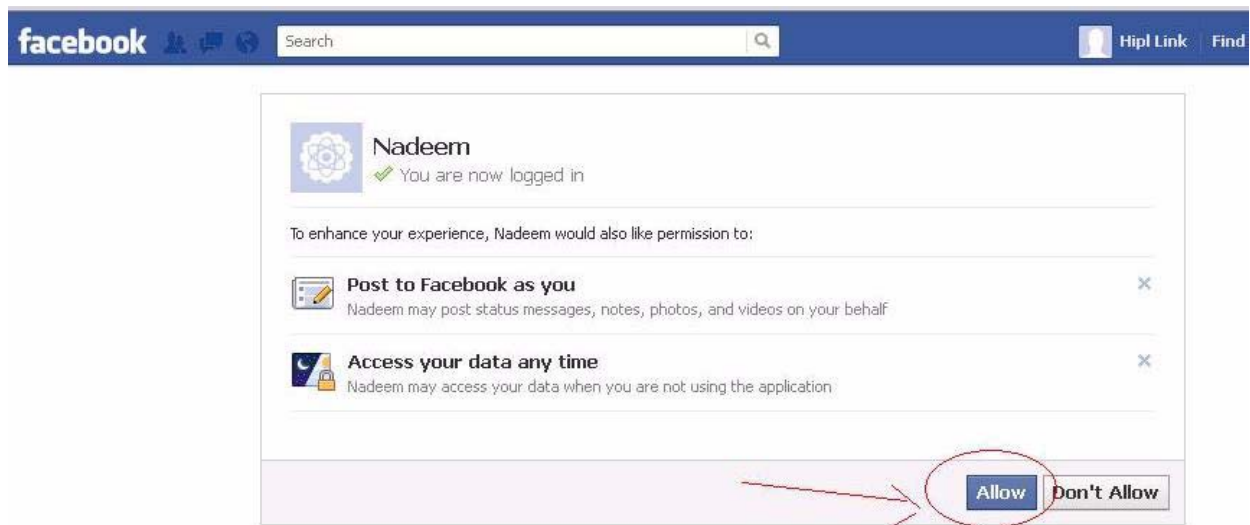
3. Login to Facebook with the credentials of the user whose receiver has been created in HipLink.



4. Click on the Okay, Go to App button



5. On the next page, click on the Allow button.



You are now ready to send messages from HipLink to Facebook.

Generic Delivery Protocol

Protocol Parameters	
Type	Generic Deliver
Executable file path	C:\generic.bat *

1. Executable file path: The path of executable (batch) file. When a message is sent via Generic Deliver Carrier, it triggers an action that results in the execution of the provided file.

GSM Carrier

There are no specific parameters to set for a Carrier using the GSM protocol.

HNP Carrier

Protocol Parameters	
Type	HNP Two-Way
Host	<input type="text" value="192.168.4.232"/> *
Service Name	<input type="text" value="hiplink"/> *
Port	<input type="text" value="10000"/> *
Connection Security	<input type="text" value="Can be PLAIN"/> ▾
Messenger Query Interval	<input type="text" value="10"/> ▾ * (seconds)
Messenger Query Retry	<input type="text" value="60"/> ▾ * (times)

The Carrier configurations are similar for both one-way and two-way protocols, with few additional configurations for two-way protocol.

All the fields in this section are pre-populated with their default values.

1. Enter HNP Manager Host address (mandatory).
2. Enter Service Name used by HNP Manager (mandatory).
3. Enter Port used by the service (mandatory)
4. Select Connection Security from the dropdown.
5. Select Messenger Query Interval from the dropdown. For two-way messaging, HipLink must query the Carrier to determine if a response to the message has been sent by the Receiver. The Messenger Query Interval specifies the amount of time (in seconds) between queries (default time is 120 seconds)
6. Select Messenger Query Retry value from the dropdown. This specifies the number of times HipLink should query the Carrier to determine if the Receiver has sent a response to the message.

HTTP Carrier

Protocol Parameters	
Type	HTTP
Target URL	https://web.mms.msg.tn *
Method*	<input checked="" type="radio"/> Post <input type="radio"/> Get
Message Field	text *
Sender Field	sender
Subject Field	

PIN Format*	
PIN	<input checked="" type="radio"/> receiver
Area code + 7 digit number	<input type="radio"/> <input type="text"/> <input type="text"/>
Area code + 3 digit prefix + 4 digit suffix	<input type="radio"/> <input type="text"/> <input type="text"/> <input type="text"/>

Custom Fields	
Field Name	Field Value
msgTermsUse	on
Send.x	Yes
Send.y	yes

Carrier Responses	
Description	Carrier Response String
Successful Message Deliver String 1	Your message has been
Successful Message Deliver String 2	
Successful Message Deliver String 3	
Successful Message Deliver String 4	
Successful Message Deliver String 5	
Error 1	Your message can not
Error 2	
Error 3	
Error 4	
Error 5	

1. Enter a Target URL where you will be posting or getting a message (mandatory).
2. Select either the Post (default) or Get method for this protocol (depending on the source code of the Carrier's HTML page).
3. Specify the Message Field (mandatory). This can be found using the View Source function of your browser.
4. Specify the Sender Field (optional).
5. Specify the Subject Field (optional).
6. Select the type of PIN Format your Carrier uses: PIN (default), Area code + 7 digit number, or Area code + 3 digit prefix + 4 digit suffix.
7. Custom Fields. These fields can be defined by the administrator to capture/post any additional information that may be required by the website (optional).

- Carrier Responses. Enter the responses that correspond to a successful message delivery, and different types of error codes. These responses will be used by HipLink to determine the status of messages sent through this protocol. The Successful Message Delivery String 1 to 5 fields are mandatory, the Error 1 to Error 5 fields are optional.

Note: You should contact your Carrier for more information on their HTTP protocol settings and field names.

MHTTP Carrier

MHTTP is used for Carriers that require multiple HTTP steps.

- Enter a Target URL where you will be posting or getting a message (mandatory).
- Enter the Referrer URL of the last accessed page (optional).
- Select either the Post (default) or Get method for this protocol (depending on the source code of the Carrier's HTML page).
- Fields. These fields can be defined by the administrator to capture/post any additional information that may be required by the website (optional). The following predefined message variables can be used as field values: \$MESSAGE, \$PIN, \$SENDER, \$SUBJECT.
- Carrier Responses. Enter the responses that correspond to a successful message delivery, and different types of error codes. These responses will be used by HipLink to determine the status of messages sent through this protocol. The Successful Message Delivery String 1 to 5 fields and Error 1 to Error 5 fields are optional.
- Click + and x to add and delete Successful Message Delivery String fields and Error fields respectively.
- Click the Add Step button to add a new step next to the last step.
- At the top right of each Step Title bar are the Group of icons.
 - Insert Step: Adds a New step next to the current step
 - Duplicate Step: Duplicates a step at the end of all the steps.
 - Move Step: Move step Up or Down.
 - Delete Step: Deletes Step.

Note: You should contact your Carrier for more information on their HTTP protocol settings and field names.

Example: Protocol Parameters

The screenshot displays the 'Edit Message Campaign Settings' window. At the top, there is a field for 'Maximum Concurrent Campaigns (1 - 100)' with the value '10'. Below this is the 'Protocol Parameters' section, which is set to 'MHTTP'. An 'Add Step' button is visible. The first step, 'Step #1', has the following configuration: Target URL is 'https://web.mms.msg.i-n *', Referrer is empty, and Method is 'Post'. Under the 'Fields' section, there is a table with two columns: 'Field Name' and 'Field Value'. The first entry is 'msgTermsUse' with a value of 'Yes'. Below the fields is the 'Carrier Responses' section, which contains a table with two columns: 'Description' and 'Carrier Response String'. The first entry is 'Successful Message Deliver String 1' with the response 'Your message has been'. The second entry is 'Error 1' with the response 'Your message can not be'.

Field Name	Field Value
msgTermsUse	Yes

Description	Carrier Response String
Successful Message Deliver String 1	Your message has been
Error 1	Your message can not be

OAI Carrier

The Carrier configurations are similar for both one-way and two-way protocols, with the only exception being Choices Configuration that is available for two-way protocol only.

Protocol Parameters		
Type	OAI Two-Way	
Messenger	OAI 2-Way	
Primary Ringtone Configuration		
Ringtone Type	Telephone ring	
Number of Ring Cycles	3	
Priority Message Ringtone Configuration		
Same as Primary Ringtone	<input type="checkbox"/>	
Ringtone Type	Continuous	
Number of Ring Cycles	5	
Other Configuration		
On Busy (during Voice Call)	Reattempt when device gets idle	
Session Timeout (mins)	10	
Choices Configuration		
Key Press	Description	Response Action
1	Confirm	Confirm x
2	Refuse	Reject x +

1. Select a Messenger from the dropdown. The OAI Carrier needs to be assigned a separate Messenger, even if there are multiple Messengers for the assigned queue.
2. Primary Ringtone Configuration:
 - a. Select a Ringtone Type from the dropdown.
 - b. Select Number of Ring Cycles from the dropdown.
3. Priority Message Ringtone Configuration:
 - a. Select Same as Primary Ringtone checkbox if you want to use the same settings for priority messages.
4. Other Configuration:
 - a. Select a value from On busy (during voice call) dropdown:
 - i. Fail message attempt: If the device is busy on another call and a new message arrives, then this message will fail immediately.
 - ii. Reattempt when device is idle: If the device is busy on another call and the new message has arrived, the Carrier will attempt to deliver it when the device is idle.
 - iii. Pre-empt the voice call: If the device is busy on another call and a new message arrives, the handset will ring to indicate the User of the incoming call which can then be answered.
 - b. Session Timeout (mins): Defines the duration of the session maintained between HipLink and the OAI server/device.
5. Choice Configuration:

Here, keys are assigned to actions defined in the Response Actions Panel. Only Response Actions that are defined without parameters will appear in the dropdown menu.

SMPP Carrier

Protocol Parameters	
Type	SMPP
SMPP Carrier ID	12 *
SMPP Carrier Type	
Host IP	192.168.4.174 *
Host Port	9898 *
Password	••••••
Originator Address	
Originator Type	
Bind Mode	Transceiver ▾

Note: This protocol is available only for HipLink installed on Windows platforms. You should contact your Carrier to determine the correct Protocol Parameters.

1. Enter the SMPP Carrier ID (mandatory). This is a string specifying the identity of your Carrier.
2. Enter the SMPP Carrier Type (optional). If provided by your Carrier.
3. Enter the Host IP (mandatory). This is either the domain name or server address of your Carrier.
4. Enter the Host Port (mandatory). This is the port number on the server.
5. Enter the Password (optional) if required by your Carrier.
6. Enter the Originator Address (optional).
7. Enter the Originator Type (optional).
8. Select Bind Mode from the dropdown.

SMTP Carrier

Protocol Parameters	
Type	SMTP
Use Global Settings Email Server	<input type="checkbox"/>
Email server	smtp.gmail.com
User Name	hiplink0@gmail.com
Password	••••••
TLS	Require TLS ▾
Email subject	Message from HipLink
Email address prefix	
Email address suffix	@tmomail.net

1. Select Use Global Settings Email Server checkbox if you want to use the same server as defined in Global Settings.
2. Enter the Email Server address to be used by this Carrier.
3. Enter the User Name if the Email Server requires User authentication.
4. Enter Password for the above User Name.
5. Select TLS from the dropdown that your Email Server supports.

6. Enter the Email Subject (optional). If you are using a Carrier that supports Subject field in their message, this text will appear as the Subject in all messages sent from HipLink.
7. Enter the Email Address Prefix (optional). This is required only for PageNet receivers. Contact PageNet for the correct information.
8. Enter the Email Address Suffix (optional). For example, @skytel.com.

SNPP Carrier

Protocol Parameters	
Type	SNPP Two-Way
SNPP Host Server	snpp.att.net *
SNPP Port Number	444 *
SNPP Server Login Name [Password]	
2-Way Response Type	Multi-Choice ▾
Messenger Query Interval	10 ▾ * (seconds)
Messenger Query Retry	5 ▾ * (times)

The Carrier configurations are similar for both one-way and two-way protocols, with a few additional configurations for two-way protocol.

1. Enter the SNPP Host Server address (mandatory).
2. Enter the SNPP Port Number (mandatory).
3. Provide the SNPP Server Login Name [Password] if the SNPP server requires User authentication (optional)
4. Select 2-Way Response Type from the dropdown.
5. Select Messenger Query Interval from the dropdown. For two-way messaging, HipLink must query the Carrier to determine if a response to the message has been sent by the Receiver. The Messenger Query Interval specifies the amount of time (in seconds) between queries. (Default time is 120 seconds.)
6. Set the Messenger Query Retry to specify the number of times HipLink should query the Carrier to determine if the Receiver has sent a response to the message.

TAP Dial-Up Carrier

Protocol Parameters	
Type	TAP Dial-Up
TAP Phone Number	4089612819 *
TAP Password	
Baud Rate	2400 *
Parity	Even ▾ *
Data Bits	7 *
Stop Bits	1 *
Max. number of Frames per Connection	10 *
Allow LF character in message body	<input checked="" type="checkbox"/>

1. Enter the TAP Phone Number (mandatory).
2. Enter your TAP Password if you received one from your Carrier (optional).
3. Select Baud Rate from the dropdown, specific to your Carrier.
4. Select Parity from the dropdown, specific to your Carrier.
5. Select Data Bits from the dropdown, specific to your Carrier.

6. Select Stop Bits from the dropdown, specific to your Carrier.
7. Enter the Maximum Number of Frames per Connection (mandatory, default value 20).
8. Check or un-check Allow LF Character in Message Body After Case. Certain TAP Carriers have problems with line feed characters (i.e., \n and \r). You might want to leave or strip these characters from the message before it is sent out.

TAP-Leased Carrier

Protocol Parameters	
Type	TAP Leased
TAP Password	<input type="text"/>
Baud Rate	<input type="text" value="2400"/> *
Parity	<input type="text" value="Even"/> *
Data Bits	<input type="text" value="7"/> *
Stop Bits	<input type="text" value="1"/> *
Max. number of Frames per Connection	<input type="text" value="20"/> *
Allow LF character in message body	<input checked="" type="checkbox"/>

1. Enter your TAP Password, if you received one from your Carrier (optional).
2. Enter the Baud Rate, Parity, Data Bits, and Stop Bits fields specific to your Carrier.
3. Enter the Maximum number of Frames per Connection (mandatory, default value 20).
4. Check or un-check the Allow LF Character in Message Body After Case. Certain TAP Carriers have problems with line feed characters (i.e., \n and \r). You might want to leave or strip these characters from the message before it is sent out.
- 5.

Twitter Carrier and Receiver Setup

Twitter is an online social networking and micro blogging service that enables its Users to send and receive text-based posts (tweets) of up to 140 characters. The HipLink Twitter Messenger Service can send message posts remotely through HipLink to a User's Twitter profile.

Protocol Parameters	
Type	Twitter
Consumer Key	rCTVuZ7DCGQjBE3jaG *
Consumer Secret	F2ir7cCTDNQjeBVhmF: *

To obtain the Consumer key & Consumer secret for Twitter Carrier, you must follow the instructions below. You will also need an Access token & Access token secret for Twitter receiver, which is also detailed below.

Configuration:

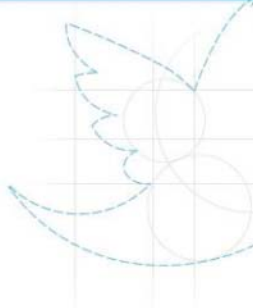
Step 1:

1. Access Twitter in browser on <https://twitter.com/>
2. Create a user account on Twitter.
3. To create application, access <https://dev.twitter.com/> in browser.
4. Click on Create App.

twitter developers Search API Health Blog Discussions Documentation

Extend your reach. Multiply your audience.

Add Twitter to your website



Recent posts from Twitter Developer Blog

- Dec 8 Tweets and Buttons
- Nov 30 Resources for mobile developers
- Nov 30 Tweet and Follow Button Refresh
- Nov 30 Platform Partner Spotlight: Mass Relevance and Crimson

Create applications that integrate Twitter

[Get started with the API](#)
Explore all of Twitter's API documentation

[Create an app](#)
Create an application to start using the Twitter API

[Discuss](#)

5. Log in with your twitter credentials.

twitter developers Search API Health Blog Discussions Documentation Sign in

Home [Tweet](#)

Sign in with your Twitter account

Username: *

New to Twitter? [Sign up](#)

Password: *

[Log in](#)

[Follow @twitterapi](#) API Terms API Status Blog Discussions Documentation A Drupal community site supported by Acquia

6. Fill in all the mandatory fields on the form.
7. Click on the Create your Twitter application button.

Create an application

Application Details

Name: *

Hiplink QA App

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

Description: *

Testing App for hiplink QA Engineers

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

WebSite: *

http://192.168.4.233

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens. (If you don't have a URL yet, just put a placeholder here but remember to change it later.)

Callback URL:

Where should we return after successfully authenticating? For @Anywhere applications, only the domain specified in the callback will be used. OAuth 1.0a applications should explicitly specify their oauth_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

Developer Rules Of The Road

Last Update - 1st of June 2011



Twitter maintains an open platform that supports the millions of people around the world who are sharing and discovering what's happening now. We want to empower our ecosystem partners to build valuable businesses around the information flowing through Twitter. At the same time, we aim to strike a balance between encouraging interesting development and protecting both Twitter's and users' rights.

So, we've come up with a set of Developer Rules of the Road ("Rules") that describe the policies and philosophy around what type of innovation is permitted with the content and information shared on Twitter.

The Rules will evolve along with our ecosystem as developers continue to innovate and find new, creative ways to use the Twitter API, so please check back periodically to see the most current version. Don't do anything prohibited by the Rules, but talk to us if you think we should make a change or give you an exception.

If you will eventually need more than 5 million user tokens for your projects, you will need to talk to us directly about access to the Twitter API.

1. Twitter Content

Yes, I agree

By clicking the "I Agree" button, you acknowledge that you have read and understand this agreement and agree to be bound by its terms and conditions.

CAPTCHA

Please type the two words below.



Create your Twitter application

8. When the application is created successfully, you will be directed to the application's Details page.

[Home](#) → [My applications](#)

Hiplink QA App

[Details](#)[Settings](#)[OAuth tool](#)[@Anywhere domains](#)[Reset keys](#)[Delete](#)

Testing App for hiplink QA Engineers
<http://192.168.4.233>

Organization

Information about the organization or company associated with your application. This information is optional.

Organization None

Organization website None

OAuth settings

Your application's OAuth settings. Keep the "Consumer secret" a secret. This key should never be human-readable in your application.

Access level	Read-only About the application permission model
Consumer key	J9CYGgBD9butKv5mC9N0Fg
Consumer secret	yp9LkJkwYyJzn4whI04poL1CbHwastzJPCvvQDgw
Request token URL	https://api.twitter.com/oauth/request_token
Authorize URL	https://api.twitter.com/oauth/authorize
Access token URL	https://api.twitter.com/oauth/access_token
Callback URL	None

Your access token

It looks like you haven't authorized this application for your own Twitter account yet. For your convenience, we give you the opportunity to create your OAuth access token here, so you can start signing your requests right away. The access token generated will reflect your application's current permission level.

[Create my access token](#)

9. Click on the Settings tab at the top.
10. On the Settings page, set the Access level to Read, write, and direct messages.
11. Click on the Update this Twitter application's settings button.

Hiplink QA App

- Details
- Settings
- OAuth tool
- @Anywhere domains
- Reset keys
- Delete

Name: *

Hiplink QA App

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

Description: *

Testing App for hiplink QA Engineers

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

Web Site: *

http://192.168.4.233

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens. (If you don't have a URL yet, just put a placeholder here but remember to change it later.)

Application Icon



Change icon:

Browse...

Maximum size of 700k. JPG, GIF, PNG.

Application Type

Access:

- Read only
- Read and Write
- Read, Write and Access direct messages

What type of access does your application need? Note: @Anywhere applications require read & write access. Find out more about our [Application Permission Model](#).

Callback URL:

Where should we return after successfully authenticating? For @Anywhere applications, only the domain specified in the callback will be used. OAuth 1.0a applications should explicitly specify their oauth_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

Organization

Organization name:

The organization or company behind this application, if any.

Organization website:

The organization or company behind this application's web page, if any.

Update this Twitter application's settings

12. Once the settings have been saved, go back to the Details tab.
13. Create an Access token by clicking on the Create my access token button.

[Home](#) → [My applications](#)

Hiplink QA App

[Details](#)[Settings](#)[OAuth tool](#)[@Anywhere domains](#)[Reset keys](#)[Delete](#)

Testing App for hiplink QA Enggineers
<http://192.168.4.233>

Organization

Information about the organization or company associated with your application. This information is optional.

Organization None

Organization website None

OAuth settings

Your application's OAuth settings. Keep the "Consumer secret" a secret. This key should never be human-readable in your application.

Access level	Read, write, and direct messages About the application permission model
Consumer key	J9CYGgBD9butKv5mC9N0Fg
Consumer secret	yp9LkJkwYyJzn4whI04poL1CbHwastzJPCvvQDgw
Request token URL	https://api.twitter.com/oauth/request_token
Authorize URL	https://api.twitter.com/oauth/authorize
Access token URL	https://api.twitter.com/oauth/access_token
Callback URL	None

Your access token

It looks like you haven't authorized this application for your own Twitter account yet. For your convenience, we give you the opportunity to create your OAuth access token here, so you can start signing your requests right away. The access token generated will reflect your application's current permission level.

[Create my access token](#)

14. Make sure the Access level for the Application settings and the Access token are same i.e. Read, write, and direct messages.

Home → My applications

Hiplink QA App

- Details
- Settings
- OAuth tool
- @Anywhere domains
- Reset keys
- Delete



Testing App for hiplink QA Engineers
<http://192.168.4.233>

Organization

Information about the organization or company associated with your application. This information is optional.

Organization	None
Organization website	None

OAuth settings

Your application's OAuth settings. Keep the "Consumer secret" a secret. This key should never be human-readable in your application.

Access level	Read, write, and direct messages About the application permission model
Consumer key	J9CYGqBD9butKv5mC9N0Fg
Consumer secret	yp9LkJkwYyJzn4whI04poL1CbHwastzJPCvvQDgw
Request token URL	https://api.twitter.com/oauth/request_token
Authorize URL	https://api.twitter.com/oauth/authorize
Access token URL	https://api.twitter.com/oauth/access_token
Callback URL	None

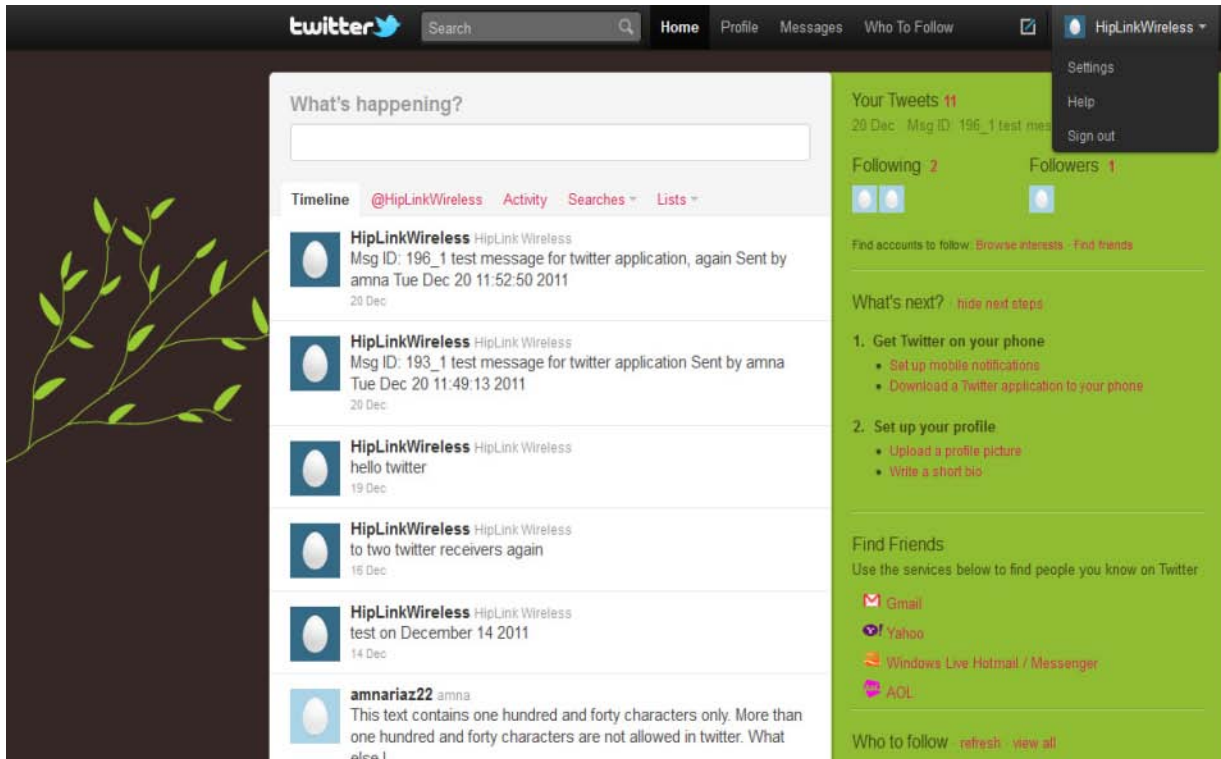
Your access token

Use the access token string as your "oauth_token" and the access token secret as your "oauth_token_secret" to sign requests with your own Twitter account. Do not share your oauth_token_secret with anyone.

Access token	385886291-7jB5z3lAd2wfe0HbDRE57UVyJV0llqPeb8kXQ
Access token secret	tycdolDH3fWioNKbuY81qDPAadc7eJj9GH1XrlbX4
Access level	Read, write, and direct messages

[Recreate my access token](#)

15. Now log on to www.twitter.com with your Twitter credentials.
16. Click on the profile name on the top-right corner.
17. Select Settings from the dropdown.



18. On the Settings page, click on the Applications tab.

twitter Search Home Profile Messages Who to Follow HipLinkWireless

HipLinkWireless's settings

Account Password Mobile Notifications Profile Design **Applications**

Name HipLink Wireless
You can change your name on your [profile settings](#).

Username No spaces, please.
Your public profile: <http://twitter.com/HipLinkWireless>

Email
Note: email will not be publicly displayed.
 Let others find me by my email address

Language English
What language would you like to Twitter in?
Interested in helping translate Twitter? Check out the [Translation Center](#).

Time Zone (GMT+05:00) Karachi

Tweet Location Add a location to your Tweets
Ever had something you wanted to share ("fireworks!", "party!", "ice cream truck", or "quicksand...") that would be better with a location? By turning on this feature, you can include location information like neighborhood, town, or exact point when you tweet.
When you tweet with a location, Twitter stores that location. You can switch location on/off before each Tweet and always have the option to delete your location history. [Learn more](#)

You may [delete all location information](#) from your past Tweets. This may take up to 30 minutes.

Tweet Media Display media that may contain sensitive content

Mark my media as containing sensitive content
If you tweet images or videos that may contain sensitive content, please check this box so that people can be warned before they see it. [Learn more](#)

Tweet Privacy Protect my Tweets
Only let people whom I approve follow my Tweets.
If this is checked, your future Tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places.

HTTPS Only Always use HTTPS
Use a secure connection where possible to encrypt your account information.

[Deactivate my account](#)

Account

From here you can change your basic account info, language settings, and your Tweet privacy and location settings.

Tips






Change your Twitter username anytime without affecting your existing Tweets, @replies, direct messages, or other data. After changing it, make sure to let your followers know so you'll continue receiving all of your Tweets with your new username.

Protect your Tweets if you don't want them to be public. Approve who can follow you and keep your Tweets out of search results.

[Learn more by visiting the help center.](#)

19. You will see newly created applications on your Twitter account.

You've allowed the following applications to access your account

-  **Hiplink QA App**
Testing App for hiplink QA Engineers
read, write, and direct messages access - Approved: Thu December 22, 2011 08:08:51 AM [Revoke Access](#)
-  **testing app for QA**
testing application
read, write, and direct messages access - Approved: Tue December 20, 2011 06:42:30 AM [Revoke Access](#)
-  **New App2**
Description
read, write, and direct messages access - Approved: Mon December 19, 2011 11:52:44 AM [Revoke Access](#)
-  **Application for hiplink**
test Description:
read-only access - Approved: Mon October 24, 2011 11:04:38 AM [Revoke Access](#)
-  **Hiplink test 1**
test app 1
read and write access - Approved: Thu October 6, 2011 09:41:05 AM [Revoke Access](#)

Applications

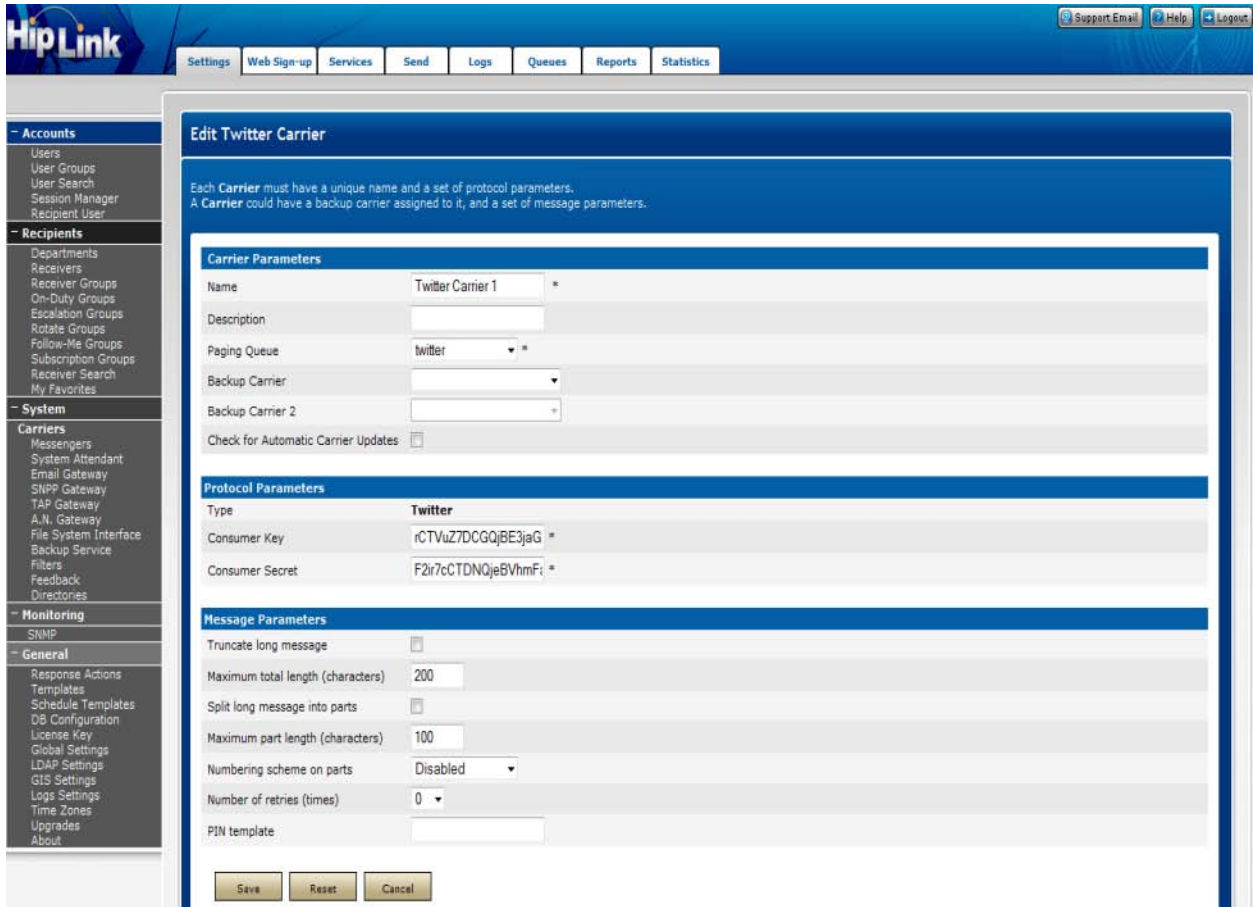
Browse and manage the different Applications you've authorized to use Twitter! [Learn more](#)

Developers

Developers can edit the registration settings for their applications [here](#).

Step 2:

1. Log into HipLink.
2. Create a Twitter messenger if you haven't already
3. Start the messenger service.
4. Create a Twitter carrier.
5. In Protocol Parameters, provide Consumer Key and Consumer Secret as given in your Twitter application's settings.



6. Create a receiver with following parameters:

- a. Primary Carrier: Twitter carrier
- b. Primary PIN: Access token: Access token secret (as given in your Twitter application's settings).

For example, if the access token is

385886291IpDbZ3eMjtPaMbvGLXmW1Wva60WWWrmBoOrZGvZm

and the access token secret is

JFenY0zWTVsCrhXyRYEO8IMgqoW5JAoCRvIV2Sd3cQ

then the pin for receiver would be:

385886291IpDbZ3eMjtPaMbvGLXmW1Wva60WWWrmBoOrZGvZm.JFenY0zWTVsCrhXyRYEO8IMgqoW5JAoCRvIV2Sd3cQ

UCP/Dial-Up Carrier

Protocol Parameters	
Type	UCP/Dial-Up
UCP Phone Number	<input type="text" value="00923226548792"/> *
Baud Rate	<input type="text" value="2400"/> *
Parity	None ▾ *
Data Bits	<input type="text" value="8"/> *
Stop Bits	<input type="text" value="1"/> *
Level	01 ▾ *
Authentication Code	<input type="text"/>

1. Enter the UCP Phone Number (mandatory).
2. Enter the Baud Rate, Parity and Data Bits.
3. Enter the Stop Bits fields specific to your Carrier.
4. Enter the operation Level: 01 for a Call input operation (default) or 30 for a message transfer operation (see the SMSC EMI specification for details, e.g., http://www.netfunitalia.it/downloads/SMSC_EMI_Specification.PDF).
5. Enter the Authentication Code (optional).

UCP/TCP Carrier

Protocol Parameters	
Type	UCP/TCP
Host	<input type="text" value="00923226542397"/> *
Level	01 ▾ *
Authentication Code	<input type="text"/>

1. Enter the Host number (mandatory).
2. Enter the operation Level: 01 for a Call input operation (default) or 30 for a message transfer operation (see the SMSC EMI specification for details, e.g., http://www.netfunitalia.it/down-loads/SMSC_EMI_Specification.PDF).
3. Enter the Authentication Code (optional).

VOIP Carrier

Protocol Parameters		
Type	VOIP	
Address (IP Address/Domain Name)	192.168.4.238 *	
Port	8001 *	
User ID	user *	
User Password	•••••••• *	
Call Max Attempts	3 ▾	
Call Retry Time Interval (0-60)	15 sec	
Call Wait Time (0-60)	30 sec	
Max Concurrent Calls (>=1)	1000	
Greeting Message	Greetings!	
IVR Menu		
Response	Option Text	Action
11	Accept	Confirm ▾ ×
222	Refuse	Reject ▾ × +
Max Status Retries (1-60)	5 *	
Status Retry Time Interval (10-900)	120 * sec	

The VoIP Carrier will allow the User to configure all the protocol settings required to support a VOIP communication. HipLink VOIP service communicates with a Dialer module to place voice calls over IP.

1. Enter the Address (IP Address/Domain Name) of the DIS module (mandatory).
2. Enter the Port number on which the Web service is exposed by the DIS module. This is assigned during the DIS installation process.
3. Enter the User ID of the User associated with the company. Each company subscribed to the DIS must have at least one User so that its credential can be used in the VoIP Carrier.
4. Enter the User Password for the above mentioned User.
5. Select Call Max Attempts from the dropdown. This defines the number of retries for the dialer to perform when the call recipient fails to accept the call.
6. Define Call Retry Time Interval. This is the time interval between two consecutive retries.
7. Define Call Wait Time. This is the time for which the dialer will wait for the recipient to accept the call on each retry.
8. Define Max Concurrent Calls that can be made on a single session. This translates to the maximum number of Receivers that can receive the voice call concurrently for a given message.
9. Define Greeting Message that will be played back (after TTS). This message will precede the message body that is added from the Send Panel.
10. Define IVR Menu. This is a list of IVR menu choices and their associated Response Actions. Response Actions are configured through Response Actions Panel.
11. Define Max Status Retries. This is the maximum number of polling retries for obtaining the status of a message when the previous one is timed out or final Status is not retrieved.
12. Define Status Retry Time Interval. This is the time interval between two consecutive status polling retries.

WCTP Carrier

Protocol Parameters	
Type	WCTP Two-Way
WCTP Host Server	wctp.att.net/wctp *
WCTP Host Server Port	80 *
Enterprise	<input type="checkbox"/>
WCTP User	hiplink
WCTP Password	click123
WCTP Post Variable	
Messenger Query Interval	10 ▾ * (seconds)
Messenger Query Retry	5 ▾ * (times)

The Carrier configurations are similar for both one-way and two-way protocols, with a few additional configurations for two-way protocol.

1. Enter the WCTP Host Server address (mandatory).
2. Enter the WCTP Host Server address (mandatory).
3. Select the Enterprise checkbox if the provided server is an enterprise Web server (optional).
4. Provide the WCTP User name if the server requires an authentication (optional).
5. Provide the WCTP Password for the above User (optional).
6. Enter the WCTP Post Variable (optional).
7. Select Messenger Query Interval from the dropdown. For two-way messaging, HipLink must query the Carrier to determine if a response to the message has been sent by the receiver. The Messenger Query Interval specifies the amount of time (in seconds) between queries (default time is 120 seconds)
8. Select Messenger Query Retry value from the dropdown. This specifies the number of times HipLink should query the Carrier to determine if the Receiver has sent a response to the message.

WAP Carrier

Protocol Parameters	
Type	WAP
Host URL	<input type="text"/> *

1. Enter Host URL for the WAP Carrier (mandatory).

XMPP Carrier

Protocol Parameters	
Type	XMPP
Profile	XMPP ▼
Host	192.168.4.232 *
Port	5223 *
User Name	user1@192.168.4.232
Password	●●●●●●●●
Resource	mobile
Connection Security	Can be PLAIN ▼
Enable Connection Caching	<input checked="" type="checkbox"/>

1. Select the XMPP Profile from the dropdown (mandatory). This is the profile used for messaging with the HipLink server using the XMPP Carrier.
2. Enter the Host address for the selected XMPP Profile (mandatory). This could be the domain name or IP of the XMPP profile.
3. Enter the Port used on the above server for the XMPP Profile (mandatory).

Note: If any of the messengers (FaceBook Messenger, GoogleTalk, Jabber.org, etc.) are selected as Profile, then Host and Port fields will be hidden).

If the XMPP Gateway is the selected profile, then these fields will be pre-populated with the values defined in XMPP Gateway.

4. Provide the User Name to be used for communicating with the selected profile (optional). This should be in the format: *username@domain* (e.g: *username@gmail.com*, *username@192.168.4.232*).
5. Provide the Password for the above User (optional).

Note: If XMPP Gateway is selected as Profile, then the User Name field will be disabled, while the Password field will be hidden. This is because the XMPP Gateway uses a default User (called *_HL_MsgrUser_*) for messaging).

6. Enter Resource (optional).
7. Select Connection Security level from the dropdown.
8. Select Enable Connection Caching checkbox, if you wish to enable connection caching.

Message Parameters:

1. Check Truncate long messages to cut-off messages that exceed a specified length.
2. Define a Maximum total length (characters) to which messages will be truncated.
3. Check Split Long Messages Into Parts checkbox if you wish to divide a long message into parts.
4. Specify Maximum Part Length (characters) for each split message.
5. Select a value from Enable Numbering on message parts field to enable numbering on message parts. When the message is delivered to the device in parts, each part contains a serial number. This will allow the Receiver to easily re-order the messages if they arrive out of order.
 - a. Disabled: Message parts will not be numbered.

- b. At the beginning: The first six characters of the message part are reserved for numbering.
 - c. At the end: The last six characters of the message part are reserved for numbering.
6. Select Number of retries from the dropdown. This number specifies the number of times HipLink will attempt to re-connect to the Carrier if a connection could not be established in the first attempt.

TO MODIFY A CARRIER

1. On the Carriers panel, find the Carrier name you want to modify and click on the Edit icon.
2. On the Edit Carrier page, edit the parameters.
3. Press Save to save the changes made on the panel, Reset to reset the fields, or Cancel to go back to the Carriers panel without saving the changes.

TO DELETE A CARRIER

1. On the Carriers panel, find the Carrier name you want to delete and select the Del checkbox.
2. Press the Delete button
3. Press OK to confirm deletion or Cancel to revoke the action.

***Note:** A Carrier cannot be deleted if it is being used by a Receiver(s). To delete a Carrier, you first need to delete its Receivers or reassign them to another Carrier(s).*

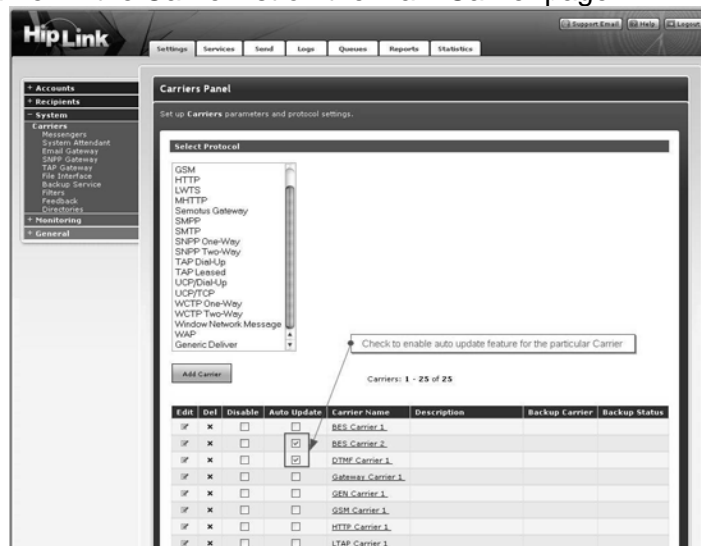
Automatic Carrier Update

The Carrier Panel allows the User to automatically update the listed Carriers with their latest versions. Users would select the list of Carrier(s) and submit requests to update. All the respective Carriers will be updated to their latest versions.

HOW TO CONFIGURE THE CARRIER FOR AUTO UPDATE

Existing Carrier

To enable the auto update feature for any Carrier that has been previously created, click the checkbox for that Carrier in the Carrier list on the Main Carrier page.



Auto Update Checkbox on the Main Carrier Panel

The auto update feature can also be enabled from the Carrier edit page. From the Carrier Panel's main page, click the edit icon next to the desired Carrier.



Auto Carrier Update Checkbox on the Add/Edit Carrier Panel

New Carrier:

On the Add Carrier page, enable the Automatic updates by selecting the Checkbox next to it. On the Add Carrier page, the Carrier List icon is provided so that you can view the list of Carriers that will correspond to specific protocol types.



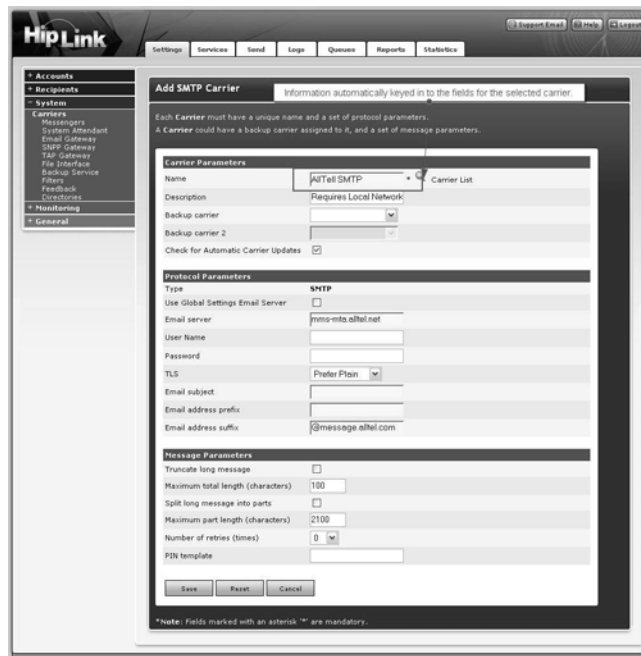
Auto Update Carrier List icon

Clicking on the magnifying glass icon will display a list of Carriers for this specific protocol type (e.g. SMTP Protocol).



Auto Carrier Update Carrier list for specific protocol (SMTP)

Click the required Carrier from the list. Once selected, the page will automatically populate some of the fields with set parameters designated for this Carrier. You can retain the information or edit it if you wish.



Add/Edit Carrier Panel with information in fields.

Note: Information fed into the fields automatically can be edited. However, changing the name of the Carrier will result as new stored information.

HOW TO AUTO UPDATE THE CARRIER:

After enabling the Carrier for auto update, the next step is to set it to update automatically. Go to the main Carrier Panel and at the bottom left side, there is a Download button. This button will lead you to the Main Automatic Carriers Update Panel. Click to go in.



Download Link on Carrier Main Panel

Once in the Automatic Carriers Update panel, you will note that the page will be populated with the list of all the Carriers that were created, regardless if the auto update feature enabled or disabled.

HipLink Support Email Help Logout

Settings Services Send Logs Queues Reports Statistics

+ Accounts

+ Recipients

- System

Carriers

- Messengers
- System Attendant
- Email Gateway
- SNPP Gateway
- TAP Gateway
- File Interface
- Backup Service
- Filters
- Feedback
- Directories

+ Monitoring

+ General

Automatic Carriers Update Panel

Update selected or all carriers from the downloaded data file.

Carrier with Auto Update enabled as well as update is available for it.

Auto Update	Select	Update Status	Carrier Name	Description
Enabled	<input checked="" type="checkbox"/>	Update Available	AllTel SMTP	Requires Local Network Connection
Disabled	<input type="checkbox"/>	N/A	BES Carrier 1	
Enabled	<input type="checkbox"/>	Not Found	BES Carrier 2	
Enabled	<input type="checkbox"/>	Not Found	DTMF Carrier 1	
Disabled	<input type="checkbox"/>	N/A	Gateway Carrier 1	
Disabled	<input type="checkbox"/>	N/A	GSM Carrier 1	
Disabled	<input type="checkbox"/>	N/A	HTTP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	LTAP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	LWTS Carrier 1	
Disabled	<input type="checkbox"/>	N/A	MHTTP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	PUCP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	SMPP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	SMTP Carrier 2	
Disabled	<input type="checkbox"/>	N/A	SMTP Carrier 3	
Disabled	<input type="checkbox"/>	N/A	SNPP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	SNPP2 Carrier 1	
Enabled	<input type="checkbox"/>	No New Updates	Sprint SMTP	Used for Backup to MHTTP
Enabled	<input type="checkbox"/>	Not Found	Sprint SMTP11	Used for Backup to MHTTP
Disabled	<input type="checkbox"/>	N/A	TAP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	TUCP Carrier 1	
Disabled	<input type="checkbox"/>	N/A	WCTP Carrier 1	
Enabled	<input type="checkbox"/>	Not Found	WCTP2 Carrier 1	
Disabled	<input type="checkbox"/>	N/A	WNM Carrier 1	

Carrier with Auto Update enabled but Not Found in Update Available carrier List.

Carrier with Auto Update Disabled i.e. N/A.

Carrier with Auto Update enabled as well as No New Update available for it

Click to Update Selected Carriers.

Click to Update All Carriers.

Click to select/unselect all

Update Selected

Update All

Click to move back to Main Carrier Panel.

Back to Carriers Panel

Automatic Carriers Update Panel

The Carrier list will consist of five columns: Auto Update, Select, Update Status, Carrier Name and Description. Under each column, the descriptions will correspond to the items that are entered for the Carrier.

©HipLink Software 2013. All Rights Reserved.

104 | Page

If the updates are disabled, the Select feature will be grayed out and not selectable. The Update Status will indicate whether or not a new update is available and will be marked as New Update available within that column. Otherwise, the status will simply display No New Update.

The Carriers with the auto update disabled will show their status as N/A (Not Applicable). Update Selected will update the Carriers that have their Select button checked. Update All will update all the Carriers which have update(s) currently available.

On a successful attempt, selected Carriers will be updated to the latest versions available. Back to Carrier Panel brings you back to the Main Carrier Panel, where you can either continue to add or move on to another area of the application.

Receivers - Create and Manage

A Receiver refers to a wireless device associated with a person on which he/she can receive messages sent through HipLink. This device could be an alphanumeric or numeric wireless device, a voice enabled device, or a fax device. Creating a comprehensive list of Receivers in the HipLink system makes it easy for Users to quickly send messages to any receiver. A person can have more than one wireless device. For each device, a separate Receiver has to be set up (e.g., John - pager, John - cell phone, John - email, etc.).

HipLink controls the Receiver type and will send only appropriate messages to the wireless devices. For example, a text message delivered to a numeric pager will contain only numeric characters, and a two-way message will be delivered only to a two-way device. In the case where a message containing text is sent to a numeric pager, HipLink will strip the text characters, send only the numeric content of the message, and log this fact in the log file.

The Receivers Panel can be accessed through the Settings menu in the Recipients section. This panel is available to all sysAdmin Users. For non-sysAdmin Users, the panel is available if one or more of the following permissions are assigned in the User Group's assigned Departments:

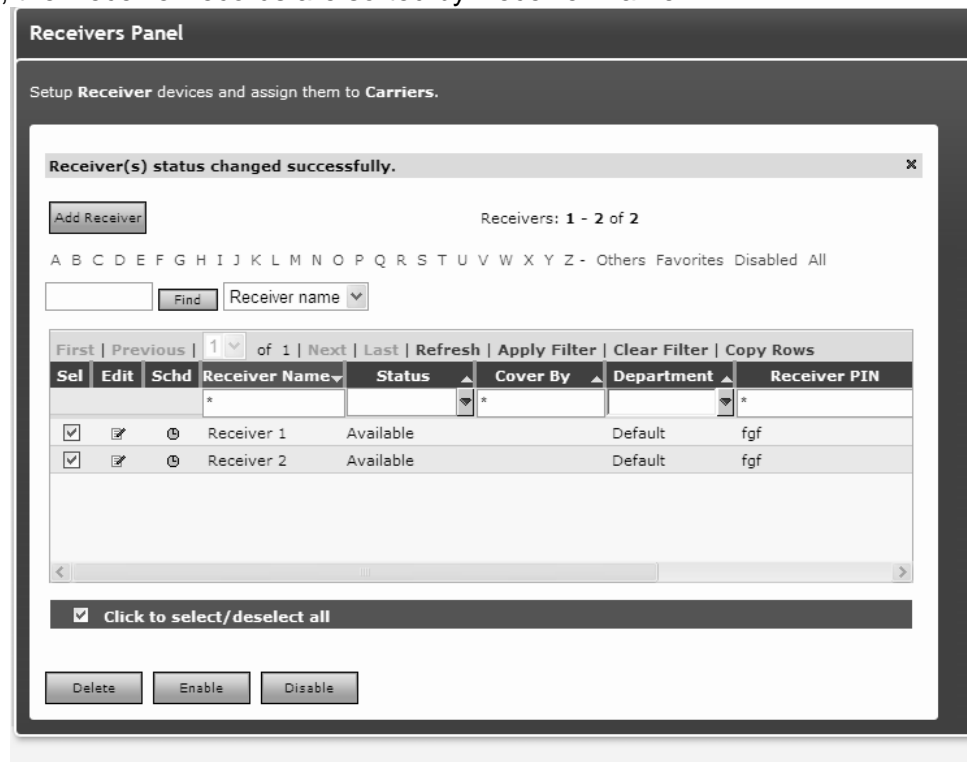
- Manage Receivers: gives Users full access on Receivers Panel for the selected Department.
- View Receivers: allows Users to view Receivers of the selected Department.

The Receiver panel contains the following columns:

1. Edit: Clicking on this button directs the User to the Edit Receiver page for the selected Receiver.
2. Delete: Selecting this checkbox and pressing the Delete button deletes the selected Receiver.
3. Schd: Clicking on this icon opens up the Receiver's schedule pop-up window.
4. Receiver Name: Displays the Receiver's name.
5. Description: Displays the Receiver's description.
6. First Name: Displays the Receiver's first name.
7. Last Name: Displays the Receiver's last name.
8. Status: Displays the status of the Receiver.
9. Cover By: In case of a disabled Receiver, this column displays the name of its Cover By Receiver.
10. Department: Displays the name of the Department that this Receiver is a Member of.
11. Receiver Pin: Displays the Receiver Pin on which messages are received.

12. Carrier: Displays the name of the Carrier assigned to this Receiver.
13. Protocol: Displays the name of the protocol for this Receivers Carrier.

By default, the Receiver records are sorted by Receiver Name.



Receivers Panel

To sort Receivers:

1. On the Receivers panel, press the button at the top of each column to sort the records in ascending order.
2. Press the button again to sort in descending order.

To filter Receivers:

1. Enter key words in the first box of Receiver Name, Description, First Name, Last Name, Cover By, Receiver Pin columns, or select a value from Status, Department, Carrier, or Protocol columns.
2. Press the Filter button.
3. HipLink will search for Receivers with this specific text, refreshes the grid, and displays the results.
4. To perform a wildcard search, use an * as a prefix, suffix, or both. For example, entering Tech* in the filter box in a particular column, may return records with the words Technical, Technician, Tech Service, etc.
5. Click on the All link to clear filter from the grid and load all the records.

Add a Receiver

1. On Receivers Panel, click the Add Receiver button to go to the Add Receiver page.
2. Enter a unique Name for the Receiver (mandatory).
3. Enter a Description for this Receiver (optional).
4. Enter the Primary PIN number for the device (mandatory).

5. Select the Primary Carrier/Delivery from the dropdown menu (mandatory). There are two predefined Carriers Fax and Voice. Custom defined Carriers have to be created before attempting to create any Receiver.
6. Select the Receiver Type from the dropdown menu according to the capabilities of the wireless device used by this Receiver:
 - a. Alpha for alphanumeric (default)
 - b. Num for numeric
 - c. 2 Way for a two-way device
 - d. Fax for a fax device

The Receiver Type is displayed in parenthesis after the Receiver name in all Add/Edit Group pages and Send panels. For example, (R): Bill Jones (Alpha).

Selecting the type Fax will automatically set the Primary Carrier/Delivery to Fax.

7. Receiver Attributes (If enabled from Global Settings): Click on the Edit link appearing with this field and from popup select single or multiple attributes to associate with the Receiver and click on OK button.

The screenshot shows the 'Edit Receiver' interface. The main window has a title bar 'Edit Receiver' and a subtitle 'Each Receiver must have a unique name, a device ID and a Primary Carrier/Delivery. Receivers can support either one-way or two-way communication.' Below this is a 'Receiver Parameters' section with the following fields:

Name	Receiver 1
Description	
Primary PIN	test@hiplink
Primary Carrier/Delivery	SMTP Carrier
Receiver Type	Alpha
Receiver Attributes	Age < 20, US citizen Edit

A 'Receiver Attributes' popup window is open, showing the following options:

<input checked="" type="checkbox"/> Age < 20	<input type="checkbox"/> Age > 20 & < 60
<input type="checkbox"/> Age > 60	<input checked="" type="checkbox"/> US citizen
<input type="checkbox"/> Non US citizen	

Buttons for 'Ok' and 'Cancel' are visible at the bottom of the popup.

Each **Receiver** must have a unique name, a device PIN, and must be assigned to a **Carrier**.

Receivers can support either one-way or two-way messaging.

Receiver Parameters

Name	<input type="text" value="Receiver 2"/> *
Description	<input type="text"/>
Primary PIN	<input type="text"/> *
Primary Carrier/Delivery	<input type="text"/> *
Receiver Type	<input type="text" value="Alpha"/>
Receiver Attributes	Edit
Keep alpha chars	<input type="checkbox"/>
Receiver Email	<input type="text"/> <input type="checkbox"/> Email Failover <input type="checkbox"/> Email CC
Owner First Name	<input type="text"/>
Owner Last Name	<input type="text"/>
<input type="checkbox"/> Define Alternate PIN/Carrier	
Alternate PIN	<input type="text"/>
Alternate Carrier/Delivery	<input type="text"/>
Time Zone	<input type="text" value="Server Time"/>
<input type="checkbox"/> Voice Enable	
Voice Phone Number	<input type="text"/>

Advanced Messaging

<input type="checkbox"/> Enable Advanced Messaging
<input type="checkbox"/> Encrypt Message

Receiver Status

Device Status	<input type="text" value="Available"/>
---------------	--

Assigned Owner

User	<input type="text"/>
<input type="checkbox"/> Can update receiver info	
<input type="checkbox"/> Can update receiver schedule info	

Departments

Member Of	<input type="text" value="1 Cardiac Department"/> *
-----------	---

Guest Settings

Hint: To select multiple items from a list, click the left mouse button while holding down either the 'Shift' or the 'Ctrl' key.

Available Departments		Guest In
<input type="text" value="1 Doctors Department"/> <input type="text" value="1 Facilities Department"/> <input type="text" value="1 IT Department"/> <input type="text" value="1 Janitorial Department"/>	<input type="button" value="Add >>"/> <input type="button" value="<< Remove"/>	<input type="text"/>

Group Assignments

Available Groups		Member In
<input type="text" value="1 - Cardiac Escalation Group (E)"/> <input type="text" value="1 - Code Blue Demo (G)"/> <input type="text" value="1 - Pediatric Dr On Duty Rotation (R)"/> <input type="text" value="1 - Primary On Duty Shift (O)"/>	<input type="button" value="Add >>"/> <input type="button" value="<< Remove"/>	<input type="text"/>

[View Groups Details](#) [View Groups Details](#)

Send a test message after 'Save' operation

<input type="button" value="Save"/>	<input type="button" value="Reset"/>	<input type="button" value="Cancel"/>
-------------------------------------	--------------------------------------	---------------------------------------

Note: Fields marked with an asterisk '' are mandatory.

8. Check the Keep alpha chars checkbox (in case of using numeric or two way devices) if you wish to keep alphabet characters.
9. Enter the Receiver Email. This shall be used in conjunction with the next two steps.
10. Check the Email Failover checkbox if you want messages to be emailed to the Receivers inbox in case of failed delivery.
11. Check the Email CC checkbox if you want sent messages to be emailed to the Receivers inbox (even if delivered successfully).
12. Check the Define Alternate PIN/Carrier box if you want to be able to use a second wireless device for this Receiver (optional).
13. Enter the Alternate PIN number for the device (mandatory if the Define Alternate PIN/Carrier box is checked).
14. Select the Alternate Carrier/Delivery from the dropdown menu (mandatory if the Define Alternate PIN/Carrier box is checked). In the case where an Alternate PIN/Carrier is defined, the order in which HipLink sends messages is as following:
 - If the Alternate PIN/Carrier box is not checked:
 - If the Primary Carrier is reachable, then send messages to the Primary PIN using the Primary Carrier.
 - If the Primary Carrier is unreachable, then send messages to the Primary PIN using the Backup Carrier of the Primary Carrier.
 - If the Alternate PIN/Carrier box is checked:
 - If the Primary Carrier is reachable, then send messages to the Primary PIN using the Primary Carrier.
 - If the Primary Carrier is unreachable, then send messages to the Alternate PIN using the Alternate Carrier.
 - If the Alternate Carrier is unreachable, then send messages to the Primary PIN using the Backup Carrier of the Primary Carrier.
 - If the Backup Carrier of the Primary Carrier is unreachable, then send messages to the Alternate PIN using the Backup Carrier of the Alternate Carrier.
15. Set the Time Zone. Select the Server Time or a different time zone if it was defined.
16. Check the Voice Enable checkbox if the Receiver has the capability to receive voice messages and you want to enable this feature (optional).
17. Enter the Voice Phone Number that is to receive voice messages.
18. Check Enable Advanced Messaging checkbox to enable advanced messaging for the Receiver. This enables the next field Encrypt Message that allows the messages sent to this Receiver to be encrypted. This requires the User to provide a Secret Key as well.
19. Receiver Status section allows defining a status of the Receiver. Receiver status could be set to:
 - Available: This is the default status of the receiver. When this is defined, Receiver is available for message sending on all Send panels.
 - Not Available: This status is set to disable the Receiver. Receiver with Not Available status would not be visible on any of the Send panels except for Scheduled Send. When a Receiver status is set to Not Available, the following fields become visible
 - **Define Schedule:** Selecting this checkbox enables the User to define a disable date for the Receiver.

If a Start Date and End Date are defined, Receiver will be disabled during this period only. If this option is not selected, Receiver will be permanently disabled.

Note: The Receiver Status is only available when the admin has checked Enable Receiver Status on the Receivers Display options. If Enable Receiver Status is not checked then Define Not Available Schedule is shown.

- **Cover By:** Selecting this checkbox enables the User to assign a Cover By device to the Receiver. A Receiver with Cover By would be visible on all Send panels and messages sent to this Receiver would be forwarded to the covering Receiver. Receiver assigned as Cover By to this Receiver will be notified of this action.
20. Assigned Owner section allows assigning an owner to the Receiver that can update Receiver and its schedule. This feature is controlled via Global Settings. User can either assign an existing HipLink User as Receiver owner or define a Login Name and Login Password, depending on the settings in Global Settings.

If Can Update Receiver Info check is selected, the assigned owner can update the Receiver by editing the Receiver record.

If Can Update Receiver Schedule Info check is selected, the assigned owner can add/modify/delete the Receiver schedule.

21. Select a Department from Member Of dropdown to make this Receiver Member of that Department (mandatory).
22. Guest Settings section allows assigning the Receiver as a Guest in other Departments (optional).
- Select a Department from Available Departments list.
 - Press Add >> button to move it to Guest In list.
 - To revert an assignment,
 - Select a Department from Guest In list.
 - Press << Remove button to move it back to Available Departments list.
23. Group Assignments section allows assigning the Receiver as a Member in Receiver Groups (optional).
- Select a Receiver Group from Available Groups list.
 - Press Add >> button to move it to Member In list.
 - To revert an assignment,
 - Select a User Group from Member In list.
 - Press << Remove button to move it back to Available Groups list.
24. At the bottom of the Add Receiver page, there is a Test Receiver check box to send a test message to the Receiver. The Test Receiver feature can be enabled/disabled from Global Settings. When you select this option HipLink will send a pre-defined text message to the configured Receiver and save the receiver.
25. Press Save to save the Receiver record, Reset to restore the fields, or Cancel to go back to Receivers panel without saving the record.

Modify a Receiver

1. On Receivers panel, find the Receiver name you want to modify and click on Edit icon.
2. On Edit Receiver page, edit the Receiver Parameters. This is similar to the Add Receiver page with additional information.
3. To edit the schedule assigned to the Receiver, click the Edit Schedule button.

4. Click the View Schedule button if you want to see a list of all the schedules assigned to this Receiver.
5. In the Receiver Status section, press the Show Not Available History button to view Disable History of the Receiver.
6. Press Save to save the changes made on the panel, Reset to reset the fields, or Cancel to go back to the Receivers panel without saving the changes.

For managing a large number of Receivers, use either of the following:

1. Alphabetical Filtering: Press one of the letter links A, B, C,..., Z, Others, Favorites, Not Available.
2. Advanced Search: Enter a keyword in the text field, select the column name from the dropdown on which you want to apply the search, and press the Find button.

Change Device Status

1. From the Settings menu, click Receiver/Receivers on the left navigation bar.
2. On the Receivers Panel, find the Receiver/Receivers name you want to Enable/Disable and check the Sel checkbox.
3. Click Enable/Disable button.
4. Selected Receiver/Receivers will be Enabled or Disabled.
5. If the Receiver gets Enabled, its status will be shown as Available on the main Receivers Panel.
6. If the Receiver gets Disabled, its status will be shown as Not Available on the main Receivers Panel

Delete a Receiver(s)

- Select a single or multiple Receiver(s).
- Press the Delete button.
- Press OK to confirm deletion, or Cancel to revoke the action.

Receiver Schedule

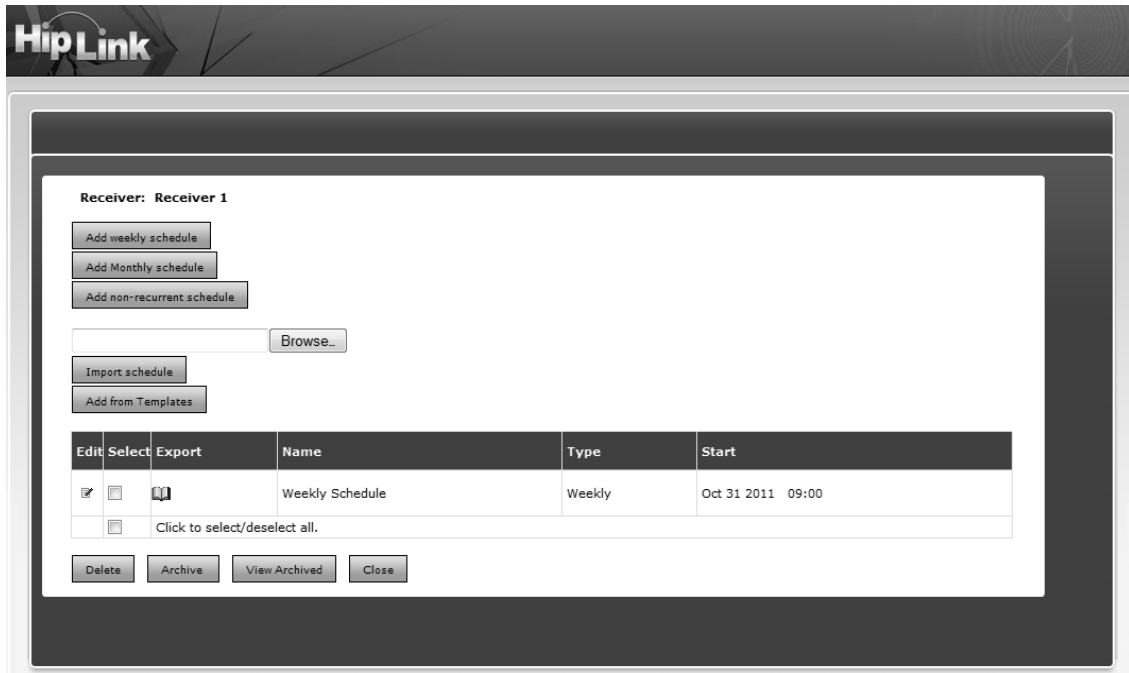
A Receiver can be assigned a time schedule that defines its availability. There are different situations in which a Receiver can get a schedule:

- A schedule can be assigned directly to a Receiver and will be in effect when messages are sent directly to it.
- A Receiver can be a Member of one or more On-Duty Groups and/or Follow-Me Groups. Within each Group, the Receiver will have a schedule assigned to it. These schedules will be effective only when messages are sent to the respective Groups.
- A Receiver can be a Member of a regular Broadcast Group which in turn is a Member of an On-Duty Group or Follow-Me Group. The schedule assigned to the Broadcast Group will affect all of its Members. As in the previous case, these schedules will be effective only when messages are sent to the respective Groups.

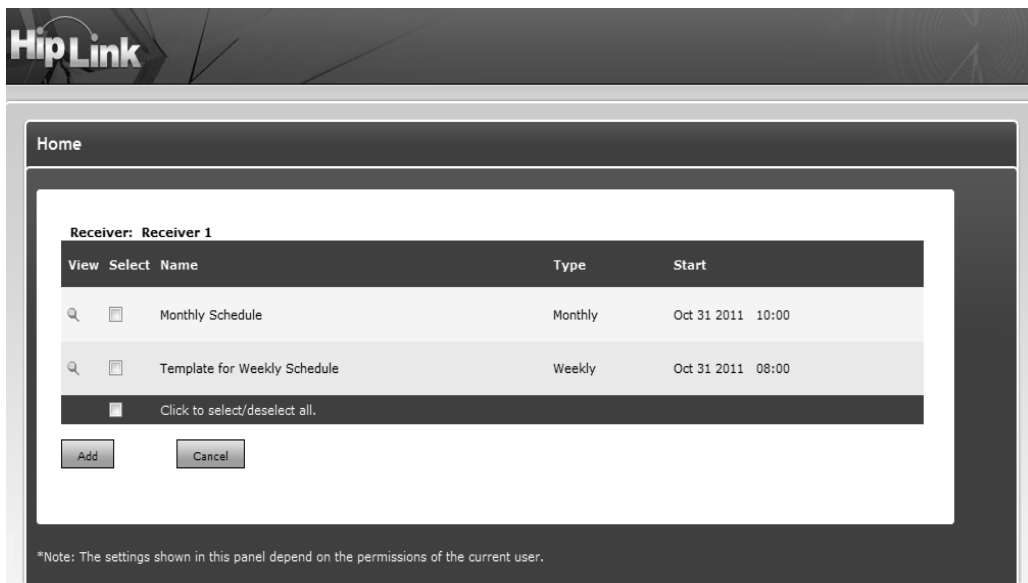
Note: *If Enable Send Receiver Schedule is enabled from Global Settings, only the Receivers that are On-Duty at the moment will be displayed on Send panels.*

1. On the Receivers panel, find the Receiver name you would like to modify and click the Edit button.
2. On the Edit Receiver page, click the Edit Schedule button

- The Schedule Main Page pop-up window allows the User to add a schedule or schedules to the Receiver. This is similar to the Schedule Templates panel, which is explained in more detail in the HipLink User Guide.



- A User can also add a schedule from the list of templates available on the Schedule Templates panel by pressing the Add from Templates button in the schedule pop-up to display the list of schedule templates.
- Select one or more schedules from the list.
- Press the Add button to assign this schedule to the Receiver, or Cancel to revoke the action.
- You can also view template details by clicking on View icon against a template.



Receiver Schedule Template Page

8. To archive a schedule, select a checkbox and press the Archive button. The archived schedule will no longer be visible on the list of assigned schedules.
9. To view the schedules archived for any Receiver, click View Archived button.

System Attendant Configuration

The System Attendant is the watchdog of the HipLink system. It surveys the HipLink Messengers and the size of the queues, and notifies the administrator by email when any of the predefined limits are exceeded.

The HipLink administrator will get an alert if one of the following thresholds is reached in a given time period:

- the maximum number of messages in the Failed queue within one hour;
- the maximum number of messages in the Completed queue within one hour;
- the number of minutes that a message stays unprocessed (idle) in the Main queue.

The HipLink administrator can also specify a command to be executed by the System Attendant when an alert is triggered. This feature allows the System Attendant not only to notify the administrator by email, but also to send the alert message to Receivers or Groups. A batch file invoking the Command Line Interface (CLI) with appropriate parameters can be easily set up to perform this task. Please refer to the Integration and Programming Guide for details about the CLI and Feedback Panel.

Alerts Notification Parameters		
Administrator email	hiplink@gmail.com *	notification email address
Alerts recipient	▼	receiver or group to send alert notifications
Number of failed messages (within an hour)	40 *	maximum number of messages in the failed queue within one hour
Number of completed messages (within an hour)	40 *	maximum number of messages in the Completed queue within one hour
Idle message time	60 *	amount of time that a message stays unprocessed in the Main queue (minutes)
Alert command		command to be executed when alert is sent
Delete Expired Web Sign-up Recipients	<input type="checkbox"/>	periodically delete expired non-confirmed Web Sign-up recipients

Note: Fields marked with an asterisk "" are mandatory.

The System Attendant settings panel

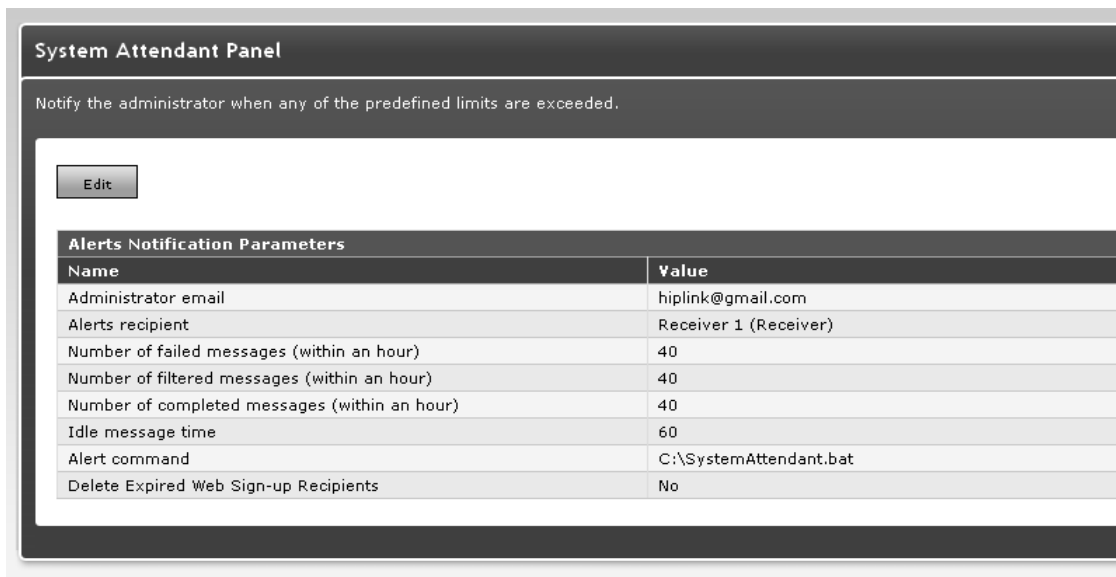
The HipLink administrator is able to set the email address where the alerts will be sent and the sender email address.

In addition to the Administrator's email, an additional Receiver or Group can be assigned to receive the alerts by filling in the Alerts Recipient field.

This field is a dropdown list populated with the existing Receivers and recipient Groups in the system. This feature enables administrators to define the Receivers or Groups and send messages/alert notifications rather than sending these messages via email using the SMTP

Email Server. This is useful in case a SMTP server is not available and offers a more sophisticated alert and notification mechanism for complex HipLink administration situations. HipLink will start cleaning up the Failed and Completed queues when there are more messages in these queues than a predefined maximum value, and when the messages in these queues are older than a given number of days.

For example, assume that HipLink Failed queue size is set to 40. Then, if there are more than 40 failed messages in the queue within a one-hour period, the administrator will receive an email with the sender name as HipLink System Attendant and the subject Failed Queue size exceeds maximum length.



The System Attendant settings panel

The System Attendant checks the efficiency of the message delivery against various benchmarks.

To set the System Attendant parameters:

1. From the Settings menu, click System Attendant on the left navigation bar.
2. On the System Attendant Panel, click any Edit icon to reach the Edit System Attendant page.
3. Enter the Administrator email address (mandatory).
4. Click Alerts recipient dropdown list, it will be populated with all the Receivers and Groups exist in the system.
5. Select the desired Receiver or Group.
6. All the other parameters except the Alert Command are set with default values. You can change the settings according to your needs by entering new values.
7. Set the path to the Alert Command to be executed by the System Attendant when an alert is triggered.
8. Click the Save button to submit your changes and return to the Monitor Panel, Reset button to fill in the previous values, or Cancel button to return without saving.

Global Settings Configuration

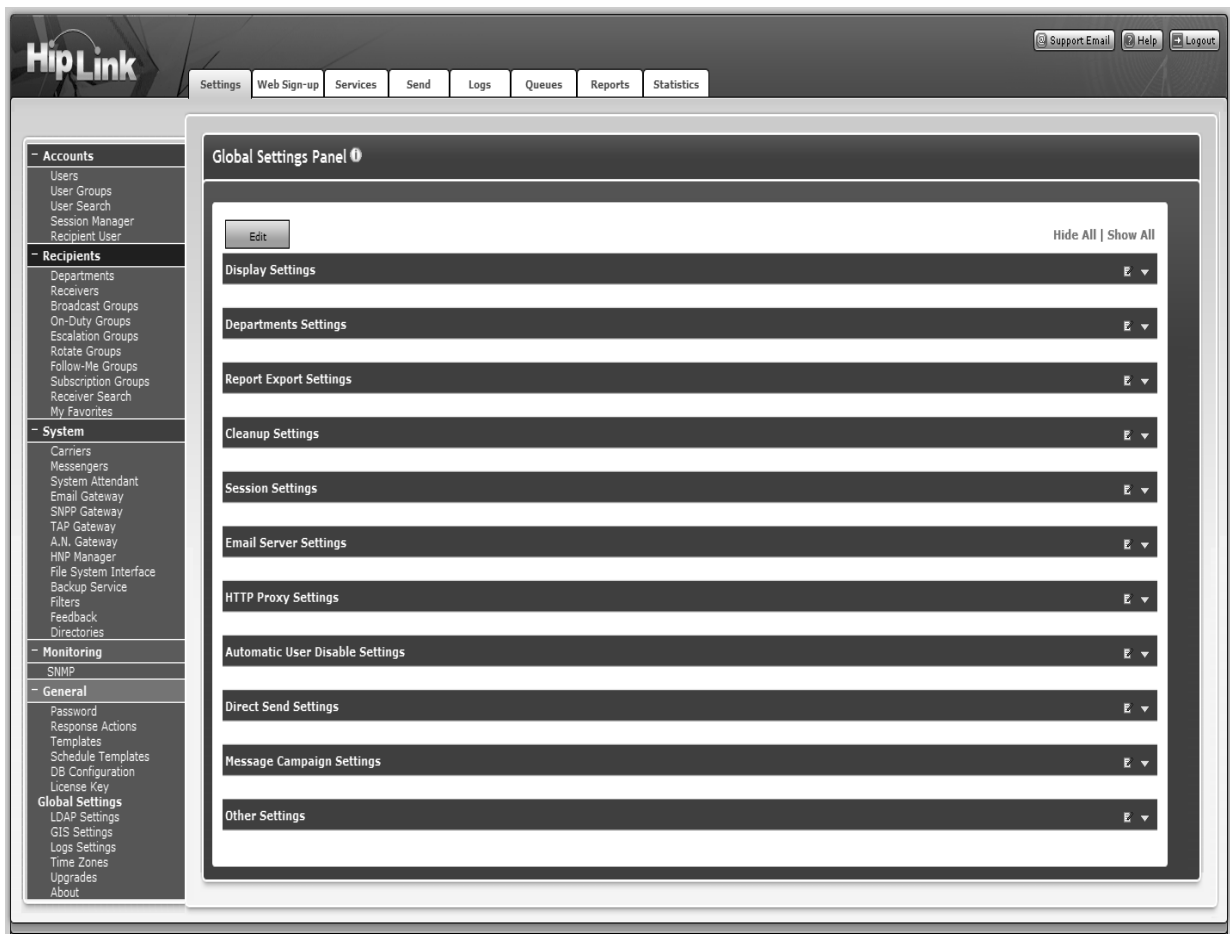
The Global Settings panel allows you to set up various parameters for the HipLink system. This panel is only accessible to sysAdmin Users.

The panel can be accessed through the Global Settings link that appears on Settings panel or on the left side under the General header in HipLink Web Application.

The HipLink system parameters are grouped in the following categories:

- Display Settings
- Departments Settings
- Report Export Settings
- Cleanup Settings
- Session Settings
- Email Server Settings
- HTTP Proxy Settings
- Automatic User Disable Settings
- Other Settings

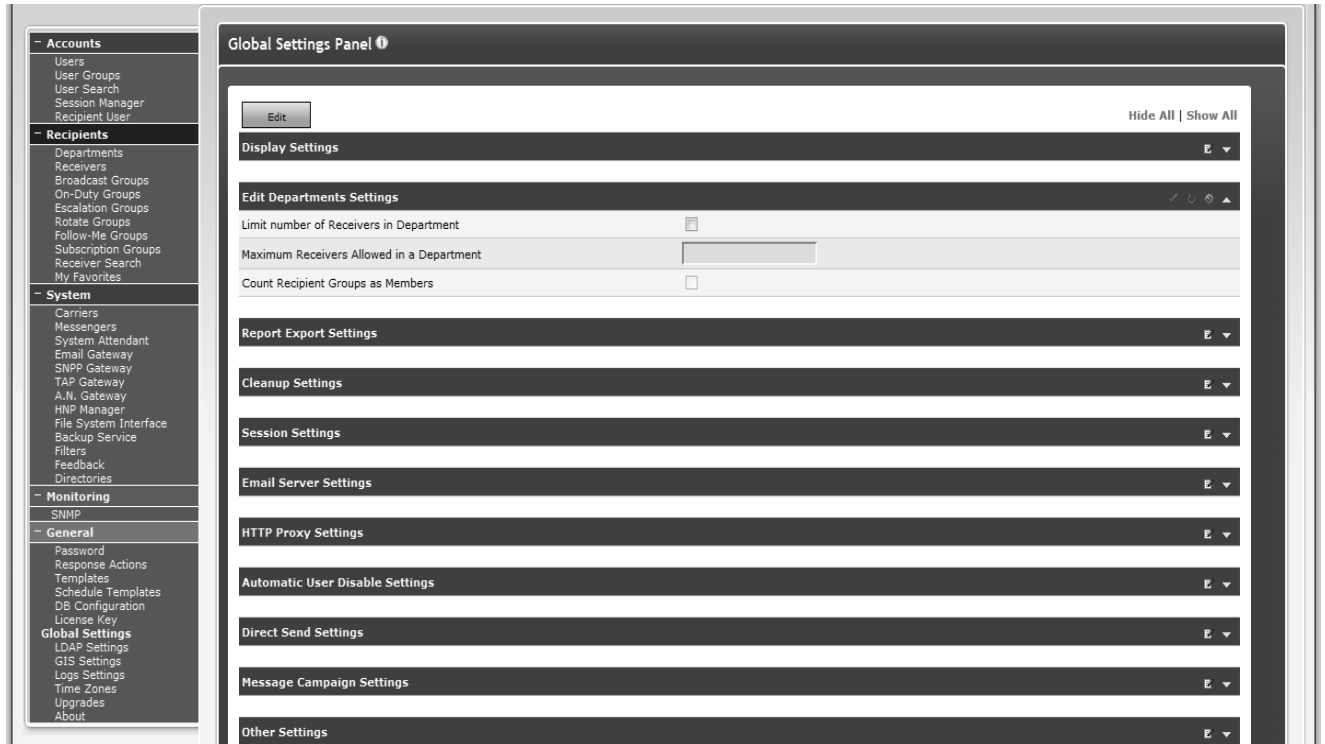
By default, all of the sections on the panel are hidden. The Show All link expands all the sections in view mode, while Hide All collapses them all. The Edit button displays all the sections in edit mode.



Global Settings Panel

In addition, there is an Edit icon next to each section which opens that particular section. A toggle button to expand/collapse the section is also there.

When a section is displayed in Edit mode (either by pressing the Edit button or by clicking on the Edit icon next to it), the Edit icon is replaced by three icons: Save, Reset, and Cancel.



Global Settings - Edit Option

Display Settings

[Support Email](#)
[Help](#)
[Logout](#)

[Settings](#)
[Web Sign-up](#)
[Services](#)
[Send](#)
[Logs](#)
[Queues](#)
[Reports](#)
[Statistics](#)

Global Settings Panel ?

[Edit](#)
Hide All | Show All

Edit Display Settings ↶ ↷ ↻ ↴

Common

Set number of records showing on each report page (10-1000) 50 *

Set maximum number of report records that can be sorted (100-99999) 1000 *

Set number of records per page (1-1000) 100 *

Enable Tooltips

Custom Header Label

Custom Header Label Text Size 2 ▾

Custom Header Label Text Color WHITE ▾

Message Sending

Enable time-stamp on all messages

Enable sender name on all messages

Put sender name at the beginning of message

Include message ID in the message automatically

Disable default Confirm and Refuse actions in 2-Way messages

Enable Send recipients in one box

Maximum Resend messages to keep for a User(10-1000) 10

Enable Authorization Code for all messages

User Description as Signature

Enable Send Subject Field

Default SMTP Subject Message from HipLink

Note: By default, the DTMF protocol cannot carry a time stamp, even if the time stamp option is enabled.

Receiver

Detail Receiver/User Display

Enable Receiver First Name

Enable Receiver Last Name

Enable Receiver Security Code

Enable Receiver Status

Allow Receiver Login

Receiver Logon via Assigned Owner

Failed Over Email Subject Failed-Over Message tr

Failed Over Email Message [message]

Enable Send Receiver Schedule

Notify Admin when receiver changes his/her own schedule

Notify Receiver on covering other receiver

Enable Receiver to send Test Message

Enable Receiver Attributes

Receiver Attributes

Age < 20		▼	x		Highest
Age > 20 & < 60	A	▼	x		
Age > 60	A	▼	x		
US citizen	A	▼	x		
Non US citizen	A		x	+	Lowest

Recipient User

Recipient User Device Name Template [@LastName][@FirstNam

Template Parameters (click to insert): First Name, Last Name, Email Address, Carrier Name, Carrier Pin

Note: Each parameter can be used only once.

Common Settings

- Set number of records showing on each report page. Set the number of records per page between 10 and 1000 (mandatory, default value 50 records).
- Set maximum number of report records that can be sorted. Set maximum number of report records that can be sorted between 100 and 99999 (mandatory, default value 1000 records).
- Set the number of records per page. Set the number of records per page, between 1 and 1000 (mandatory, default value 100 records).
- Enable Tool-tips (optional, enabled by default). These are the pop-up help descriptions that appear when you move the mouse cursor over a link.
- Custom Header Label (optional). Define custom header for HipLink. This is useful in case there is more than one instance of HipLink in use.
- Custom Header Label Text Size (optional). Select text size for the header.
- Custom Header Label Text Color (optional). Select text color for the header.

Message Sending

- Enable time stamp on all messages (optional). If this setting is enabled, Include the time stamp checkbox on all Send panels will be checked and grayed out.
HipLink allows Receivers to work in different time zones than the HipLink server. The Receiver time zone setting takes effect when the option to include the timestamp in the body of the message is enabled.
By default, the DTMF protocol cannot carry a time stamp, even if the time stamp option is enabled.
- Enable sender name on all messages (optional). If this setting is enabled, include the sender name checkbox on all Send panels will be checked and grayed out.
- Put sender name at the beginning of message (optional). If this setting is enabled, the name of the sender will be included at the beginning of the message.
- Include message ID in the message automatically (optional). If this setting is enabled, the message ID will be included at the beginning of the message automatically.
- Disable default Confirm and Refuse actions in 2-Way messages (optional). If enabled, the Default Confirm and Refuse Actions defined on Two-Way Send panel would be disabled.
- Enable Send recipients in one box. If enabled, this option lists Receivers and Receiver Groups in one list box on the Send panel.
- Maximum Resend messages to keep for a User (10-1000) (mandatory). Define the maximum number of resend messages to be kept for each User of HipLink.
- Enable authorization code for all messages. If enabled, all Send panels will have the Authorization Code field enabled and mandatory.
- User Description as Signature. Use the User Description as a signature instead of the User name (disabled by default)
- Enable Send Subject Field (optional). If enabled, it will allow the text to be sent in the Subject field of an SMTP message.
- Default SMTP Subject (optional). If defined, would be used as the subject for the SMTP messages sent via HipLink.

Receiver

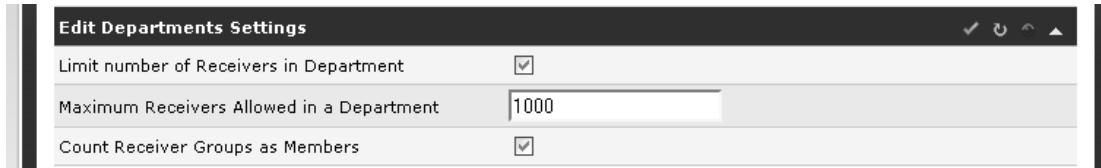
- Detail Receiver/User Display (optional, disabled by default). If enabled, it will display the Detail field of Users, Receivers, and Groups in all of the lists.
- Enable Receiver First Name. If enabled, this option allows the Receiver's first name to be entered in the Receiver Panel.

- Enable Receiver Last Name. If enabled, this option allows the Receiver's last name to be entered in the Receiver Panel.
- Enable Receiver Security Code. If enabled, this option adds the Security Code field to Add/Edit Receiver Panel when the Receiver Login is enabled via assigned Owner.
- Enable Receiver Status. If enabled, this option allows choosing between the different statuses of Receivers (mainly categorized as enabled and disabled) and helps to define the backup person for the current Receiver.
- Allow Receiver login. This allows a Receiver to log on from the main HipLink Screen and manage his/her subscription Groups.
- Receiver Logon via Assigned Owner. If a User, who is designated as the owner of a Receiver, logs onto the Receiver Login Page with his/her credentials, he/she will be shown the list of all the Receivers of which he/she is the owner of.
- Failed Over Email Subject. Subject of an email to be delivered in case of a message sending failure. This email will be sent to an email ID which is provided in the Receiver Email field with the enabled Email Fail Over option on the Add/Edit Receiver panel.
- Failed Over Email Message. Message body of an email to be delivered in case of message sending failure. This email will be sent to an email ID provided in the Receiver Email field with the enabled Email Fail Over option on Add/Edit Receiver panel.
- Enable Send Receiver Schedule (optional). If enabled, only the Receivers that are On-Duty at that moment are displayed on all the Send panels (i.e., Standard Send, Quick Send, etc.).
- Notify Admin when Receiver changes his/her own schedule: Whenever a Receiver changes his/her schedule, an email notification will be sent to the Administrator notifying him/her about the changes the Receiver has made to his/her schedule.
- Notify Receiver on covering other Receiver (optional). Enabling this option allows sending a notification to all those Receivers that have been assigned as Cover By to other Receivers.
- Enable Receiver to send Test Message: If this option is enabled, then a Test Receiver button appears next to the Receiver name. Clicking this button sends a test message, verifying the pin and Carrier settings of the Receiver. This also creates the Receiver while testing the process.
- Enable Receiver Attributes: This will allow the ability to save multiple attributes for any particular Receiver when enabled. A new field, Receiver Attributes, will be displayed on Add/Edit Receiver page with Edit link to associate selected Attributes with that particular Receiver. You can add or delete as many Attributes as you want from the Global Settings page by clicking on the + or - sign respectively and also can change the order in which they will appear on the Receiver Panel.

Recipient User

Recipient User Device Name Template. Define Template for the Recipient User Device name.

Department Settings

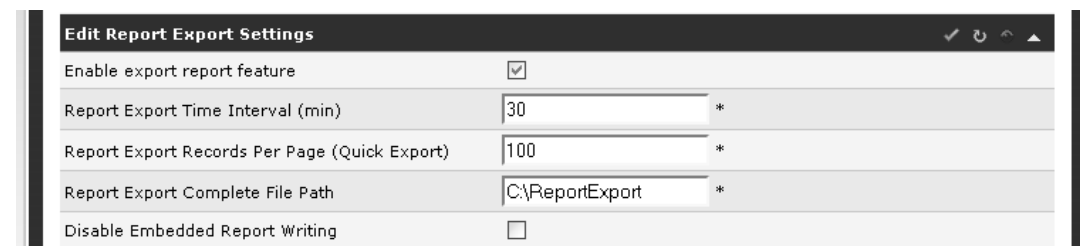


Edit Departments Settings	
Limit number of Receivers in Department	<input checked="" type="checkbox"/>
Maximum Receivers Allowed in a Department	1000
Count Receiver Groups as Members	<input checked="" type="checkbox"/>

Editing Department Settings

- Limit the number of Receivers in Department. Set the Receiver Limit for Departments.
- Maximum Receivers Allowed in a Department. Set the maximum number of Receivers that can be allocated in a Department.
- Count Receiver Groups as Members. Include/ Exclude Groups of Department as its Member in the count.

Report Export Settings

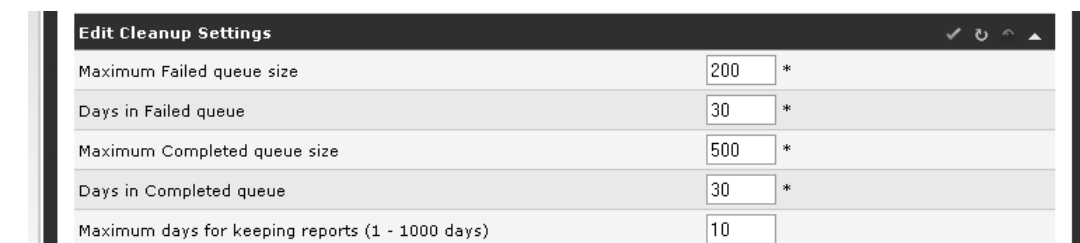


Edit Report Export Settings	
Enable export report feature	<input checked="" type="checkbox"/>
Report Export Time Interval (min)	30 *
Report Export Records Per Page (Quick Export)	100 *
Report Export Complete File Path	C:\ReportExport *
Disable Embedded Report Writing	<input type="checkbox"/>

Editing Report Export Settings

- Enable export report feature. Enable or disable the report export feature (optional, disabled by default).
- Report Export Time Interval. Set the amount of time (in minutes) at which the report will be exported (mandatory if Enable export report feature is enabled).
- Report Export Records Per Page. Set the number of records per page that would be exported.
- Report Export Complete File Path. Set the path of the exported report file (mandatory if Enable export report feature is enabled).
- Disable Embedded Report Writing. When disabled, reporting runs as a separate service.

Cleanup Settings



Edit Cleanup Settings	
Maximum Failed queue size	200 *
Days in Failed queue	30 *
Maximum Completed queue size	500 *
Days in Completed queue	30 *
Maximum days for keeping reports (1 - 1000 days)	10

- Maximum Failed queue size. Set the maximum number of message files residing in the Failed queue (mandatory, default value 200 files).

- Days in Failed queue. Set the number of days messages will be kept in the Failed queue (mandatory, default value 30 days).
- Maximum Completed queue size. Set the maximum number of message files residing in the Completed queue (mandatory, default value 500 files).
- Days in Completed queue. Set the number of days messages will be kept in the Completed queue (mandatory, default value 30 days).
- Maximum days for keeping reports. Specify the number of days reports will be kept (mandatory, default value 10 days).

Session Settings

Edit Session Settings	
Temporary session	<input checked="" type="checkbox"/>
Session Timeout (minutes)	60 *
User password expires after (days)	3
Minimum user password length in characters	5
User password needs at least a numeric, an alphabetic and a special char	<input type="checkbox"/>

Editing Session Settings

- Temporary session. Enables Temporary Session Management.
- Session Timeout (minutes). Maintain Session for User for specified interval.
- User password expires after (days). Set the number of days a User password is valid for.
- Minimum User password length in characters. Minimum number of characters required in a Password.
- User password needs at least a numeric, an alphabetic and a special character. Specify format of your password. This bounds the User to keep its password with at least one alpha numeric as well as with special character value.

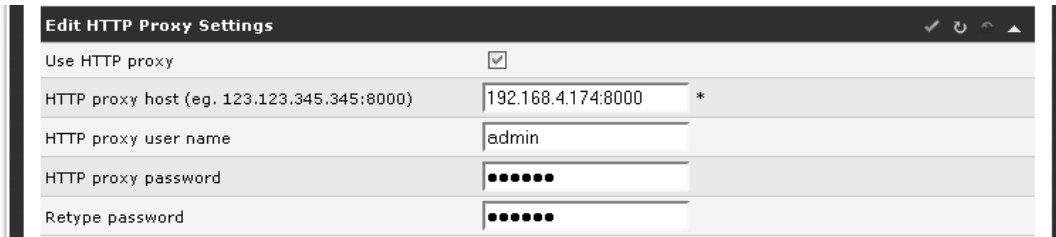
Email Server Settings

Edit Email Server Settings	
SMTP server address	smtp.gmail.com *
SMTP username	hiplink0@gmail.com
SMTP password
Sender email address	hiplink0@gmail.com
TLS	Prefer TLS

Editing Email Server Settings

- **SMTP server address.** Address of your mail server
- **SMTP username.** Valid User (email login ID) to access the SMTP Server.
- **SMTP password.** Password against above mentioned User ID.
- **Sender email address.** Sender email address.
- **TLS.** Security Formats for SMTP Server used.

HTTP Proxy Settings

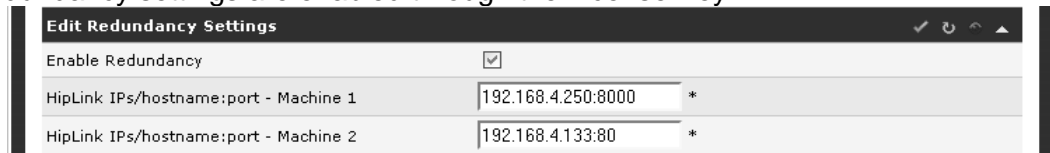


Editing HTTP Proxy Settings

- Use HTTP proxy. This feature allows HipLink to use a HTTP proxy while sending messages using the HTTP protocol. It should be enabled only if the network where HipLink is operating requires proxy based access (optional, disabled by default).
- HTTP proxy host. Set the IP address (or hostname) and the port used by the HTTP Proxy, e.g., 123.123.345.345:8000 (optional).
- HTTP proxy User name. Set the User name used by the HTTP Proxy (optional).
- HTTP proxy password. Set the password used by the HTTP Proxy (optional).

Redundancy Settings

The Redundancy settings are enabled through the License Key.



Editing Redundancy Settings

- Enable Redundancy: Enable/disable Redundancy (optional, disabled by default).
- HipLink IPs/hostname:port - Machine 1: port of the first (main) computer
- HipLink IPs/hostname:port - Machine 2: port of the second (backup) computer.

Automatic User Disable Settings

Automatic User Disable Settings allows disabling inactive Users automatically. When these settings are configured, Users who are inactive for an extended amount of time will be disabled automatically. Users, however, can activate their account by sending a request to the administrator.

Edit Automatic User Disable Settings

Enable

Warning Email Settings

Dispatch Warning Email

Dispatch Warning Email after (days) *

Warning Email Subject *

Warning Email Body *

Disable Notification Email Settings

Disable user after (days) *

Dispatch Disable Notification Email

Disable Notification Email Subject *

Disable Notification Email Body *

Deletion Notification Email Settings

Send Delete Notification Email to Admin after (days) *

Note: ($i < j < k$) i.e. i must be less than j must be less than k , where:
 i : No. of days after which Warning Email will be dispatched
 j : No. of days after which user will be disabled
 k : No. of days after which Delete Notification will be sent to Admin

- **Enable:** Check the box to enable the Automatic User Disabling feature. When unselected, Users will not be disabled automatically. However, they can still be disabled manually from Users panel.

Selecting this checkbox activates the following three settings:

Warning Email Settings

- **Dispatch Warning Email:** Select the checkbox to enable Warning Email dispatch. When unselected, Users will be disabled without being warned.
- **Dispatch Warning Email after (days):** Number of days after which warning email will be dispatched to the inactive Users. This is the number of days after the last login of the Users.
- **Warning Email Subject:** Subject line for warning email
- **Warning Email Body:** Body of warning email
Note: *If the Users activate their account after receiving Warning Email, they will not be disabled.*

Disable Notification Email Settings

- **Disable User after (days):** Number of days after which inactive Users will be disabled.
- **Dispatch Disable Notification Email:** Select the checkbox to enable Disable Notification Email dispatch. When unselected, Users will be disabled without being notified.
- **Disable Notification Email Subject:** Subject line for Disable Notification Email
- **Disable Notification Email Body:** Body of Disable Notification Email

Note: Disable User interval should not be less than Dispatch Warning Email interval.

Deletion Notification Email Settings

- Send Delete Notification Email to Admin after (days): Number of days after which admin will be notified about deleting disabled Users.

Note: Send Delete Notification Email to Admin interval should not be less than Disable User interval.

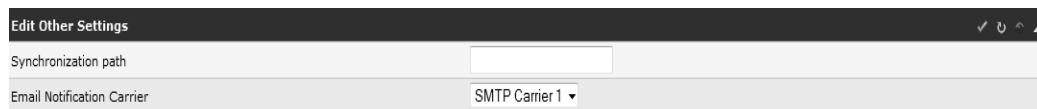
Message Campaign Settings



Editing Message Campaign Settings

- Maximum Concurrent Campaigns (1-100): Number of concurrent message campaigns (for Quota, Escalation, and Web Sign-up Send) to be dispatched.

Other Settings



Editing Other Settings

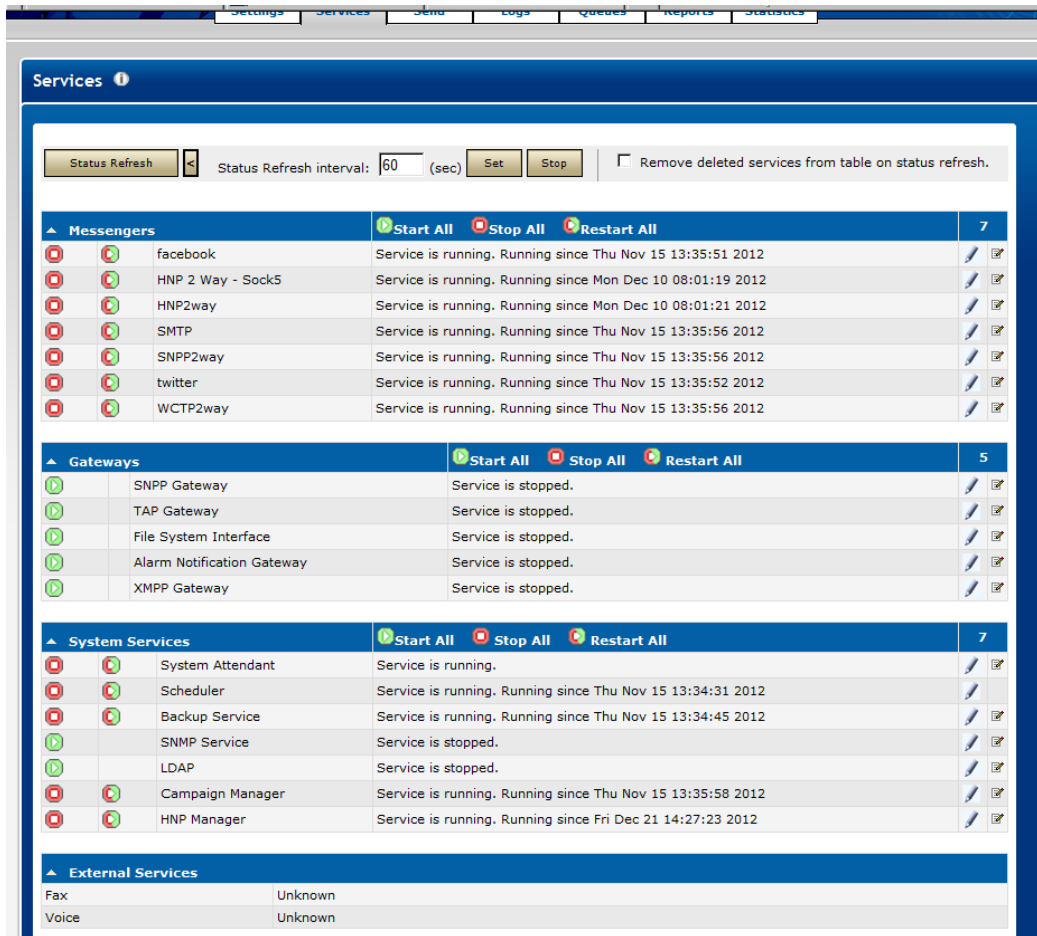
- Synchronization path: *Not Available*.
- Email Notification Carrier: SMTP Carrier to be used for the system generated email settings.

Starting HipLink and Services Menu

At this point, HipLink is configured and ready to be started.

The Services menu allows you to manually start or stop the HipLink Messengers, Scheduler Service, and System Attendant. This is necessary after creating or modifying a Messenger, the System Attendant, or Global Settings.

Note: It is strongly recommended that only administrators have access to start and stop HipLink services.



Click on the Start or Stop icon to change the status of a HipLink service. If the service is busy starting or stopping then no icon will appear.

The Services menu allows the Administrator to see the status of the external Fax and Voice services if they are installed.

All services are grouped separately as per their type in Messengers, Gateways, System Services. Start All, Stop All, Restart All options allow to start, stop or restart all services of particular sections collectively.

STARTING OR STOPPING OR RESTARTING SERVICES

To manually start and stop the Messenger services:

1. Click Services in the menu bar to reach the Services Menu.
2. Find the Name of the service you want to start or stop.
3. Click the Start or Stop icon to change the service status.
4. To restart manually, click Restart icon that co-exists along with stop icon.

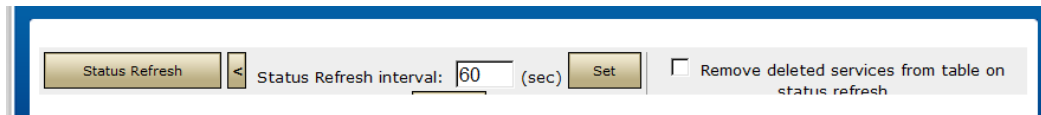
The System Attendant is checking permanently the status of the other HipLink services. If a service is not responding it will be automatically restarted by the System Attendant.

The System Attendant will not restart the services that have been stopped manually.

All HipLink services will be restarted automatically when the server is rebooted. This feature helps to provide a better server uptime.

The Log and Setting icons that are with each service allows the Administrator to view logs and edit or view the service settings respectively.

Auto Refresh Timer can be set by clicking Refresh Status button. Arrow button next to Refresh Status button allows to change Refresh Status settings.



Auto Refresh Timer settings

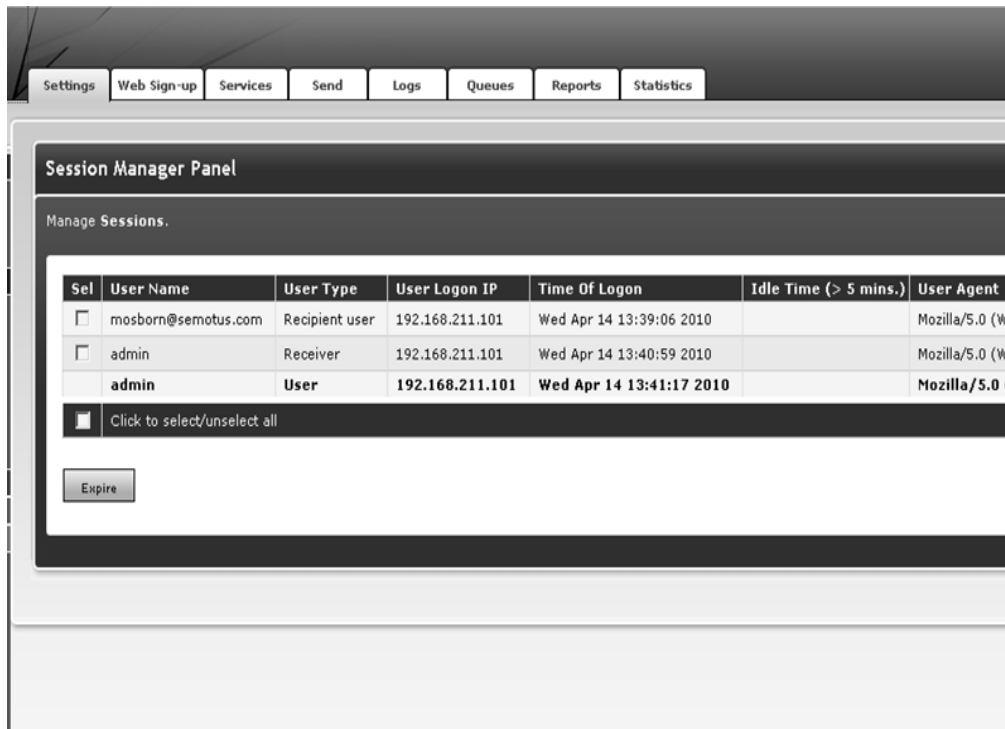
Note: When viewing this bar if the browser window is small, the two buttons Set and Stop are moved below the Status Refresh Interval section and user might not be able to see them.

Advanced Configuration & Administration Tools

Session Manager

The Session Manager displays the logged in sessions of users, recipient users and receivers. It allows ending active sessions of the users at any time. For example, administrators may want to log everyone off before restarting the server for some reason. This can be easily done this way.

The Session Manager feature is available to sysAdmin users only. The user logged in will see their session displayed in bold and it cannot be terminated.



Session Manager Panel

To terminate session(s):

From the Settings menu, click Session Manager on the left navigation bar.

Tick the check-boxes next to the active sessions in the table on the Session Manager Panel that should be terminated.

Click the Expire button.

Advanced Messaging Module

HipLink supports two versions of Mobile Applications. One is on Blackberry devices and is supported via SNPP and WCTP protocols. The other is for Apple and Android OS and is support via the HipLink HNP protocol. For complete set up and operation of HNP there is a full Guide that can be requested.

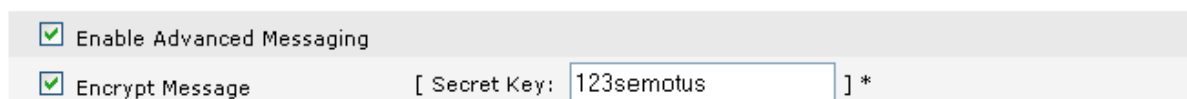
If this option has been licensed, HipLink Users can send fully encrypted messages to Receivers through the Mobile Apps HipLink also provides the facility to send encrypted messages to their recipients.

Blackberry App Setup

The carrier selected in the receiver setup must be either: SNPP (1 Way and 2 Way) or WCTP (1 Way and 2 Way)

Follow the steps:

- Go to the Add Receiver Page,
- scroll down to Enable Advance Messaging option.
- If you checked Enabled Advance Messaging then Encrypt Message will become available.
- If you intend to send secure messages to the Recipients then select Encrypt Messages and provide the secret key.
- The secret key provided here must also be provided in Decryption key of Mobile Device App in settings menu.



The screenshot shows a configuration panel with two rows. The first row has a checked checkbox followed by the text 'Enable Advanced Messaging'. The second row has a checked checkbox followed by the text 'Encrypt Message', a label '[Secret Key: ' in a light gray box, a text input field containing '123semotus', and a closing bracket followed by an asterisk ']*'.

Enable Advance Messaging from Receiver Panel.

Control Panel

For both versions of the applications there is a single Control Panel Using this Advanced Messaging functionality, the HipLink administrator can control the settings on any of the Receivers' mobile client application.

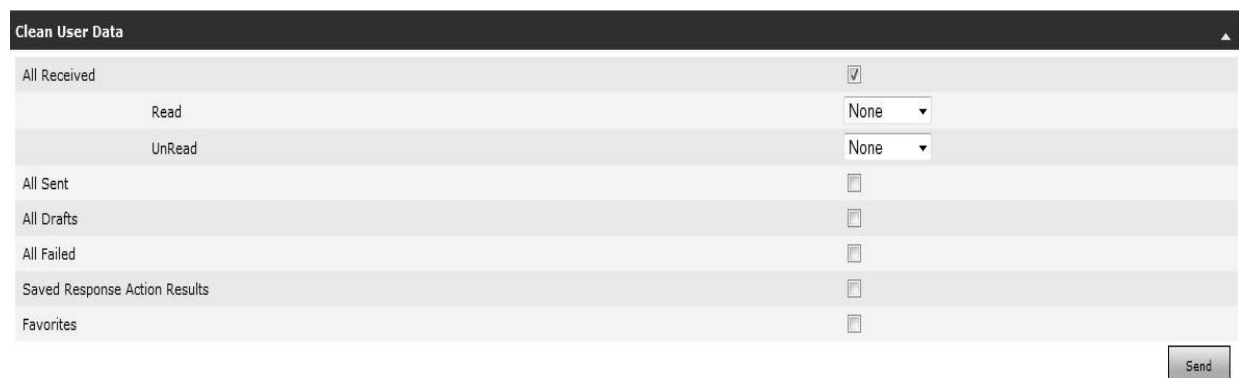
1. Select Enable Advance Messaging if you want to send secure message to the Receiver in encrypted format and also to control the configuration settings on the Receivers mobile client application [Check Control Panel Section].
2. Encrypt Message field will become active only if you have enabled the Advance Messaging and defined the secret key here that will be used at the device client application to decrypt the message. [Use same key at both ends to decrypt message successfully and this encryption messaging functionality will only work for the messages received at the device client application].

This feature enables the administrator User to modify the settings on the HipLink device client at the Receiver end by sending a configuration message to the Receiver's device from the HipLink console.



Advanced Messaging Control Panel

Clean User Data: This section will hold the configuration parameters required to control the Data management related parameters (i.e. Delete Unread/Read/Sent messages etc).



Advanced Messaging Control Panel- Clean User Data

All Received: Select this checkbox if you want to clean all the messages based on their type under the following categories:

- **Read:** Select any value from the dropdown; at present, options available are: None – All – Secure - Unsecure
- **Unread:** Select any value from the dropdown; at present, options available are: None – All – Secure - Unsecure
- **All Sent:** Select this field if you want to delete all of the messages from the HipLink client application which are stored in the Sent item folder.
- **All Drafts:** Select this field if you want to delete all of the messages from the HipLink client application which are stored in the Draft item folder.
- **All Failed:** Select this field if you want to delete all of the messages from the HipLink client application which are stored in the failed item folder.
- **Saved Response Action Results:** Select this field if you want to delete all of the messages from the HipLink client application which are stored in the Saved Response action result folder.
- **Favorites:** Select this field if you want to delete all of the messages from HipLink client's application which is stored in the Favorites item folder.

After selecting the fields for the action to perform, click the Send button to send a message to the client which will not be visible to the User but can make the desired changes on the targeted Receiver device client configuration.

Configuration Settings

This section will hold the Configuration Settings related to the following sections:

- Display Settings
- Message Configuration
- Startup
- Server Settings
- Cleanup
- Alert Configuration

Configuration Settings	
Display Settings	
Show Time	<input type="checkbox"/>
Show Recipient Info	<input type="checkbox"/>
Show Message Properties	<input type="checkbox"/>
Is one line enabled	<input type="checkbox"/>
Message Configuration	
Message Reception Type	Plain ▾
Enable Auto Delete	<input type="checkbox"/>
Save Sent Messages	<input type="checkbox"/>
Startup	
Enable Splash Screen	<input type="checkbox"/>
Force Login First	<input type="checkbox"/>
SMS Push Port	0
Server Settings	
Server Address	
Server Port	0
Secure Connection	<input type="checkbox"/>
Remember Session	<input type="checkbox"/>
Cleanup	
Clean Inbox Messages after	01 ▾ Days
Clean Sent Messages after	01 ▾ Days
Clean Draft Messages after	01 ▾ Days
Alert Configuration	
Normal Message	None ▾
Important Message	None ▾
Warning Message	None ▾
Critical Message	None ▾
Emergency Message	None ▾

Display Settings

- **Show Time:** If checked, then the time message delivered to the device client will be displayed with the message.
- **Show Recipient Info:** Check this checkbox if the Receiver wants to see the recipient information with the received message.
- **Show Message Properties:** If checked, the message properties will also be displayed with the message on the device client.
- **Is one line enabled:** If the checkbox is selected, then the message will be displayed in one line on the device client application.

Message Configuration

- **Message Reception Type:** Select the supported message types (Plain, Secure, Both) that the Receiver can receive on the device client. If Plain is selected, then the Secure message sent to the Receiver device cannot be received at the device client application.
- **Enable Auto Delete:** If checked, messages read will be deleted automatically.
- **Save Sent Messages:** Check this box if the Receiver would like to save all of his/her sent messages.

Startup

- Enable Splash Screen: If checked, the startup splash screen will be displayed every time a Receiver launches the HipLink device client application.
- Force Login First: Check this box if the Receiver would like to log in every time before seeing the messages inbox and other features.
- SMS Push Port: Define the port number that will be used for push messaging.

Server Settings

- Server Address: Enter the HipLink server address which the Receiver client will be connected to, to send and receive messages and perform other supported operations.
- Server Port: Enter the port number to connect with the server.
- Secure Connection: If checked, this will enable a secure connection.
- Remember Session: Check this box if the User does not want to enter his/her login credentials each time the HipLink client is accessed. If this feature is enabled, it will remember the User session.

Cleanup

- Clean Inbox Messages after: All messages that are older than the selected number of days will be automatically deleted in the Inbox.
- Clean Sent Messages after: All messages that are older than the selected number of days will be automatically deleted in the Sent Box.
- Clean Draft Messages after: All messages that are older than the selected number of days will be automatically deleted in the Draft folder.

Alert Configuration

- Normal Message: Set the alert notification type for Normal messages to None or Default.
- Important Message: Set the alert notification type for Important messages to None or Default.
- Warning Message: Set the alert notification type for Warning messages to None or Default.
- Critical Message: Set the alert notification type for Critical messages to None or Default.
- Emergency Message: Set the alert notification type for Emergency messages to None or Default.

After selecting the desired options, click the Send button to send a message to the client. The message will not be visible to the User, but the desired changes can be made on the targeted Receiver device client configuration.

CONFIGURE PERMISSIONS

This section will not be visible at the device client end and admin can restrict the User permissions to access the selected features of the application using this panel.

Permission	Checked
View Message	<input checked="" type="checkbox"/>
Receive Message	<input type="checkbox"/>
Send Message	<input type="checkbox"/>
Query Message	<input type="checkbox"/>
Confirm / Reject Message	<input type="checkbox"/>
Favorites	<input checked="" type="checkbox"/>
Query Receiver	<input type="checkbox"/>
Response Actions	<input type="checkbox"/>
Settings	Limited Access

Advanced Message Control Panel - Configure Permissions

Permission for the following features is shown in the Configure Permissions list. If checked, the Receiver will be able to use the feature on the device client application. Otherwise, it will be disabled or not visible on the device client.

- View Message
- Receive Message
- Send Message
- Query Message
- Confirm/Reject Message
- Favorites
- Query Receiver
- Response Actions

Settings (Dropdown Menu)

Settings are used to restrict the User's rights to modify the settings sent by the admin User to the device client application. The following permissions will be available under the dropdown menu:

- Full Access: User has full access to the settings panel on the device and can modify the selected settings depending on his/her needs.
- Limited Access: User has limited access to the settings panel on the device and can modify the selected settings depending on his/her needs.
- Very Limited Access: User has very limited access to the settings panel on the device and can modify the selected settings depending on his/her needs.
- Read Only: User will not be allowed to modify the settings on the device client. The User can only view the settings set by the Admin User.
- Lock: If selected, the settings panel will be locked for the User on the device client.

After selecting the fields against their respective action which you want to perform, click the Send button to send a message to the client which will not be visible to the User but can make the desired changes on targeted Receiver device client configuration.

HNP Manager

HipLink Notification Protocol (HNP) is an IP based communication mechanism that allows HipLink to send notifications to HipLink clients on desktop computers or mobile platforms using any OS. This protocol uses the XMPP messenger driver for message delivery. There is not any distinction on the HipLink side for the receiver device whether it is Blackberry, Android, iPhone or a desktop client.

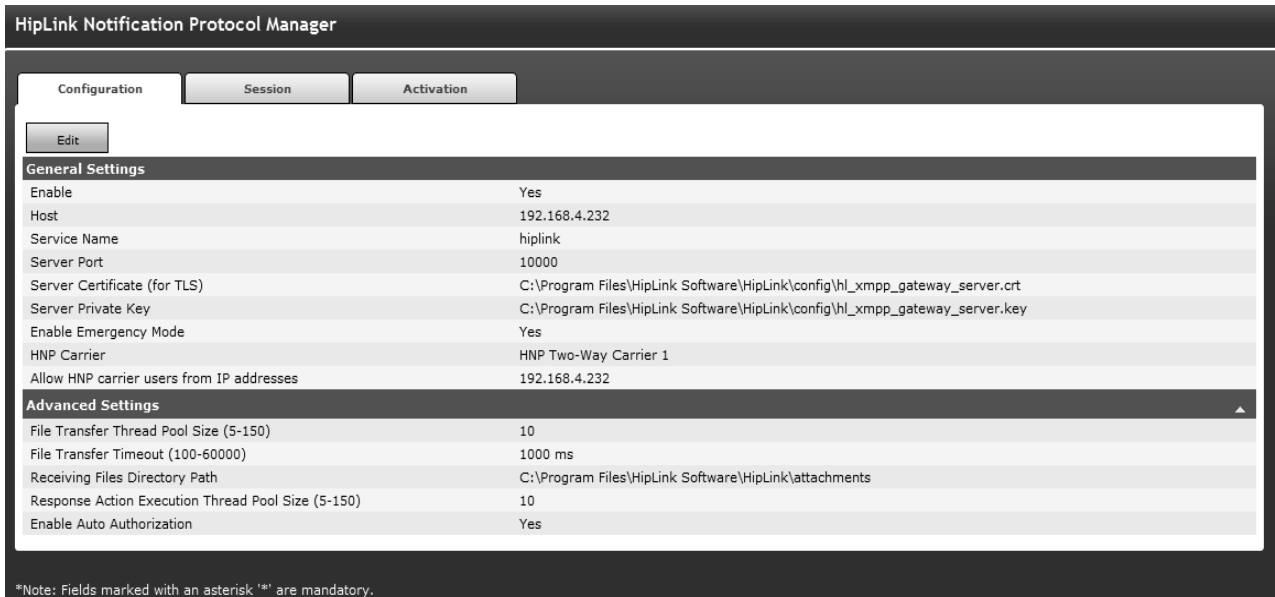
HNP Manager is an interface to manage HNP's settings. It gives the user control over HNP user's sessions and activation. It also shows which HNP users are online along with their presence status.

HNP Manager is an optional feature that is available based on the HipLink license key. The panel can be accessed from Settings tab's left navigation bar in Systems menu, as well as from the main Settings panel.

There are three tabs on HNP Manager panel:

- Configuration
- Session
- Activation

Configuration



General Settings	
Enable	Yes
Host	192.168.4.232
Service Name	hiplink
Server Port	10000
Server Certificate (for TLS)	C:\Program Files\HipLink Software\HipLink\config\hl_xmpp_gateway_server.crt
Server Private Key	C:\Program Files\HipLink Software\HipLink\config\hl_xmpp_gateway_server.key
Enable Emergency Mode	Yes
HNP Carrier	HNP Two-Way Carrier 1
Allow HNP carrier users from IP addresses	192.168.4.232

Advanced Settings	
File Transfer Thread Pool Size (5-150)	10
File Transfer Timeout (100-60000)	1000 ms
Receiving Files Directory Path	C:\Program Files\HipLink Software\HipLink\attachments
Response Action Execution Thread Pool Size (5-150)	10
Enable Auto Authorization	Yes

Note: Fields marked with an asterisk "" are mandatory.

HNP Manager Configuration Tab

This tab allows the user to configure settings for HNP. The tab is further divided into two sections:

1. General Settings
2. Advanced Settings

General Settings:

This section is used to setup HNP Gateway server settings. It contains the following fields:

1. **Edit:** Click on this button to display the panel in edit mode.
2. **Enable:** Select this checkbox to enable the HNP Manager service.
3. **Host:** Provide IP address / server name of the HipLink server where HNP Manager is configured. This could be the same HipLink server or a different one whose HNP Manager is being used.
4. **Service Name:** Provide the name of the service used by HNP Manager.
5. **Service Port:** Provide the port number used by the service.
6. **Server Certificate (for TLS):** Provide the path to the Server Certificate to be used for TLS connection. For the server certificate that comes bundled-in with HipLink, the path is provided by default.
7. **Server Private Key:** Provide the path to the Server Private Key used for the above certificate. Leave the default value if you are using the default certificate.
8. **Enable Emergency Mode:** Select this checkbox if you want to allow the users to login to HipLink on desktop / mobile devices without any receiver credentials. When this checkbox is selected, the following field becomes visible:
9. **HNP Carrier:** Select the HNP carrier to be used for sending notifications to Emergency users (i.e. users logged in Emergency Mode).
10. **Allow HNP carrier users from IP addresses:** When an IP address is defined in this

field, only the HipLink carriers on the provided IP can use HNP Manager of this server; the carriers of all other IPs are restricted from using this HNP Manager.

Advanced Settings:

This section is used to setup file transfer and response action execution settings. It contains the following fields:

1. **File Transfer Thread Pool Size (5-150):** Provide the pool size for file transfer thread.
2. **File Transfer Timeout (100-60000):** Provide the file transfer timeout (in ms). This is the time after which the file transfer will be cancelled.
3. **Receiving Files Directory Path:** Provide the path for storing the files received with notifications. The path to the HipLink's attachment directory is provided by default.
4. **Response Action Execution Thread Pool Size (5-150):** Provide the pool size for response action thread.
5. **Enable Auto Authorization:** When this checkbox is selected, an HNP user will be able to login to HNP client on a device without requiring authorization from the HNP Manager.

Session

Configuration Session Activation

Sessions: 1 - 2 of 2

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z - Others All

Find User name Refresh interval (30 - 600) : 300 (sec) Set Stop

First | Previous | 1 of 1 | Next | Last | Refresh | Apply Filter | Clear Filter | Copy Rows⁽¹⁾

Sel	Platform	Emergency Mode	User Name	Creation time	Assigned User	IP Address	Client Name
<input type="checkbox"/>		*	hnp	Tue Jul 31 11:57:20 2012	admin	192.168.5.122	HipLink Mobile - 2.1.4
<input type="checkbox"/>			hnp-2way	Tue Jul 31 12:13:00 2012	admin	192.168.5.176	HipLink Desktop - 1.0

Click to select/deselect all

Expire

Note: Fields marked with an asterisk '' are mandatory.

HNP Manager Session Tab

This tab gives the user control over HNP receivers' sessions. It contains the following columns:

1. **Platform:** Displays the icon of the platform being used by HNP receiver.

2. **Emergency Mode:** A check mark is displayed in this column, if the user is logged in without receiver credentials i.e. in Emergency Mode.
3. **User Name:** Displays the name of the logged-in receiver.
4. **Creation Time:** Displays the time the user session was created.
5. **Assigned User:** Displays the name of the HipLink user being used as Assigned Owner for the HNP receiver.
6. **IP Address:** Displays the IP address of the HipLink client.
7. **Client Name:** Displays the name of HipLink client (Desktop / Mobile / Mobile App) on which HNP receiver is logged in.
8. **Details:** Displays the details about HipLink client's operating system.

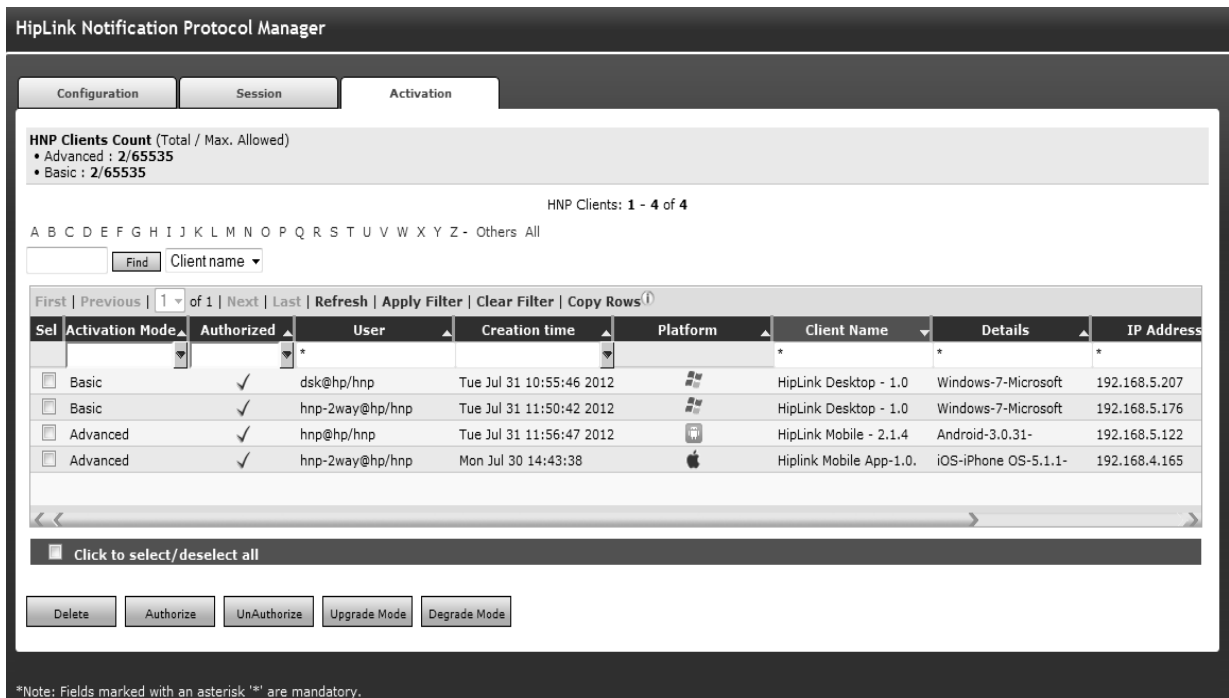
To Expire a User Session:

1. On Session tab, select the user(s) whose session you want to expire.
2. Click on Expire button.
3. Click the OK button to confirm expiry, or click Cancel to revoke this action.

The tab refreshes automatically every 300 seconds (by default). User can define a different refresh interval, between 30 to 600 seconds.

The filters and paging defined on this tab are same as on all other panels of HipLink.

Activation



HipLink Notification Protocol Manager

Configuration Session **Activation**

HNP Clients Count (Total / Max. Allowed)
 • Advanced : 2/65535
 • Basic : 2/65535

HNP Clients: 1 - 4 of 4

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z - Others All

Find Client name

First | Previous | 1 of 1 | Next | Last | Refresh | Apply Filter | Clear Filter | Copy Rows

Sel	Activation Mode	Authorized	User	Creation time	Platform	Client Name	Details	IP Address
<input type="checkbox"/>	Basic	✓	dsk@hp/hnp	Tue Jul 31 10:55:46 2012	Windows	HipLink Desktop - 1.0	Windows-7-Microsoft	192.168.5.207
<input type="checkbox"/>	Basic	✓	hnp-2way@hp/hnp	Tue Jul 31 11:50:42 2012	Windows	HipLink Desktop - 1.0	Windows-7-Microsoft	192.168.5.176
<input type="checkbox"/>	Advanced	✓	hnp@hp/hnp	Tue Jul 31 11:56:47 2012	Android	HipLink Mobile - 2.1.4	Android-3.0.31-	192.168.5.122
<input type="checkbox"/>	Advanced	✓	hnp-2way@hp/hnp	Mon Jul 30 14:43:38	iOS	Hiplink Mobile App-1.0.	iOS-iPhone OS-5.1.1-	192.168.4.165

Click to select/deselect all

Delete Authorize UnAuthorize Upgrade Mode Degrade Mode

Note: Fields marked with an asterisk '' are mandatory.

HNP Manager Activation Tab

This tab allows the user to monitor and control HNP receivers' authorizations. It contains

the following columns:

1. **Activation Mode:** Displays the mode of activation for the logged-in user. There are two types of activation modes:
 - **Basic:** In this mode, user can only receive notifications (messages) on HipLink client.
 - **Advanced:** In this mode, user can execute all the operations supported by
2. **Authorized:** A check mark is displayed in this column, if the user has been authorized.
3. **User:** Displays the name of the HNP receiver, in the format receiver@service_name
4. **Creation Time:** Displays the time the user session was created.
5. **Platform:** Displays the icon of the platform being used by HNP receiver.
6. **Client Name:** Displays the name of HipLink client (Desktop / Mobile / Mobile App) on which HNP receiver is logged in.
7. **Details:** Displays the details about HipLink client's operating system.
8. **IP Address:** Displays the IP address of the HipLink client.
9. **Activation Key:** Displays the activation key assigned to the HNP client (on a device) at the time of authorization. This is a unique key that identifies the device on which an HNP receiver has been authorized. If another receiver tries to login on the same device, it is notified that the activation key already exists. In order to allow a new receiver to login on this device, the existing activation should be deleted first.

To Delete an Activation:

1. On Activation tab, select the user(s) whose activation you want to delete.
2. Click on Delete button.
3. Click the OK button to confirm deletion, or click Cancel to revoke this action.

To Authorize a User:

1. On Activation tab, select the user(s) who have not yet been authorized and you want to authorize them.
2. Click on Authorize button.
3. Click the OK button to confirm the action, or click Cancel to revoke this action.

To Unauthorize a User:

1. On Activation tab, select the user(s) who are authorized and you want to unauthorize them.
2. Click on UnAuthorize button.

3. Click the OK button to confirm the action, or click Cancel to revoke this action.

To Upgrade Activation Mode:

1. On Activation tab, select the user(s) in Basic mode, who you want to upgrade to Advanced Mode.
2. Click on Upgrade Mode button.
3. Click the OK button to confirm the action, or click Cancel to revoke this action.

To Degrade Activation Mode:

1. On Activation tab, select the user(s) in Advanced mode, who you want to degrade to Basic Mode.
2. Click on Degrade Mode button.
3. Click the OK button to confirm the action, or click Cancel to revoke this action. The filters and paging defined on this tab are same as on all other panels of HipLink.

Groups

Once created, Receivers can be organized for group messaging purposes into simple groups such as a broadcast to all members or task oriented groups such as On-Duty, Escalation, Rotation or Follow-Me Groups.

All Receivers and Groups names must be unique. Receivers and Groups are commonly referred as Recipients. In all recipient lists the type of the Groups is appended to the name. The group codes are as follows: (E) for Escalation Group, (F) for Follow-Me Group, (G) for Broadcast Group, (O) for On-Duty Group, and (R) for Rotate Group.

The following are instructions for setting up different group types.

Broadcast Groups

A Broadcast Group is a Group of wireless devices that have been defined as Receivers in HipLink. A Broadcast Group can also contain other Groups of Receivers (i.e., Broadcast Groups, On-Duty Groups, Escalation Groups, Rotate Groups, and Follow-Me Groups) as Members. Grouping Receivers (and Groups of Receivers) makes it possible for Users to send messages to all of the Receivers in the Group simultaneously. You can organize Broadcast Groups for your company in any logical way.

Note: Any Group can be a Member of any other Group. HipLink will check for basic redundancy and will send out only one message for a Receiver that is also a Member of a Group within that Group. However, it is the responsibility of the HipLink administrator to make Groups that make sense and avoid infinite loops.

For example, a Broadcast Group named Sales Team could include all Members of the sales team in a company. When a manager (or any HipLink User) wants to alert sales personnel about a price change, they can select this Broadcast Group from the Broadcast Groups list in any Send Panel.

Note: If a device is no longer being used, the Receiver can be deleted. This would automatically remove the Receiver from all Groups that it is associated with.

Add Broadcast Group

Each Broadcast Group must have a list of members formed by Receivers and Groups.

Broadcast Group Parameters

Name: Broadcast Group *

Description:

Owner Settings

Set the owner: 1234567890

Alert the owner of membership changes

Departments

Member Of: Default

Guest Settings

Hint: To select multiple items from a list, click the left mouse button while holding down either the 'Shift' or the 'Ctrl' key.

Available Departments: Default

Guest In:

Buttons: Add >>, << Remove

Buttons: Save, Reset, Cancel

Give the new Broadcast Group a unique name. If the Department feature is enabled, then you will also have to assign this Broadcast Group to a Department.

WORKING WITH BROADCAST GROUP: To add a new Broadcast Group:

Step A: Create a Broadcast Group Record.

1. From the Settings menu, click Broadcast Groups on the left navigation bar.
2. On the Broadcast Groups Panel, click the Add Group button to reach the Add Broadcast Group page.
3. Enter a unique Name for this Group (mandatory).
4. Enter a Description of this Group (optional).
5. Enable Owner Settings if you want to assign any owner to this Broadcast Group (optional).
6. Check Alert the owner of membership changes checkbox (optional).
 - If anyone makes changes (enable/disable Receiver, changing Broadcast Group's name and description, adding or removing recipients) in the Broadcast Group other than the owner, an email will be sent to the owner of this Group about those changes.

- If an owner is changed in any Broadcast Group, emails will be sent to the new and old owners.
 - If the Receiver changes his/her schedule, a notification will be sent to the Group owner.
 - If a Receiver disables himself/herself (from main Receiver panel or edit Receiver page), a notification will be sent to the Group owner.
 - Non sysAdmin Users can only see non sysAdmin Users in the Owner dropdown.
 - SysAdmin Users can see all of the Users in the Owner dropdown.
 - If the Department feature is not enabled then there will be a configuration parameter in the Broadcast Group that states Limit access to sysAdmin and owner.
 - If User enables the Limit Access checkbox, then that Broadcast Group will not be visible to any non sysAdmin User.
7. If the Department feature is not enabled, skip to step 9.
 8. Specify the Department for this new Group.
 9. If Users who have rights to send messages only to other Departments also need to send messages to this Group, you can allow them to do so by adding their Department to the Guest In box.
 10. Click the Save button to reach the Add/Edit Broadcast Group Members page.

Step B: Assign Broadcast Group Members

1. Select the Receivers and/or Groups you want to include in the Member List and click the Add button. To select multiple items on a list, click the left mouse button while holding down either the Shift or Ctrl key.
Note: The type of the Group is coded as follows: (E) for Escalation Group, (F) for Follow-Me Group, (G) for Broadcast Group, (O) for On-Duty Group, and (R) for Rotate Group.
2. The Member List will display the Members of this Broadcast Group.
3. When you are finished, click Done.

Step C: Assign Broadcast Group Members using Receiver Attributes

1. Under the Members List section, the Show Attributes link will be available. Clicking on this link will display the Select Attributes section with all of the available attributes checkboxes. This section will provide you the additional capability to filter out the Receiver records based on their assigned attributes.

Add/Edit Broadcast Group Members

Each Broadcast Group must have a list of members formed by Receivers and Groups.

Edit	Broadcast Group Name	Description
	Broadcast Group	

Show parent Show Members

Members List

Hint: To select multiple items from a list, click the mouse button while holding down either the 'Shift' or 'Ctrl' key.

Show Attributes

Receivers

- Receiver 1
- Receiver 2
- Receiver 3
- Receiver 5
- Receiver 8
- saghir FB

Groups (E) (F) (G) (O) (R) (S)

- aa Emergency PG (G)
- aa Escalation PG (E)
- aa Follow-Me PG (F)
- bg (G)
- es1 (E)
- fol (F)

Add

Show Group Members

Refresh Members

Set	Member Name	Type	Status	Device Pin	Carrier	Email CC
<input type="checkbox"/>	Receiver 4	Receiver	Enabled	xyz	SMTP Carrier 1	
<input type="checkbox"/>	Receiver 6	Receiver	Enabled	wer	SMTP Carrier 1	
<input type="checkbox"/>	Receiver 7	Receiver	Enabled	retr	SNPP Two-Way	
<input type="checkbox"/> Click to select/deselect all						

Remove Enable Disable

Save Changes

Move To >> aa Emergency PG (G)

Done Print Members Export All

The Add/ Edit Broadcast Group Members

Example: Selecting attribute Age < 20 and US citizen checkbox will only list Receivers, which belongs to attribute Age < 20 and US citizen as shown in above figure and make selection easier.

Note: If Enable Receiver Attributes feature is turned off from Global Settings than no link to filter Receivers based on their attributes will be displayed on this page. The Enable Receiver Attributes can also be enabled or disabled from Receiver's Display Settings page in Global Settings.

Note: select a Group and click the Show Group Members link to see the Members of that Group on a separate Web page. (This is useful if you want to see who is On-Duty right now.)

To modify a Broadcast Group:

1. From the Settings menu, click Broadcast Groups on the left navigation bar.
2. On the Broadcast Groups Panel, find the Group name you want to modify and click the Edit icon.
3. On the Add/Edit Broadcast Group Members page, press the Edit icon to modify the Name or the Description (from the Edit Broadcast Group page). To add or remove Members to or from the Member List, select the Receivers and Groups and click Add or Remove respectively.

4. On the Add/Edit Broadcast Group Members, click the Print Members button to open a new browser window with a list of the Group Members that you can easily send to the printer by clicking on the Print button displayed at the bottom of the page.
5. When you are finished, click Done.

To delete a Broadcast Group:

1. From the Settings menu, click Broadcast Groups on the left navigation bar.
2. On the Broadcast Groups Panel, find the Group name you want to remove and click the Delete icon.
3. Click the OK button to confirm deletion or click Cancel to revoke this action.

The Save Changes button saves the changes made without moving back to the Main Page, whereas the Done button leaves the Add/Edit Broadcast Group Panel without saving the changes. The User is advised to click the Save changes before clicking Done.

Note: *A Broadcast Group can be a Member of one or many On-Duty Groups and/or Follow-Me Groups. Within such a Group, the Broadcast Group will have assigned a schedule. The Schedule button on the Edit Broadcast Group panel allows a global view to all schedules assigned to this Group. Please see the On-Duty Groups and Follow-Me Groups sections below to learn more details about setting schedules.*

On-Duty Groups

An On-Duty Group is a Group of Receivers (and/or other Groups of Receivers) and the work schedules of the people who use them. Messages sent to On-Duty Groups are only delivered to Members who are On-Duty at that time.

For example, an On-Duty Group named Maintenance Team that includes ten Members of the maintenance team was created. A User sent a message to this On-Duty Group on Monday evening at 8:15 pm., when they mistakenly set the alarm off. In this case, only two maintenance Members received the message on their wireless devices, because they were on-duty at that time. If the Rotating property is enabled, then only the first maintenance Member would get the message.

Add On-duty Group

Each **On-duty Group** must have a list of members formed by **Receivers** and **Groups**.

On-duty Group Parameters

Name *

Description

Rotating

Owner Settings

Set the owner

Alert the owner of membership changes

Departments

Member Of

Guest Settings

Hint: To select multiple items from a list, click the left mouse button while holding down either the 'Shift' or the 'Ctrl' key.

Available Departments

Guest In

Give the new On-Duty Group a unique name. If the Department feature is enabled, then you will also have to assign this On-Duty Group to a Department.

Working with an On-Duty Group:

To add a new On-Duty Group:

Step A: Create an On-Duty Group record.

1. From the Settings menu, click On-Duty Groups on the left navigation bar.
2. On the On-Duty Groups Panel, click the Add Group button to reach the Add On-Duty Group page.
3. Enter a unique Name for this Group (mandatory).
4. Enter a Description of this Group (optional).
5. Check the Rotating checkbox if you want to enable the Rotating property inside the On-Duty Group (optional).

Note: *The Rotating property has an effect only if there is two or more Members On-Duty at the same time. If the Rotating property is enabled, then the message will be sent by rotation to the next Member in the Group who has a valid schedule at that given time. In other words, the schedule has a higher precedence than the Rotating property.*

6. Enable Owner Settings if you want to assign any owner to this Receiver Group (optional).
7. Check Alert the owner of membership changes checkbox (optional).
 - If anyone makes changes (scheduling Receivers, enable/disable Receiver, changing Receiver Group's name and description, repositioning of Receivers) in the On-Duty Group other than the owner, an email will be sent to the owner of this Group about those changes.

- If the owner is changed in any Receiver Group, emails will be sent to new and old owners.
 - If the Receiver changes his schedule, a notification will be sent to the Group owner.
 - If the Receiver disables himself/herself (from main Receiver panel or edit Receiver page), a notification will be sent to the Group owner.
 - Non sysAdmin Users can only see non sysAdmin Users in the Owner dropdown.
 - SysAdmin Users can see all of the Users in Owner dropdown.
 - If the Department feature is not enabled, then there will be a configuration parameter in the Receiver Group that states Limit access to sysAdmin and owner.
 - If a User enables the Limit Access checkbox, then that Receiver Group will not be visible to any non sysAdmin User.
8. If the Department feature is not enabled, skip to step 10.
 9. Specify the Department for this new Group.
 10. If Users who only have rights to send messages to other Departments will also need to send messages to this Group, then you can allow them to do so by adding their Department to the Guest In box.
 11. Click the Save button to reach the Add/Edit On-Duty Group Members page.

Add/Edit On-duty Group Members

Each Receiver Group must have a list of members formed by Receivers and Groups.

Edit	Schedule	On-duty Group Name	Description
<input type="checkbox"/>	<input type="checkbox"/>	On-duty Group 1	

Show parent Show Members

Members List

Hint: To select multiple items from a list, click the mouse button while holding down either the 'Shift' or 'Ctrl' key.

Show Attributes

Receivers

- Receiver 4
- Receiver 6
- Receiver 7
- Receiver 8
- samz
- smtp

Groups (E) (F) (G) (O) (R) (S)

- Follow-Me Group 1 (F)
- Nadeem (O)
- OD1 (O)
- od2 (O)
- Receiver Group 1 (G)
- RG1 (G)

Add Show Group Members

Refresh Members

Sel	Edit	Active	Archived	Member Name	Type	Schedule	On-Duty Now	Up	Down	Last Rotating Sent	Status	Device Pin	Carrier	Ema
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Receiver 5	Receiver	✓	✓				Enabled	123	SMTP Carrier 4	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Receiver 1	Receiver	✓	✓				Enabled	test@hiplink.com	smtp owais	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Receiver 2	Receiver	✓					Enabled	test@hiplink.com	smtp owais	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Receiver 3	Receiver						Enabled	test@hiplink.com	smtp owais	

Click to select/deselect all

Remove Enable Disable

Save Changes

Move To >> Escalation Group 1 (E)

Done Print Members Export All

Give the new On-Duty Group a unique name. If the Department feature is enabled, then you will also have to assign this On-Duty Group to a Department.

Step B: Assign On-Duty Group Members

1. Select the Receiver or Group you want to include in the Member List and click the Add button.

Note: The type of the Group is coded as follows: (E) for Escalation Group, (F) for Follow- Me Group, (G) for Broadcast Group, (O) for On-Duty Group, and (R) for Rotate Group.

2. Repeat as necessary.
3. The Member List will display the Members of this On-Duty Group.

Note: Select a Group and click the Show Group Members link to see the Members of that Group on a separate Web page (useful if you want to see who is On-Duty right now).

Step C: Assign Receiver Group Members Using Receiver Attributes

1. Under the Members List section, the Show Attributes link will be available. Clicking on this link will display the Select Attributes section with all of the available attribute checkboxes. This section will provide you with the additional capability to filter out the Receiver records based on their assigned attributes.

Example: Selecting attribute Age < 20 and US citizen checkbox will only list Receivers, which belongs to attribute Age < 20 and US citizen as shown in above figure and make selection easier.

Note: If the Enable Receiver Attributes feature is turned off from Global Settings, then there will not be a link displayed to filter Receivers based on their attributes.

On-Duty Group: Group One
Member: Receiver 1

Add weekly schedule
Add Monthly schedule
Add non-recurrent schedule

Browse...

Import schedule
Add from Templates

Edit	Select	Export	Name	Type	Start
	<input type="checkbox"/>		Click to select/unselect all.		

Delete Archive View Archived Close

Creating the schedules for the On-Duty Group Members

Step D: Creating the schedules for the On-Duty Group Members:

1. Click the Edit icon next to Group Member for which a Schedule is to be edited (or assigned).
2. A Schedule window will pop up.
3. On-Duty Group schedules can be either added manually, imported from a standard schedule file, or can be added from already defined Schedule Templates. (See the Schedule Templates section for details.) There are three types of schedules that can be added manually: weekly, monthly, and nonrecurrent.
 - To create a weekly schedule, click Add Weekly Schedule, then continue with Step D (Weekly).
 - To create a monthly schedule, click Add Monthly Schedule, then continue with Step D (Monthly).
 - To create a nonrecurring (once-only) schedule, click Add Nonrecurrent Schedule, then continue with Step D (Nonrecurrent).
 - To import a schedule file type, the full path, or click Browse..., select a standard schedule file (i.e., a file with .ics extension) from your computer and then click Import schedule. If the import operation is successful, click the OK button to return to the Schedule Templates Panel.
 - To add a schedule from Templates, click Add from Templates, then continue with Step D (Templates).

Add Weekly Schedule

Add/Edit a weekly schedule

On-Duty Group: Group One
Member: Receiver 1

On-duty Time

Scheduled Name: *
Time Frame: Start: 00:00 * End: 01:00 * Duration: 01:00

Recurrence pattern *

Recurrence every 1 week(s) on
 Sunday Monday Tuesday Wednesday Thursday Friday

Range of recurrence

Start: 12/19/2006

No end date
 End after
 End by

Ok Cancel

Creating a weekly schedule for the On-Duty Group Members

Step D (Weekly): Create a Weekly Schedule for an On-Duty Group Member:

1. Choose a Name for the Schedule (mandatory).
2. Enter a Time frame for the day of this Schedule (mandatory). Enter the Start and End time for the schedule and the duration will be calculated for you. Alternatively, you can enter the Start time and the Duration (hh:mm), and then the end time will be calculated for you when you click on the next field.
3. Set the Recurrence pattern. Choose the number of weeks for the recurrence of this schedule and the days on which this schedule should apply. For example, if you pick 1

week and Monday, then the schedule will be in effect on every Monday, but if you pick 2 weeks and Monday, then the schedule will be in effect every 2nd Monday.

4. Set the Range of recurrence. The start date of this Schedule defaults to today's date. You can change it by directly editing the text box (use the MM/DD/YYYY format), or by clicking on the calendar icon to select a date. By default the recurrence never ends. If you want it to end after a certain number of occurrences, click the second radio button and enter the number of occurrences. To end at a certain date, click the third radio button and enter a date in the text box (use the MM/DD/YYYY format) or click on the calendar icon to select a date.
5. When you are done, click OK. You may then either set up a schedule for another Member of this On-Duty Group, or if you are done, then click the Close button on that Pop-up window.

Creating a monthly schedule for the On-Duty Group Members

Step D (Monthly): Create a Monthly Schedule for an On-Duty Group Member:

1. Choose a Name for the Schedule (mandatory).
2. Enter a Time frame for the day of this Schedule (mandatory). Enter the Start and End time for the schedule and the duration will be calculated for you. Alternatively, you can enter the Start time and the Duration (hh:mm), and then the end time will be calculated for you when you click on the next field.
3. Select your preferred type of Recurrence pattern using the radio buttons.
4. Set the Range of recurrence. The start date of this Schedule defaults to today's date. You can change it by directly editing the text box (use the DD/MM/YYYY format), or by clicking on the calendar icon to select a date. By default the recurrence never ends. If you want it to end after a certain number of occurrences, click the second radio button and enter the number of occurrences. To end at a certain date, click the third radio button and enter a date in the text box (use the DD/MM/YYYY format) or click on the calendar icon to select a date.
5. When you are done, click Ok. You may then either set up a schedule for another Member of this On-Duty Group, or if you are done, then click the Close button on that Pop-up window.

Creating a weekly non-recurrent schedule for the On-Duty Group Members

Step D (Non-recurrent): Create a Non-recurrent Schedule for an On-Duty Group Member:

1. Choose a Name for the Schedule (mandatory).
2. Enter a Time frame for the day of this Schedule (mandatory). When you enter the Start and End time for the schedule, then the duration will be calculated for you. Alternatively, you can enter the Start time and the Duration (hh:mm), and then the end time will be calculated for you when you click on the next field.
3. Choose the date of this Schedule by editing the Date text box (use the DD/MM/YYYY format), or by clicking on the calendar icon to select a date.
4. When you are done click OK. You may then either set up a schedule for another Member of this On-Duty Group, or if you are done then click the Close button on that Pop-up window.

On-Duty Group: Emergency On Call Group				
Member: Receiver 1				
View	Select	Name	Type	Start
	<input type="checkbox"/>	Monthly Stalling	Monthly	Dec 19 2006 03:00
	<input type="checkbox"/>	Weekly posting	Weekly	Dec 19 2006 04:00
		<input type="checkbox"/>	Click to select/unselect all.	

Adding a Schedule from Templates for an On-Duty Group Member

Step D (Templates): Add a Schedule from Templates for an On-Duty Group Member:

1. Check the Select checkbox in front of the Schedule Template name you want to add (or click the View icon to see the schedule details before adding it).
2. Click the OK button to confirm addition or click Cancel to revoke this action.

To modify an On-Duty Group:

1. From the Settings menu, click the On-Duty Groups on the left navigation bar.
2. On the On-Duty Groups Panel, find the Group name you want to modify and click the Edit icon.
3. On the Add/Edit On-Duty Group Members page, press the Edit icon to modify the Name or the Description (from the Edit On-Duty Group page). To add Members to the Member List, select the Receivers and Receiver Groups and click the Add button.

4. Click the Print Members button to open a new browser window with a list of the Group Members that you can easily send to the printer by clicking on the Print button displayed at the bottom of the page.
5. When you are finished, click Done.

To delete an On-Duty Group:

1. From the Settings menu, click On-Duty Groups on the left navigation bar.
2. On the On-Duty Groups Panel, find the Group name you want to remove and click the Delete icon.
3. Click the OK button to confirm deletion or click Cancel to revoke this action.

To archive an On-Duty Group schedule:

1. From the Settings menu, click On-Duty Groups on the left navigation bar.
2. On the On-Duty Groups Panel, find the Group name you want to modify and click the Edit icon.
3. On the Add/Edit On-Duty Group Members panel, click the Edit icon of the Member schedule that you want to archive. Select the Schedule and click on the Archive button.
4. On the On-Duty Group Member page, click the checkbox for the schedule that you want to archive (or click the select all checkbox at the bottom of the table).
5. After clicking on the Archive button, a message prompt will be displayed: Please confirm to archive the selected schedules. Click the OK button to archive the schedule or the Cancel button to revoke this action.
6. From the Add/Edit On-Duty Group Members panel you can choose to display the active schedules by clicking on the Clock icon, or by clicking the Edit Schedule icon and clicking the View Archive button.

Add/Edit On-duty Group Members

Each Receiver Group must have a list of members formed by Receivers and Groups.

Edit	Schedule	On-duty Group Name	Description
		On-duty Group 1	

Show parent Show Members

Members List

Hint: To select multiple items from a list, click the mouse button while holding down either the 'Shift' or 'Ctrl' key.
Show Attributes

Receivers

- owais_xmpp
- Receiver 3
- Receiver 4
- Receiver 8
- samz
- Voice

Groups (E) (F) (G) (O) (R) (S)

- Fax Group (G)
- Nadeem (O)
- usmaniowais Emergency PG (G)
- usmaniowais Escalation PG (E)
- usmaniowais Follow-Me PG (F)
- Voice Receiver Group (G)

Add

Show Group Members

Refresh Members

Sel	Edit	Active	Archived	Member Name	Type	Schedule	On-Duty Now	Up	Down	Last Rotating Sent	Status	Device Pin	Carrier	Email CC
<input type="checkbox"/>				Receiver 5	Receiver	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				Enabled	123	SMTP Carrier 4	
<input type="checkbox"/>				Receiver 6	Receiver						Enabled	123	SMTP Carrier 1	
<input type="checkbox"/>				Receiver 7	Receiver						Enabled	123	SMTP Carrier 1	
<input type="checkbox"/>				OD1	On-duty						Enabled			
<input type="checkbox"/>				RG1	Group						Enabled			

Click to select/deselect all

Remove Enable Disable

Save Changes

Move To >> Fax Group (G)

Done Print Members Export All

Define the work schedules for each On-Duty Group Member. The Member List will display the Members of this On-Duty Group and the work schedules of the people who use the devices.

The On-Duty Now flag allows Users to see who is on duty at the present moment. Here the Save Changes button saves the changes made without moving back to the Main Page, whereas the Done button leaves the Add/Edit Receiver Group Panel without saving the changes. The User is advised to click Save Changes before clicking Done, to save any changes made.

To view the Member schedule for an On-Duty Group:

1. From the Settings menu, click On-Duty Groups on the left navigation bar.
2. On the On-Duty Groups Panel, click the Edit Icon next to reach the Add/Edit On-Duty Group Members panel.
3. On the Add/Edit On-Duty Group Members panel, click on the Schedule Icon to view the Member schedule.

2012 GLOBAL SCHEDULE FOR RECIPIENT GROUP ONE (ON-DUTY)

◀ Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec ▶

Member of	Fri Dec 1		Sat Dec 2	
	am	pm	am	pm
Emergency On Call Group				
Group One				

Member of	Mon Dec 4		Tue Dec 5	
	am	pm	am	pm
Emergency On Call Group				
Group One				

Member of	Thu Dec 7		Fri Dec 8	
	am	pm	am	pm
Emergency On Call Group				
Group One				

Viewing the Member's Schedule of an On-Duty Group

Note: Within each Group, the On-Duty Group can be a Member of one or many On-Duty Groups and/or Follow-Me Groups. Within each such Group, the On-Duty Group will have assigned a schedule. The Schedule button on the Edit On-Duty Group panel allows a global view to all schedules assigned to this Group.

2012 GLOBAL SCHEDULE FOR RECIPIENT EMERGENCY ON CALL GROUP (O

◀ Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec ▶

Member of	Fri Dec 1		Sat Dec 2	
	am	pm	am	pm
Emergency On Call Group				

Member of	Mon Dec 4		Tue Dec 5	
	am	pm	am	pm
Emergency On Call Group				

Member of	Thu Dec 7		Fri Dec 8	
	am	pm	am	pm
Emergency On Call Group				

Viewing the schedule of an On-Duty Group

Schedule of a Not Available Receiver:

If a Receiver status becomes Not Available, than its schedule for that On-Duty/Follow-Me Group is shown in Red.

2012 MEMBER SCHEDULE FOR ON-DUTY GROUP: ON-DUTY GROUP 1
 ◀ Jan Feb Mar Apr **May** Jun Jul Aug Sep Oct Nov Dec ▶

Member	Sun Apr 1	Mon Apr 2	Tue Apr 3
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Wed Apr 4	Thu Apr 5	Fri Apr 6
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Sat Apr 7	Sun Apr 8	Mon Apr 9
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Tue Apr 10	Wed Apr 11	Thu Apr 12
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Fri Apr 13	Sat Apr 14	Sun Apr 15
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Mon Apr 16	Tue Apr 17	Wed Apr 18
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Thu Apr 19	Fri Apr 20	Sat Apr 21
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Sun Apr 22	Mon Apr 23	Tue Apr 24
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Wed Apr 25	Thu Apr 26	Fri Apr 27
Receiver 1	am	pm	am
Receiver 5	am	pm	am
Member	Sat Apr 28	Sun Apr 29	Mon Apr 30
Receiver 1	am	pm	am
Receiver 5	am	pm	am

Receiver1 is not available and hence shown in red. Whereas, Receiver5 remains enable and shown in blue.

Escalation Groups

An Escalation Group is a Group that allows you to specify a delay between the message send time for each Receiver and/or Receiver Group. When Users send messages to Members of an Escalation Group, each Member will receive the message at different times according to the intervals the administrator has set up, until the message is confirmed by one of the Receivers. This is beneficial when a User (the sender of a message) requires an answer in a given time before contacting the next Receiver.

For example, a User may send a message to Ann, asking if she can give a presentation to a potential customer. If Ann does not respond to the message in 30 minutes (the delay interval set up between the first and the second Receiver), the message is sent to Jill, the second Receiver in line. The escalation process continues until one of the Receivers answers the message in the Confirmation Send Panel, or all of the Receivers in the Escalation Group have been contacted.

Add Escalation Group

Each **Escalation Group** must have a list of members formed by **Receivers** and **Groups**.

Escalation Group Parameters

Name *

Description

Rotating

Cycles

Owner Settings

Set the owner

Alert the owner of membership changes

Departments

Member Of

Guest Settings

Hint: To select multiple items from a list, click the left mouse button while holding down either the 'Shift' or the 'Ctrl' key.

Available Departments

Guest In

Give the new Escalation Group a unique name. If the Department feature is enabled, then you will also have to assign this Escalation Group to a Department. Click Save to complete this step.

WORKING WITH AN ESCALATION GROUP:

To add a new Escalation Group:

Step A: Create an Escalation Group record.

1. From the Settings menu, click Escalation Groups on the left navigation bar.
2. On the Escalation Groups Panel, click the Add Group button to reach the Add Escalation Group page.
3. Enter a unique Name for this Group (mandatory).
4. Enter a Description of this Group (optional).
5. Check the Rotating checkbox if you want to enable the Rotating property inside the Escalation Group (optional).

Note: If the Rotating property is enabled, then the message will be sent by rotation to the next Member in the Group and the escalation process will start from there. In other words the rotation property has a higher precedence than the Escalation property.

6. Select Cycle from the dropdown menu. The default value is 1, you can select 10 maximum.
Example: If the Cycle number is 5, then the Escalation cycle will execute on the Member list until 5 cycles are completed. This cycle terminates as soon as any message gets confirmed.
7. Enable Owner Settings if you want to assign any owner to this Receiver Group (optional).
8. Check the Alert the owner of membership changes checkbox (optional).

- If anyone makes changes (enable/disable Receiver, changing Receiver Group's name and description, repositioning of Receivers) in the Escalation Group other than the owner, an email will be sent to the owner of this Group about those changes.
 - If the owner is changed in any Receiver Group, emails will be sent to the new and old owners.
 - If the Receiver changes his/her schedule, notification will be sent to the Group owner.
 - If the Receiver disables himself/herself (from main Receiver panel or edit Receiver page), notification will be sent to a Group owner.
 - Non sysAdmin Users can only see non sysAdmin Users in the Owner dropdown.
 - SysAdmin Users can see all of the Users in Owner dropdown.
 - If the Department feature is not enabled then there will be a configuration parameter in the Receiver Group that states Limit access to sysAdmin and owner.
 - If the User enables the Limit Access checkbox, then that Receiver Group will not be visible to any non sysAdmin User.
9. If the Department feature is not enabled, skip to step 10.
 10. Specify the Department for this new Group.
 11. If Users who only have rights to send messages to other Departments will also need to send messages to this Group, then you can allow them to do so by adding their Department to the Guest In box.
 12. Click the Save button to reach the Add/Edit Escalation Group Members page.

Add/Edit Escalation Group Members

Each Receiver Group must have a list of members formed by Receivers and Groups.

Edit	Escalation Group Name	Description
<input checked="" type="checkbox"/>	Escalation Group 1	

Show parent Show Members

Members List

Show Attributes

Receivers: Receiver 6
Groups (E) (F) (G) (O) (R) (S): Fax Group (G)

Escalation Delay: :01 (minutes)

Buttons: Add Receiver, Add Group, Refresh Members

Sel	Member Name	Type	Escalation Delay	Up	Down	Delay	Status	Device Pin	Carrier	Email CC
<input type="checkbox"/>	Receiver 5	Receiver	1 minute(s).		▼	:01 ▼	Enabled	123	SMTP Carrier 4	
<input type="checkbox"/>	Receiver 6	Receiver	2 minute(s).	▲	▼	:02 ▼	Enabled	123	SMTP Carrier 1	
<input type="checkbox"/>	Receiver 7	Receiver	3 minute(s).	▲	▼	:03 ▼	Enabled	123	SMTP Carrier 1	
<input type="checkbox"/>	Receiver 5	Receiver	4 minute(s).	▲	▼	:04 ▼	Enabled	123	SMTP Carrier 4	
<input type="checkbox"/>	Receiver 6	Receiver	5 minute(s).	▲		:05 ▼	Enabled	123	SMTP Carrier 1	

Click to select/deselect all

Buttons: Remove, Enable, Disable, Save Changes, Move To >> (Fax Group (G)), Done, Print Members, Export All

Specify a delay between Receivers and/or Groups. The Members of the new Escalation Group and the delay between Receivers will be displayed.

Note: *The Next in line column is displayed only if the Rotating property is enabled.*

Step B: Assign Escalation Group Members.

1. Set the Escalation Delay to be used between each Member of the Escalation Group. Note that the first Receiver does not require a delay. A delay greater than 5 minutes is recommended for the other Receivers.
2. Select a Receiver or Group and click the Add button. Escalation messages will be sent in the order they are added to the Member List.

Note: The type of the Group is coded as follows: (E) for Escalation Group, (F) for Follow-Me Group, (G) for Receiver Group, (O) for On-Duty Group, and (R) for Rotate Group.

3. To change the order of the Members of the list, press the Up or Down icons. To change the Escalation Delay, use the New Delay dropdown list available on each row.
4. When you are finished, click Done.

Note: select a Group and click the Show Group Members link to see the Members of that Group on a separate Web page. (This is useful if you want to see who is on duty right now.)

To modify an Escalation Group:

1. From the Settings menu, click Escalation Groups on the left navigation bar.
2. On the Escalation Groups Panel, find the Group name you want to modify and click the Edit icon.
3. On the Add/Edit Escalation Group Members page, press the Edit icon to modify the Name or the Description (from the Edit Escalation Group page). To add Members to the Member List, select the Receivers or Receiver Groups and click the Add Receiver or Add Receiver Group button respectively. To delete a Member from the Member List, check mark the Member from the Sel column and press the Remove button. To change the order of the Members of the list, press the Up or Down icons. To change the Escalation Delay, use the Delay dropdown list available on each row.

Add/Edit Escalation Group Members

Each Receiver Group must have a list of members formed by Receivers and Groups.

Edit	Escalation Group Name	Description
<input type="checkbox"/>	Escalation Group 1	

Show parent Show Members

Members List

Show Attributes

Receivers: Receiver 6 Groups (E) (F) (G) (O) (R) (S): Fax Group (G)

Escalation Delay: :01 (minutes)

Buttons: Add Receiver, Add Group, Refresh Members

Set	Member Name	Type	Escalation Delay	Up	Down	Delay	Status	Device Pin	Carrier	Email CC
<input type="checkbox"/>	Receiver 5	Receiver	1 minute(s).		▼	:01 ▼	Enabled	123	SMTP Carrier 4	
<input type="checkbox"/>	Receiver 6	Receiver	2 minute(s).	▲	▼	:02 ▼	Enabled	123	SMTP Carrier 1	
<input type="checkbox"/>	Receiver 7	Receiver	3 minute(s).	▲	▼	:03 ▼	Enabled	123	SMTP Carrier 1	
<input type="checkbox"/>	Receiver 5	Receiver	4 minute(s).	▲	▼	:04 ▼	Enabled	123	SMTP Carrier 4	
<input type="checkbox"/>	Receiver 6	Receiver	5 minute(s).	▲		:05 ▼	Enabled	123	SMTP Carrier 1	

Click to select/deselect all

Buttons: Remove, Enable, Disable, Save Changes, Move To >> Fax Group (G), Done, Print Members, Export All

The Add/ Edit Escalation Group Members

4. Click the Print Members button to open a new browser window with a list of the Group Members. You can send to the printer by clicking on the Print button displayed at the bottom of the page.
5. When you are finished, click Done.

Step C: Assign Receiver Group Members Through Receiver Attributes

1. Under the Members List section, the Show Attributes link will be available. Clicking on this link will display the Select Attributes section with all of the available attribute checkboxes. This section will provide you the additional capability to filter out the Receiver records based on their assigned attributes.

Example: Selecting attribute Age < 20 and US citizen checkbox will only list Receivers, which belongs to attribute Age < 20 and US citizen as shown in above figure and make selection easier.

Note: If the Enable Receiver Attributes feature is turned off from Global Settings, than no link to filter the Receivers based on their attributes will be displayed on this page.

To delete an Escalation Group:

1. From the Settings menu, click Escalation Groups on the left navigation bar.
2. On the Escalation Groups Panel, find the Group name you want to remove and click the Delete icon.

3. Click the OK button to confirm deletion or click Cancel to revoke this action.

Note: An Escalation Group can be a Member of one or many On-Duty Groups and/or Follow-Me Groups. Within each such Group, the Escalation Group will have assigned a schedule. The Schedule button on the Edit Escalation Group panel allows a global view to all schedules assigned to this Group. Please see the On-Duty Groups and Follow-Me Groups sections to learn more details about setting schedules.

Rotate Groups

A Rotate Group is a Group that allows you to send messages to different Receivers or Groups in a rotation. A Group is created by simply adding Receivers or Groups in the order that you would like them to receive the messages. This order can be changed later. When a message is sent to the Group, HipLink will check which Receiver is flagged to receive the message based on this order.

For example, a Rotate Group named Intervention Team might include three Receivers and one On-Duty Group, (e.g., Bill Phone, Jane Mobile, Jess Cell and the Intervention On-Duty Group). The first message sent to the Group will go to Bill Phone, the second one to Jane Mobile, the third to Jess Cell and then the fourth will go to whoever is On-Duty at that time in the Intervention On-Duty Group. HipLink will keep track of who got the last message and always send the next message to the next Receiver in line.

WORKING WITH ROTATION GROUP:

To add a new Rotate Group:

Step A: Create a Rotate Group record.

1. From the Settings menu, click Rotate Groups on the left navigation bar.
2. On the Rotate Groups Panel, click the Add Group button to reach the Add Rotate Group page.
3. Enter a unique Name for this Group (mandatory).
4. Enter a Description of this Group (optional).
5. Enable Owner Settings if you want to assign any owner to this Receiver Group (optional).
6. Check Alert the owner of membership changes checkbox (optional).
 - If anyone makes changes (enable/disable Receiver, changing Receiver Group's name and description, repositioning of Receivers) in the Rotate Group other than the owner, an email will be sent to the owner of this Group about those changes.
 - If the owner is changed in any Receiver Group, emails will be sent to the new and old owners.
 - If the Receiver changes his/her schedule, notification will be sent to the Group owner.
 - If the Receiver disables himself/herself (from main Receiver panel or edit Receiver page), notification will be sent to a Group owner.
 - Non sysAdmin Users can only see non sysAdmin Users in the Owner dropdown.
 - SysAdmin Users can see all of the Users in Owner dropdown.
 - If the Department feature is not enabled then there will be a configuration parameter in the Receiver Group that states Limit access to sysAdmin and owner.
 - If the User enables the Limit Access checkbox, then that Receiver Group will not be visible to any non sysAdmin User.
7. If the Department feature is not enabled, skip to step 9.

8. Specify the Department for this new Group.
9. If Users who only have rights to send messages to other Departments will also need to send messages to this Group, then you can allow them to do so by adding their Department to the Guest In box.
10. Click the Save button to reach the Add/Edit Rotate Group Members page.

Add Rotate Group

Each **Rotate Group** must have a list of members formed by **Receivers** and **Groups**.

Rotate Group Parameters

Name: Rotate Group 1 *

Description: [Text Box]

Owner Settings

Set the owner: admin

Alert the owner of membership changes

Departments

Member Of: Default

Guest Settings

Hint: To select multiple items from a list, click the left mouse button while holding down either the 'Shift' or the 'Ctrl' key.

Available Departments

Default

Guest In

Add >>

<< Remove

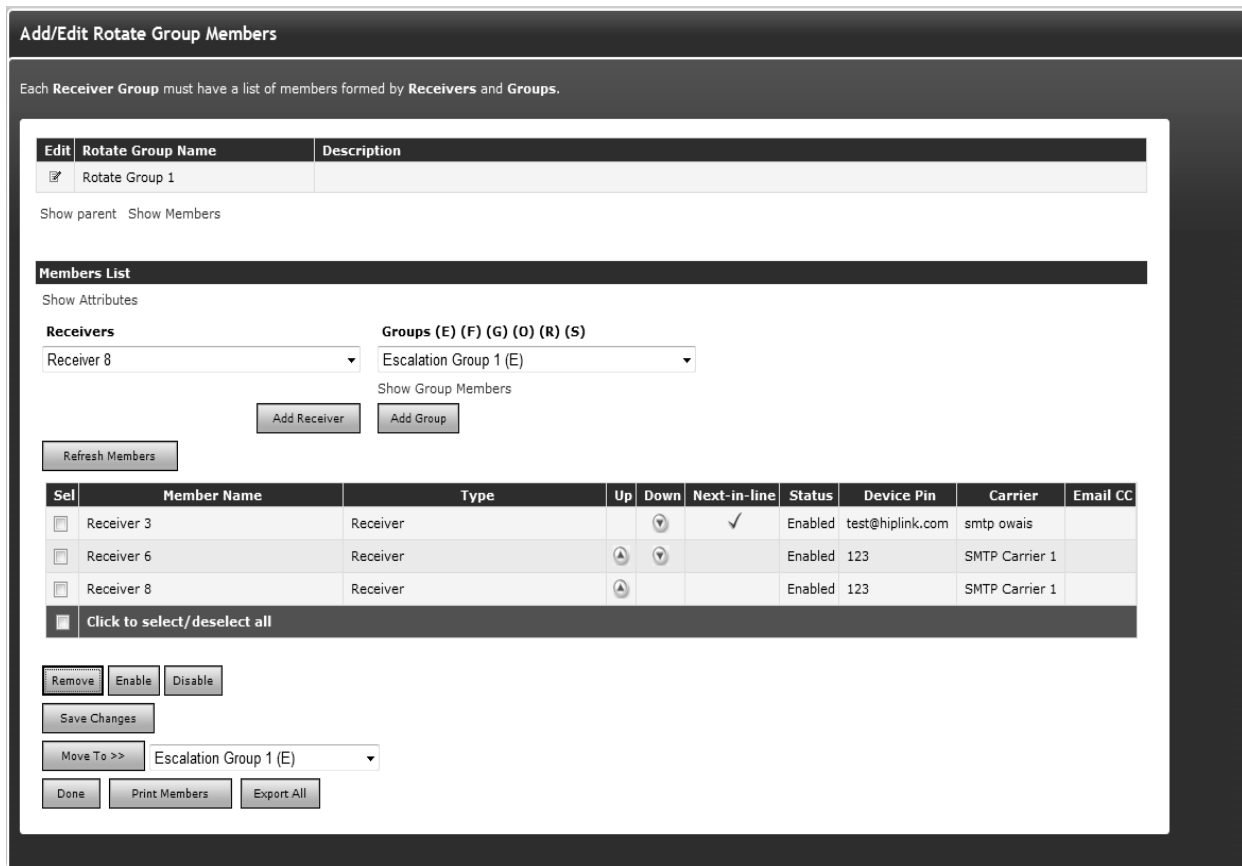
Save Reset Cancel

Give the new Rotate Group a unique name. If the Department feature is enabled, then you will also have to assign this Rotate Group to a Department.

Step B: Assign Rotate Group Members.

1. Select a Receiver or Group and then click the Add Receiver or Add Group button respectively. Rotate Group messages will be sent in rotation to the Receiver that is flagged Next-in- Line in the Member List.
Note: The type of the Group is coded as follows: (E) for Escalation Group, (F) for Follow-Me Group, (G) for Receiver Group, (O) for On-Duty Group, and (R) for Rotate Group.
2. To change the order of the Members of the list, press the Up or Down icons.
3. Click the Print Members button to open a new browser window with a list of the Group Members. You can send to the printer by clicking on the Print button displayed at the bottom of the page.
4. When you are finished, click Done.

Note: A Rotate Group can be a Member of one or many On-Duty Groups and/or Follow-Me Groups. Within each such Group, the Rotate Group will have assigned a schedule. The Schedule button on the Edit Rotate Group panel allows a global view to all schedules assigned to this Group. Please see the On-Duty Group and Follow-Me Group sections below to learn more details about setting schedules.



The Add/ Edit Rotate Group Members

Step C: Assign Receiver Group Members using Receiver Attributes

- Under the Members List section, the Show Attributes link will be available. Clicking on this link will display the Select Attributes section with all of the available attribute checkboxes, this section will provide you with the additional capability to filter out the Receiver records based on their assigned attributes.

Example: Selecting attribute Age < 20 and US citizen checkbox will only list Receivers, which belongs to attribute Age < 20 and US citizen as shown in above figure and make selection easier.

Note: If Enable Receiver Attributes feature is turned off from Global Settings, than no link to filter Receivers based on their attributes will be displayed on this page.

Follow-Me Groups

Follow-Me Groups allow you to send messages to a specific Receiver, who has more than one device. The Receiver can then receive messages depending on the time schedule for each device. This could also be achieved with an On-Duty Group, but the Follow-Me interface is more suited for this purpose, i.e., for one person with multiple Receivers rather than multiple people with one Receiver each.

For example, a Follow-Me Group named Follow John Doe might include three different Receivers: John Doe Cell, John Doe Pager and John Doe Email. On weekday mornings when John gets to work, messages are sent to his text-enabled cell phone. In the afternoon while he

is giving lectures, they are sent to his pager. And at night while he is at home, they are sent to his email address.

WORKING WITH FOLLOW-ME GROUP:

Step A: Create a Follow-Me Group record.

1. From the Settings menu, click Follow-Me Groups on the left navigation bar.
2. On the Follow-Me Groups Panel, click the Add Group button to reach the Add Follow-Me Group page.
3. Enter a unique Name for this Group (mandatory).
4. Enter a Description of this Group (optional).
5. Check the Rotating checkbox if you want to enable the Rotating property inside the Follow- Me Group (optional).

Note: *The Rotating property has an effect only if there are two or more Members scheduled to receive messages at the same time. If the Rotating property is enabled, then the message will be sent by rotation to the next Member in the Group who has a valid schedule at that given time. In other words, the schedule has a higher precedence than the rotating property.*

6. Enable Owner Settings if you want to assign any owner to this Receiver Group (optional).
7. Check Alert the owner of Membership changes checkbox (optional).
 - If anyone makes changes (scheduling Receivers, enable/disable Receiver, changing Receiver Group's name and description, repositioning of Receivers) in the Follow-Me Group other than the owner, an email will be sent to the owner of this Group about those changes.
 - If the owner is changed of any Receiver Group, emails will be sent to the new and old owners.
 - If the Receiver changes his/her schedule, notification will be sent to the Group owner.
 - If the Receiver disables himself/herself (from main Receiver panel or edit Receiver page), notification will be sent to a Group owner.
 - Non sysAdmin Users can only see non sysAdmin Users in the Owner dropdown.
 - SysAdmin Users can see all of the Users in Owner dropdown.
 - If the Department feature is not enabled then there will be a configuration parameter in the Receiver Group that states Limit access to sysAdmin and owner.
 - If the User enables the Limit access checkbox, then that Receiver Group will not be visible to any non sysAdmin User.
8. If the Department feature is not enabled, skip to step 10.
9. Specify the Department for this new Group.
10. If Users, who only have rights to send messages to other Departments, will also need to send messages to this Group, then you can allow them to do so by adding their Department to the Guest In box.
11. Click the Save button to reach the Add/Edit Follow-Me Group Members page.

Add Follow-Me Group

Each Follow-Me Group must have a list of members formed by Receivers and Groups.

Follow-Me Group Parameters

Name *

Description

Rotating

Owner Settings

Set the owner

Alert the owner of membership changes

Departments

Member Of

Guest Settings

Hint: To select multiple items from a list, click the left mouse button while holding down either the 'Shift' or the 'Ctrl' key.

Available Departments **Guest In**

Default	Add >>		<< Remove
---------	--------	--	-----------

Editing the Follow-Me Group settings

Step B: Assign Follow-Me Group Members

1. Select the Receiver or Group you want to include in the Member List and click the Add button.

Note: The type of the Group is coded as follows: (E) for Escalation Group, (F) for Follow-Me Group, (G) for Receiver Group, (O) for On-Duty Group, and (R) for Rotate Group.

2. Repeat as necessary.
3. The Member List will display the Members of this Follow-Me Group.

Note: select a Group and click the Show Group Members link to see the Members of that Group on a separate Web page. This is useful if you want to see who is On-Duty right now.

Add/Edit Follow-Me Group Members

Each Receiver Group must have a list of members formed by Receivers and Groups.

Edit	Schedule	Follow-Me Group Name	Description
		Follow-Me Group 1	

Show parent Show Members

Members List

Hint: To select multiple items from a list, click the mouse button while holding down either the 'Shift' or 'Ctrl' key.

Show Attributes

Receivers

- owais_xmpp
- Receiver 5
- Receiver 6
- Receiver 8
- samz
- Voice

Groups (E) (F) (G) (O) (R) (S)

- Escalation Group 1 (E)
- Fax Group (G)
- Nadeem (O)
- OD1 (O)
- On-duty Group 1 (O)
- RG1 (G)

Add

Show Group Members

Refresh Members

Sel	Edit	Active	Archived	Member Name	Type	Schedule	On-Duty Now	Status	Device Pin	Carrier	Email CC
<input type="checkbox"/>				Receiver 3	Receiver	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enabled	test@hiplink.com	smtp owais	
<input type="checkbox"/>				Receiver 4	Receiver			Enabled	123	msn nadeem	
<input type="checkbox"/>				Receiver 7	Receiver			Enabled	123	SMTP Carrier 1	

Click to select/deselect all

Remove Enable Disable

Save Changes

Move To >> Escalation Group 1 (E)

Done Print Members Export All

The On-Duty Now flag allows Users to see who is currently on duty at the present moment.

Step C: Assign Receiver Group Members Using Receiver Attributes

- Under the Members List section, Show Attributes link will be available. Clicking on this link will display the Select Attributes section with all of the available attributes checkboxes, this section will provide you the additional capability to filter out the Receiver records based on their assigned attributes.

Example: Selecting attribute Age < 20 and US citizen checkbox will only list receivers, which belongs to attribute Age < 20 and US citizen as shown in above figure and make selection easier.

Note: If the Enable Receiver Attributes feature is turned off from Global Settings, than no link to filter receivers based on their attributes will be displayed on this page.

Sel	Edit	Active	Archived	Member Name	Type	Schedule	On-Duty Now	Status	Device Pin	Carrier	Email CC
<input type="checkbox"/>				Receiver 3	Receiver	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enabled	test@hiplink.com	smtp owais	
<input type="checkbox"/>				Receiver 4	Receiver			Enabled	123	msn nadeem	
<input type="checkbox"/>				Receiver 7	Receiver			Enabled	123	SMTP Carrier 1	

Click to select/deselect all

Adding/Editing weekly schedules for Follow-Me Groups

Step D: Create the schedules for the Follow-Me Group Members:

1. Click the Edit icon next to the Group Member for which the Schedule is to be edited or assigned.
2. Follow-Me Group schedules can be either added manually, imported from a standard schedule file, or can be added from already defined Schedule Templates (see the Schedule Templates section for details). There are three types of schedules that can be added manually: weekly, monthly, and nonrecurrent.
 - To create a weekly schedule click Add Weekly Schedule, then continue with Step D (Weekly).
 - To create a monthly schedule click Add Monthly Schedule, then continue with Step D (Monthly).
 - To create a nonrecurring (once-only) schedule click Add Nonrecurring Schedule, then continue with Step D (Nonrecurrent).
 - To import a schedule file type the full path or click Browse, select a standard schedule file (i.e., a file with .ics extension) from your computer and then click Import Schedule. If the import operation is successful click the OK button to return to the Schedule Templates Panel.
 - To add a schedule from Templates, click Add from Templates, then continue with Step D (Templates).

Add Weekly Schedule

Add/Edit a weekly schedule

Follow-me Group: System Follow Me group
Member: Receiver 1

On-duty Time

Scheduled Name: *

Time Frame: Start: 00:00 * End: 01:00 * Duration: 01:00

Recurrence pattern *

Recurrence every 1 week(s) on

Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Range of recurrence

Start: 12/19/2006

No end date
 End after occurrences
 End by

Ok Cancel

Adding/Editing weekly schedules for On-Duty Groups

Step D (Weekly): Create a Weekly Schedule for a Follow-Me Group Member:

1. Choose a Name for the Schedule (mandatory).
2. Enter a Time frame for the day of this Schedule (mandatory). Enter the Start and End time for the schedule and the duration will be calculated for you. Alternatively, you can enter the Start time and the Duration (hh:mm), and then the end time will be calculated for you when you click on the next field.
3. Set the Recurrence pattern. Choose the number of weeks for the recurrence of this schedule and the days on which this schedule should apply. For example if you pick 1 week and Monday then the schedule will be in effect on every Monday, but if you pick 2 weeks and Monday, then the schedule will be in effect every 2nd Monday.

- Set the Range of recurrence. The start date of this Schedule defaults to today's date. You can change it by directly editing the text box (use the MM/DD/YYYY format), or by clicking on the calendar icon to select a date. By default the recurrence never ends. If you want it to end after a certain number of occurrences, click the second radio button and enter the number of occurrences. To end at a certain date, click the third radio button and enter a date in the text box (use the MM/DD/YYYY format) or click on the calendar icon to select a date.
- When you are done, click OK. You may then either set up a schedule for another Member of this Group, or if you are done, then click the Close button on that Pop-up window.

Add Monthly Schedule

Add/Edit a monthly schedule

Follow-me Group: System Follow Me group
Member: Receiver 1

On-duty Time

Scheduled Name: [text box] *

Time Frame: Start: [00][00] * End: [01][00] * Duration: [01:00]

Recurrence pattern *

Day 1 of every 1 month(s)

The First Sunday of every 1 month(s)

And continue for 1 days

Adding/Editing monthly schedules for Follow-Me Group Members

Step D (Monthly): Create a Monthly Schedule for a Follow-Me Group Member:

- Choose a Name for the Schedule (mandatory).
- Enter a Time frame for the day of this Schedule (mandatory). Enter the Start and End time for the schedule and the duration will be calculated for you. Alternatively, you can enter the Start time and the Duration (hh:mm), and then the end time will be calculated for you when you click on the next field.
- Select your preferred type of Recurrence pattern using the radio buttons.
- Set the Range of recurrence. The start date of this Schedule defaults to today's date. You can change it by directly editing the text box (use the DD/MM/YYYY format), or by clicking on the calendar icon to select a date. By default the recurrence never ends. If you want it to end after a certain number of occurrences, click the second radio button and enter the number of occurrences. To end at a certain date, click the third radio button and enter a date in the text box (use the DD/MM/YYYY format) or click on the calendar icon to select a date.
- When you are done, click OK. You may then either set up a schedule for another Member of this Group, or if you are done, then click the Close button on that Pop-up window.

Adding/Editing weekly nonrecurrent schedules for Follow-Me Group Members

Step D (Nonrecurrent): Create a Nonrecurrent Schedule for a Follow-Me Group Member:

1. Choose a Name for the Schedule (mandatory).
2. Enter a Time frame for the day of this Schedule (mandatory). When you enter the Start and End time for the schedule, then the duration will be calculated for you. Alternatively, you can enter the Start time and the Duration (hh:mm), and then the end time will be calculated for you when you click on the next field.
3. Choose the date of this Schedule by editing the Date text box (use the DD/MM/YYYY format), or by clicking on the calendar icon to select a date.
4. When you are done, click OK. You may then either set up a schedule for another Member of this Group, or if you are done, then click the Close button on that Pop-up window.

View		Select	Name	Type	Start
	<input type="checkbox"/>	Monthly Stalling	Monthly	Dec 19 2006	03:00
	<input type="checkbox"/>	Weekly posting	Weekly	Dec 19 2006	04:00
		<input type="checkbox"/>	Click to select/unselect all.		

Viewing the schedules for Follow-Me Group Members

Step D (Templates): Add a Schedule from Templates for a Follow-Me Group Member:

1. Check the Select checkbox in front of the Schedule Template name you want to add (or click the View icon to see the schedule details before adding it) and then click Add button.
2. Click the OK button to confirm addition or click Cancel to revoke this action.

To view the Member Schedule for a Follow-Me Group:

1. From the Settings menu, click Follow-Me Group on the left navigation bar.
2. On the Follow-Me Group Panel, click the Edit Icon next to reach the Add/Edit Follow-Me Group Members panel.
3. On the Add/Edit Follow-Me Group Members Panel, click on the Schedule Icon to view the Member Schedule.

To modify a Follow-Me Group:

1. From the Settings menu, click Follow-Me Groups on the left navigation bar.

2. On the Follow-Me Groups Panel, find the Group name you want to modify and click the Edit icon.
3. On the Add/Edit Follow-Me Group Members page, press the Edit icon to modify the Name or the Description (from the Edit Follow-Me Group page). To add Members to the Member List, select the Receivers and Receiver Groups and click the Add button.
4. Click the Print Members button to open a new browser window with a list of the Group Members. Send to the printer by clicking on the Print button displayed at the bottom of the page.
5. When you are finished, click Done.

To delete a Follow-Me Group:

1. From the Settings menu, click Follow-Me Groups on the left navigation bar.
2. On the Follow-Me Groups Panel, find the Group name you want to remove and click the Delete icon.
3. Click the OK button to confirm deletion or click Cancel to revoke this action.

To archive a Follow-Me Group schedule:

1. From the Settings menu, click Follow-Me Groups on the left navigation bar.
2. On the Follow-Me Groups Panel, find the Group name you want to modify and click the Edit icon.
3. On the Add/Edit Follow-Me Group Members panel, click the Edit icon for the Follow-Me Group Member you want to modify.
4. On the Schedule Main page, click the checkbox for the schedule that you want to archive (or click the Select All checkbox at the bottom of the table).
5. Click the Archive button to confirm or click the Close button to revoke this action.
6. From the Add/Edit Follow-Me Group Members panel you can choose to display the active schedules by clicking on the Active icon, or the archived schedules by pressing on the Archived icon.

2007 MEMBER SCHEDULE FOR FOLLOW-ME GROUP: FIRE DEPARTMENT						
	Jan		Feb		Mar	
	Apr		May		Jun	
	Jul		Aug		Sep	
	Oct		Nov		Dec	
Member	Thu Mar 1		Fri Mar 2		Sat Mar 3	
	am	pm	am	pm	am	pm
st Group	[Grid of 12 cells]					
st Group	[Grid of 12 cells]					
Member	Sun Mar 4		Mon Mar 5		Tue Mar 6	
	am	pm	am	pm	am	pm
st Group	[Grid of 12 cells]					
st Group	[Grid of 12 cells]					

Viewing the Member schedule for Follow-Me Group's Members

Note: A Follow-Me Group can be a Member of one or many On-Duty Groups and/or Follow-Me Groups. Within each such a Group, the Follow-Me Group will have assigned a schedule. The Schedule button on the Edit Follow-Me Group panel allows a global view to all schedules assigned to this Group.

2007 MEMBER SCHEDULE FOR FOLLOW-ME GROUP: FIRE DEPARTMENT

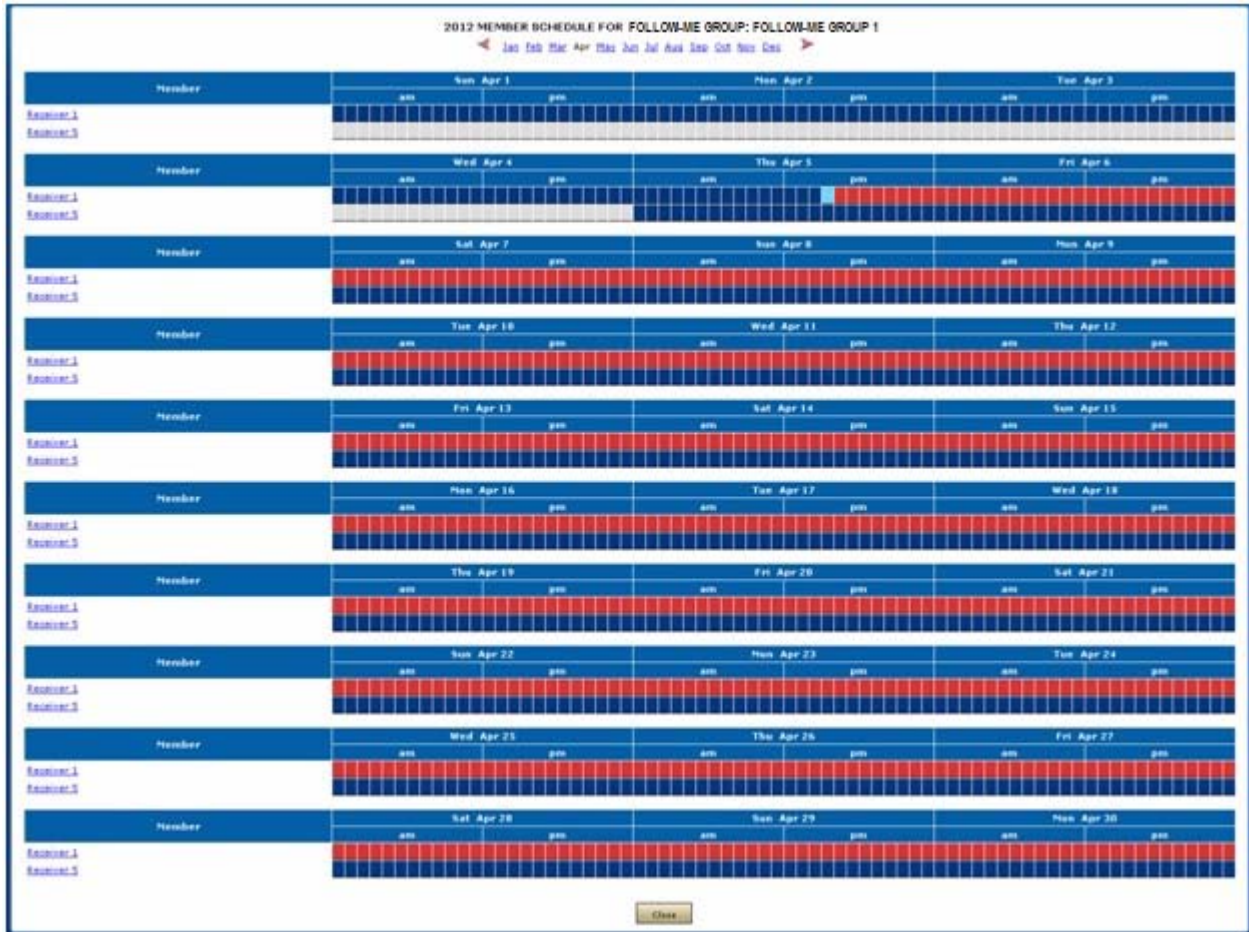
◀ Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec ▶

Member	Thu Mar 1		Fri Mar 2		Sat Mar 3	
	am	pm	am	pm	am	pm
First Group						
Member	Sun Mar 4		Mon Mar 5		Tue Mar 6	
	am	pm	am	pm	am	pm
First Group						
Member	Wed Mar 7		Thu Mar 8		Fri Mar 9	
	am	pm	am	pm	am	pm
First Group						
Member	Sat Mar 10		Sun Mar 11		Mon Mar 12	
	am	pm	am	pm	am	pm
First Group						

Viewing the global schedule for Follow-Me Group's Members

Schedule of a Not Available Receiver:

If a Receiver status becomes Not Available, than its schedule for that On-Duty/Follow-Me Group is shown in Red.



Receiver1 is not available and hence shown in red. Whereas, Receiver5 remains enable and shown in blue.

SUBSCRIPTION GROUPS

Subscription Groups is an optional feature that allows messages, either wireless text, voice or email, to be sent to a Group whose Members have elected or opted-in to receive informational alerts related to that Group description. This Group function provides for the dissemination of update type messages to an audience that has a specific interest to the topic or title of the Group and decides on their own to subscribe. Members of a Group may be part of a business unit that may be directly affected by an outage or slow down or need to know as conditions change. Only Receivers can be added as Members. Other Groups cannot be included here as Members.

Examples of the subscription type Groups could be weather related, such as Snow Updates, Market updates and Interest Rate Change, or system related messages like website down or any other application that may be running. Other usages could be geographic such as Northeast Region Alerts or even client Groups that indicate an active incident within strategic accounts of a company and its resolution.

WORKING WITH A SUBSCRIPTION GROUP:

To add a new Subscription Group:

Step A: Create a Subscription Group record.

1. From the Settings menu, click Subscription Groups on the left navigation bar.
2. On the Subscription Groups Panel, click the Add Group button to reach the Add Subscription Group page.
3. Enter a unique Name for this Group (mandatory).
4. Enter a Description of this Group (optional).
5. Enter the common Topic of interest for which the subscribed receivers will receive alerts.
6. Check Alert the owner of membership changes checkbox (optional).
 - If anyone makes changes (enable/disable receiver, changing Receiver Group's name and description, adding, removing receivers) in the Subscription Group other than the owner, an email will be sent to the owner of this Group about those changes.
 - If the Receiver disables himself/herself (from main Receiver Panel or edit Receiver page), notification will be sent to a Group owner.
 - The User who has created a Subscription Group can become the owner of that Group.
7. Click the Save button to reach the Add/Edit Rotate Group Members page.

Give the new Subscription Group a unique name.

Step B: Assign Subscription Group Members.

1. Select a Receiver and then click the Add button respectively. Subscription Group messages will be sent to the Receivers selected.
2. Click the Print Members button to open a new browser window with a list of the Group Members that you can easily send to the printer by clicking on the Print button displayed at the bottom of the page.
3. To disable a Receiver from receiving an alert, select that Receiver from the list and click on the Disable button.
4. To copy a list of Receivers for a certain subscription Group to another subscription Group, select that subscription Group from the dropdown menu and click Copy To >>.
5. When you are finished, click Done.

Note: see next section for for Show Member and Show Parents of Viewing Receiver Groups & Members.

Step C: Assign Receiver Group Members Using Receiver Attributes

- Under the Members List section, the Show Attributes link will be available. Clicking on this link will display the Select Attributes section with all of the available attribute checkboxes. This section will provide you the additional capability to filter out the Receiver records based on their assigned attributes.

Example: Selecting attribute Age < 20 and US citizen checkbox will only list receivers, which belongs to attribute Age < 20 and US citizen as shown in above figure and make selection easier.

Note: If the Enable Receiver Attributes feature is turned off from Global Settings, than no link to filter Receivers based on their attributes will be displayed on this page.

HOW TO SUBSCRIBE TO A GROUP.

The administrator can assign Receivers to the Group at the time of creation or later. Once created, the Subscription Groups are public and visible. Certain Receivers who are so enabled by the Administrators can login and subscribe/unsubscribe to these Groups.

Each Receiver Group must have a list of members formed by Receivers and Groups.

Edit	Subscription Group Name	Description
	Subscription Group	

Show parent Show Members

Members List

Hint: To select multiple items from a list, click the mouse button while holding down either the 'Shift' or 'Ctrl' key.

Show Attributes

Receivers

- Receiver 2
- Receiver 3
- Receiver 4
- Receiver 8
- samz
- Voice

Refresh Members

Sel	Member Name	Type	Status	Device Pin	Carrier	Email CC
<input type="checkbox"/>	Receiver 5	Receiver	Enabled	123	SMTP Carrier 4	
<input type="checkbox"/>	Receiver 6	Receiver	Enabled	123	SMTP Carrier 1	
<input type="checkbox"/>	Receiver 7	Receiver	Enabled	123	SMTP Carrier 1	

Click to select/deselect all

Remove Enable Disable

Save Changes

Copy To >> Escalation Group 1 (E)

Done Print Members Export All

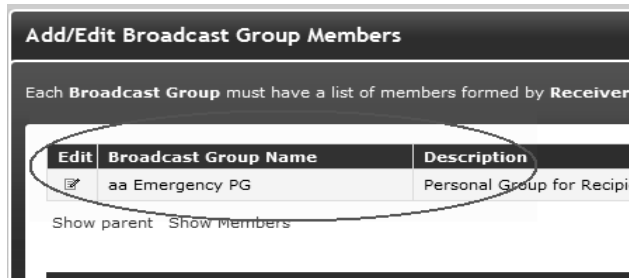
The Add/Edit Subscription Group Members

Viewing Group Parent & Members

Any Group may contain several other Groups. Receivers can also be part of other Broadcast Groups and keeping track of the hierarchy can be a little tricky. HipLink provides its Users the ability to view a Group's parent as well as child Members.

To view these, navigate to a the Group's EDIT page by clicking on the EDIT icon on Broadcast Group main page.

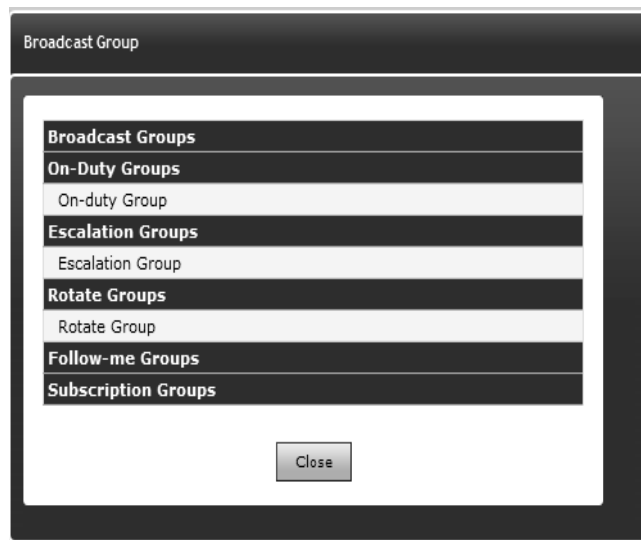
On the EDIT page, right below the Group name, there will be two hyperlinks available titled Show Parent & Show Members.



Show Parent & Show Members of Broadcast Group

To View Parent Members of a Group

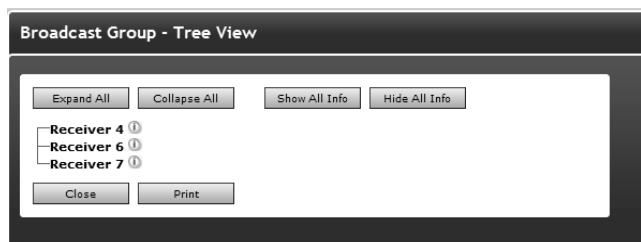
To view the parent Members of a Group, click on the Show Parent hyperlink. It will spawn a new pop-up window which will show a list of all other Groups which have this particular Group as a Member added in them.



Show Parent Pop-up Showing Empty List

To View Child Members of a Group

To view child Members of a Group, click on the show Member's hyperlink. It will spawn a new popup window which will show a tree view with all the Members of this Group shown as leaves of this tree.



Group Members tree view

However, if the Members of the Group include Receivers as well as other Groups, then the Groups would be expanded to show the children of that Group. If it's a nested Group then a tree with levels right up to the last leaf node (i.e., Receiver) would be shown.

on the Show All Info button on top. Also, the User can view the information of selected Receivers/Receiver Groups by clicking on the icon adjacent to a record.



Selected record information displayed

Queue Panel

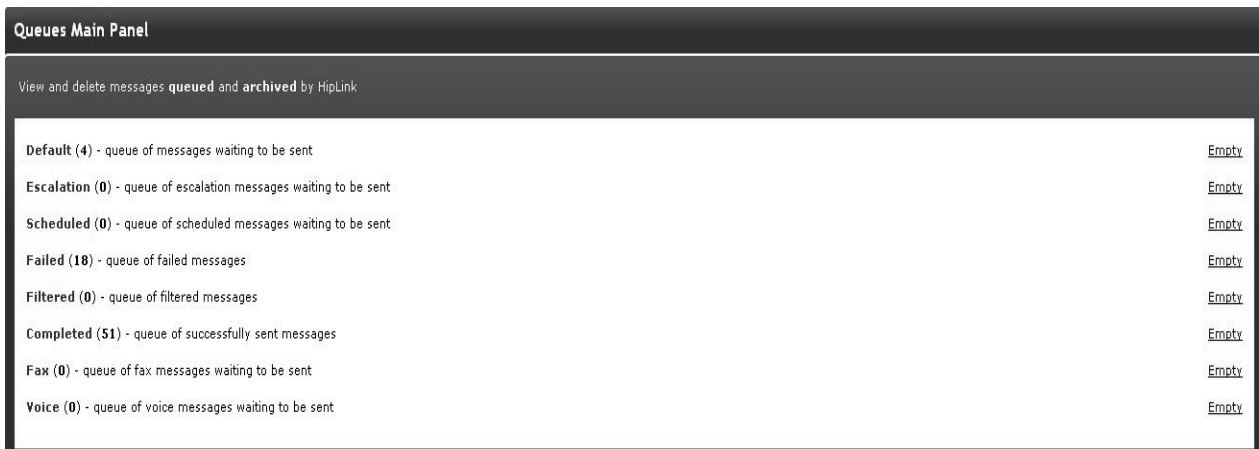
The HipLink queues line up messages to be sent. When a User sends a message, it is lined up in a dedicated queue: Main, Escalation, Scheduled, Fax, or Voice Queue. The Queue menu allows permitted Users to view and, if necessary, delete messages in these queues before the Messengers are picking them up.

Note: If the multiple Paging Queues feature is enabled by the License Key, then the Main paging queue is replaced by the Default queue.

Messages that have been successfully processed and sent to the Carrier are stored in the Completed queue. Unsuccessful messages that are not sent to the Carrier are stored in the Failed Queue.

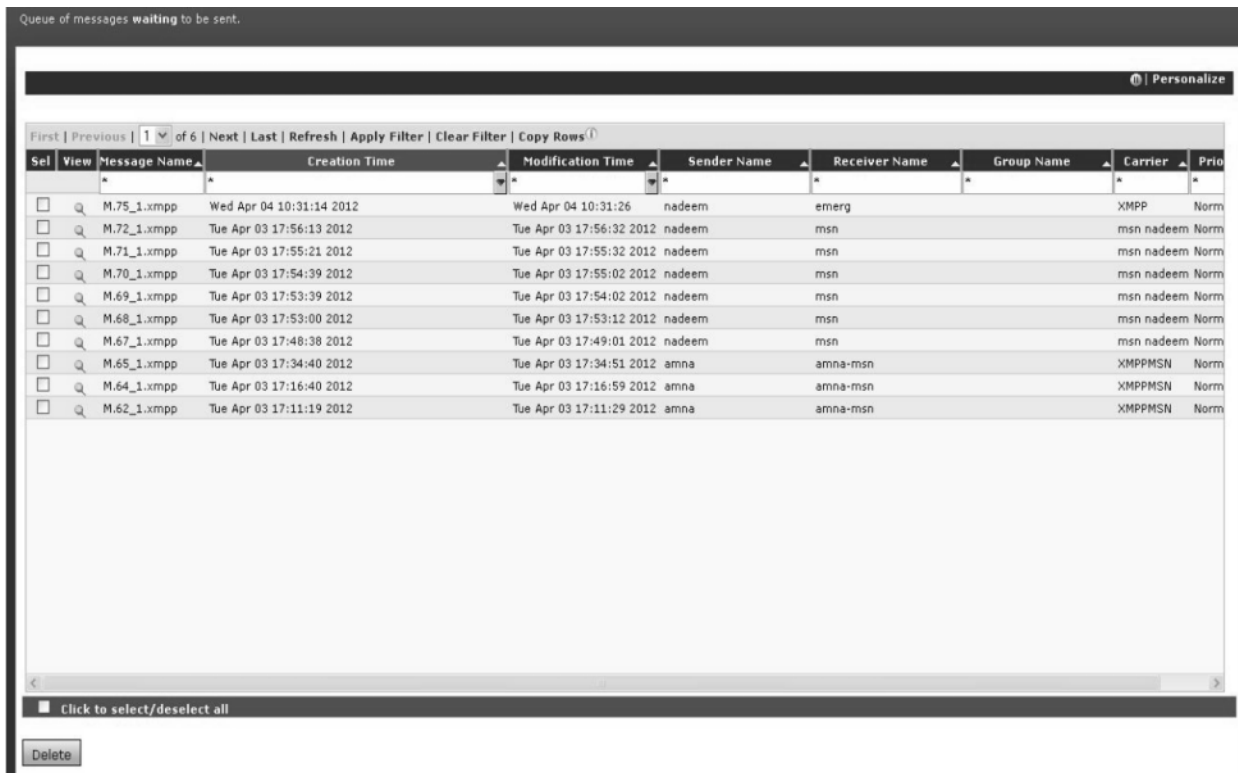
Queue Main Panel

The Queue Panel lists all the system queues present in the system. They include Default, Escalation, Scheduled, Failed, Filtered, Completed, Fax, and Voice as well as any custom paging queue created by a user. In front of every queue name, the numbers of files currently present in that queue are listed in brackets. The queue panel is auto-refreshed at every 30 seconds to update these message file numbers. Furthermore, the user is given the option to delete all message files present in a queue by clicking on the EMPTY link present for every queue.



Queue Main Panel

Inside a queue, the message files present currently in that queue are displayed in a grid. The grid consists of the following columns:



Queue Main Panel General Grid View

1. **Select:** Allows a user to select a single or multiple message files.
2. **View:** Allows a user to view the contents of a message file.
3. **Message Name:** Lists the message file name.
4. **Creation Time:** Lists the time at which the message file was created
5. **Modification Time:** Lists the time at which the message file was last accessed/modified by messenger service.
6. **Sender Name:** Lists the name of the user who has sent this message.
7. **Receiver Name:** Lists the name of the receiver to which the message was sent. (It would be empty for a quick message)

8. Group Name: Lists the name of the receiver group to which the message was sent. (It would be empty if the message was sent to individual receivers instead of a receiver group)
9. Carrier: Lists the carrier of the receiver to which the message was sent.
10. Priority: Lists whether the sent message was of NORMAL or HIGH priority.

To Sort Queue Grid

1. On the Queue grid, click on the button at the top of each column to sort the records in ascending order.
2. Click on the button again to sort in descending order.

To Filter Queue Grid

1. To perform SEARCH on the queue grid, enter the key words in the first box of Message Name, Creation Time, Modification Time, Sender Name, Receiver Name, Group Name, Carrier & Priority columns.
2. Click on the Apply Filter link.
3. The records which match the given filter would be displayed.
4. To perform a wildcard search, use an * as a prefix, suffix, or both.
5. Click on the Clear Filter link to clear the filter text from the grid and load all the results.
6. Click on the First, Previous, Next, and Last links to navigate through the grid records.
7. Click on the Page Number combo box to navigate directly to a particular page.
8. Click on Copy Rows to copy the selected grid record rows to clipboard.

To Personalize Queue Grid

This section allows user to personalize the Reports panel. User can choose to turn on/ off columns on the panel, save the size and order of the columns, and page refresh time interval. The settings can be saved permanently or only for the current session. The settings saved in this section are personal to a user and do not effect settings for any other user's Report panel.

The screenshot shows the 'Queues -> Completed' interface. At the top, it says 'Queue of messages waiting to be sent.' Below this is a 'Personalize' panel with the following settings:

- Refresh Interval (30 - 600) : 600 sec [Set]
- Creation Time Modification Time Sender Name Do not save current column widths
- Receiver Name Group Name Carrier Do not save the current order of columns
- Priority
- [Reset Layout] [Reset To Default]
- [Make Permanent]

Below the settings panel is a data grid with the following columns: Sel, View, Message Name, Creation Time, Modification Time, Sender Name, Receiver Name, Group Name, Carrier, and Priority. The grid contains three rows of data:

Sel	View	Message Name	Creation Time	Modification Time	Sender Name	Receiver Name	Group Name	Carrier	Priority
<input type="checkbox"/>	<input type="checkbox"/>	M.157_1.fb	Thu Apr 05 10:21:16 2012	Thu Apr 05 10:21:27 2012	nadeem	-facebook		Facebook	Norm
<input type="checkbox"/>	<input type="checkbox"/>	M.156_1.xmpp	Thu Apr 05 10:14:45 2012	Thu Apr 05 10:14:52 2012	amina	amna-msn		XMPPMSN	Norm
<input type="checkbox"/>	<input type="checkbox"/>	M.155_1.xmpp	Thu Apr 05 10:14:45 2012	Thu Apr 05 10:14:52 2012	amina	amna-msn		XMPPMSN	Norm

Personalizing a Grid

1. Click on the Personalize link on the top-right corner of the page to display the Personalize section.

2. Select / un-select check boxes to turn on/ off columns on the panel.
3. By default, page refresh time interval is 600 seconds. You can set a custom time interval (30600 seconds) by providing a value in the box.
4. Refresh Interval field and clicking on Set button.
5. You can choose to keep the current column width and column order by selecting the corresponding check boxes.
6. The panel contains three buttons:
 - a) Reset Layout: Resets Personalize section to last saved values.
 - b) Reset To Default: Restores the default settings of Personalize section.
 - c) Make Permanent: Saves Personalized settings permanently.

Default Queue

The Default Queue collects the messages waiting to be sent. To view messages from the Default Queue:

1. From the Queue menu, click Default on the left navigation bar.
2. Find the Message Name and/or Creation Time and click the View icon.
1. To delete messages from the Default Queue:
 1. Find the Message Name and/or Creation Time and click the Delete icon.
 2. Click the OK button to confirm deletion or click Cancel to revoke this action.
 3. Click Refresh to view your changes.

Escalation Queue

The Escalation Queue collects the escalation messages and sends them to the Main Queue: To view messages from the Escalation Queue:

1. From the Queue menu, click Escalation on the left navigation bar.
2. Find the Message Name and/or Creation Time and click the View icon.

To delete messages from the Escalation Queue:

3. Find the Message Name and/or Creation Time and click the Delete icon.
4. Click the OK button to confirm deletion or click Cancel to revoke this action.
5. Click Refresh to view your changes.

Scheduled Queue

The Schedule Queue collects scheduled messages and sends them to the Main Queue: To view messages from the Schedule Queue:

1. From the Queue menu, click Schedule on the left navigation bar.
2. Find the Message Name and/or Creation Time and click the View icon.

To delete messages from the Scheduled Queue:

1. Find the Message Name and/or Creation Time and click the Delete icon.
2. Click the OK button to confirm deletion or click Cancel to revoke this action.
3. Click Refresh to view your changes.

Failed Queue

The Failed queue collects messages that could not be sent. To view messages from the Failed queue:

1. From the Queue menu, click Failed on the left navigation bar.
2. Find the Message Name and/or Creation Time and click the View icon.

3. Check the Select box and click the Resend button if you want to resend a failed message.

To delete messages from the Failed queue:

1. Find the Message Name and/or Creation Time and click the Delete icon.
2. Click the OK button to confirm deletion or click Cancel to revoke this action.

Completed Queue

The Completed queue collects all successfully sent messages. To view messages from the Completed queue:

1. From the Queue menu, click Completed on the left navigation bar.
2. Find the Message Name and/or Creation Time and click the View icon.

To delete messages from the Completed queue:

3. From the Queue menu, click Completed on the left navigation bar.
4. Find the Message Name and/or Creation Time and click the View icon.
5. Click the OK button to confirm deletion or click Cancel to revoke this action.
6. Click Refresh to view your changes.

Fax Queue

The Fax Queue collects the messages waiting to be sent via the HipLink Fax Module.

Note: *The Fax Queue menu entry is displayed only if the Fax sending feature is enabled by the License Key.*

To view messages from the Fax Queue:

1. From the Queue menu, click Fax on the left navigation bar.
2. Find the Message Name and/or Creation Time and click the View icon.

To delete messages from the Fax Queue:

1. Find the Message Name and/or Creation Time and click the Delete icon.
2. Click the OK button to confirm deletion or click Cancel to revoke this action.
3. Click Refresh to view your changes.

Voice Queue

The Voice Queue collects the messages waiting to be sent via the HipLink Voice Module.

Note: The Voice Queue menu entry is displayed only if the Voice/VOIP sending feature is enabled by the License Key.

To view messages from the Voice Queue:

1. From the Queue menu, click Voice on the left navigation bar.
2. Find the Message Name and/or Creation Time and click the View icon.

To delete messages from the Voice Queue:

3. Find the Message Name and/or Creation Time and click the Delete icon.
4. Click the OK button to confirm deletion or click Cancel to revoke this action.
5. Click Refresh to view your changes.

Logs Setting Panel

Logs track the operations in HipLink system. A log will display date, time, user (who performed the activity), and relevant activity. The panel can be accessed through Logs tab that appears at the top after Send tab in HipLink Web Application.

The Logs panel is available to all members of sysAdmin user group. For custom users, this panel is available if view Logs permission is assigned in User Group Permissions.

This panel allows users to configure HipLink logs settings by enabling them to modify, delete or export loggers. This panel is available to all sysAdmin users. For non-sysAdmin users, the panel is visible if the user has permissions to modify any of the services. For sysAdmin users, the panel will contain all the HipLink services. For non-sysAdmin users, only those services would be visible for which users have been assigned permissions.

The panel contains following columns:

Edit: Clicking on this button opens up Logger Details pop-up. This is described in detail below.

Export: Clicking on this button exports the log file in zipped format.

Type: The type of service.

Module Name: Displays module name.

Level: Displays the level of logs.

By default, the logs are sorted on Type. You can sort logs on any column in ascending or descending order by clicking the button at the top of each column. The columns on the Logs Settings panel can be resized and relocated to suit a user's needs.

The panel uses color coding to distinguish the active services from inactive ones. The currently running services are highlighted in green; services that are stopped appear in black, while inactive services are grayed out.

The screenshot shows the HipLink interface with the 'Logs Settings Panel' open. The panel contains a table with the following columns: Sel, Edit, Exp, Type, Module Name, and Level. The table lists various services and their log levels. Below the table are buttons for 'Change Level', 'Delete', and 'Archive', along with a legend for service status: Running (green), Stopped (black), and InActive (gray).

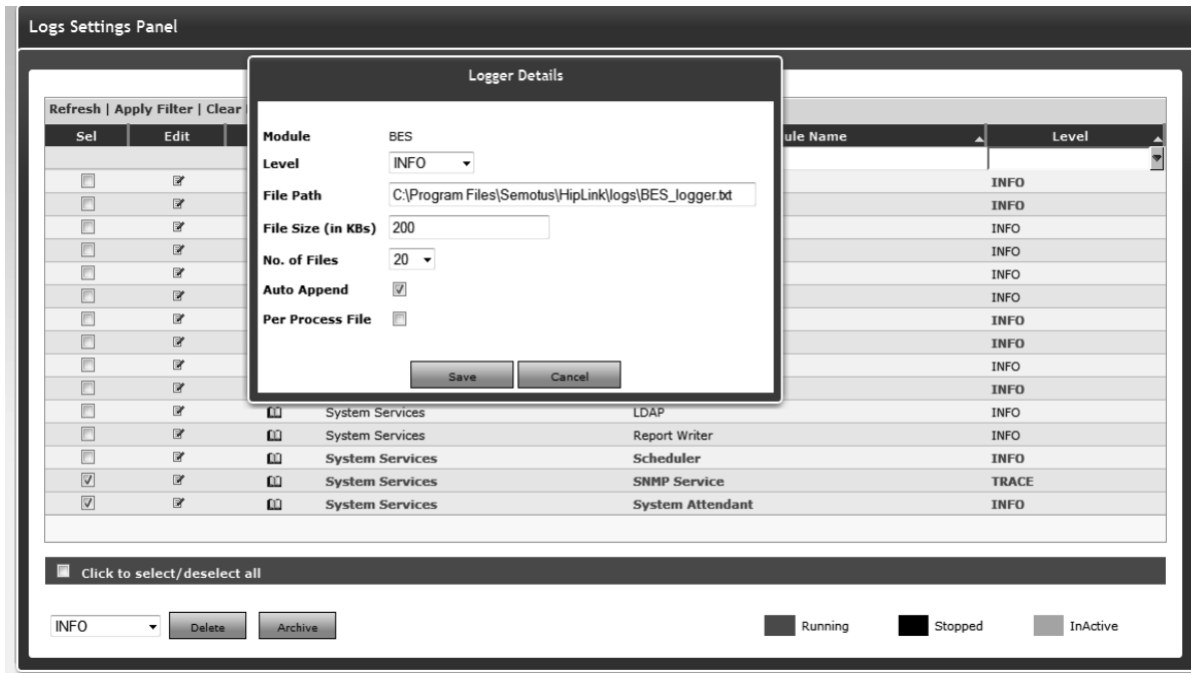
Sel	Edit	Exp	Type	Module Name	Level
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Gateway Services	Alarm Notification Gateway	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Gateway Services	Email Gateway	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Gateway Services	File System Interface	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Gateway Services	SNPP Gateway	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	General	Confirmations	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	General	Errors	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	General	Main	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	General	Messages	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	cap messenger	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	gsm messenger	INFO
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	GSM	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	HTTP	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	LWTS	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	mhttp messenger	INFO
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	MHTTP	TRACE
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Messengers	OAI 2	INFO

Filter Logs

- Enter key words in the first box of Module Name column, or select a value from Type or Level columns.
- Click on the Apply Filter link.
- HipLink will search for logs that match the filter criteria, refresh the page, and display the results.
- Click on the Clear Filter link to clear filter from the grid and load all the records.

Edit Logs

- Click on Edit icon against the logger you wish to edit.
- In Logger Details pop-up that opens, update values in the fields.
- Press Save to update the loggers, or Cancel to close the window without making any changes.



Log Settings Edit Page.

Export Logs

- Click on Exp icon against the logger you wish to export.
- Save the zipped file on your local machine.

Change Logging Level

- Select the logger(s) you wish to update.

- From Change Level dropdown, select the level you wish to set for the logger(s).
- Confirm your action in the message pop-up.

Delete Logs

- Select the logger(s) you wish to delete.
- Press Delete button.
- Confirm your action in the message pop-up.

Archive Logs

- Select the logger(s) you wish to archive.
- Press Archive button.
- Confirm your action in the message pop-up.

Note: All actions on Logs Settings panel require the services of the effected loggers to be restarted from Services panel.

Upgrade Panel

The Upgrade panel allows files to be uploaded to the upgrade process. This panel is available to sysAdmin users only.

Upgrades can be added to HipLink by uploading a local file. A URL or server path can also be used if the file is not local. The path must be accessible and mapped.

The panel displays the list of service packs/ patches that have been applied.

Name	Version	Type	Description	Copy Time	Install Time	
Win32 HipLink 4.5 Patch	10.0	Patch	This patch removes 2Way Choices from the message replaced against the respective Response Command variable.	Thu Apr 29 14:53:49 2010	Thu Apr 29 14:54:06 2010	Rollback
Win32 HipLink 4.5 Patch	2.2	Patch	This patch reduces the Wait period for VOIP Messages	Wed Apr 28 18:10:21 2010	Wed Apr 28 18:15:09 2010	
HipLink 4.5 CR1 Service Pack 7 for IIS	7.1	Service Pack	Service Pack 7 of HipLink 4.5 Candidate Release 1 for IIS	Wed Apr 28 13:39:41 2010	Wed Apr 28 13:43:04 2010	
HipLink 4.5 CR1 Service Pack 6 for IIS	6.2	Service Pack	Service Pack 6 of HipLink 4.5 Candidate Release 1 for IIS	Wed Apr 28 12:41:28 2010	Wed Apr 28 12:44:08 2010	

Upgrades Panel

Time Zone

HipLink allows Users and Receivers to work in different time zones than the HipLink server. Each User and Receiver has a time zone setting which determines the time difference (in hours) between its time zone and that of the HipLink server.

HipLink comes with a predefined time zone, called Server Time that uses as reference the time zone of the server where HipLink is installed. The default offset is of 0 hours which means that the Server Time has the same time zone as the server time.

The default time zone Server Time can be modified but cannot be deleted. New time zones can be added if needed.

Note: All the Receiver schedules created by a User are displayed using the time zone of that User. All HipLink database records are stored, and all messages are generated and processed using the HipLink server time zone. The Receiver time zone is used only when the option to include the timestamp in the body of the message is enabled.

To add a new Time Zone:

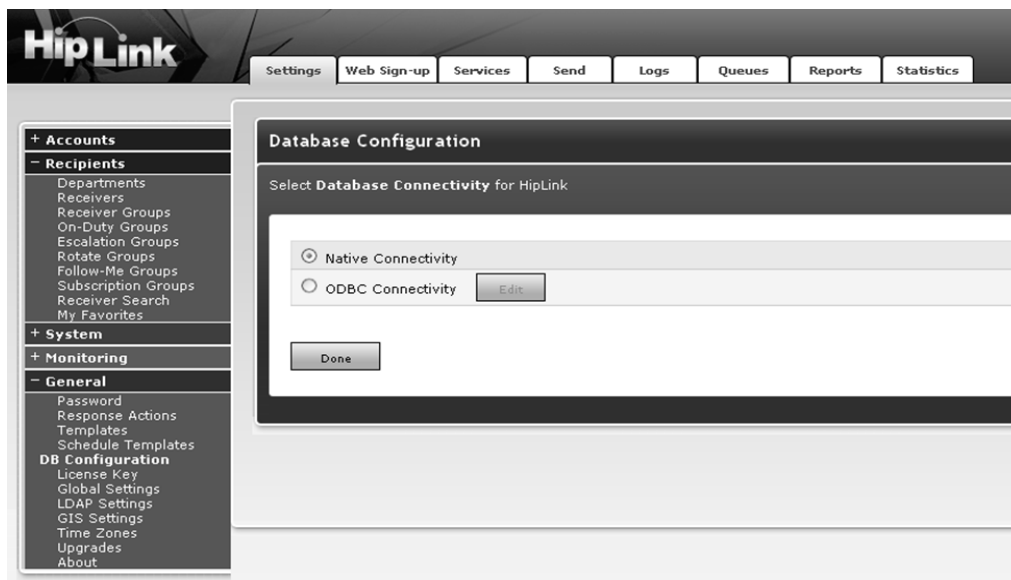
1. From the Settings menu, click Time Zones on the left navigation bar.
2. On the Time Zone Panel, click the Add Time Zone button to reach the Add Time Zone page.
3. Enter a unique Name for this Time Zone (required).
4. Enter a Description of this Time Zone (optional).
5. Enter the Offset in hours. This is the difference in hours between the new Time Zone and the HipLink server time zone set by the Server Time.
6. Click the Save button.

Name	Value	Comment
Name	Local Zone	mandatory
Description	The local time zone	optional
Offset	-12 Hours	optional

ODBC Conversion and Configuration

DB Configuration

HipLink supports changing from our native SQLite data source to an ODBC data source within the GUI if the license key supports ODBC. This will allow the end User/admin to move the data over or back when running the ODBC Conversion program. When the ODBC option is selected below the following screen is activated.



Database Configuration Settings



ODBC Connectivity Settings

- DSN: Allows the configuration to support DSN or DSNLESS
Note: Recommend DSN (see ODBC conversion documentation for full details on recommendation).
- Database Type: Select either SQL Server (2000, 2005 supported) or Oracle (9i and higher).
- DSN Name: System DSN name created with the Windows/UNIX DSN module/service GUI. This is a required field for a proper connection.
- Connection String: Required only when using DSNLESS connection, provide desired connection string to your database (see local/internal Database Admin for further details as this is not a HipLink value).
- Database User/Password: The required credentials for accessing the Database, it is recommended the User have full access to the HipLink database to make sure there are no access issues.

Note: A strong password is recommended here to prevent unwanted access to the database backend outside of HipLink.

Enhanced LDAP configuration

LDAP Settings

HipLink supports connectivity with an AD/LDAP server for Authentication of User and recipient Users within the product if licensed. The details below provide insight into the functions of each field which combined allows a User to be authenticated via AD/LDAP.

Enable LDAP support	<input checked="" type="checkbox"/>
XS Compatibility	<input checked="" type="checkbox"/>
LDAP Server *	192.168.2.50
LDAP Server Port *	389 ⓘ
LDAP Backup Server	
LDAP Backup Server Port	389
LDAP Base DN *	DC=semdatacenter,DC=
Active Directory	<input checked="" type="checkbox"/>
LDAP User RDN Template(s) *	CN=?,CN=Users(object)
LDAP User Name Attribute is User ID	<input checked="" type="checkbox"/>
LDAP User Name Attribute *	sAMAccountName
Domain Name *	semdatacenter
Security Layer	Plain - No security services ▾
Create User Account Automatically	<input type="checkbox"/> ⓘ Warning
Restrict Non-LDAP Users	<input type="checkbox"/> ⓘ
User Group Associated to Automatically Created User	Demo - Portland Mgr ▾
Enable Single Sign-On	<input type="checkbox"/> ⓘ

LDAP Settings

Compatibility: Basic level allowing authentication only. May or may not be present depending on licensing.

LDAP Server/Port: IP or Hostname and port of the LDAP/AD Server. 389 is normally the default and 636 is the SSL enabled port.

Backup LDAP Server/Port: IP or Hostname and port of the Backup LDAP/AD Server. 389 is normally the default and 636 is the SSL enabled port. This is only used if the previous LDAP/AD server is not reachable.

LDAP Base DN: The top level of the LDAP directory tree is the base, referred to as the base DN. A base DN usually takes one of the three forms listed here. Let's assume one works at a US electronic commerce company called FooBar, Inc., which is on the Internet at foobar.com. **o="FooBar, Inc.", c=US** (base DN in X.500 format) In this example, o=FooBar, Inc. refers to the organization, which in this context should be treated as synonymous with the company name. c=US indicates that the company headquarters is in the US. Once upon a time, this was the preferred method of specifying your base DN. Times and fashions change, though; these days, most companies are (or plan to be) on the Internet. And what with Internet globalization, using a country code in the base DN probably made things more confusing in the end. In time, the X.500 format evolved into the other formats listed below.

o=foobar.com (base DN derived from the company's Internet presence) This format is fairly straightforward, using the company's Internet domain name as the base. Once you get past the o= portion (which stands for organization=), everyone at your company should know where the rest came from. This was, until recently, probably the most common of the currently used formats.

dc=foobar, dc=com (base DN derived from the company's DNS domain components) As with the previous format, this uses the DNS domain name as its basis. But where the other format leaves the domain name intact (and thus human-readable), this format is split into domain components: foobar.com becomes dc=foobar, dc=com. In theory, this could be slightly more

versatile, though it's a little harder for end Users to remember. By way of illustration, consider foobar.com. When foobar.com merges with gizmo.com, you simply start thinking of dc=com as the base DN. Place the new records into your existing directory under dc=gizmo, dc=com, and you're ready to go. (Of course, this approach does not help if foobar.com merges with wocket.edu.) This is the format I'd recommend for any new installation

Active Directory: If select the system defaults to the standard MS Active Directory settings.

LDAP User RDN Template(s): Relative Distinguished Name (RDN) is the location within the LDAP directory where the record resides. Most items that you'll store in an LDAP directory will have a name, and the name is frequently stored in the cn (Common Name) attribute, here is a sample: CN=?,CN=Users(objectClass=user)

LDAP User Name Attribute is User ID: A shortcut selection for the User Name location

LDAP User Name Attribute: Allows entry of a different attribute to authenticate the User Name against.

Domain Name: Name of the corporate domain; .com/.org/.net/.ca etc. are not required within this field. This field is available if Active Directory check is on.

Security Layer: Specifies the Security options used within the current organizations LDAP, the 3 below are available at this time:

1. Plain – No security services
2. Secure Socket Layer (SSL)
3. Windows Integrated Security (for AD only)

Create User Accounts Automatically: Instead of having an administrator create the Users, this option (with User Group Associated to Automatically Created User enabled) will allow the system to create an account when a User successfully provides their credentials to the HipLink system.

Restrict Non-LDAP Users: When enabled, allows the system to only allow in LDAP type of accounts. This is an option we would recommend only using in High security environments as it will block the default admin account types.

User Group Associated to Automatically Created User: This dropdown contains all the User Groups in HipLink. It is accessible if **Create User Account Automatically** check is on. User can select the HipLink User Group that would be assigned to LDAP Users logging in automatically.

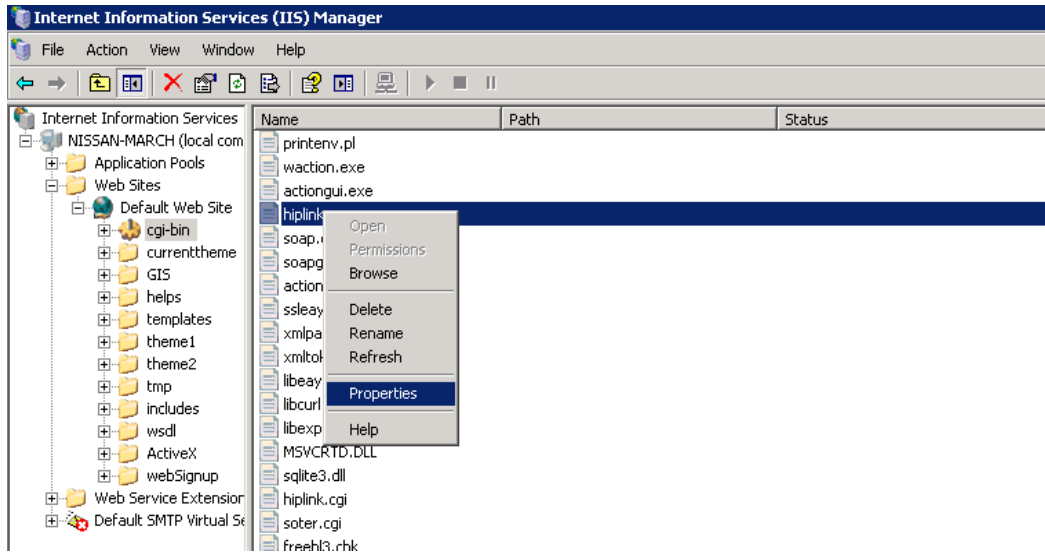
Enable Single Sign-On: Allows IIS enabled systems to support pass through authentication from the Windows Domain login attempt. Requires additional setup information, Contact HipLink support for the needed documentation.

Single Sign-on Configuration Guide

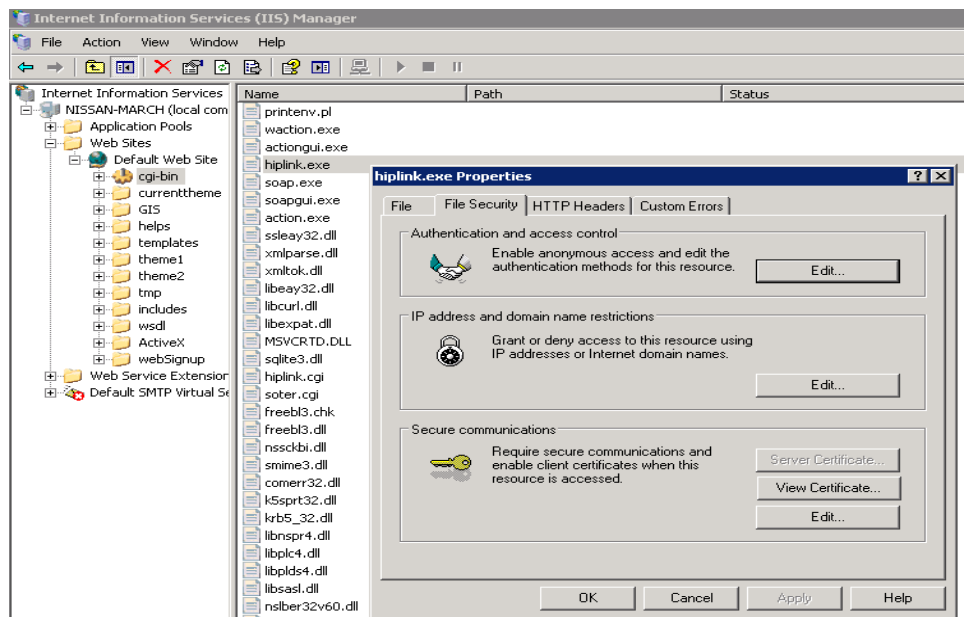
Single Sign on can be configured on the system using the following steps:

Step 1: Go to the Startup Control Panel Administrative tools and open the Internet Information Service.

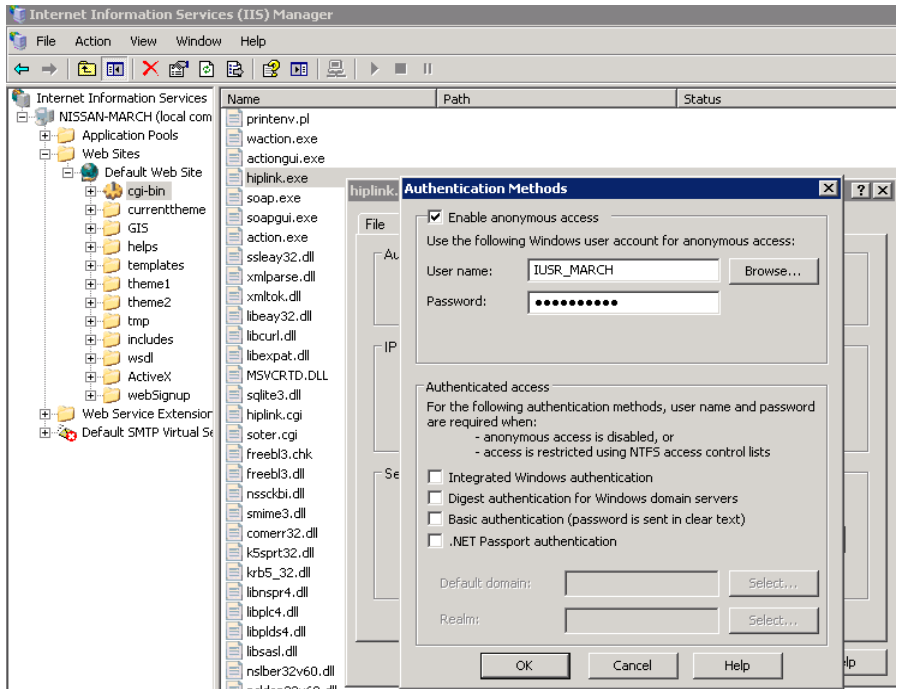
Step 2: In the internet information service, go to the website where Hiplink is installed, select cgi-bin and view the properties of Hiplink.cgi and Hiplink.exe as shown below:



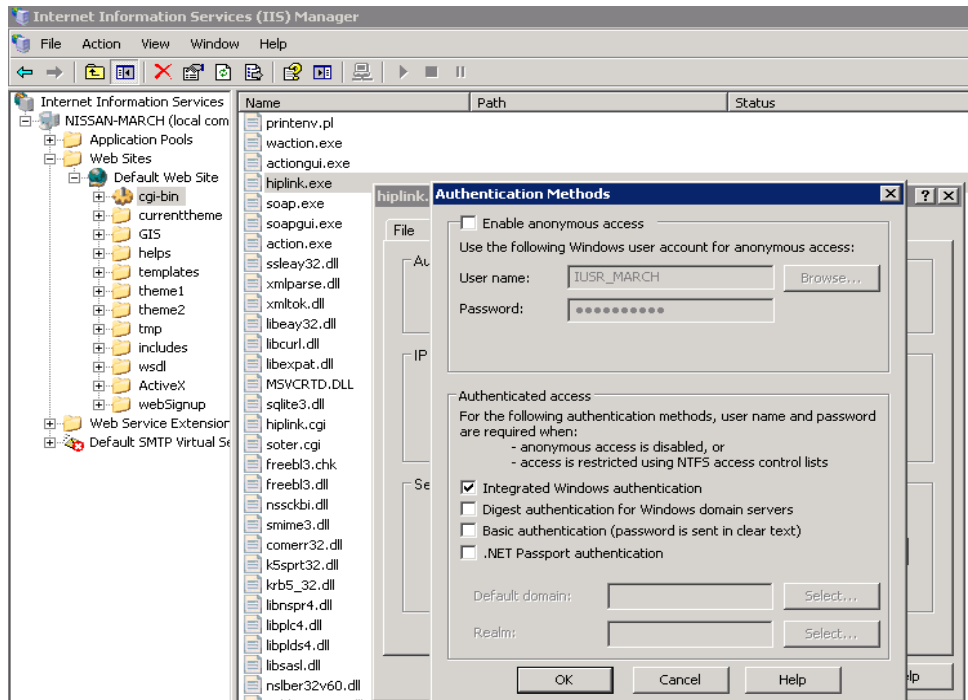
The following window will open out. Now in the properties move to the File Security tab and press the Edit button.



Step 3: After clicking the Edit button under the Anonymous Access and Authentication control, the following default settings for authentication control will get loaded:



Now change the settings to the settings mentioned as under with only the integrated window authentication checked:



Click OK, Apply and Save the settings.

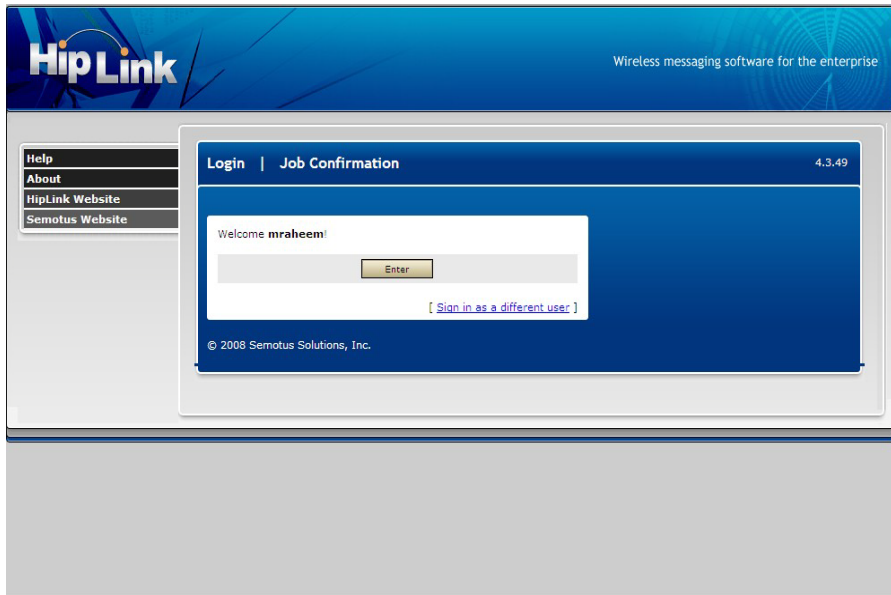
Note: Above settings have to be applied for both *Hiplink.cgi* and *Hiplink.exe*

Step 4: Login to Hiplink under the general tab, configure LDAP according to your own configurations with Enable Single Sign on checked.

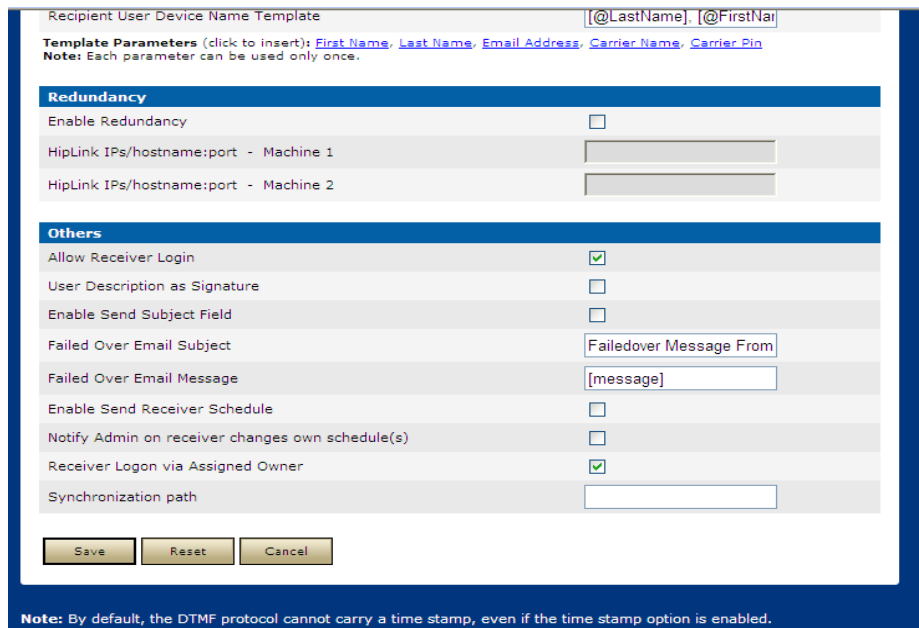
LDAP Integration Settings Panel	
Specify LDAP Integration Settings.	
LDAP Integration Wizard	
Enable LDAP support	<input checked="" type="checkbox"/>
XS Compatibility	<input checked="" type="checkbox"/>
LDAP Server *	192.168.4.6
LDAP Server Port *	389 ⓘ
LDAP Backup Server	
LDAP Backup Server Port	389
LDAP Base DN *	DC=cmarks,dc=com
Active Directory	<input checked="" type="checkbox"/>
LDAP User RDN Template(s) *	CN=?,CN=Users(objectCl
LDAP User Name Attribute is User ID	<input checked="" type="checkbox"/>
LDAP User Name Attribute *	sAMAccountName
Domain Name *	cmarks
Security Layer	None ▾
Create User Account Automatically	<input checked="" type="checkbox"/> ⓘ
Restrict Non-LDAP Users	<input type="checkbox"/> ⓘ
User Group Associated to Automatically Created User	sysAdmin ▾
Enable Single Sign-On	<input checked="" type="checkbox"/> ⓘ
<input type="button" value="Done"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>	

Step 5: Single sign-on for Hiplink User:
 Now login to HipLink again with the credentials of the User registered on the provided domain.
 User will be logged in normally as shown:

Now logout and view the login screen. The following screen will be visible showing that Single Sign-On has been configured properly.



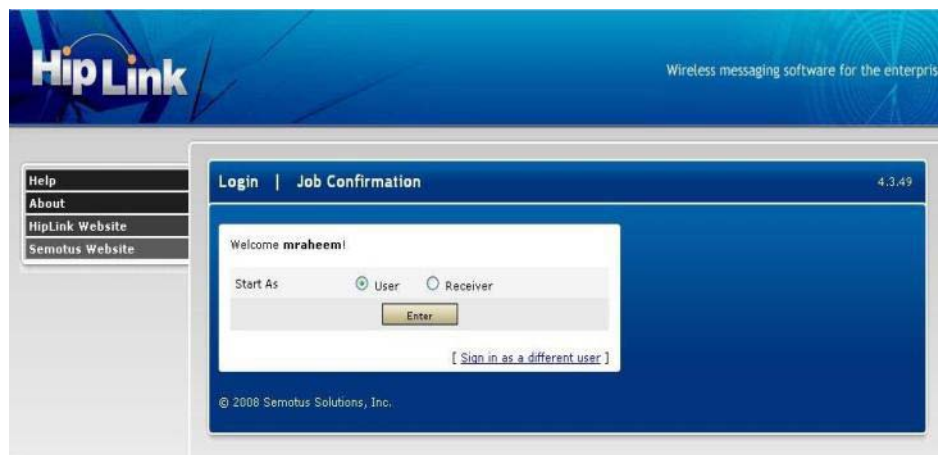
Step 6: Following is the procedure for enabling the Single Sign-on for the Receivers. Login to Hiplink and move to the General Section > Global Settings > Edit global settings and check Allow Receiver Login and Receiver Login via assigned owner under the Others tab as shown below:



Now go to Recipients section > Receivers > Edit a Receiver and configure an assigned owner for that Receiver that is registered on the domain as shown below:

Receiver Parameters	
Name	R1 <input type="button" value="Edit Schedule"/> <input type="button" value="View Schedule"/>
Description	R1
Primary PIN	hiplink@gmail.com *
Primary Carrier/Delivery	SMTP Carrier 1 *
Receiver Type	Alpha
Keep alpha chars	<input type="checkbox"/>
Receiver Email	<input type="text"/> <input type="checkbox"/> Email Failover <input type="checkbox"/> Email CC
<input type="checkbox"/> Define Alternate PIN/Carrier	
Alternate PIN	<input type="text"/>
Alternate Carrier/Delivery	<input type="text"/>
Time Zone	Server Time
<input type="checkbox"/> Voice Enable	
Voice Phone Number	<input type="text"/>
Assigned Owner	
User	<input type="text"/>
Departments	admin mraheem musharib noman obaid saira
Member Of	
Guest Settings	

Save the setting for the Receiver, logout from HipLink, and then the Single Sign-on welcome page will be displayed with radio button to select between User and Receiver for login as shown below:



Step 7: Single Sign on for Recipient User:

To use the Single Sign on feature for Recipient Users, after configuration of LDAP, go to Add, Modify or Delete Recipient User, select the authentication type as LDAP for the Recipient User and enter the User Name for the LDAP as shown below:

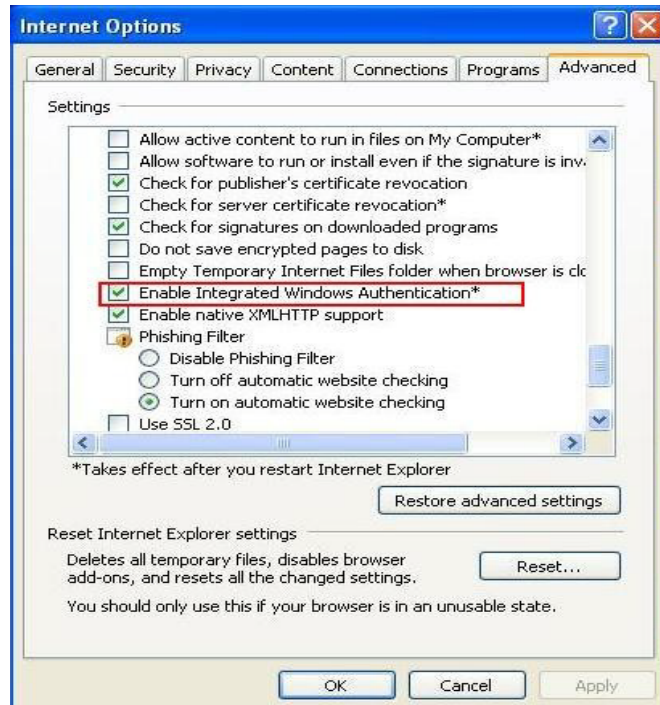
Recipient User

Add, modify or delete Recipient User.

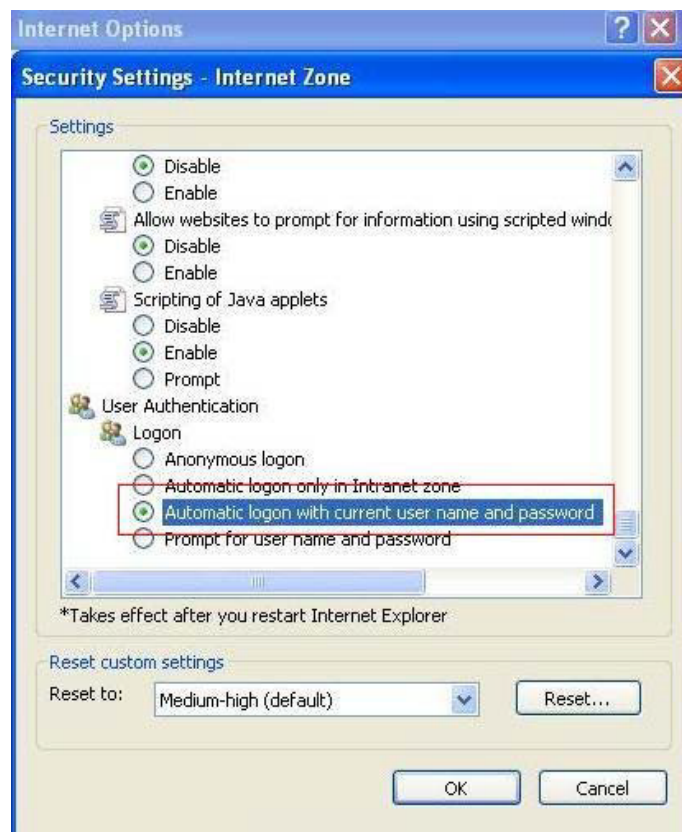
User Parameters	
Email	mraheem@123.com *
First Name	Musharib *
Last Name	Raheem *
Department	Default *
Description	
Authentication Type	LDAP *
LDAP Username	mraheem] * Test ▾
Permissions	
Disable login	<input type="checkbox"/>
Number of Devices Allocated	2 ▾
Allow access to Subscription Groups	<input checked="" type="checkbox"/>
Allow Device Add	<input checked="" type="checkbox"/>
Allow Device Edit	<input checked="" type="checkbox"/>
Allow Device Delete	<input checked="" type="checkbox"/>

Now, save the settings and logout. The Single Sign-on welcome screen will display a multiple option of logging in either as a User, Receiver or a Recipient User as shown below:

Along with the above mentioned settings, the client browser needs to be configured with the following options (The settings given below are particular to Internet Explorer.):

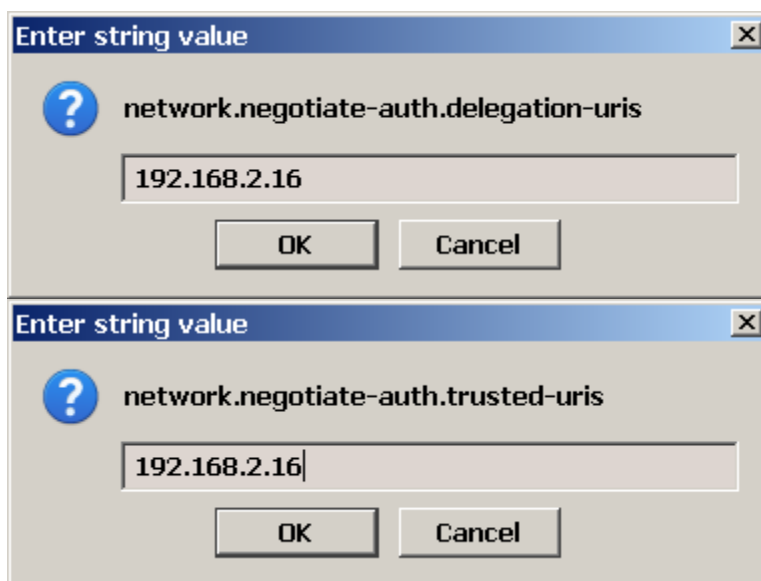


The settings given below are particular to Mozilla Firefox:



Here the User will be required to input his/her I.P. address to enable single sign on using his credentials required for LDAP login.

Go to about:config in Mozilla for the following two value changes:



Filters

The Message and API Filters are licensed components. Please note: these services are not available without the license key with the added feature that supports this service. If you do not have the license key that supports these services, please contact HipLink Software and request an update of the license key for the services.

HipLink features a way to filter messages throughout the application. Based on the conditions defined in a filter, a particular action is taken i.e. to pass or suppress or to throttle messages.

A sequencing of filters is maintained so that the filter at the top gets executed first and then the next one and so on. The order can be changed by the user by using a mouse.

The key idea behind this service is that specific messages can be directed to receivers and other receivers can be blocked from getting these system messages; thus providing more control over the messages' communication throughout the system.

To help troubleshoot any issues, the service provides logging of different errors, warnings and important Informational messages, which are logged in the Windows Event Log.

Full configuration and Setup instructions are in the HipLink User Guide

Feedback Action Panel

HipLink allows users to add response actions with Feedback events that will be executed upon the status of a message. The following are the types of status that a message can have which allow feedback events to be executed:

- Message backed-up
- Message completed
- Message confirmed
- Message delivered
- Message filtered
- Message finalized
- Message rejected

Note: Only the admin User Group has permission to set up Feedback Actions, and it is the responsibility of the HipLink administrators to write and maintain the scripts, batch files, or applications invoked as Feedback Actions.

Example: To add a feedback event Final event select this event and press Add. This event will be added as a Feedback Action, now specifies the Response Action(s) to be executed when a message state matches the state of Event.

See the *HipLink Integration Guide* for full instructions to define Feedback Events.

Dial-Up Modem Settings

The TAP Dial-Up, TAP Leased, and DTMF protocols require that dial-up modems are properly installed on the HipLink server.

Most of the modems (such as Practical Peripherals, US Robotics, D-Link, NetComm) work just fine with ATZ or AT&F initialization strings. Practical Peripherals modems seem to work perfectly with HipLink on all platforms. They seem to work well with basically any init string. In case of problems, the following initialization string is known to work on various platforms (especially HP, which can have some problems with US Robotics modems):

```
ATE1V1X1Q0&C1&D2&M0&K0B1&N3
```

Some Carriers (e.g., Verizon) may require the &M0 setting on (i.e., no error control, ARQ). For example: ATZ&M0.

Note 1: Generally external modems are recommended. Internal modems (including Win modems) don't work well with TAP Carriers.

Note 2: Initialization strings are platform, modem, and Carrier dependant. It is recommended to use serial communication tools (such as Hyperterminal for Windows or Minicom for UNIX

platforms) in order to determine the appropriate initialization string. Please see the `minicom.txt` from `/usr/local/hiplink/bin` for details.

Below is a list of useful modem settings that may be required:

Setting	Description
V1	Display result codes in words (verbal mode)
Q0	Result codes displayed
X1	Result code set options (X1-...X7)
E1	Command mode echo enabled
&C1	Normal Carrier Detect operations
&D2	Normal DTR operations
&Hn	Transmit Data Flow Control (&H1...&H3 depends on your hardware)
&H1	Hardware Flow Control
&H2	Software Flow Control
&H3	Use both (if not sure what your hardware supports)
&K0	Data compression disabled
&Mn	Error control (ARQ)
&M0	No error control (some Carriers requires it, e.g., Verizon)
&M4	Normal error control mode
S7=70	Set the number of seconds (e.g., 70s) the modem waits for a Carrier

Export/Import Utility

You can export important data to a file format that can be easily modified or analyzed, and if needed, imported back into HipLink. This utility is useful when the administrator wants to modify a large number of Receiver or Group records externally, rather than through the HipLink User Interface.

Exporting Records

The Export feature of this utility exports the following data records into individual text files:

- Carriers
- Users
- User Groups
- Departments
- Receivers
- Receiver Groups
- On-Duty Groups
- Escalation Groups
- Follow-Me Groups
- Rotate Groups

To export records:

Important: *Never try to import data from a file that has not been created by HipLink. HipLink will only import tab delimited text files and will confirm the integrity of the data before it is imported. If a record has been corrupted, it will be skipped by the Utility.*

1. Start the Export/Import Utility by clicking on the Import-Export Utility icon in the HipLink folder under the Windows Start menu (or by running `ieutility.exe` for both Windows and UNIX platforms).

HipLink Export-Import Data Utility

Copyright 2001 Semotus Systems Corp.

- a. Import HipLink data
- b. Export HipLink data
- c. Exit

Choice:

2. Enter choice 2 to export HipLink data and the IE Utility will prompt you:
Please enter delimiter character:
3. Enter | (pipe) or tab only as the delimiter character and press the Enter key (tab is the default delimiter):
Please enter HipLink configuration directory:
4. Enter the path of the configuration directory. The default location for this directory in Windows is
C:\Program Files\HipLink_FAX\config. For UNIX platforms, the default path is /usr/local/hiplink/config. The IE Utility will prompt you:
Please enter export directory:
5. Enter the Export directory. This is the location where HipLink will save the exported text files
6. The utility will export all Carriers, Users, User Groups, Departments, Receivers, Receiver Groups, On-Duty Groups, Escalation Groups, Rotate Groups, Follow-Me Groups, and Time Zone records into tab (or other character) delimited text files with the following names in your Export directory:
carrier.txt
user.txt
usergroup.txt
department.txt
receiver.txt
group.txt
onduty.txt
escalation.txt
rotate.txt
follow.txt
timezone.txt
You can now open any of these files in most spreadsheet applications for editing.

Importing Records

You should only import files that have been exported through the HipLink Export/Import Utility. The Export/Import Utility will only import tab delimited files that contain the proper formatting, field names and data structure that exist in HipLink.

To export records:

1. Start the Export/Import Utility by clicking on the Import-Export Utility icon in the HipLink folder under the Windows Start menu (or by running ieutility.exe for both Windows and UNIX platforms).
HipLink Export-Import Data Utility
Copyright 2001 Semotus Systems Corp.
 - a. Import HipLink data
 - b. Export HipLink data
 - c. Exit

Choice:

2. Enter choice 1 to import HipLink data and the IE Utility will prompt you: Please enter delimiter character:

3. Enter the delimiter character used when the data was exported and press the Enter key (tab is the default delimiter): Please enter HipLink configuration directory:
4. Enter the path of the configuration directory. The default location for this directory in Windows is C:\Program Files\HipLink\config. For UNIX platforms, the default path is /usr/local/hiplink/config. The IE Utility will prompt you: Please enter import directory:
5. Enter the Import directory. This the location from where HipLink will import the text files.
6. Before starting to import the files, the IE Utility will prompt you: WARNING: The entries in database will be replaced with new entries if they have the same name Continue processing? [Y/N]
7. Enter Y to continue. If the data records being imported have the same Name as the existing records, they will be overwritten. Type Y to accept this, or N to stop the import process.
8. Before your records are imported, HipLink will perform a backup of your existing files. These files will be located in directories labeled \config\backup. At the end of the import process, the IE Utility will prompt you: Would you like to remove backup files? [Y/N]
9. Type Y to delete your backup files, or N to keep them. It may be a good idea to keep your files until after you've checked your data within the HipLink application.

File Formats

The IE Utility application exports data in tab delimited text files. The table headers of these files have the labels as shown below.

Carriers File (carrier.txt)

```

NAME
COMPANY NAME DESCRIPTION PROTOCOL EMAIL
SPLIT TRUNCATE
MAX SPLIT LENGTH
MAX TRUNCATE LENGTH RETRY LIMIT
EXPIRATION LIMIT BACKUP CARRIER NAME
DISABLED
SNPP URL SNPP PORT
SNPP QUERY INTERVAL SNPP QUERY RETRY
SNPP LEVEL
SNPP CALLER ID
SMTP SERVER ADDRESS SMTP PREFIX PIN
SMTP POSTFIX PIN TAP PHONE
TAP PASSWORD
TAP BAUD RATE TAP PARITY
TAP DATA BITS TAP STOP BITS
GATEWAY SERVER ADDRESS GATEWAY ACCOUNT
GATEWAY PASSWORD
GATEWAY TERMINAL ID GATEWAY TIMEOUT GATEWAY PRIORITY DTMF PHONE
FIRST TIME WAIT ECOND TIME WAIT
WCTP SERVER ADDRESS WCTP PORT
WCTP VARIABLE
WCTP QUERY RETRY WCTP QUERY INTERVAL HTTP URL
HTTP METHOD HTTP PIN STYLE TTP SENDER FIELD
HTTP SUBJECT FIELD HTTP MESSAGE FIELD HTTP PHONE FIELD 1
HTTP PHONE FIELD 2
HTTP PHONE FIELD 3
HTTP CUSTOM FIELD 1

```

HTTP CUSTOM FIELD 2
HTTP CUSTOM FIELD 3
HTTP CUSTOM FIELD 4
HTTP CUSTOM FIELD 5
HTTP CUSTOM FIELD 6
HTTP CUSTOM FIELD 7
HTTP CUSTOM FIELD 8
HTTP CUSTOM FIELD 9
HTTP CUSTOM FIELD 10
HTTP CUSTOM DESCRIPTION 1
HTTP CUSTOM DESCRIPTION 2
HTTP CUSTOM DESCRIPTION 3
HTTP CUSTOM DESCRIPTION 4
HTTP CUSTOM DESCRIPTION 5
HTTP CUSTOM DESCRIPTION 6
HTTP CUSTOM DESCRIPTION 7
HTTP CUSTOM DESCRIPTION 8
HTTP CUSTOM DESCRIPTION 9
HTTP CUSTOM DESCRIPTION 10
HTTP SUCCESS STRING HTTP ERROR STRING 1
HTTP ERROR STRING 2
HTTP ERROR STRING 3
HTTP ERROR STRING 4
HTTP ERROR STRING 5
BES SERVER
BES APPLICATION PORT BES URI
SMPP SMSC ID SMPP TYPE
SMPP HOST
SMPP PORT TUCP HOST TUCP LEVEL TUCP AUTH
PUCP DEVICE PUCP LEVEL PUCP PHONE PUCP AUTH
PUCP BAUD RATE PUCP PARITY PUCP DATA BITS PUCP STOP BITS
GENERIC EXE PATH WAP HOST
QUEUE ID MHTTP STEP 0
MHTTP URL 0
MHTTP METHOD 0
MHTTP REFERER 0
MHTTP SUCCESS 0
MHTTP CUSTOM FIELD 0 0
MHTTP CUSTOM FIELD 1 0
MHTTP CUSTOM FIELD 2 0
MHTTP CUSTOM FIELD 3 0
MHTTP CUSTOM FIELD 4 0
MHTTP CUSTOM FIELD 5 0
MHTTP CUSTOM FIELD 6 0
MHTTP CUSTOM FIELD 7 0
MHTTP CUSTOM FIELD 8 0
MHTTP CUSTOM FIELD 9 0
MHTTP CUSTOM DESCRIPTION 0 0
MHTTP CUSTOM DESCRIPTION 1 0
MHTTP CUSTOM DESCRIPTION 2 0
MHTTP CUSTOM DESCRIPTION 3 0

MHTTP CUSTOM DESCRIPTION 4 0
MHTTP CUSTOM DESCRIPTION 5 0
MHTTP CUSTOM DESCRIPTION 6 0
MHTTP CUSTOM DESCRIPTION 7 0
MHTTP CUSTOM DESCRIPTION 8 0
MHTTP CUSTOM DESCRIPTION 9 0
MHTTP ERROR STRING 0 0
MHTTP ERROR STRING 1 0
MHTTP ERROR STRING 2 0
MHTTP ERROR STRING 3 0
MHTTP ERROR STRING 4 0
MHTTP STEP 1
MHTTP URL 1
MHTTP METHOD 1
MHTTP REFERER 1
MHTTP SUCCESS 1
MHTTP CUSTOM FIELD 0 1
MHTTP CUSTOM FIELD 1 1
MHTTP CUSTOM FIELD 2 1
MHTTP CUSTOM FIELD 3 1
MHTTP CUSTOM FIELD 4 1
MHTTP CUSTOM FIELD 5 1
MHTTP CUSTOM FIELD 6 1
MHTTP CUSTOM FIELD 7 1
MHTTP CUSTOM FIELD 8 1
MHTTP CUSTOM FIELD 9 1
MHTTP CUSTOM DESCRIPTION 0 1
MHTTP CUSTOM DESCRIPTION 1 1
MHTTP CUSTOM DESCRIPTION 2 1
MHTTP CUSTOM DESCRIPTION 3 1
MHTTP CUSTOM DESCRIPTION 4 1
MHTTP CUSTOM DESCRIPTION 5 1
MHTTP CUSTOM DESCRIPTION 6 1
MHTTP CUSTOM DESCRIPTION 7 1
MHTTP CUSTOM DESCRIPTION 8 1
MHTTP CUSTOM DESCRIPTION 9 1
MHTTP ERROR STRING 0 1
MHTTP ERROR STRING 1 1
MHTTP ERROR STRING 2 1
MHTTP ERROR STRING 3 1
MHTTP ERROR STRING 4 1
MHTTP STEP 2
MHTTP URL 2
MHTTP METHOD 2
MHTTP REFERER 2
MHTTP SUCCESS 2
MHTTP CUSTOM FIELD 0 2
MHTTP CUSTOM FIELD 1 2
MHTTP CUSTOM FIELD 2 2
MHTTP CUSTOM FIELD 3 2
MHTTP CUSTOM FIELD 4 2

MHTTP CUSTOM FIELD 5 2
MHTTP CUSTOM FIELD 6 2
MHTTP CUSTOM FIELD 7 2
MHTTP CUSTOM FIELD 8 2
MHTTP CUSTOM FIELD 9 2
MHTTP CUSTOM DESCRIPTION 0 2
MHTTP CUSTOM DESCRIPTION 1 2
MHTTP CUSTOM DESCRIPTION 2 2
MHTTP CUSTOM DESCRIPTION 3 2
MHTTP CUSTOM DESCRIPTION 4 2
MHTTP CUSTOM DESCRIPTION 5 2
MHTTP CUSTOM DESCRIPTION 6 2
MHTTP CUSTOM DESCRIPTION 7 2
MHTTP CUSTOM DESCRIPTION 8 2
MHTTP CUSTOM DESCRIPTION 9 2
MHTTP ERROR STRING 0 2
MHTTP ERROR STRING 1 2
MHTTP ERROR STRING 2 2
MHTTP ERROR STRING 3 2
MHTTP ERROR STRING 4 2
MHTTP STEP 3
MHTTP URL 3
MHTTP METHOD 3
MHTTP REFERER 3
MHTTP SUCCESS 3
MHTTP CUSTOM FIELD 0 3
MHTTP CUSTOM FIELD 1 3
MHTTP CUSTOM FIELD 2 3
MHTTP CUSTOM FIELD 3 3
MHTTP CUSTOM FIELD 4 3
MHTTP CUSTOM FIELD 5 3
MHTTP CUSTOM FIELD 6 3
MHTTP CUSTOM FIELD 7 3
MHTTP CUSTOM FIELD 8 3
MHTTP CUSTOM FIELD 9 3
MHTTP CUSTOM DESCRIPTION 0 3
MHTTP CUSTOM DESCRIPTION 1 3
MHTTP CUSTOM DESCRIPTION 2 3
MHTTP CUSTOM DESCRIPTION 3 3
MHTTP CUSTOM DESCRIPTION 4 3
MHTTP CUSTOM DESCRIPTION 5 3
MHTTP CUSTOM DESCRIPTION 6 3
MHTTP CUSTOM DESCRIPTION 7 3
MHTTP CUSTOM DESCRIPTION 8 3
MHTTP CUSTOM DESCRIPTION 9 3
MHTTP ERROR STRING 0 3
MHTTP ERROR STRING 1 3
MHTTP ERROR STRING 2 3
MHTTP ERROR STRING 3 3
MHTTP ERROR STRING 4 3

Users File (user.txt)

NAME
DESCRIPTION
PASSWORD
USER GROUP NAME
ALLOW GUI
ALLOW CLI
IP
EMAIL
HOST_AS_IP
ACCESS CODE
TIMEZONE
TIMEZONE NAME

LDAP USER

User Group File (usergroup.txt)

USER GROUP NAME
DESCRIPTION
ALLOW ACCESS USER SETTING
ALLOW ACCESS RECEIVER SETTING
ALLOW ACCESS GROUP SETTING
ALLOW ACCESS CARRIER SETTING
ALLOW ACCESS ACTION SETTING
ALLOW ACCESS TEMPLATE SETTING
ALLOW ACCESS DAEMON SETTING
ALLOW MODIFY LICENSE KEY
ALLOW ACCESS DIRECTORY SETTING
ALLOW ACCESS USER GROUP SETTING
ALLOW USE TEMPLATE
ALLOW ACCESS SYSTEM SETTING
ALLOW VIEW LOG
ALLOW VIEW MESSAGE QUEUE
ALLOW ACCESS MONITOR SETTING
ALLOW SEND MESSAGE TO RECEIVER
ALLOW SEND MESSAGE TO GROUP
ALLOW ACCESS GLOBAL SETTING
ALLOW STANDARD MESSAGE SENDING
ALLOW 2WAY MESSAGE SENDING
ALLOW QUICK MESSAGE SENDING
ALLOW SCHEDULE MESSAGE SENDING
ALLOW CASCADE MESSAGE SENDING
ALLOW ACCESS EMAIL GATEWAY SETTING
ALLOW VIEW GROUP REPORT
ALLOW ACCESS FILEINTERFACE SETTING
ALLOW SEND FAX
ALLOW SEND VOICE
ALLOW SEND ARCIMSVOICE
ALLOW MANAGE GROUP USER
ALLOW SUPPORT EMAIL
START PAGE DEPARTMENT VISIBILITY 0

ALLOW SEND TO RECEIVERS IN DEPARTMENT 0
ALLOW SEND TO GROUPS IN DEPARTMENT 0
ALLOW MODIFY RECEIVERS IN DEPARTMENT 0
ALLOW MODIFY GROUPS IN DEPARTMENT 0
USER GROUP PERMISSION 0
ALLOW VIEW REPORT 0
ALLOW MANAGE USER GROUP 0
USER GROUP PERMISSION 1
ALLOW VIEW REPORT 1
ALLOW MANAGE USER GROUP 1
USER GROUP PERMISSION 2
ALLOW VIEW REPORT 2
ALLOW MANAGE USER GROUP 2

Department File (department.txt)

NAME
DESCRIPTION

Receivers File (receiver.txt)

NAME
PIN
EMAIL
TWO WAY ENABLE
CARRIER NAME
DEVICE TYPE
DEPARTMENT NAME
REMARK
ALT CARRIER NAME
ALT CARRIER PIN
VOICE ENABLED
DISABLE
DISABLE START TIME
DISABLE END TIME
TIMEZONE
TIMEZONE NAME
USE ALTER CARRIER
AD CODE
EMAIL FAILOVER
EMAIL CC
VOICE NUMBER
FIRST NAME
LAST NAME
SECURITY CODE
LOGIN NAME
LOGIN PASSWORD
UPD RECE INFO
UPD RECE SCHD
DEVICE STATUS
COVER BY
FORWARD TO NUM
KEEP ALPHA

AD CODESCHEDULED
RECEIVER SCHEDULE NAME 0
SCHEDULED RECEIVER NAME 0
SCHEDULED RECEIVER START HOUR 0
SCHEDULED RECEIVER START MINUTE 0
SCHEDULED RECEIVER END HOUR 0
SCHEDULED RECEIVER END MINUTE 0
SCHEDULED RECEIVER DURATION (MINUTES) 0
SCHEDULED RECEIVER RECURENT END TYPE 0
SCHEDULED RECEIVER RECURENT START DATE 0
SCHEDULED RECEIVER RECURENT END DATE 0
SCHEDULED RECEIVER RECURENT OCCURANCE 0
SCHEDULED RECEIVER SCHEDULE TYPE 0
SCHEDULED RECEIVER SCHEDULE TYPE 0
SCHEDULED RECEIVER RECURENT DAY IN WEEK 0
SCHEDULED RECEIVER RECURENT INTERVAL (WEEK) 0
SCHEDULED RECEIVER RECURENT MONTH TYPE 0
SCHEDULED RECEIVER RECURENT DAY IN MONTH 0
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 0
SCHEDULED RECEIVER RECURENT MONTH TYPE 0
SCHEDULED RECEIVER RECURENT WEEK IN MONTH 0
SCHEDULED RECEIVER RECURENT DAY IN WEEK 0
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 0

Receiver Groups File (group.txt)

NAME DESCRIPTION
DEPARTMENT NAME
RECEIVER MEMBER 0
RECEIVER MEMBER 1
RECEIVER MEMBER 2
RECEIVER MEMBER 3
GROUP MEMBER 0
GROUP MEMBER 1
ESCALATION MEMBER 0
ONDUTY MEMBER 0
ROTATE MEMBER 0
FOLLOW MEMBER 0

On-Duty Groups File (onduty.txt)

NAME DESCRIPTION
DEPARTMENT NAME
RECEIVER MEMBER 0
RECEIVER SEQUENCE ID 0
RECEIVER MEMBER 1
RECEIVER SEQUENCE ID 1
RECEIVER MEMBER 2
RECEIVER SEQUENCE ID 2
RECEIVER MEMBER 3
RECEIVER SEQUENCE ID 3
GROUP MEMBER 0

GROUP SEQUENCE ID 0
GROUP MEMBER 1
GROUP SEQUENCE ID 1
ESCALATION MEMBER 0
ESCALATION SEQUENCE ID 0
FOLLOW MEMBER 0FOLLOW SEQUENCE ID 0
SCHEDULED RECEIVER SCHEDULE NAME 0
SCHEDULED RECEIVER NAME 0
SCHEDULED RECEIVER START HOUR 0
SCHEDULED RECEIVER START MINUTE 0
SCHEDULED RECEIVER END HOUR 0
SCHEDULED RECEIVER END MINUTE 0
SCHEDULED RECEIVER DURATION (MINUTES) 0
SCHEDULED RECEIVER RECURENT END TYPE 0
SCHEDULED RECEIVER RECURENT START DATE 0
SCHEDULED RECEIVER RECURENT END DATE 0
SCHEDULED RECEIVER RECURENT OCCURANCE 0
SCHEDULED RECEIVER SCHEDULE TYPE 0
SCHEDULED RECEIVER RECURRENENT MONTH TYPE 0
SCHEDULED RECEIVER RECURRENENT WEEK IN MONTH 0
SCHEDULED RECEIVER RECURRENENT DAY IN WEEK 0
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 0
SCHEDULED RECEIVER RECURRENENT DAY IN MONTH 0
SCHEDULED RECEIVER RECURRENENT INTERVAL (WEEK) 0
SCHEDULED RECEIVER SEQUENCE ID 0
SCHEDULED RECEIVER SCHEDULE NAME 1
SCHEDULED RECEIVER NAME 1
SCHEDULED RECEIVER START HOUR 1
SCHEDULED RECEIVER START MINUTE 1
SCHEDULED RECEIVER END HOUR 1
SCHEDULED RECEIVER END MINUTE 1
SCHEDULED RECEIVER DURATION (MINUTES) 1
SCHEDULED RECEIVER RECURENT END TYPE 1
SCHEDULED RECEIVER RECURENT START DATE 1
SCHEDULED RECEIVER RECURENT END DATE 1
SCHEDULED RECEIVER RECURENT OCCURANCE 1
SCHEDULED RECEIVER SCHEDULE TYPE 1
SCHEDULED RECEIVER RECURRENENT MONTH TYPE 1
SCHEDULED RECEIVER RECURRENENT WEEK IN MONTH 1
SCHEDULED RECEIVER RECURRENENT DAY IN WEEK 1
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 1
SCHEDULED RECEIVER RECURRENENT DAY IN MONTH 1
SCHEDULED RECEIVER RECURRENENT INTERVAL (WEEK) 1
SCHEDULED RECEIVER SEQUENCE ID 1
SCHEDULED RECEIVER SCHEDULE NAME 2
SCHEDULED RECEIVER NAME 2
SCHEDULED RECEIVER START HOUR 2
SCHEDULED RECEIVER START MINUTE 2
SCHEDULED RECEIVER END HOUR 2
SCHEDULED RECEIVER END MINUTE 2
SCHEDULED RECEIVER DURATION (MINUTES) 2

SCHEDULED RECEIVER RECURENT END TYPE 2
SCHEDULED RECEIVER RECURENT START DATE 2
SCHEDULED RECEIVER RECURENT END DATE 2
SCHEDULED RECEIVER RECURENT OCCURANCE 2
SCHEDULED RECEIVER SCHEDULE TYPE 2
SCHEDULED RECEIVER RECURENT MONTH TYPE 2
SCHEDULED RECEIVER RECURENT WEEK IN MONTH 2
SCHEDULED RECEIVER RECURENT DAY IN WEEK 2
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 2
SCHEDULED RECEIVER RECURENT DAY IN MONTH 2
SCHEDULED RECEIVER RECURENT INTERVAL (WEEK) 2
SCHEDULED RECEIVER SEQUENCE ID 2
SCHEDULED RECEIVER SCHEDULE NAME 3
SCHEDULED RECEIVER NAME 3
SCHEDULED RECEIVER START HOUR 3
SCHEDULED RECEIVER START MINUTE 3
SCHEDULED RECEIVER END HOUR 3
SCHEDULED RECEIVER END MINUTE 3
SCHEDULED RECEIVER DURATION (MINUTES) 3
SCHEDULED RECEIVER RECURENT END TYPE 3
SCHEDULED RECEIVER RECURENT START DATE 3
SCHEDULED RECEIVER RECURENT END DATE 3
SCHEDULED RECEIVER RECURENT OCCURANCE 3
SCHEDULED RECEIVER SCHEDULE TYPE 3
SCHEDULED RECEIVER RECURENT MONTH TYPE 3
SCHEDULED RECEIVER RECURENT WEEK IN MONTH 3
SCHEDULED RECEIVER RECURENT DAY IN WEEK 3
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 3
SCHEDULED RECEIVER RECURENT DAY IN MONTH 3
SCHEDULED RECEIVER RECURENT INTERVAL (WEEK) 3
SCHEDULED RECEIVER SEQUENCE ID 3
SCHEDULED GROUP SCHEDULE NAME 0
SCHEDULED GROUP NAME 0
SCHEDULED GROUP START HOUR 0
SCHEDULED GROUP START MINUTE 0
SCHEDULED GROUP END HOUR 0
SCHEDULED GROUP END MINUTE 0
SCHEDULED GROUP DURATION (MINUTES) 0
SCHEDULED GROUP RECURENT END TYPE 0
SCHEDULED GROUP RECURENT START DATE 0
SCHEDULED GROUP RECURENT END DATE 0
SCHEDULED GROUP RECURENT OCCURANCE 0
SCHEDULED GROUP SCHEDULE TYPE 0
SCHEDULED GROUP RECURENT MONTH TYPE 0
SCHEDULED GROUP RECURENT WEEK IN MONTH 0
SCHEDULED GROUP RECURENT DAY IN WEEK 0
SCHEDULED GROUP RECURENT INTERVAL (MONTH) 0
SCHEDULED GROUP RECURENT DAY IN MONTH 0
SCHEDULED GROUP RECURENT INTERVAL (WEEK) 0
SCHEDULED GROUP SEQUENCE ID 0
SCHEDULED GROUP SCHEDULE NAME 1

SCHEDULED GROUP NAME 1
SCHEDULED GROUP START HOUR 1
SCHEDULED GROUP START MINUTE 1
SCHEDULED GROUP END HOUR 1
SCHEDULED GROUP END MINUTE 1
SCHEDULED GROUP DURATION (MINUTES) 1
SCHEDULED GROUP RECURENT END TYPE 1
SCHEDULED GROUP RECURENT START DATE 1
SCHEDULED GROUP RECURENT END DATE 1
SCHEDULED GROUP RECURENT OCCURANCE 1
SCHEDULED GROUP SCHEDULE TYPE 1
SCHEDULED GROUP RECURRENT MONTH TYPE 1
SCHEDULED GROUP RECURRENT WEEK IN MONTH 1
SCHEDULED GROUP RECURRENT DAY IN WEEK 1
SCHEDULED GROUP RECURRENT INTERVAL (MONTH) 1
SCHEDULED GROUP RECURRENT DAY IN MONTH 1
SCHEDULED GROUP RECURRENT INTERVAL (WEEK) 1
SCHEDULED GROUP SEQUENCE ID 1
SCHEDULED FOLLOW SCHEDULE NAME 0
SCHEDULED FOLLOW NAME 0
SCHEDULED FOLLOW START HOUR 0
SCHEDULED FOLLOW START MINUTE 0
SCHEDULED FOLLOW END HOUR 0
SCHEDULED FOLLOW END MINUTE 0
SCHEDULED FOLLOW DURATION (MINUTES) 0
SCHEDULED FOLLOW RECURENT END TYPE 0
SCHEDULED FOLLOW RECURENT START DATE 0
SCHEDULED FOLLOW RECURENT END DATE 0
SCHEDULED FOLLOW RECURENT OCCURANCE 0
SCHEDULED FOLLOW SCHEDULE TYPE 0
SCHEDULED FOLLOW RECURRENT MONTH TYPE 0
SCHEDULED FOLLOW RECURRENT WEEK IN MONTH 0
SCHEDULED FOLLOW RECURRENT DAY IN WEEK 0
SCHEDULED FOLLOW RECURRENT INTERVAL (MONTH) 0
SCHEDULED FOLLOW RECURRENT DAY IN MONTH 0
SCHEDULED FOLLOW RECURRENT INTERVAL (WEEK) 0
SCHEDULED FOLLOW SEQUENCE ID 0
SCHEDULED ESCALATION SCHEDULE NAME 0
SCHEDULED ESCALATION NAME 0
SCHEDULED ESCALATION START HOUR 0
SCHEDULED ESCALATION START MINUTE 0
SCHEDULED ESCALATION END HOUR 0
SCHEDULED ESCALATION END MINUTE 0
SCHEDULED ESCALATION DURATION (MINUTES) 0
SCHEDULED ESCALATION RECURENT END TYPE 0
SCHEDULED ESCALATION RECURENT START DATE 0
SCHEDULED ESCALATION RECURENT END DATE 0
SCHEDULED ESCALATION RECURENT OCCURANCE 0
SCHEDULED ESCALATION SCHEDULE TYPE 0
SCHEDULED ESCALATION RECURRENT MONTH TYPE 0
SCHEDULED ESCALATION RECURRENT WEEK IN MONTH 0

SCHEDULED ESCALATION RECURRENT DAY IN WEEK 0
SCHEDULED ESCALATION RECURRENT INTERVAL (MONTH) 0
SCHEDULED ESCALATION RECURRENT DAY IN MONTH 0
SCHEDULED ESCALATION RECURRENT INTERVAL (WEEK) 0
SCHEDULED ESCALATION SEQUENCE ID 0

Escalation Groups File (escalation.txt)

NAME DESCRIPTION
DEPARTMENT NAME
RECEIVER MEMBER 0
RECEIVER DELAY TIME 0
RECEIVER SEQUENCE ID 0
RECEIVER MEMBER 1
RECEIVER DELAY TIME 1
RECEIVER SEQUENCE ID 1
RECEIVER MEMBER 2
RECEIVER DELAY TIME 2
RECEIVER SEQUENCE ID 2
RECEIVER MEMBER 3
RECEIVER DELAY TIME 3
RECEIVER SEQUENCE ID 3
GROUP MEMBER 0
GROUP DELAY TIME 0
GROUP SEQUENCE ID 0
GROUP MEMBER 1
GROUP DELAY TIME 1
GROUP SEQUENCE ID 1
GROUP MEMBER 2
GROUP DELAY TIME 2
GROUP SEQUENCE ID 2
ESCALATION MEMBER 0
ESCALATION DELAY TIME 0
ESCALATION SEQUENCE ID 0
ONDUTY MEMBER 0
ONDUTY DELAY TIME 0
ONDUTY SEQUENCE ID 0
ONDUTY MEMBER 1
ONDUTY DELAY TIME 1
ONDUTY SEQUENCE ID 1
FOLLOW MEMBER 0
FOLLOWME DELAY TIME 0
FOLLOW SEQUENCE ID 0
ROTATE MEMBER 0
ROTATE DELAY TIME 0
ROTATE SEQUENCE ID 0

Rotate Groups File (rotate.txt)

NAME DESCRIPTION
DEPARTMENT NAME
NEXT IN LINE SEQ
RECEIVER MEMBER 0

RECEIVER SEQUENCE ID 0
RECEIVER MEMBER 1
RECEIVER SEQUENCE ID 1
RECEIVER MEMBER 2
RECEIVER SEQUENCE ID 2
RECEIVER MEMBER 3
RECEIVER SEQUENCE ID 3
GROUP MEMBER 0
GROUP SEQUENCE ID 0
GROUP MEMBER 1
GROUP SEQUENCE ID 1
GROUP MEMBER 2
GROUP SEQUENCE ID 2
ESCALATION MEMBER 0
ESCALATION SEQUENCE ID 0
ESCALATION MEMBER 1
ESCALATION SEQUENCE ID 1
ONDUTY MEMBER 0
ONDUTY SEQUENCE ID 0
ONDUTY MEMBER 1
ONDUTY SEQUENCE ID 1
FOLLOW MEMBER 0
FOLLOW SEQUENCE ID 0
ROTATE MEMBER 0
ROTATE SEQUENCE ID 0

Follow-Me Groups File (follow.txt)

NAME DESCRIPTION
DEPARTMENT NAME
RECEIVER MEMBER 0
RECEIVER SEQUENCE ID 0
RECEIVER MEMBER 1
RECEIVER SEQUENCE ID 1
RECEIVER MEMBER 2
RECEIVER SEQUENCE ID 2
RECEIVER MEMBER 3
RECEIVER SEQUENCE ID 3
GROUP MEMBER 0
GROUP SEQUENCE ID 0
GROUP MEMBER 1
GROUP SEQUENCE ID 1
ESCALATION MEMBER 0
ESCALATION SEQUENCE ID 0
FOLLOW MEMBER 0
FOLLOW SEQUENCE ID 0
SCHEDULED RECEIVER SCHEDULE NAME 0
SCHEDULED RECEIVER NAME 0
SCHEDULED RECEIVER START HOUR 0
SCHEDULED RECEIVER START MINUTE 0
SCHEDULED RECEIVER END HOUR 0
SCHEDULED RECEIVER END MINUTE 0

SCHEDULED RECEIVER DURATION (MINUTES) 0
SCHEDULED RECEIVER RECURENT END TYPE 0
SCHEDULED RECEIVER RECURENT START DATE 0
SCHEDULED RECEIVER RECURENT END DATE 0
SCHEDULED RECEIVER RECURENT OCCURANCE 0
SCHEDULED RECEIVER SCHEDULE TYPE 0
SCHEDULED RECEIVER RECURENT MONTH TYPE 0
SCHEDULED RECEIVER RECURENT WEEK IN MONTH 0
SCHEDULED RECEIVER RECURENT DAY IN WEEK 0
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 0
SCHEDULED RECEIVER RECURENT DAY IN MONTH 0
SCHEDULED RECEIVER RECURENT INTERVAL (WEEK) 0
SCHEDULED RECEIVER SEQUENCE ID 0
SCHEDULED RECEIVER SCHEDULE NAME 1
SCHEDULED RECEIVER NAME 1
SCHEDULED RECEIVER START HOUR 1
SCHEDULED RECEIVER START MINUTE 1
SCHEDULED RECEIVER END HOUR 1
SCHEDULED RECEIVER END MINUTE 1
SCHEDULED RECEIVER DURATION (MINUTES) 1
SCHEDULED RECEIVER RECURENT END TYPE 1
SCHEDULED RECEIVER RECURENT START DATE 1
SCHEDULED RECEIVER RECURENT END DATE 1
SCHEDULED RECEIVER RECURENT OCCURANCE 1
SCHEDULED RECEIVER SCHEDULE TYPE 1
SCHEDULED RECEIVER RECURENT MONTH TYPE 1
SCHEDULED RECEIVER RECURENT WEEK IN MONTH 1
SCHEDULED RECEIVER RECURENT DAY IN WEEK 1
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 1
SCHEDULED RECEIVER RECURENT DAY IN MONTH 1
SCHEDULED RECEIVER RECURENT INTERVAL (WEEK) 1
SCHEDULED RECEIVER SEQUENCE ID 1
SCHEDULED RECEIVER SCHEDULE NAME 2
SCHEDULED RECEIVER NAME 2
SCHEDULED RECEIVER START HOUR 2
SCHEDULED RECEIVER START MINUTE 2
SCHEDULED RECEIVER END HOUR 2
SCHEDULED RECEIVER END MINUTE 2
SCHEDULED RECEIVER DURATION (MINUTES) 2
SCHEDULED RECEIVER RECURENT END TYPE 2
SCHEDULED RECEIVER RECURENT START DATE 2
SCHEDULED RECEIVER RECURENT END DATE 2
SCHEDULED RECEIVER RECURENT OCCURANCE 2
SCHEDULED RECEIVER SCHEDULE TYPE 2
SCHEDULED RECEIVER RECURENT MONTH TYPE 2
SCHEDULED RECEIVER RECURENT WEEK IN MONTH 2
SCHEDULED RECEIVER RECURENT DAY IN WEEK 2
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 2
SCHEDULED RECEIVER RECURENT DAY IN MONTH 2
SCHEDULED RECEIVER RECURENT INTERVAL (WEEK) 2
SCHEDULED RECEIVER SEQUENCE ID 2

SCHEDULED RECEIVER SCHEDULE NAME 3
SCHEDULED RECEIVER NAME 3
SCHEDULED RECEIVER START HOUR 3
SCHEDULED RECEIVER START MINUTE 3
SCHEDULED RECEIVER END HOUR 3
SCHEDULED RECEIVER END MINUTE 3
SCHEDULED RECEIVER DURATION (MINUTES) 3
SCHEDULED RECEIVER RECURENT END TYPE 3
SCHEDULED RECEIVER RECURENT START DATE 3
SCHEDULED RECEIVER RECURENT END DATE 3
SCHEDULED RECEIVER RECURENT OCCURANCE 3
SCHEDULED RECEIVER SCHEDULE TYPE 3
SCHEDULED RECEIVER RECURRENT MONTH TYPE 3
SCHEDULED RECEIVER RECURRENT WEEK IN MONTH 3
SCHEDULED RECEIVER RECURRENT DAY IN WEEK 3
SCHEDULED RECEIVER RECURENT INTERVAL (MONTH) 3
SCHEDULED RECEIVER RECURRENT DAY IN MONTH 3
SCHEDULED RECEIVER RECURRENT INTERVAL (WEEK) 3
SCHEDULED RECEIVER SEQUENCE ID 3
SCHEDULED GROUP SCHEDULE NAME 0
SCHEDULED GROUP NAME 0
SCHEDULED GROUP START HOUR 0
SCHEDULED GROUP START MINUTE 0
SCHEDULED GROUP END HOUR 0
SCHEDULED GROUP END MINUTE 0
SCHEDULED GROUP DURATION (MINUTES) 0
SCHEDULED GROUP RECURENT END TYPE 0
SCHEDULED GROUP RECURENT START DATE 0
SCHEDULED GROUP RECURENT END DATE 0
SCHEDULED GROUP RECURENT OCCURANCE 0
SCHEDULED GROUP SCHEDULE TYPE 0
SCHEDULED GROUP RECURRENT MONTH TYPE 0
SCHEDULED GROUP RECURRENT WEEK IN MONTH 0
SCHEDULED GROUP RECURRENT DAY IN WEEK 0
SCHEDULED GROUP RECURRENT INTERVAL (MONTH) 0
SCHEDULED GROUP RECURRENT DAY IN MONTH 0
SCHEDULED GROUP RECURRENT INTERVAL (WEEK) 0
SCHEDULED GROUP SEQUENCE ID 0
SCHEDULED GROUP
SCHEDULE NAME 1
SCHEDULED GROUP NAME 1
SCHEDULED GROUP START HOUR 1
SCHEDULED GROUP START MINUTE 1
SCHEDULED GROUP END HOUR 1
SCHEDULED GROUP END MINUTE 1
SCHEDULED GROUP DURATION (MINUTES) 1
SCHEDULED GROUP RECURENT END TYPE 1
SCHEDULED GROUP RECURENT START DATE 1
SCHEDULED GROUP RECURENT END DATE 1
SCHEDULED GROUP RECURENT OCCURANCE 1
SCHEDULED GROUP SCHEDULE TYPE 1

SCHEDULED GROUP RECURRENT MONTH TYPE 1
SCHEDULED GROUP RECURRENT WEEK IN MONTH 1
SCHEDULED GROUP RECURRENT DAY IN WEEK 1
SCHEDULED GROUP RECURRENT INTERVAL (MONTH) 1
SCHEDULED GROUP RECURRENT DAY IN MONTH 1
SCHEDULED GROUP RECURRENT INTERVAL (WEEK) 1
SCHEDULED GROUP SEQUENCE ID 1
SCHEDULED FOLLOW
SCHEDULE NAME 0
SCHEDULED FOLLOW NAME 0
SCHEDULED FOLLOW START HOUR 0
SCHEDULED FOLLOW START MINUTE 0
SCHEDULED FOLLOW END HOUR 0
SCHEDULED FOLLOW END MINUTE 0
SCHEDULED FOLLOW DURATION (MINUTES) 0
SCHEDULED FOLLOW RECURRENT END TYPE 0
SCHEDULED FOLLOW RECURRENT START DATE 0
SCHEDULED FOLLOW RECURRENT END DATE 0
SCHEDULED FOLLOW RECURRENT OCCURANCE 0
SCHEDULED FOLLOW SCHEDULE TYPE 0
SCHEDULED FOLLOW RECURRENT MONTH TYPE 0
SCHEDULED FOLLOW RECURRENT WEEK IN MONTH 0
SCHEDULED FOLLOW RECURRENT DAY IN WEEK 0
SCHEDULED FOLLOW RECURRENT INTERVAL (MONTH) 0
SCHEDULED FOLLOW RECURRENT DAY IN MONTH 0
SCHEDULED FOLLOW RECURRENT INTERVAL (WEEK) 0
SCHEDULED FOLLOW SEQUENCE ID 0
SCHEDULED ESCALATION
SCHEDULE NAME 0
SCHEDULED ESCALATION NAME 0
SCHEDULED ESCALATION START HOUR 0
SCHEDULED ESCALATION START MINUTE 0
SCHEDULED ESCALATION END HOUR 0
SCHEDULED ESCALATION END MINUTE 0
SCHEDULED ESCALATION DURATION (MINUTES) 0
SCHEDULED ESCALATION RECURRENT END TYPE 0
SCHEDULED ESCALATION RECURRENT START DATE 0
SCHEDULED ESCALATION RECURRENT END DATE 0
SCHEDULED ESCALATION RECURRENT OCCURANCE 0
SCHEDULED ESCALATION SCHEDULE TYPE 0
SCHEDULED ESCALATION RECURRENT MONTH TYPE 0
SCHEDULED ESCALATION RECURRENT WEEK IN MONTH 0
SCHEDULED ESCALATION RECURRENT DAY IN WEEK 0
SCHEDULED ESCALATION RECURRENT INTERVAL (MONTH) 0
SCHEDULED ESCALATION RECURRENT DAY IN MONTH 0
SCHEDULED ESCALATION RECURRENT INTERVAL (WEEK) 0
SCHEDULED ESCALATION SEQUENCE ID 0

Time Zone (timezone.txt)

TIME_ZONE_NAME
TIME_ZONE_DESCRIPTION

OFFSET
Server Time
Server Time - 0 hour offset
0

Important: *Never try to import data from a file that has not been created by HipLink. HipLink will only import tab delimited text files and will confirm the integrity of the data before it is imported. If a record has been corrupted, it will be skipped by the Utility. After importing/exporting data, check the log file*
/config/import_export_log.txt.

Backup Service

The Backup Service provides full backups of the HipLink database. These backups can be scheduled to happen at a user-defined interval. Everything that can be set in the Settings menu of the GUI will be saved in the backup file. The HipLink Administrator can edit various settings related to this backup process. Restoring a backup is as easy as pressing the restore button next to the backup file that you want to use.

Warning: *It is strongly recommended to make a backup of the current HipLink configuration (by pressing the Backup Now button), before restoring from an old version. Restoring from an old backup file will, by design, overwrite the entire current HipLink database with the old version.*

Set the Backup Service parameters

1. From the Settings menu, click Backup Service on the left navigation bar.
2. On the Backup Service Panel, click the Edit button to reach the Edit the Configuration of Backup Service page.
3. Enter the Backup Directory where the backups will be stored (mandatory).
4. Set the Backup Start-Time (24 hours clock). This is the time of the first backup. Subsequent backups are scheduled based on the Backup Interval. See step 6.
5. Set the Backup Keep Days. This is the number of days that the backup files will be kept.
6. Set the Backup Interval (hour). This is the number of hours that HipLink waits between backups. For example if you set the Backup Start Time to be 03:00 and the Backup Interval to be 24 hours, then backups will be made every day at 3 am.
7. Finally you can choose to enable or disable the detailed log file.

Restore from a Backup

1. From the Settings menu, click Backup Service on the left navigation bar.
2. Press the icon under the Restore column, next to the backup file that you want to restore. It is strongly recommended to make a backup of the current HipLink configuration (by pressing the Backup Now button), before restoring from an old version. Restoring from an

old backup file will, by design, overwrite the entire current HipLink database with the old version.

Note: *Upgrading HipLink from one version to another implies very often database conversion from the previous format to the new format. When this is the case, the installer will check the version of the backup, and only compatible backups will be restored. The HipLink version is included in the name of the backup file.*

Special Module Configuration

HipLink Fax Module

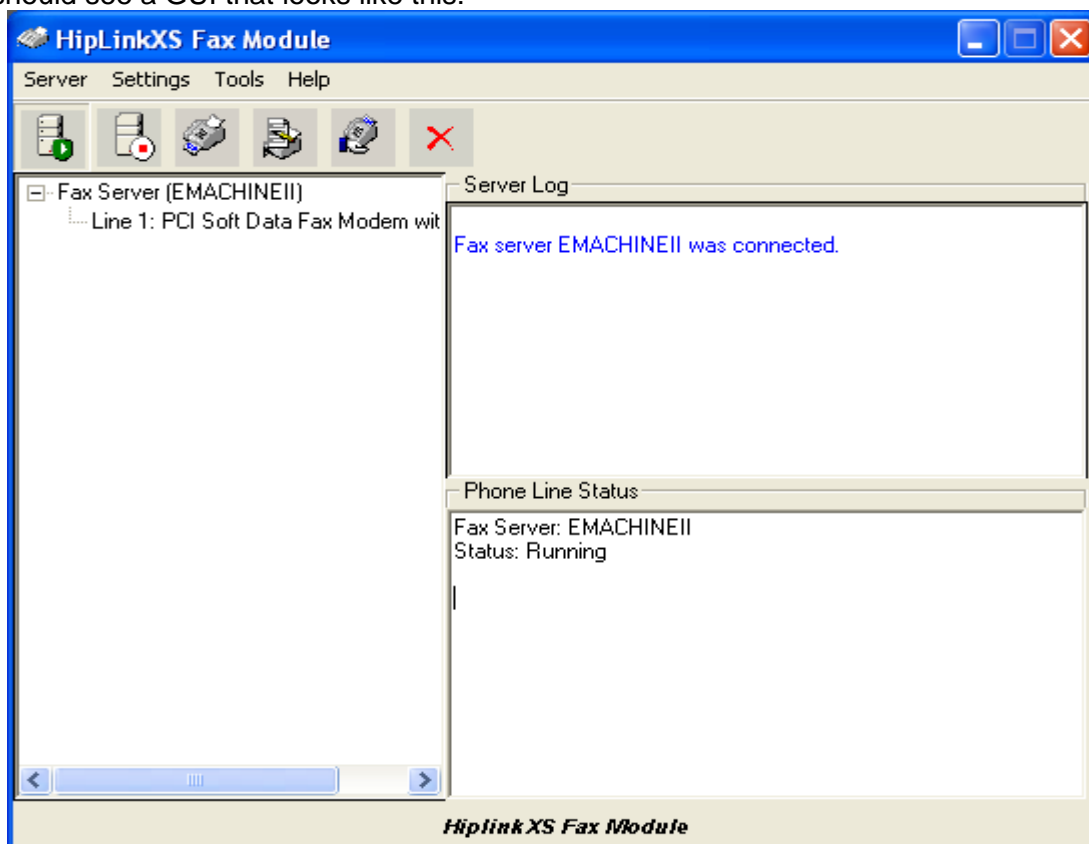
Prerequisites

1. The HipLink Fax Module works in conjunction with the Microsoft Fax Service for Windows 2000/XP. Before reading this section, please read the Microsoft documentation about the Fax Service.
2. Follow the Microsoft instructions for installing your modem(s). You will have to install at least one modem for the Fax Module to work.
3. For each type of document that you want the Fax Module to handle, you will need to install its corresponding application. For example, to use PDF, you should install Adobe Acrobat on the same machine as the HipLink Fax Module.

Administering the Fax Module

Launch the Fax Module administration application by choosing Start > Programs > HipLink Group > Hiplink Fax.

You should see a GUI that looks like this:



Note: you will not see the Fax Server information until you have connected to modem in Step 5.

1. Enter License Key

If you did not already do so during the installation, you will have to enter a valid License Key now. If there is any problem, please contact HipLink Technical Support.

To enter a new License Key:

- a. From the Settings menu, click License Key.
- b. Enter your new License Key in the appropriate field and then click OK.

2. Edit Directory Settings

There are three directories that can be configured. They are the:

- a. Spool Directory, where the files that wait in the fax spool queue reside. The default directory is: C:\Program Files\HipLink Group\Hiplink Fax. If the HipLink Server is installed on the same computer as the Fax Module, then no further configuration is necessary. If not, it is necessary to share this directory with permissions such that the HipLink Server can write files to the Spool Directory.
- b. Archive Directory for Completed Fax Requests. By default this directory is C:\Program Files\HipLinkGroup\Hiplink Fax\Archive\Completed.
- c. Archive Directory for Failed Fax Requests. By default this directory is C:\Program Files\HipLinkGroup\Hiplink Fax\Archive\Failed.

To edit the Directory Settings:

- a. From the Settings menu, click Directories.
- b. Edit the paths and then click OK.

3. Enter HipLink Server URL

If you did not already do so during the installation, you will have to enter a valid HipLink URL now. To enter a new HipLink Server URL:

- a. From the Settings menu, click Server URL.
- b. Enter your new URL in the appropriate field and then click OK.

4. Edit Fax Server Options

These are options related to the operation of the Fax Server itself.

To edit Fax Server options:

- a. From the Settings menu, click Fax Server.
- b. The Server Name is the Windows computer name for the Fax Server.
- c. The Days unsent fax is kept field represents the number of days that faxes will be left in the spool while trying to phone a busy phone number.
- d. The Print banner on top of each sent page: (branding) checkbox enables or disables banners in the cover page of the fax.

5. Connect to the Fax Modem

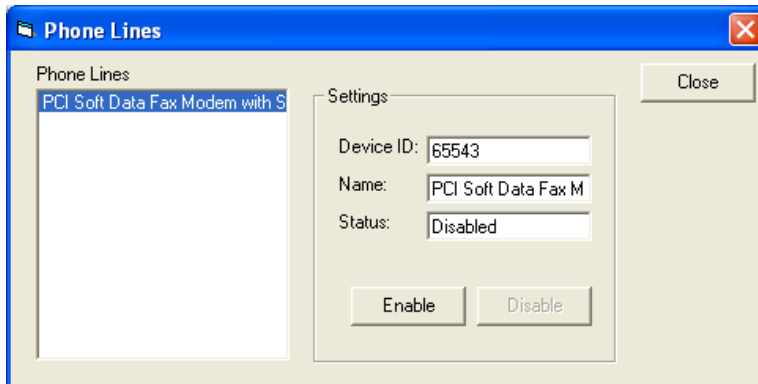
If you followed the second prerequisite, then a fax modem should be installed and you should be able to connect to it by clicking the Server Connect icon. You can also connect by selecting the Server menu, and then clicking Connect.



6. Enable/Disable Phone Lines

To edit the Settings of the Phone Line(s):

- a. From the Settings menu, click Phone Lines.



- b. Highlight the phone line that you wish to modify.
 - c. You can enable or disable a line by checking or unchecking the Enabled checkbox and then click Save.
 - d. Click OK when you are done.
7. Tools

The fax module provides three links to Microsoft fax tools. Please refer to the Microsoft documentation for these tools. From the Tools menu, the three tools are:

- a. Cover Pager Editor
- b. Fax Queue Monitor
- c. Fax Server Property

HipLink Voice Module

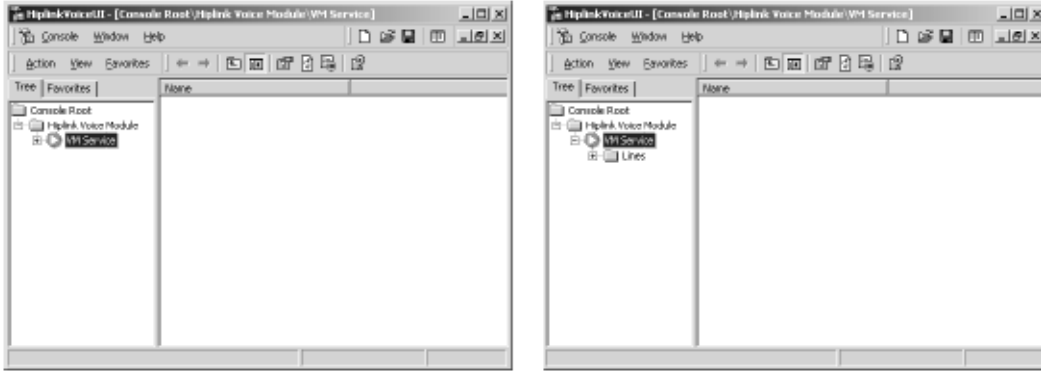
The HipLink Voice Module allows a HipLink administrator to receive incoming calls and to send outgoing voice calls. In both cases, the Module creates the interface to allow Users to control telephony IVR (Interactive Voice Response) session flows, and to perform HipLink functions over the phone. The way to program the IVR interface is by writing an XML document: SVXML. Semotus Voice XML is described in the *Integration & Programmer Guide*.

At the present moment, the Voice Module only works with the Dialogic Board: D/41JCT-LS, to connect to the telephone lines and media resources. Your CT ADE license key determines the number of lines that may be used. Additionally, the way in which the lines may be used (inbound/outbound/both) is determined by the HipLink ES Voice Module license key.

The following section briefly describes the GUI used for administering the Voice Module.

Administering the Voice Module

When you start the HipLink Voice UI application, you will see a window that looks like the images shown below:



Expanding the main folder, HipLink Voice Module will display the VM Service Node and the folder Lines.

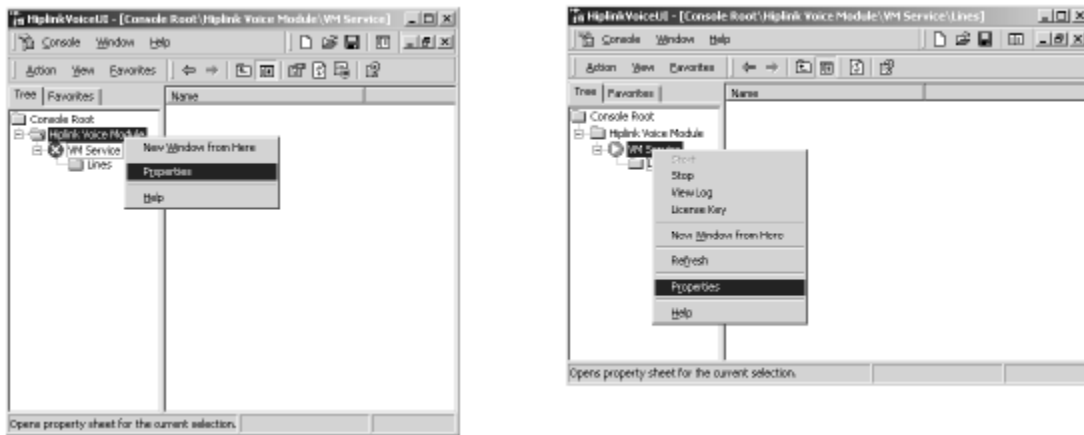
Note: Lines cannot be expanded until the Voice Module Service is started.

There are three primary functions of this interface:

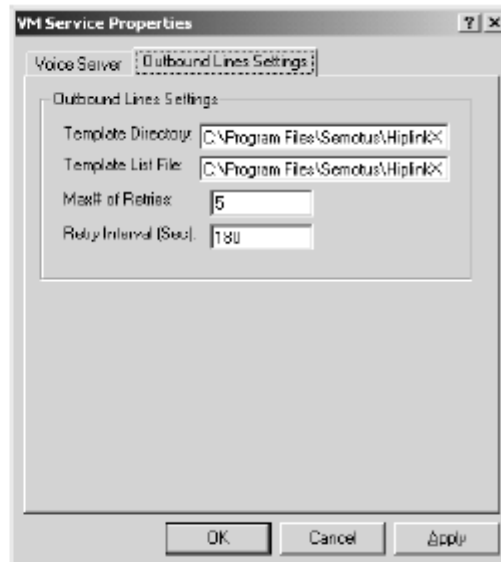
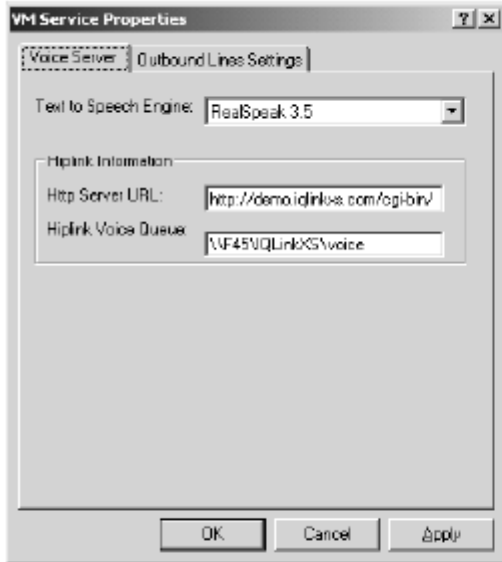
- Managing and Controlling the Voice Service
- Managing and Controlling the Lines.
- Recording/Playing voice files.

Managing and Controlling the Voice Service

The voice service properties can be set by selecting the HipLink Voice Module folder or the VM Service and right-clicking to pop up the menu and select properties:



This will display a property page with the follow fields:



After you have made changes to these settings, the VM Service will need to be restarted in order for your changes to take effect.

To start the VM Service:

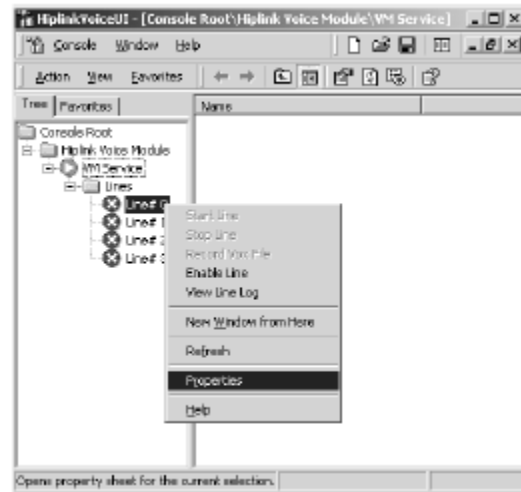
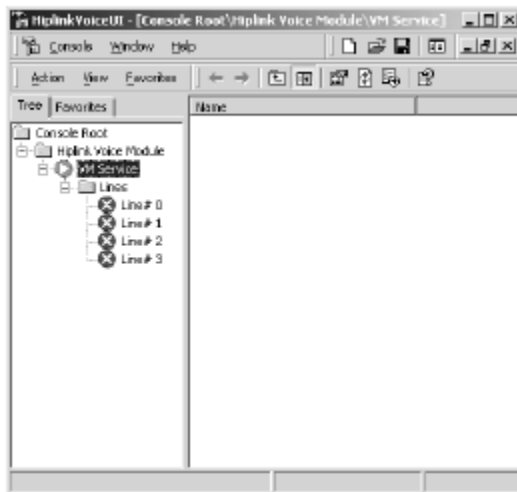
1. Select the VM Service node.
2. Right-click on the node and select the Start option from the pop-up menu.

To stop the VM Service

1. Select the VM Service node.
2. Right-click on the node and select the Stop option from the pop-up menu.

Managing and Controlling Lines

The line properties can be set by selecting the line node then right-clicking to pop-up the menu and selecting Properties.



Inbound Line Settings

To be able to answer incoming calls, one or more lines of Voice Server should be set to the Inbound mode. Each line must point to a SVXML script. Different lines may share the same script, or they may each use their own unique script. For example, one line might use a

general_welcome.svxml script, and two others might share tech_support.svxml. After the lines have been started, the server will automatically handle incoming calls based on these scripts.



To configure a phone line for Inbound use:

1. Set the line to Enabled and Stopped.
2. Open the properties window for the line.
3. Chose Inbound Mode.
4. Enter the path for the appropriate SVXML script.
5. Click OK when you are done.

Outbound Line Setting

To be able to make outbound calls, one or more lines of Voice Server should be set to the Outbound mode. Two directories need to be specified for these calls. HipLink Voice Queue is used for internal communication between the HipLink server and the Voice Module. Outgoing message files and voice attachments are spooled here. The HipLink Server needs to be able write to this directory. If the HipLink Server is installed on the same computer as the Voice Module, then no further configuration is necessary. If not, it is necessary to modify the HipLink Voice Service to log on under a windows account that has access to the spool directory.



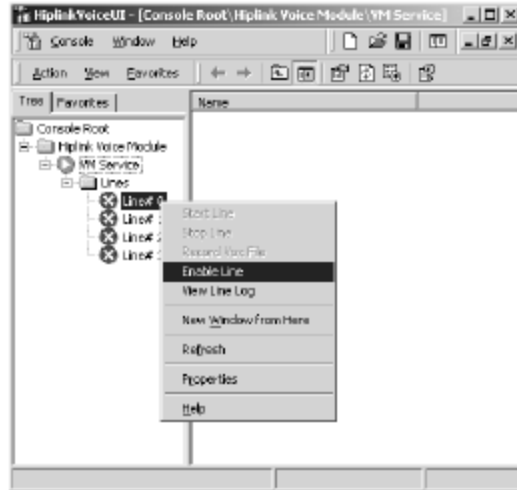
To configure a phone line for outbound use:

1. Set the line to Enabled and Stopped.
2. Open the properties window for the line.
3. Chose Outbound Mode.
4. Click OK when you are done.

Controlling Line Status

A line can be enabled or disabled. Once that a line is enabled it can be started and stopped.

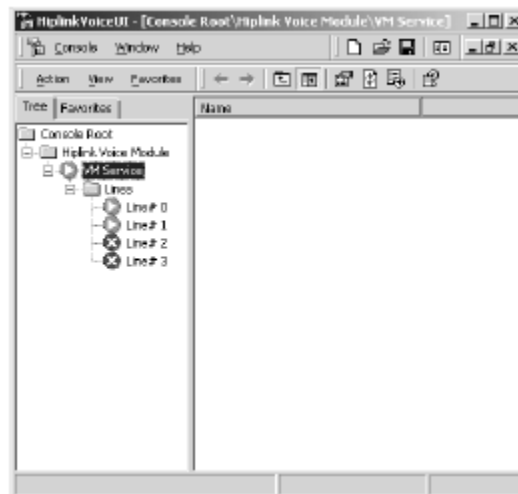
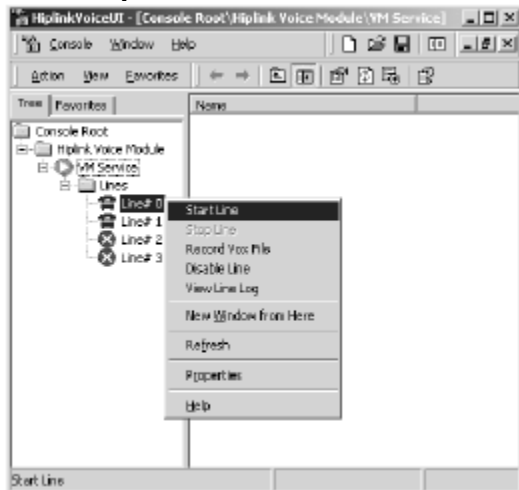
Enable/Disable Line



In order to change the line status:

1. Select the VM Service node.
2. Right-click on the node and select Enable Line or Disable Line depending on what options are available in the popup menu.

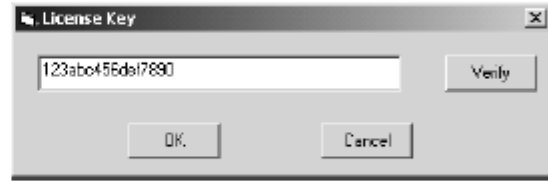
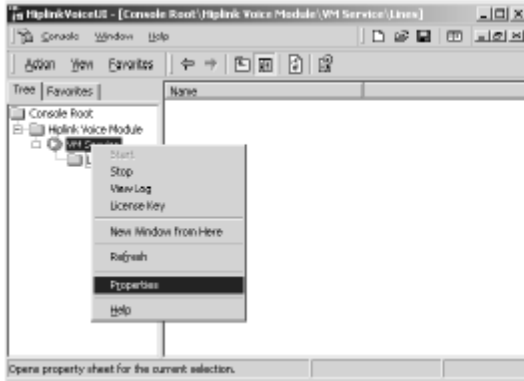
Start/Stop Line



In order to start or stop the line:

1. Select the VM Service node.
2. Right-click on the node and select Start Line or Stop Line depending on what options are available in the popup menu.

License Key

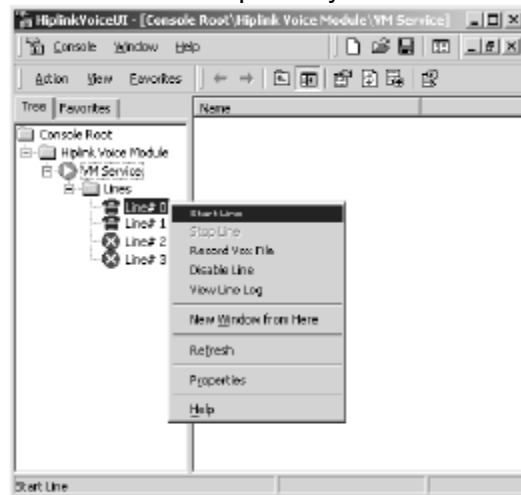
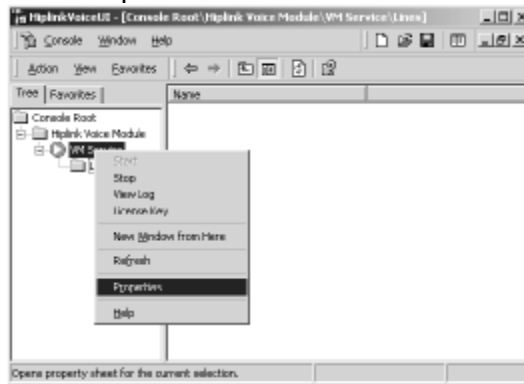


To change the License Key:

1. Right-click on the VM Service and select License Key.
2. In the License Key window enter the new key.
3. Click the Verify button to see the number of lines enabled by the License Key.
4. Click the OK button to save and close the License Key window.

Log Files

Log files are kept for the Voice Module Service and for each line separately.



To view the VM Service log file:

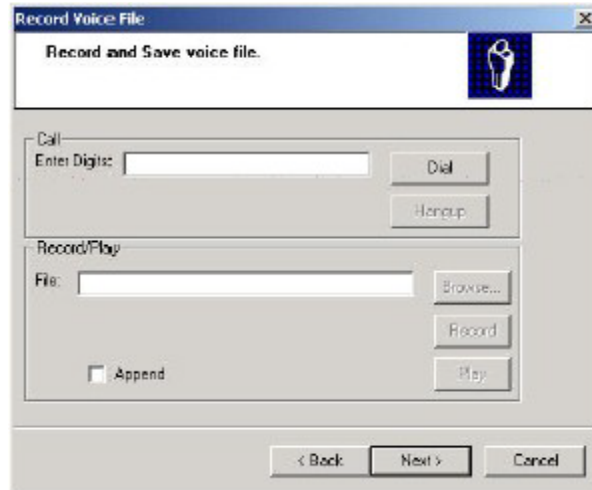
1. Right-click on the VM Service and select View Log.
2. The VM Service log file will open in Notepad.

To view a line log file:

1. Right-click on the line and select View Line Log.
2. The line log file will open in Notepad.

RECORDING/PLAYING VOICE FILES

Using the recording mode, you can use a regular phone to record and play back voice files.



To record a voice file:

1. Before recording, a line needs to be in the enabled and stopped state.
2. Right-click on the stopped line and select the Record Vox File option from the pop-up menu. This will start a wizard. Click the Next button.
3. Enter the phone number of your phone and click Dial. Your phone should ring. Answer it.
4. Enter a file name for the new voice file to be created and press the Record button. If you want to append the recording to an existing file rather than to create a new one, then you should select the Append checkbox. If the Append checkbox is not selected, then an existing file with that name would be overwritten.
5. A female voice will prompt you to speak after the tone. Record your message and press the # key on the phone when you are done.
6. Click the Next button to finish.

To play a voice file:

1. Follow steps 1 to 3 outlined above for recording.
2. Enter a file name for the voice file you wish to play and click on the Play button. You will hear the voice file played back to you.
3. Click the OK button to finish.