

iPECS

NMS

User Guide

Please read this manual carefully before operation. Retain it for future reference.

iPECS is an Ericsson-LG Brand



Copyright

Copyright © 2013 Ericsson-LG Enterprise Co., Ltd. All Rights Reserved

This material is copyrighted by Ericsson-LG Enterprise Co., Ltd. Any unauthorized reproductions, use or disclosure of this material, or any part thereof, is strictly prohibited and is a violation of Copyright Laws.

Ericsson-LG Enterprise reserves the right to make changes in specifications at any time without notice.

The information furnished by Ericsson-LG Enterprise in this material is believed to be accurate and reliable, but is not warranted to be true in all cases.

Ericsson-LG Enterprise and iPECS UCS are trademarks of Ericsson-LG Enterprise Co., Ltd.

Revision History

Issue	Date	Description of Changes
1.0a	Aug. 2008	Initial Release
1.0b	Sep. 2008	Access Control, System DB, Prompt Upload, System Greeting
1.0c	Nov. 2008	MIFM1200 Support
1.0d	Aug. 2009	iPECS-MG100/300 System Support, iPECS-Micro Support
1.0e	Jul. 2010	Change LG-Ericsson CI
2.0a	Feb. 2012	iPECS ES Switch Support & Network Topology
2.0b	Sep. 2012	Change Ericsson-LG CI
2.1a	May. 2014	iPECS UCP Support
2.1b	Sep, 2014	iPECS eMG Support

Table of Contents

- 1. Introduction4**
 - 1.1 Overview 4
 - 1.2 Feature Summary 4
- 2. Installation.....6**
 - 2.1 System Requirements 6
 - 2.2 Software Installation Procedure 7
 - 2.3 iPECS System Admin Configuration..... 36
- 3. Getting Started39**
 - 3.1 Checking Windows Service Status 39
 - 3.2 Accessing iPECS-NMS Server using Web Browser 41
- 4. NMS Management43**
 - 4.1 Modify Superuser Configuration 43
 - 4.2 NMS Server Management 43
- 5. Device Management47**
 - 5.1 Device Configuration 47
 - 5.2 Device Group Configuration 49
 - 5.3 Web Admin Configuration 51
- 6. User Management53**
 - 6.1 User Configuration..... 53
 - 6.2 User Access Control..... 57
- 7. Alarm/Fault Management59**
 - 7.1 Alarm/Fault Analysis..... 59
 - 7.2 Alarm/Fault Configuration 61
 - 7.3 Types and Definitions of alarm/Fault Events 63
- 8. Network Topology.....79**
 - 8.1 Displaying Topology Diagram 79

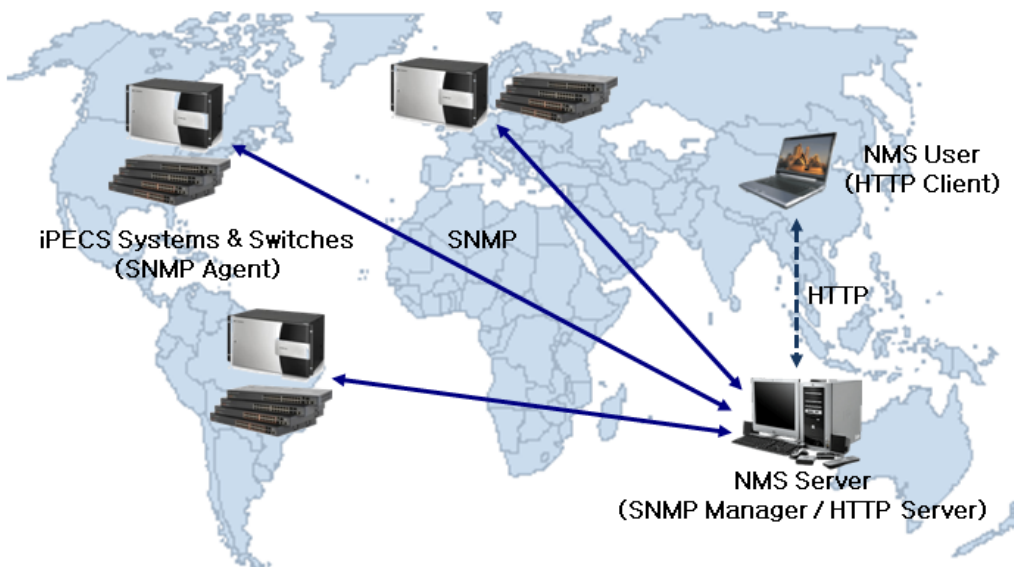
8.2 Basic Features of Topology Diagram	80
8.3 Additional Features of Topology Diagram.....	81
9. Network Traffic Monitoring	84
9.1 Ping Test	84
9.2 Traceroute Test.....	86
9.3 Device Network Traffic	87
10. Log & History Management	92
10.1 NMS Access Log.....	92
10.2 NMS Operation Log.....	94
11. System Information	97
11.1 System Configuration Information.....	97
11.2 Device Inventory Information.....	100
12. System Configuration and Status	103
12.1 Device Based Status	103
12.2 CO Channel Status	110
12.3 Station Channel Status.....	111
13. System Call Statistics.....	113
13.1 Call Traffic Analysis	113
13.2 Call Traffic Configuration.....	119
13.3 SMDR Analysis.....	120
13.4 SMDR Statistics.....	121
13.5 DECT Statistics.....	122
14. System Device Traffic Monitoring	133
14.1 iPECS Device Ping Test	133
14.2 iPECS Device Network Traffic.....	136
15. System Maintenance.....	139
15.1 Firmware Upgrade	139
15.2 System DB Management.....	142
15.3 Prompt Upload	147
15.4 System Greeting Management.....	149

16. Switch Information	153
16.1 Device Information.....	153
16.2 CPU and Memory Usage Information.....	155
17. Switch Interface Information	158
17.1 Port Information	158
17.2 Port Mirroring Information	159
17.3 Port Statistics Information.....	159
18. Switch VLAN Information.....	162
18.1 Telephony OUI Information	162
18.2 Static VLAN Port Mode	163
18.3 VoIP Port Information	163
19. Switch Spanning Tree Information.....	165
19.1 Spanning Tree Information.....	165
20. Switch Traffic Control Information	167
20.1 DiffServ Information	167
20.2 Rate Limit Information	171
20.3 Storm Control Information.....	172
21. Switch LLDP Information	173
21.1 LLDP Device Information	173
22. NMS Local Database Backup & Restore	177
22.1 Backup & Restore Basic Configuration Database	178
22.2 Backup & Restore Entire Database.....	183

1. Introduction

1.1 Overview

iPECS NMS is a Web-based MS-Windows® application software that provides system monitoring and management features communicating with multiple iPECS systems and switches using standard Simple Network Management Protocol (SNMP) for communication across the network. The purpose of this software is to assist in operation of the iPECS systems and switches allowing for convenient and efficient management operation and problem status of the devices being monitored. The Web-based software architecture provides network managers the added benefit of remote accessibility to the NMS server using a Web browser interface for the NMS client.



1.2 Feature Summary

iPECS-NMS is comprised of Common, System and Switch features, and brief overview of each feature is as follows.

- NMS Server Management and Common Features

NMS server configuration and user management features are provided together with device registration of systems and switches. NMS operational history can be checked using the NMS access log & operation log, and network topology shows device connections among switches and systems with diagram & table. Ping, Traceroute and traffic monitoring features can be used to check network connectivity and traffic information of network devices. Alarm/fault

feature provides important or abnormal status information that happened in systems and switches. Event message management and searches can also be performed on those alarm/fault information.

- System Features

System features provide various services such as system information, device status information, iPECS device traffic and maintenance. System information can be used to check general system configuration, attendant & station/CO groups together with device inventory information. Device status information provides device-based and CO/station channel-based status information as well as detailed device information. Call Statistics operations present tables and graphs with traffic analysis data from iPECS systems. In regard to Station Message Detail Recording (SMDR) data, the System Management facet of the program additionally provides searching operations in table format for detailed analysis. iPECS device firmware can be upgraded using Firmware Upgrade operations for specified systems at a designated time, and system database, system greeting and prompt files can be uploaded or downloaded.

- Switch Features

Switch features include services to provide switch device information and information of interfaces, VLAN, spanning tree, traffic and LLDP. Switch device information provides general configuration information including device network configuration, and also CPU & memory utilization information. Interface information can be checked for port status, configuration and statistics information. VLAN information shows telephony OUI and VoIP port list as well as brief VLAN configuration information, and spanning tree information provides port-based spanning tree configuration and status information. Traffic information is comprised of DiffServ information, rate limit and storm control information. LLDP information provides local device information and detailed information of remote devices that are connected to each switch device.

2. Installation

2.1 System Requirements

2.1.1 NMS Server Minimum Requirements

- When 20 or less devices are to be registered
 - CPU : Intel dual core 2.33 GHz or higher
 - RAM : 4 GB or higher
 - HDD : At least 10 GB of free disk space
 - O/S : Microsoft Windows 7 Professional / Windows Server 2008 / Windows Server 2012
 - Display : 1280 * 800 or higher

- When 200 or less devices are to be registered
 - CPU : Intel dual core Xeon 2.4 GHz or higher
 - RAM : 4 GB or higher
 - HDD : At least 20 GB of free disk space
 - O/S : Microsoft Windows 7 Professional / Windows Server 2008 / Windows Server 2012
 - Display : 1280 * 800 or higher

- When 500 or less systems are to be registered
 - CPU : Intel Quad-Core Xeon 2.66 GHz or higher
 - RAM : 4 GB or higher
 - HDD : At least 50 GB of free disk space
 - O/S : Microsoft Windows 7 Professional / Windows Server 2008 / Windows Server 2012
 - Display : 1280 * 800 or higher

2.1.2 iPECS System & Device Requirements

- iPECS-LiK MFIM Firmware version 5.0 or higher
- iPECS-MG MPB Firmware version 1.0 or higher
- iPECS UCP Firmware version 1.0 or higher
- iPECS eMG Firmware version 1.0.3 or higher
- Gateways and IP-phones developed before iPECS Phase 3 can be used for basic NMS features. However, in order to support all the additional features provided by NMS (e.g. iPECS device traffic monitoring), those developed after iPECS Phase 4 should be used, and firmware should be upgraded with latest versions that support NMS features.

- SNMP and LLDP-related settings should be properly configured for iPECS switches in order to use all the features provided by iPECS-NMS. Please refer to user's manuals of the switches for details of corresponding configurations.

2.2 Software Installation Procedure

2.2.1 iPECS-NMS Software Components

Software components needed for iPECS-NMS are :

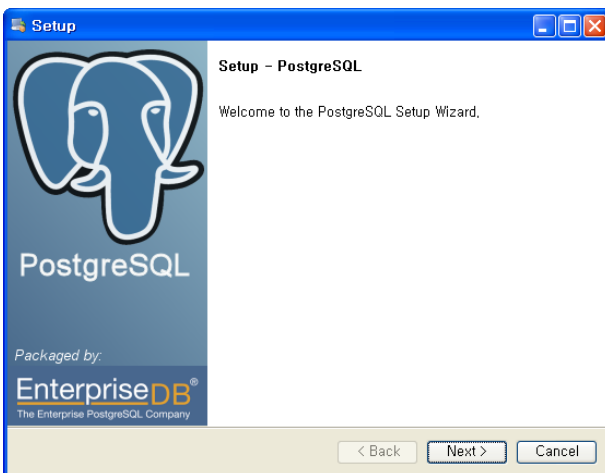
- PostgreSQL DBMS (PostgreSQL Global Development Group)
- Apache HTTP Server (The Apache Software Foundation)
- PHP Hypertext Preprocessor (The PHP Group) : required version 5.2.X
- Zend Optimizer (Zend Technologies Ltd.)
- Microsoft Message Queue (Microsoft Corporation)
- iPECS-NMS Installation Package (Ericsson-LG)

Software components listed above should be installed in the sequence described in this document. Since there are additional configurations during the installation procedure, the installer should read this section carefully before starting software installation.

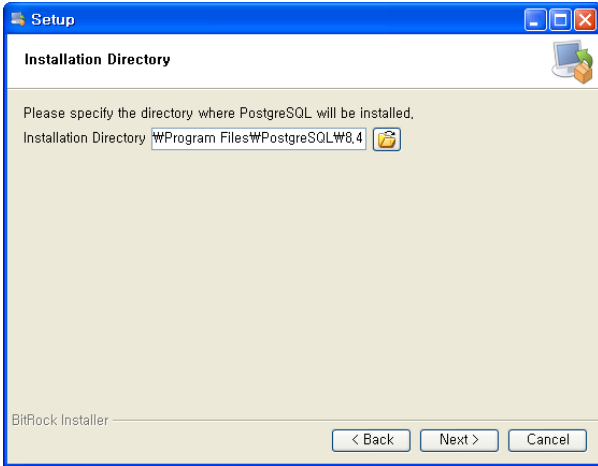
2.2.2 Installing Software Components

< PostgreSQL Installation >

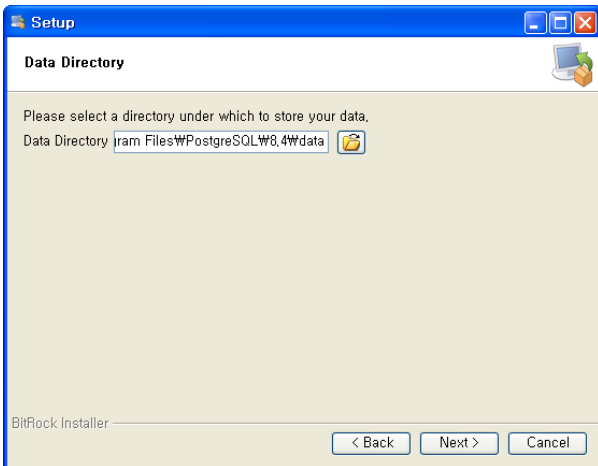
After decompressing the 'PostgreSQL' software into a temporary folder, double-click on 'postgresql-8.4.9-1-windows.exe' file to start the installation procedure (8.4.9 is the software version in this manual).



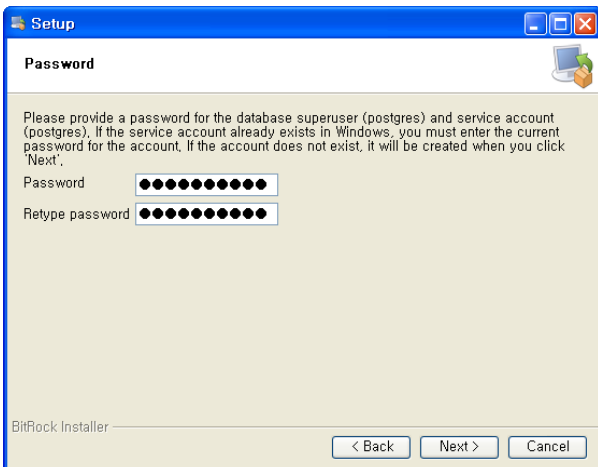
On the Setup - PostgreSQL window, click [Next] to proceed.



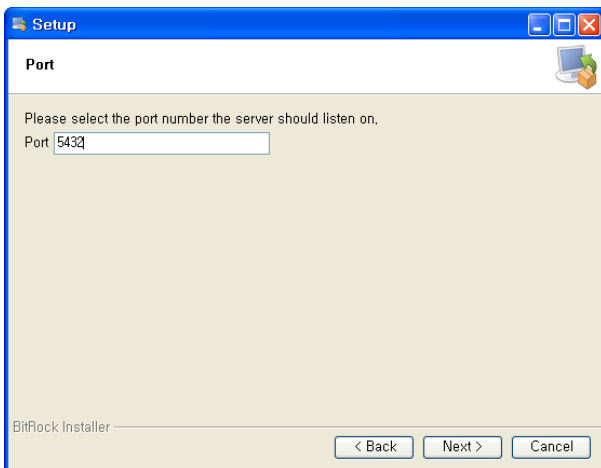
On the Installation Directory screen, note the default location for the PostgreSQL files, or click on the folder icon to select a directory where the files should be installed. Click [Next >] to continue.



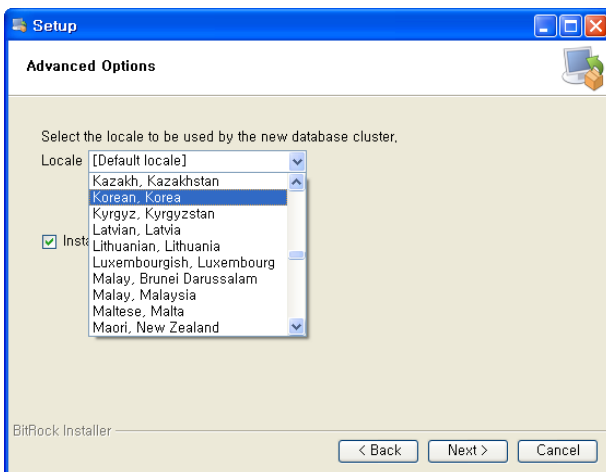
On the Data Directory screen, note the default location for your data, or click on the folder icon to select a directory where your data should be stored. Click [Next >] to continue.



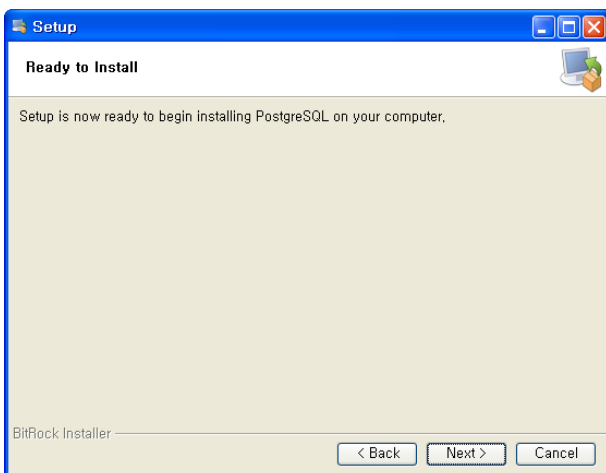
'Password' field value should be noted because they will be used for 'iPECS-NMS Control' program when configuring 'Database User Information'.



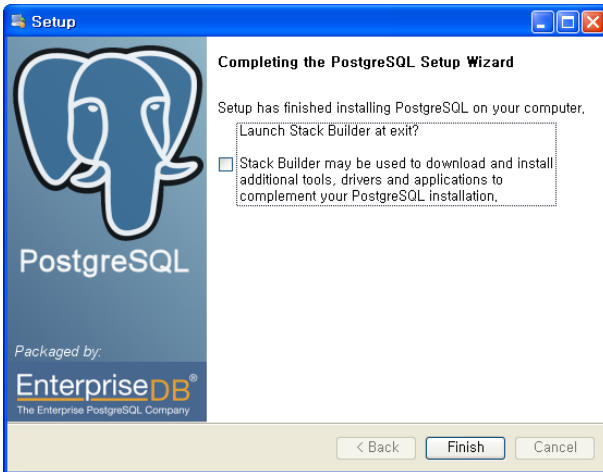
On the port screen, enter the port number the server should listened on, and click [Next].



On the Advanced Options, select the locale to be used and click [Next >].



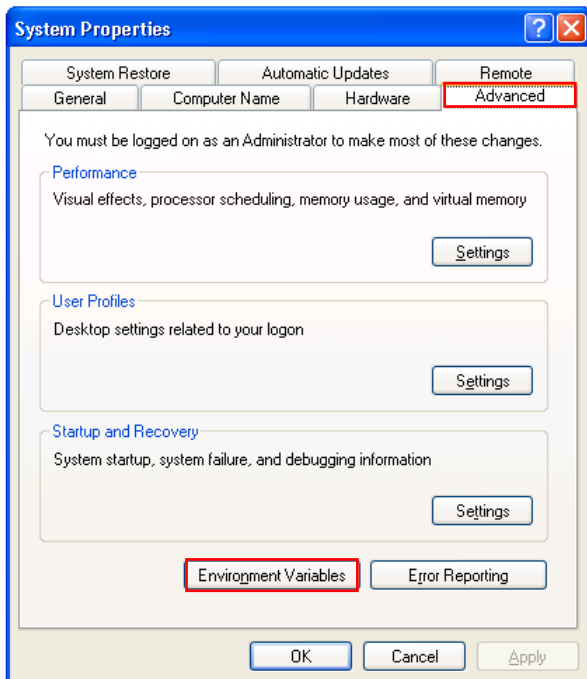
When the ready to install screen appears, click [Next >] to begin the installation.



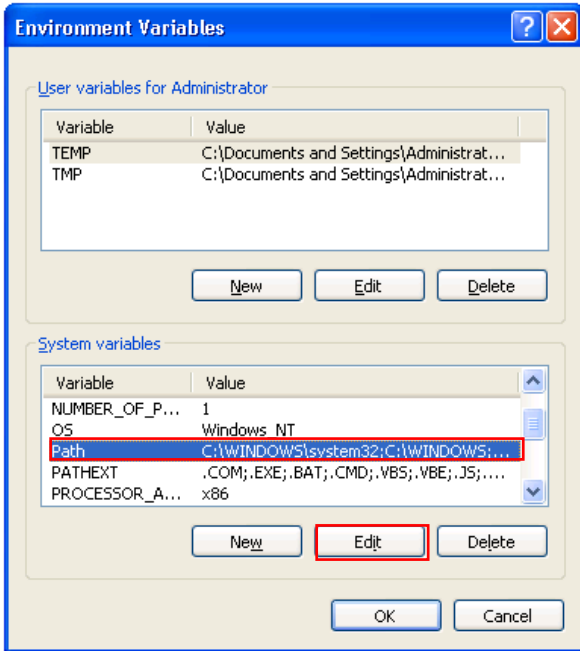
After the Setup is completed, the Setup Complete screen will be displayed; click [Finish]. (Because Stack Builder does not need to be executed, 'Launch Stack Builder at exit' check-box may be unchecked before finishing.)

In order for 3rd-party applications like iPECS NMS to use 'PostgreSQL', a path to the 'PostgreSQL' binary files folder must be set-up. 'PostgreSQL' does not configure the Path during the installation procedure, so this should be done manually.

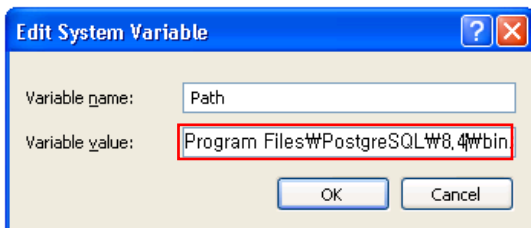
To set-up the Path, perform the following steps :



Access the 'Control Panel' → 'System Properties', and click on the 'Advanced' tab. Then, click on the [Environment Variables] button at the bottom of the screen.



In the System variables pane, select the Path variable item, and then click [Edit].



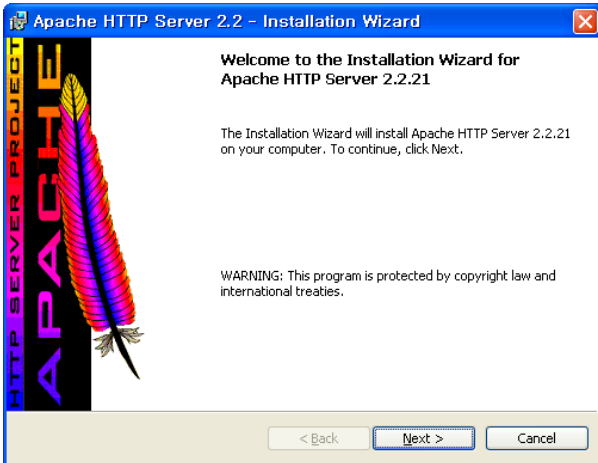
On the Edit System Variable screen, check if the 'bin' directory of PostgreSQL already exists in the Variable value field. If it does not exist, append the directory name of the 'bin' folder at the end of the path variable, and then click [OK].

NOTE - When entering the path to the PostgreSQL 'bin' folder, type a semicolon (;) at the end of the variable, and then the directory name of 'bin' folder. In this example, the ';C:\WProgram Files\Postgres\PostgreSQL\8.4\bin' string was appended at the end of the 'Path' variable.

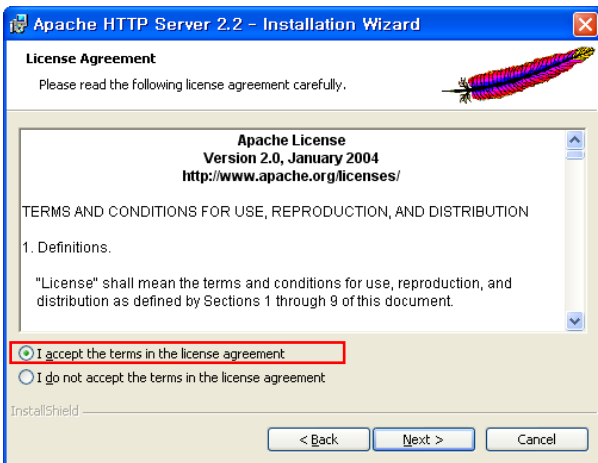
The modified 'Path' variable is applied after restarting Windows. However, since the new 'Path' is not required until the iPECS NMS Control program is executed, continue the installation without restarting Windows at this time.

< Apache HTTP Server Installation >

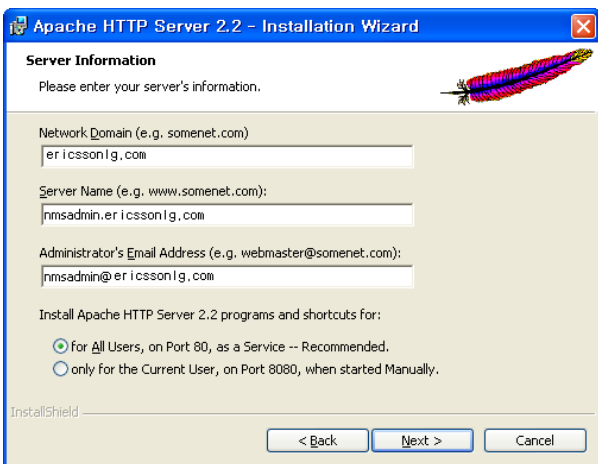
Double-click on the 'apache_2.2.21-win32-x86-no_ssl.msi' or 'httpd-2.2.21-win32-x86-openssl-0.9.8r.msi' file (2.2.21 or 0.9.8 is the software version used in this manual).



Click [Next >] button to proceed with the installation.



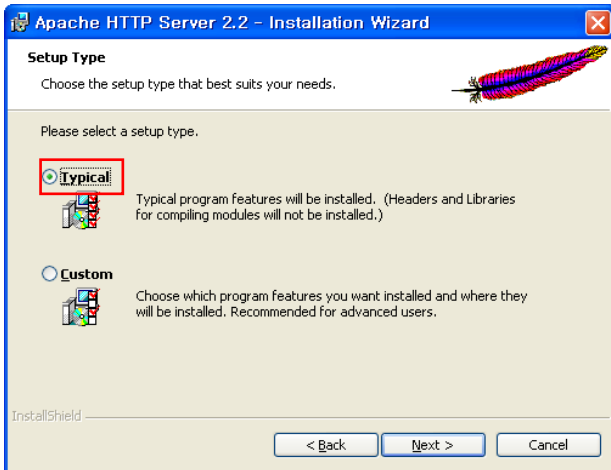
Read the 'Apache License' notes within the License Agreement screen; click [I accept the terms in the license agreement] to accept the terms and then click [Next >] button to proceed. A 'Read This First' screen will display. Once you have read the screen, click [Next >].



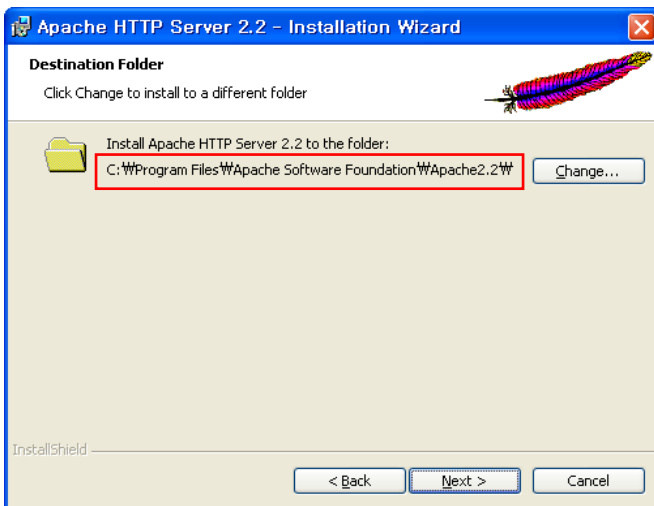
In the Server Information screen, fill in the blanks for ‘Network Domain’, ‘Server Name’, and ‘Administrator’s Email Address’ fields:

- Administrator’s Email Address’ field must be entered.
- If HTTP port 80 (the normal HTTP server port) is to be used, select [for All Users, on Port 80, as a Service – Recommended].

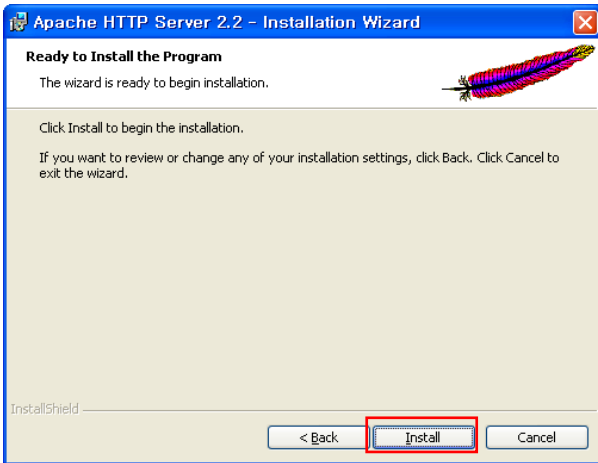
When finished, click [Next >] to proceed.



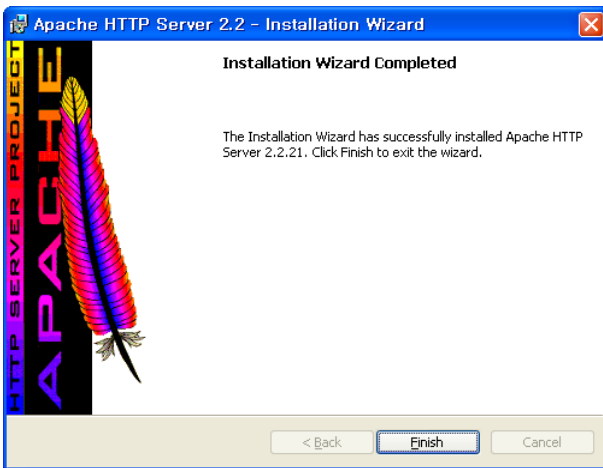
Select the type of installation; if customized installation is not needed, select [Typical] and click [Next >].



On the ‘Destination Folder’ screen, note the default location for the Apache HTTP Server files, or click on the Change button to select a folder where the files should be installed. Click [Next >] to continue.

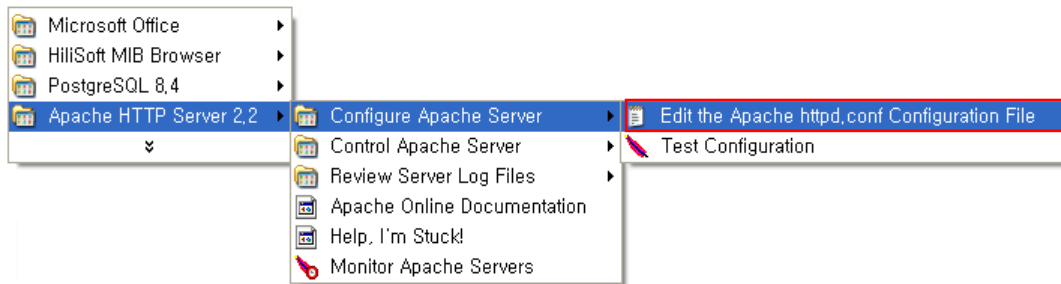


Click [Install] on the ‘Ready to Install the Program’ window to start installation.



When done, the ‘Installation Wizard Completed’ screen will appear; click [Finish].

As the last Installation step, you may wish to modify the Server Side Includes (SSI) related configuration for better security of the Server and AcceptEx related configuration for more stable communication with ‘Apache HTTP Server’. SSI exists in HTML files and makes it possible to provide dynamic Web pages. However, because it can be used to execute CGI scripts or shell commands in the Web server, the server may be vulnerable to security attacks. The use of AcceptEx may cause a communication slow-down problem in some cases, and so it is desirable to disable the use of AcceptEx in Apache HTTP Server. In order to remedy these situations, the Apache HTTP Server (httpd.conf) configuration file should be modified:



From the Windows Start menu, select 'Apache HTTP Server 2.2' → 'Configure Apache Server' → 'Edit the Apache httpd.conf Configuration File'; Or, open 'Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf' using 'Notepad' or other text editor program.

```
#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs">
  #
  # Possible values for the Options directive are "None", "All",
  # or any combination of:
  #   Indexes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
  #
  # Note that "MultiViews" must be named *explicitly* --- "Options All"
  # doesn't give it to you.
  #
  # The Options directive is both complicated and important. Please see
  # http://httpd.apache.org/docs/2.2/mod/core.html#options
  # for more information.
  #
  # Options Indexes FollowSymLinks
  Options IncludesNoExec
#
# AllowOverride controls what directives may be placed in .htaccess files.
# It can be "All", "None", or any combination of the keywords:
#   Options FileInfo AuthConfig Limit
#
AllowOverride None

#
# Controls who can get stuff from this server.
#
Order allow,deny
Allow from all
</Directory>
Win32DisableAcceptEx
#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
```

Find the 'Options Indexes FollowSymLinks' option string in the opened configuration file (httpd.conf), and comment (disable) it by typing the pound sign (#) before the beginning of the string as shown in the screen capture (shown). Then, type 'Options IncludesNoExec' on the next line; Win32DisableAcceptEx can be inserted after the '</Directory>' line as in the example below, or appended at the end of the file.

```

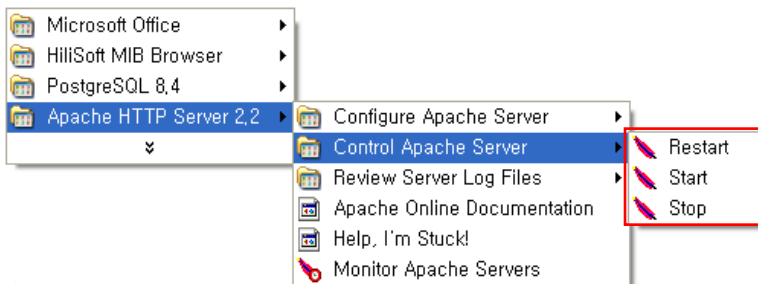
<IfModule log_config_module>
#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t %r" "%s %b %r" "%{Referer}i" "%{User-Agent}i" combined
LogFormat "%h %l %u %t %r" "%s %b" common

<IfModule logio_module>
# You need to enable mod_logio.c to use %I and %O
LogFormat "%h %l %u %t %r" "%s %b %r" "%{Referer}i" "%{User-Agent}i" %I %O combinedio
</IfModule>

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here. Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
# CustomLog "logs/access.log" common

#
# If you prefer a logfile with access, agent, and referer information
# (Combined Logfile Format) you can use the following directive.
#
#CustomLog "logs/access.log" combined
</IfModule>
    
```

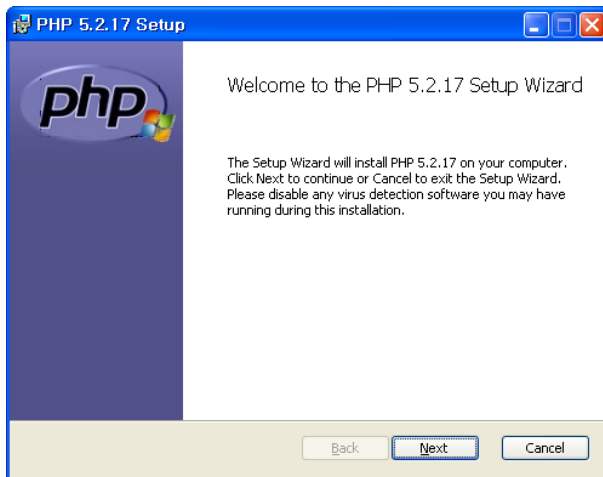
Apache HTTP Server writes the access log into the ‘access.log’ file, and the size of the file grows relatively faster depending on the number of access lines to the server. Therefore, as an option, in order to prevent unwanted waste of HDD space by disabling writes to the access log, find CustomLog “logs/access.log” common string in the configuration file (shown) and disable it by typing pound sign (‘#’) before the beginning of the string. When finished, save the configuration file and then close the text editor program.



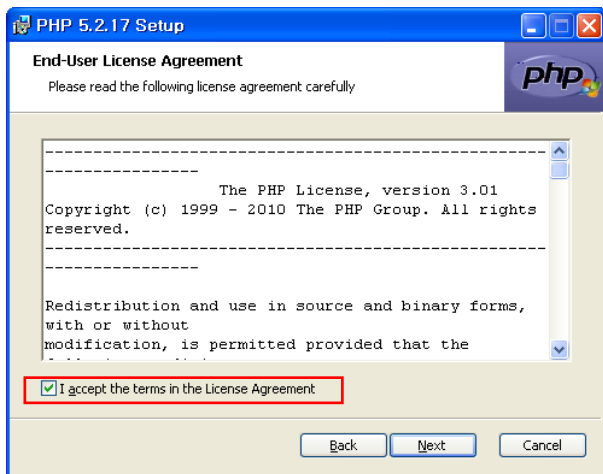
The modified configuration will be applied after restarting Windows or Apache HTTP Server 2.2. However, since the new configuration is not required until the iPECS NMS Control program is executed, continue the installation without restarting Windows at this time.

< PHP Hypertext Preprocessor Installation >

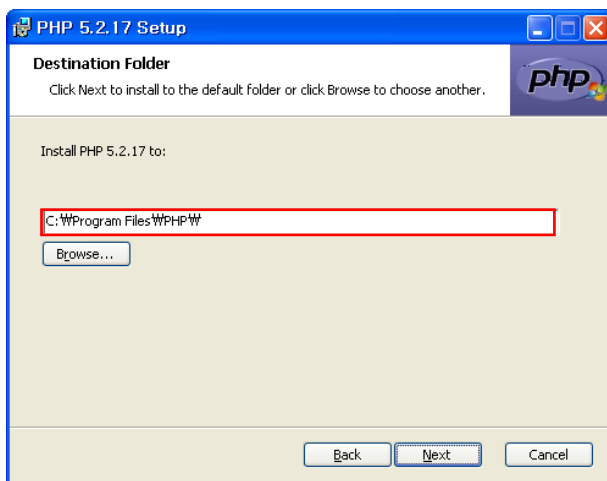
Double-click on the php-5.2.17-Win32-VC6-x86.msi file to start the PHP Hypertext Preprocessor installation procedure (5.2.17 is the software version used in this manual). The NMS require PHP 5.2.X version. Because ‘Zend Optimizer’ installed for iPECS-NMS supports PHP version upto 5.2, PHP version 5.2 should be installed even though higher version may be available.



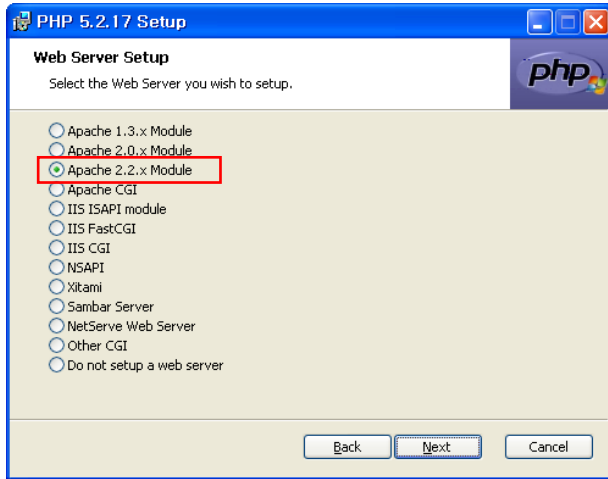
On the 'Welcome to the PHP Setup Wizard' screen, click [Next] to proceed.



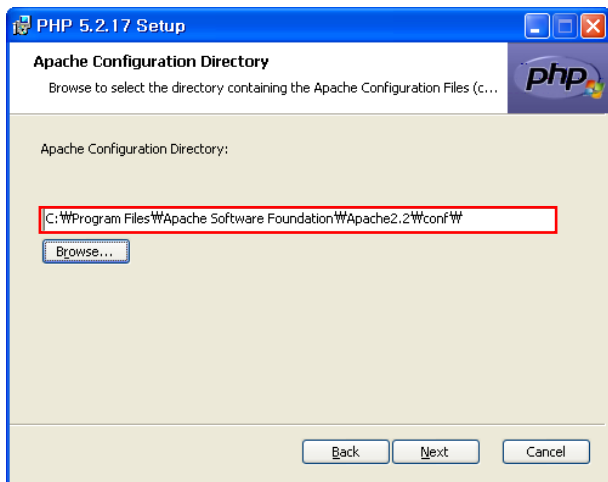
First read the PHP License within the End-User License Agreement screen; click [I accept the terms in the License Agreement] to accept the terms and then click [Next >] to proceed.



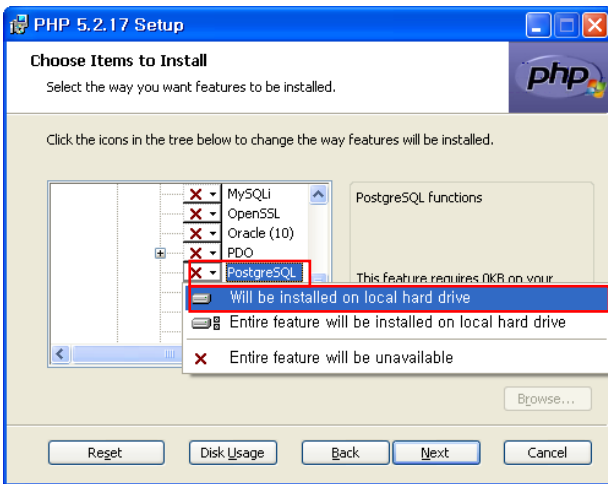
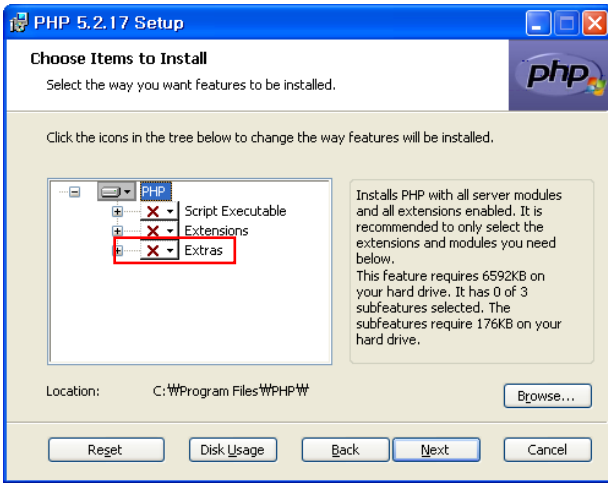
On the Destination Folder screen, note the default location for the PHP Hypertext Preprocessor, or click ‘Browse’ and enter the folder location where the files should be installed. Click [Next >] to continue.



On the Web Server Setup screen, select the web server that was installed (Apache version 2.2.21 was installed, so the ‘Apache 2.2.x Module’ is selected on the screen shot shown). Then click on the [Next] button to proceed.

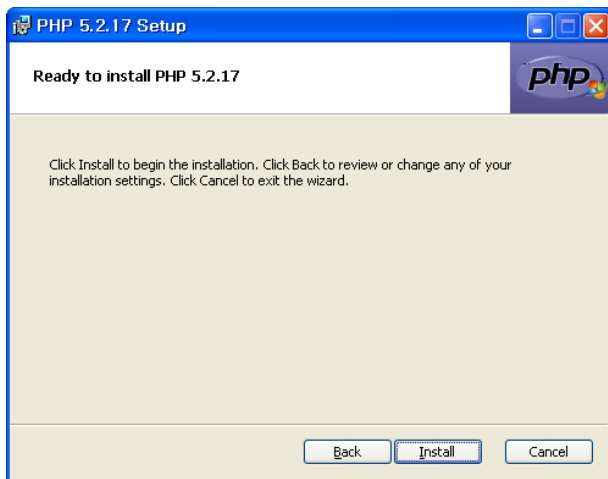


Within the Apache Configuration Directory screen, select the configuration (conf) folder in the Apache HTTP Server installation directory, and then click [Next]. In this document, ‘C:\Program Files\Apache Software Foundation\Apache2.2\conf’ directory is selected.

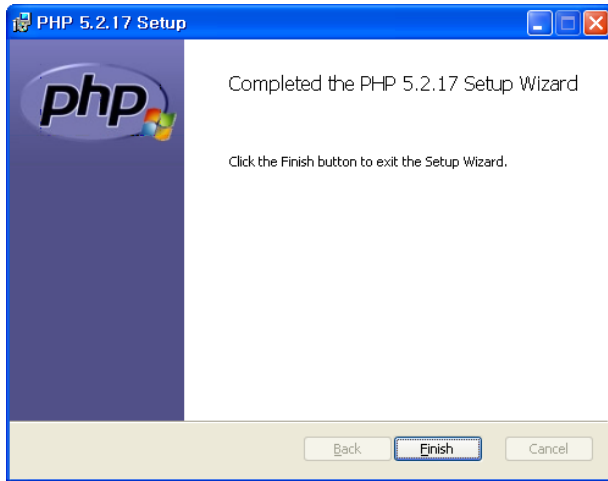


On the 'Choose Items to Install' screen, click on the expansion box to the left of the [Extensions] node to view the sub-tree.

Find the 'PostgreSQL' node on the sub-tree, and then click down arrow to show pop-up menu. Select 'Will be installed on local hard drive,' and then click [Next].

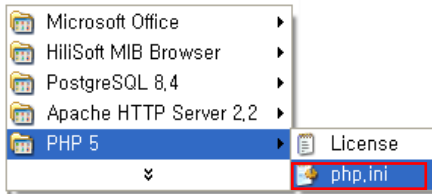


On the Ready to Install PHP screen, click [Install] to start installation.

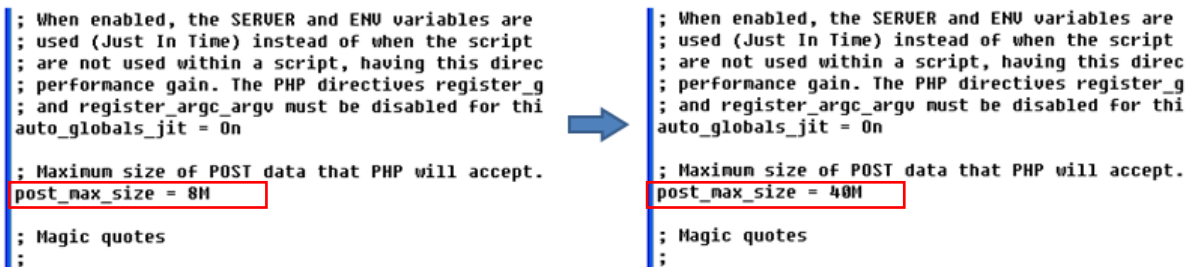


After the installation is completed, click [Finish] to complete installation process.

As the last step, in order to prevent possible file transfer failure cause by restrictive maximum file size and execution time limits from default PHP configuration, those settings in the PHP configuration file ('php.ini') should be modified.



From the Windows Start menu, select 'PHP 5' → 'php.ini' to open the PHP configuration file, Or open 'Program Files\WPHPW\php.ini' using the Notepad or other text editor program.)



Find the 'post_max_size' configuration line, and change the configuration value from 8M to 40M.

```

; File Uploads ;
; File Uploads ;
; File Uploads ;

; Whether to allow HTTP file uploads.
file_uploads = On

; Temporary directory for HTTP uploaded fi
; specified).
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
upload_max_filesize = 2M

; Maximum number of files that can be uplo
max_file_uploads = 20
    
```

➔

```

; File Uploads ;
; File Uploads ;
; File Uploads ;

; Whether to allow HTTP file uploads.
file_uploads = On

; Temporary directory for HTTP uploaded fi
; specified).
;upload_tmp_dir =

; Maximum allowed size for uploaded files.
upload_max_filesize = 40M

; Maximum number of files that can be uplo
max_file_uploads = 20
    
```

Find the 'upload_max_filesize' configuration line, and change its value from 2M to 40M.

```

; Resource Limits ;
; Resource Limits ;
; Resource Limits ;

max_execution_time = 30 ; Maximum execution
max_input_time = 60 ; Maximum amount of tin
;max_input_nesting_level = 64 ; Maximum input v
memory_limit = 128M ; Maximum amount of ne
    
```

➔

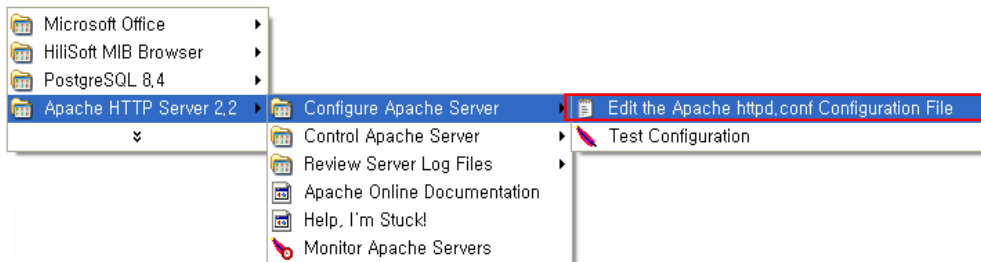
```

; Resource Limits ;
; Resource Limits ;
; Resource Limits ;

max_execution_time = 90 ; Maximum execution
max_input_time = 60 ; Maximum amount of tin
;max_input_nesting_level = 64 ; Maximum input v
memory_limit = 128M ; Maximum amount of ne
    
```

Find the configuration line of 'max_execution_time', and change its value from 30 to 90. After finishing the modification, save the configuration file and then close the text editor program.

PHP installation package modifies the configuration file of Apache HTTP Server to add its directory path during its installation process. However, because PHP may not add the correct path name, it is needed to check and correct the path if not correct.



From the Windows Start menu, select 'Apache HTTP Server 2.2' → 'Configure Apache Server' → 'Edit the Apache httpd.conf Configuration File'; Or, open 'Program Files\Apache Software Foundation\Apache2.2\conf\httpd.conf' using 'Notepad' or other text editor program).

```

#BEGIN PHP INSTALLER EDITS - REMOVE ONLY ON UNINSTALL
PHPIniDir ""
LoadModule php5_module "php5apache2_2.dll"
#END PHP INSTALLER EDITS - REMOVE ONLY ON UNINSTALL
    
```

↓

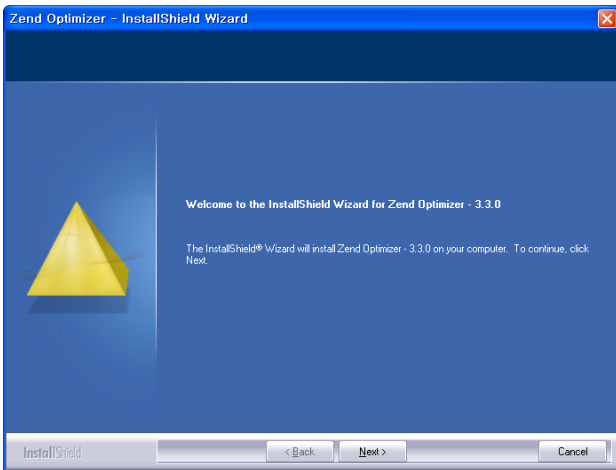
```

#BEGIN PHP INSTALLER EDITS - REMOVE ONLY ON UNINSTALL
PHPIniDir "C:\Program Files\PHP"
LoadModule php5_module "C:\Program Files\PHP\php5apache2_2.dll"
#END PHP INSTALLER EDITS - REMOVE ONLY ON UNINSTALL
    
```

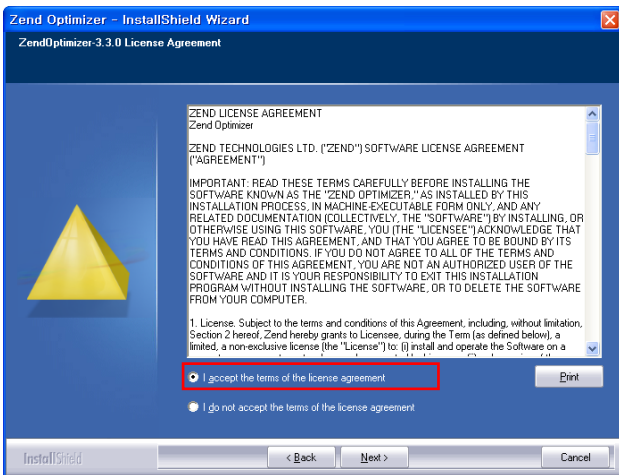
If the PHP installation paths for ‘PHPInDir’ and ‘LoadModule’ are not configured correctly in the Apache configuration file, modify the path values with correct ones and save the changes.

< Zend Optimizer Installation >

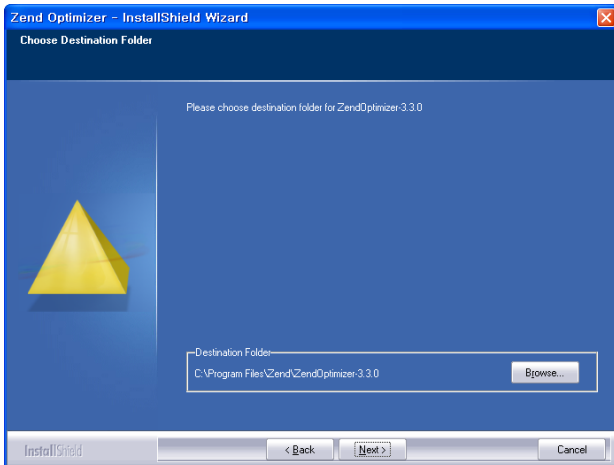
Double-click on ‘ZendOptimizer-3.3.3-Windows-i386.exe’ file (3.3.3 is the software version used in this document).



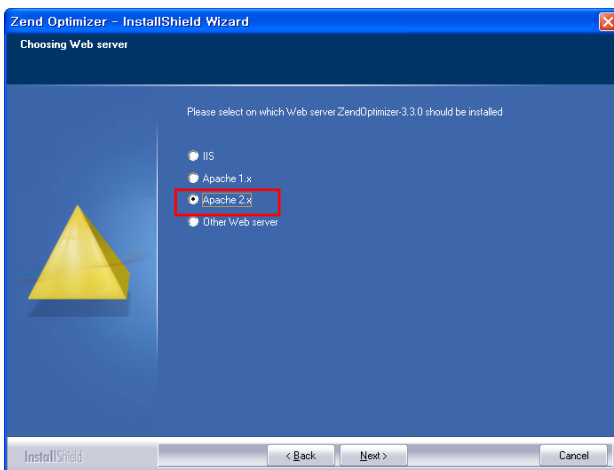
On ‘Welcome to the InstallShield Wizard’ window, click [Next >] button to proceed.



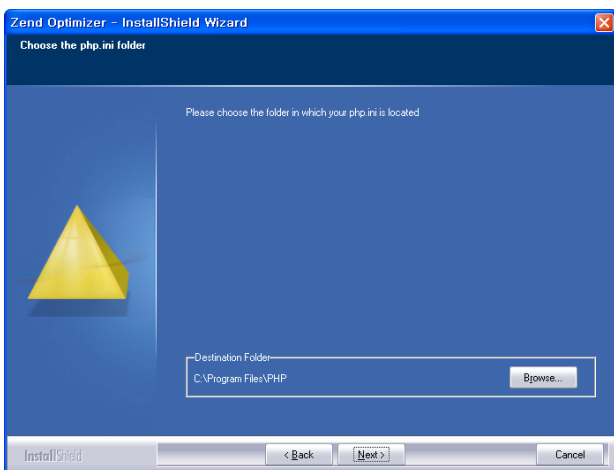
First read ‘Zend Optimizer License Agreement’ notes. If you agree to the terms and conditions, select ‘I accept the terms of the license agreement’, and click the [Next >] button.



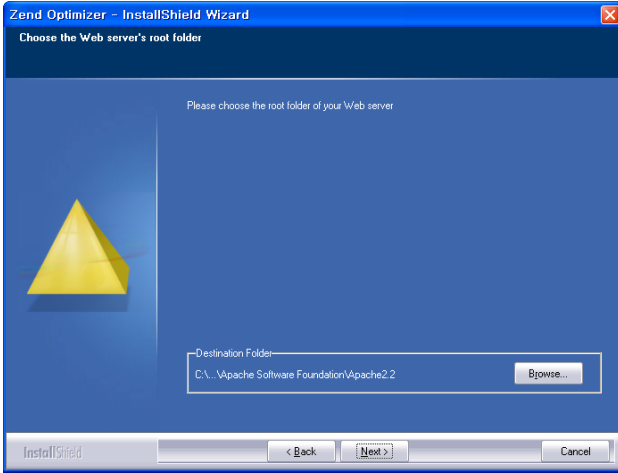
On 'Choose Destination Folder' window, select a folder in which 'Zend Optimizer' is to be installed, or note the default location for installation, then click the [Next] button.



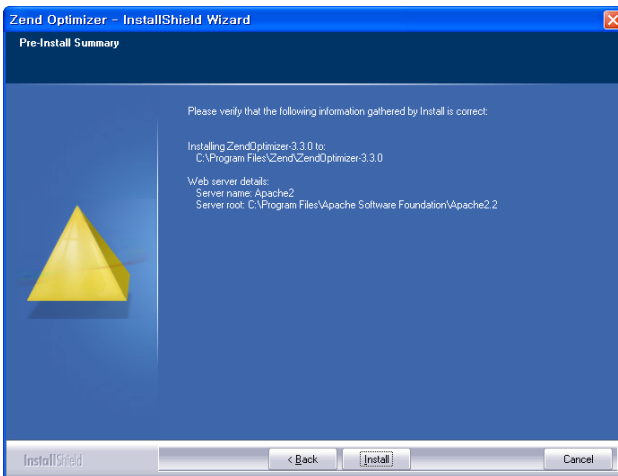
Then, on the 'Choose Web server' window, select the web server installed in the previous procedure, and then click the [Next >] button to proceed. Since Apache version 2.2.21 was installed, [Apache 2.x] is selected.



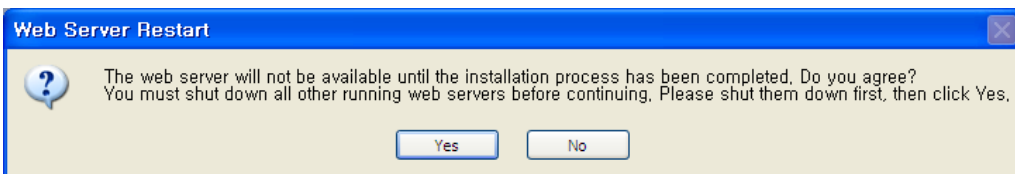
On ‘Choose the php.ini folder’ window, the directory of ‘PHP Hypertext Preprocessor’ software is configured. The ‘php.ini’ file is saved in the ‘Program Files\WPHP’ directory. After selecting (or noting the default) directory, click the [Next >] button.



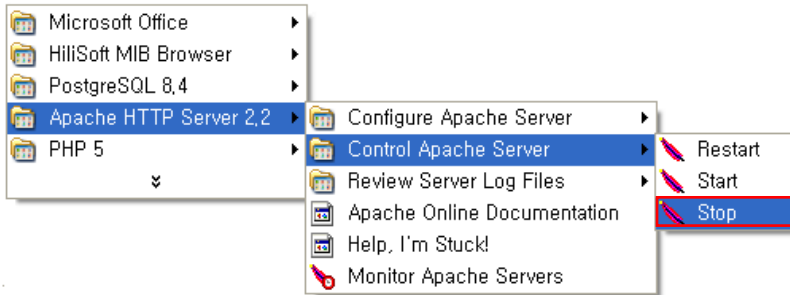
On ‘Choose the Web server root folder’ window, the ‘Apache HTTP Server’ installation folder is configured. In this document, the ‘C:\Program Files\Apache Software Foundation\Apache2.2’ directory is selected.



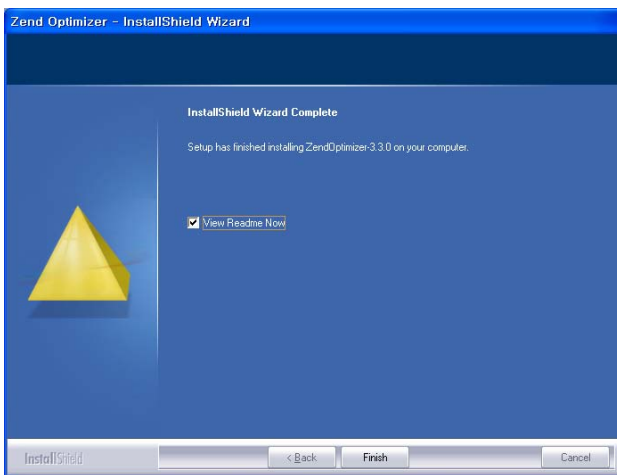
The ‘Pre-Install Summary’ window shows the settings that were configured in the previous steps. After checking all the configurations, click on the [Install] button to complete the installation of ‘Zend Optimizer’.



Following installation, the ‘Web Server Restart’ window may appear. Before clicking on the [Yes] button, you must stop the Apache HTTP Server execution by selecting ‘Apache HTTP Server 2.2 → Control Apache Server → Stop’ from the Windows Start menu. Then click on the [Yes] button.



After the installation is complete, start the Apache HTTP Server again by selecting ‘Apache HTTP Server 2.2 → Control Apache Server → Start’ from the Windows Start menu.

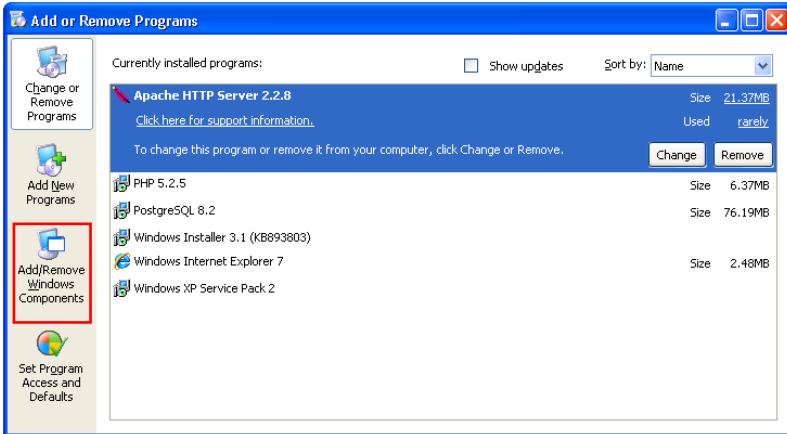


When the ‘InstallShield Wizard Complete’ window appears, click [Finish] button.

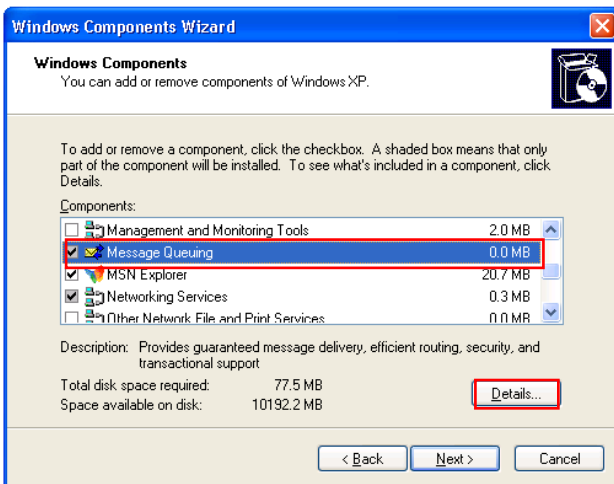
< Microsoft Message Queue (MSMQ) Installation >

iPECS NMS utilizes Microsoft Message Queue (MSMQ)—one of the software components provided with Microsoft Windows. In many cases, MSMQ is not installed when the Windows OS is installed; verify if it has been installed. In order for the MSMQ to be properly installed, the server should have a ‘Computer Name’ previously configured. Check this by viewing System Properties in the Control Panel.

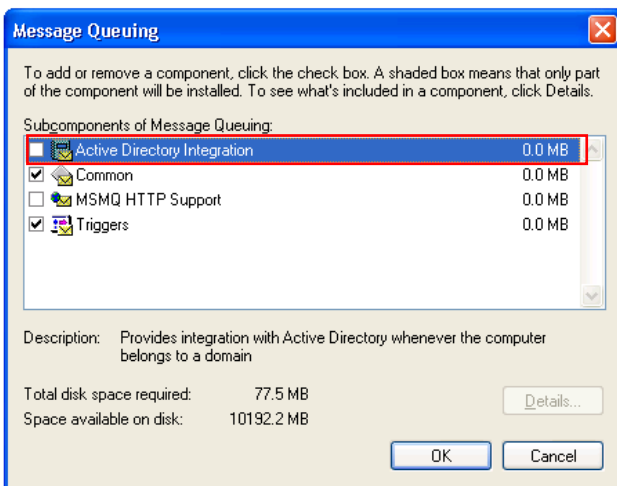
- For Windows XP Professional



To verify MSMQ installation, from the Control Panel, select ‘Add or Remove Programs’. Click ‘Add/Remove Windows Components’.



In the ‘Windows Components Wizard’ screen, locate the Message Queuing item and verify if it is installed. If it has not been installed (box is not checked), click the checkbox, and then click [Details...].



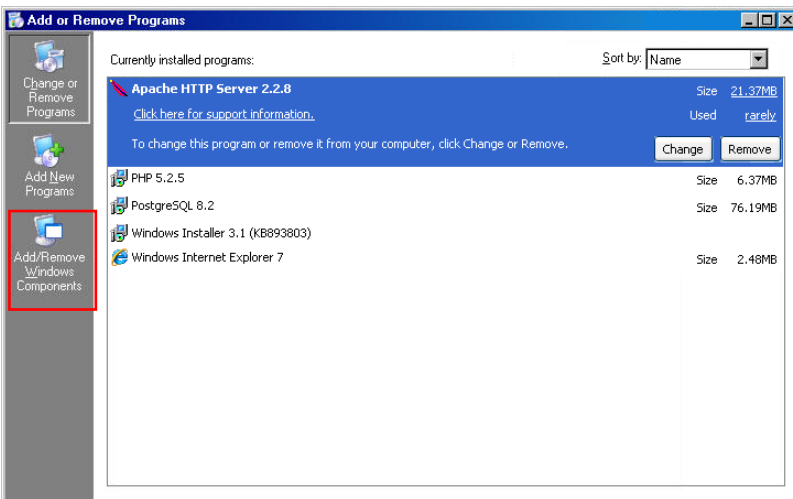
Message Queuing includes Active Directory Integration. If a domain controller or controller server that provides directory service does not exist, clear the Active Directory Integration checkbox, and click [OK].

After returning to the Windows Components screen, click the [Next >] to start installation.

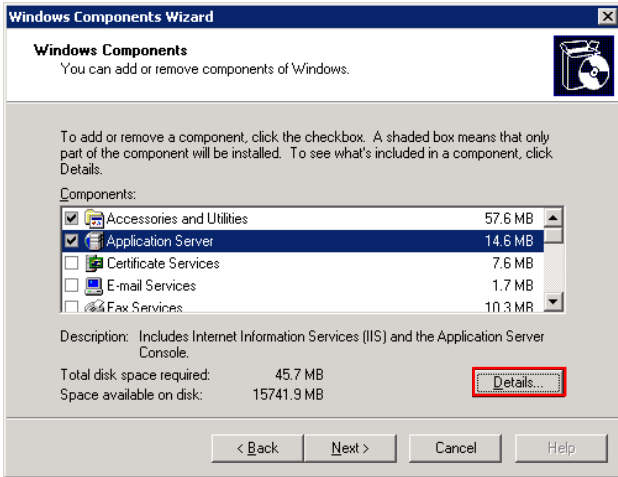


After installation is completed, click [Finish].

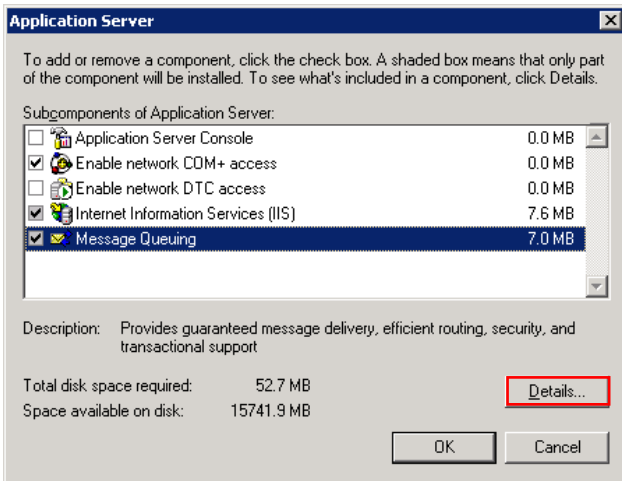
- For Windows 2003 Server



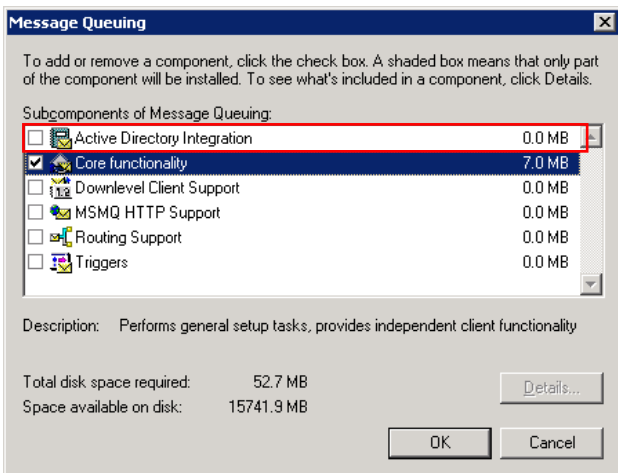
From the Control Panel, select 'Add or Remove Programs'. Click 'Add/Remove Windows Components' on 'Add or Remove Programs' window that appears.



In the Windows Components screen, click on Application Server and click [Details...].



In the 'Application Server' screen, locate the 'Message Queuing' item and verify it is installed. If it is not installed (box is not checked), click on checkbox, and then click [Details...].



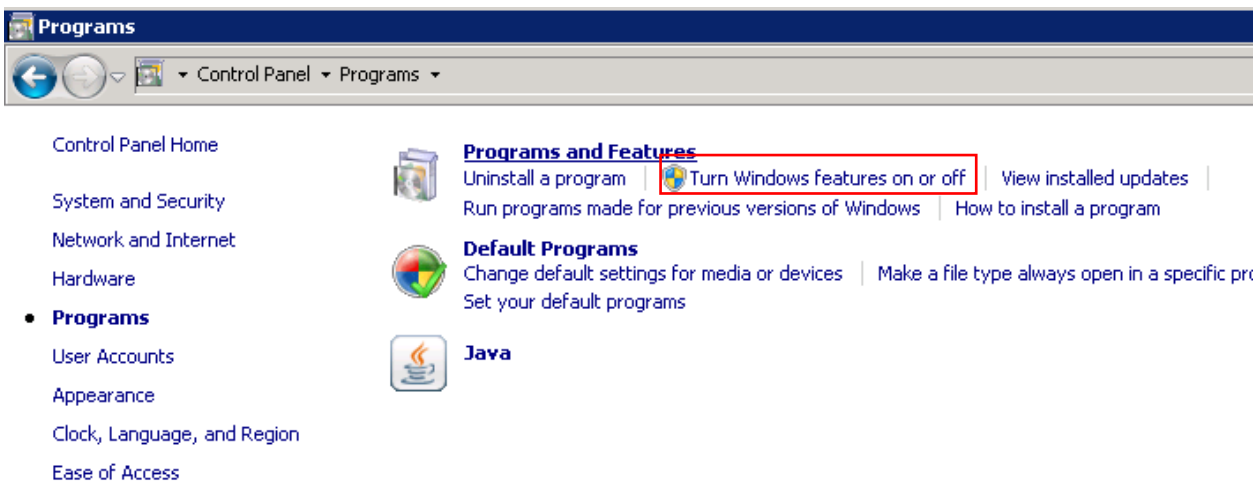
'Message Queuing' includes 'Active Directory integration'. If a domain controller or controller server that provides directory service does not exist, clear the 'Active Directory Integration' checkbox, and click [OK].

After returning to the Windows Components screen, click [Next >] to start installation.

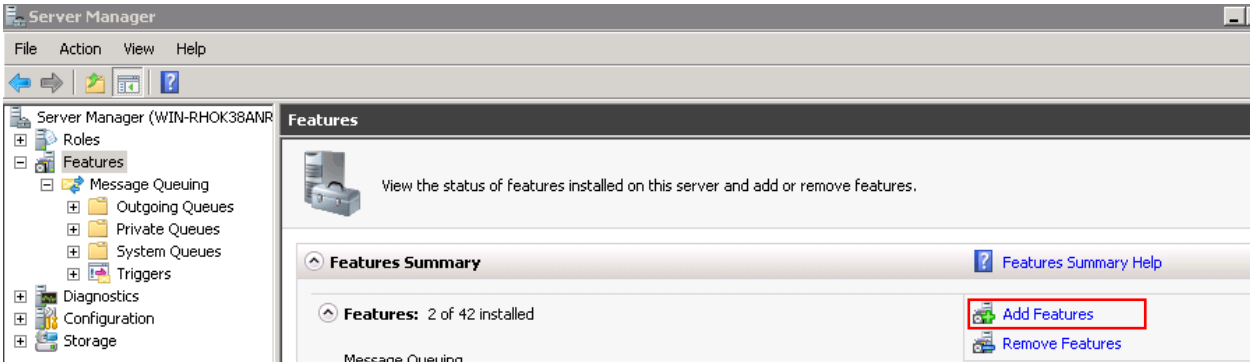


After the installation is completed, click [Finish] to complete the installation procedure.

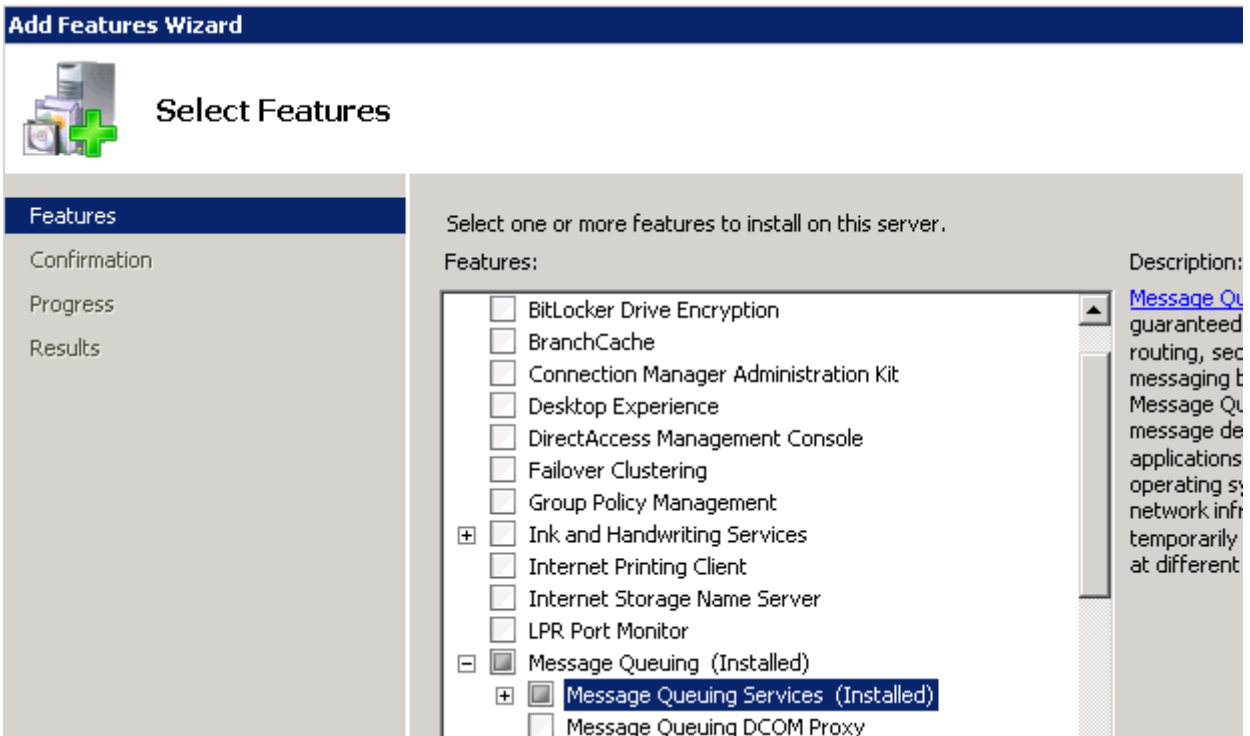
- For Windows 2008 Server



From the Control Panel, select 'Programs'. Click 'Turn Windows features on or off' on 'Programs' window that appears.



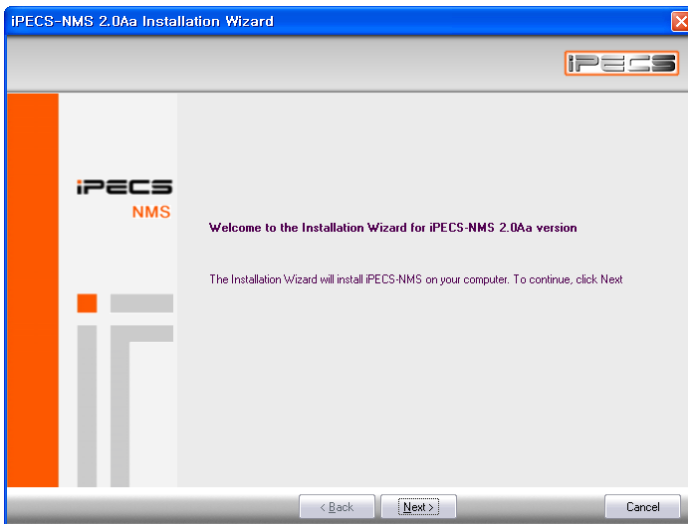
In the 'Server Manager' windows, select 'Features' and click 'Add Features'.



In the 'Add Features Wizard' screen, locate the 'Message Queuing Services' item and verify it is installed. If it is not installed (box is not checked), click on checkbox and install it.

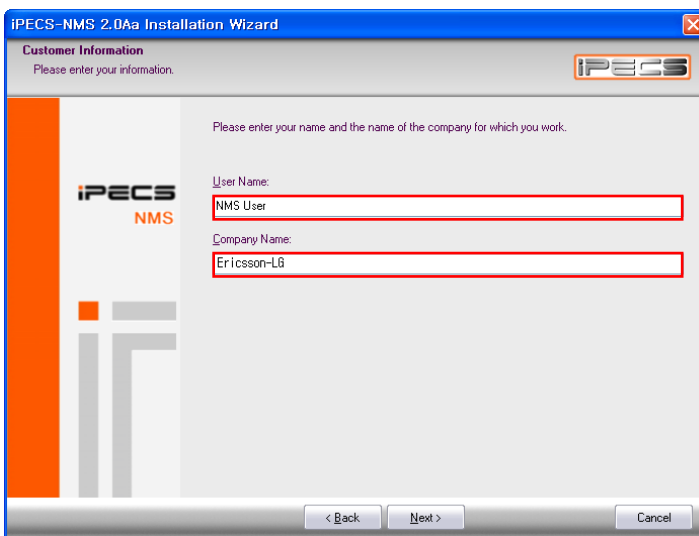
< iPECS-NMS Software Package Installation >

Click iPECS_NMS_Setup.exe file to start installation; the InstallShield Wizard screen should display.

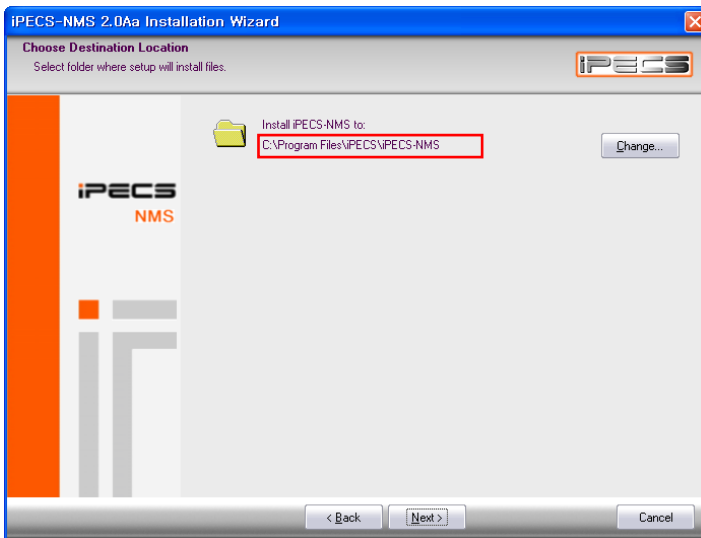


Click [Next >] to proceed.

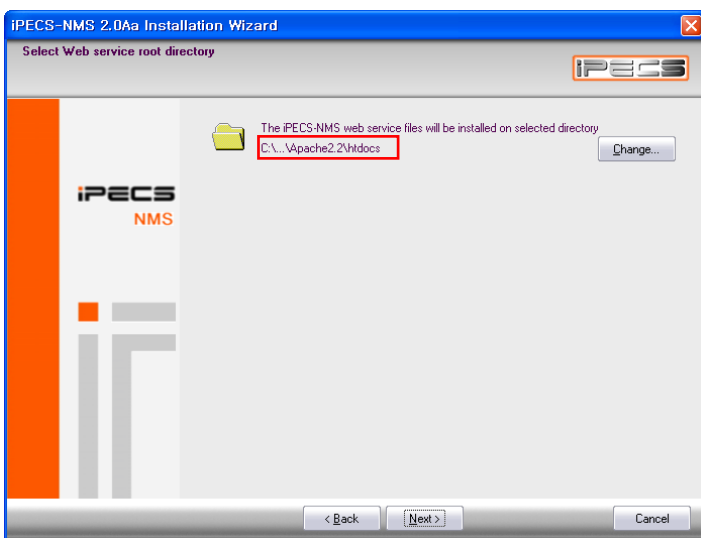
NOTE - If required software components have not been properly installed or iPECS-NMS Service is installed and running, a warning message may appear. In this case, verify installation of required software or terminate the iPECS-NMS Service, and then restart the installation procedure.



In the Customer Information window, enter the User Name and Company Name fields, and click [Next].

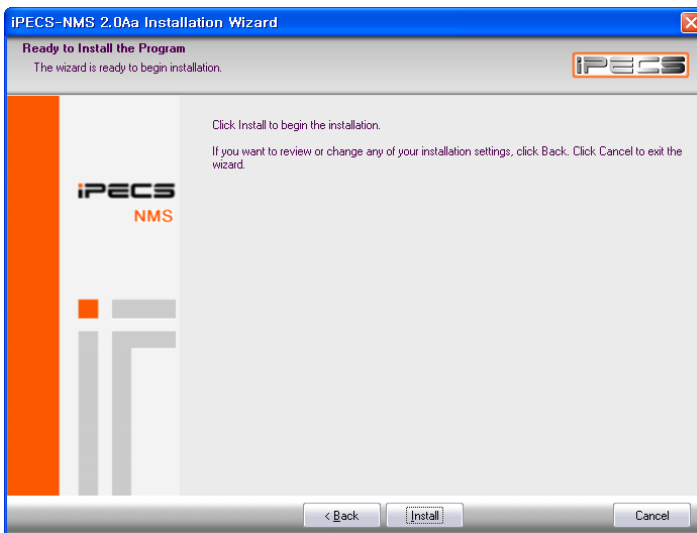


Normally the default destination location for program files need not be modified, click [Next>] to continue. If a different destination is desired, click [Change] and select the new location, and then click [Next >].

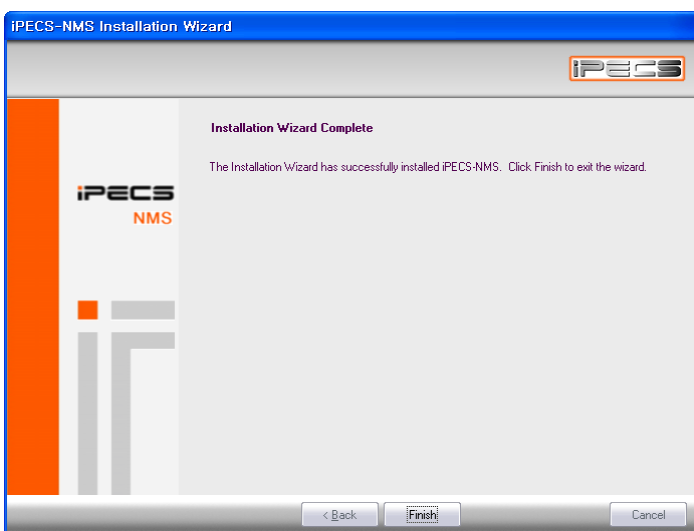


On the Select Web service root directory screen, select the 'htdocs' folder under the Apache HTTP Server installation directory, 'Apache Software Foundation\Apache2.2\htdocs' was used in this example. After the folder is chosen, click [Next >] to proceed.

NOTE - If the location for the Apache server files was changed, that directory should be selected by clicking [Change...].



Click [Install] to begin software installation.



After the installation is completed, click [Finish].

To apply changed configurations, restart your computer.

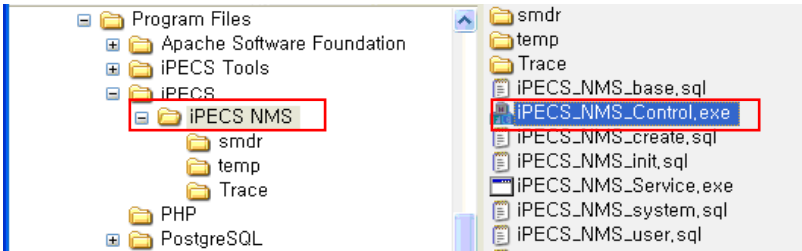
< Executing iPECS-NMS Application >

The iPECS-NMS application is comprised of two programs :

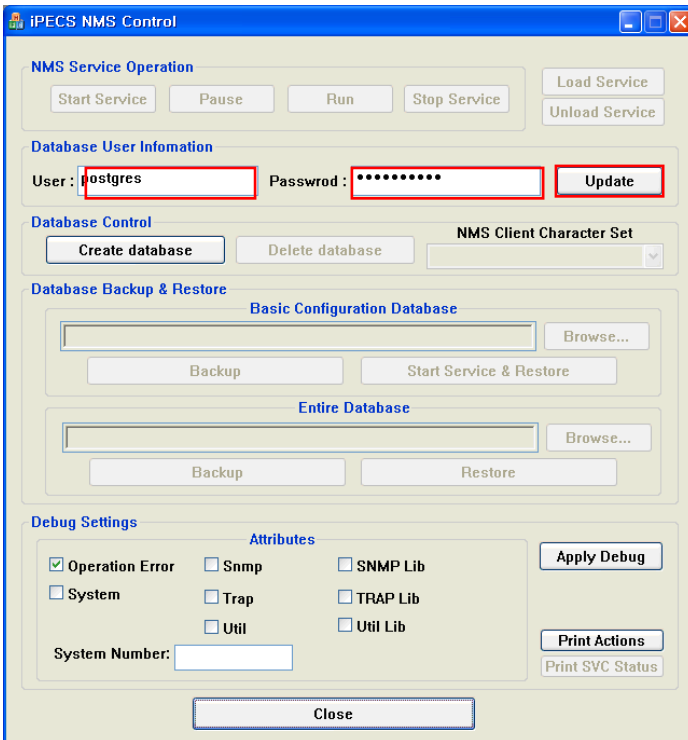
- iPECS-NMS Control' (iPECS_NMS_Control.exe)
- iPECS-NMS Service' (iPECS_NMS_Service.exe)

iPECS NMS Service is the main program, which runs as a Windows Service application. iPECS-NMS Control registers iPECS-NMS Service to the Windows Service list and manages the NMS Service operation and database.

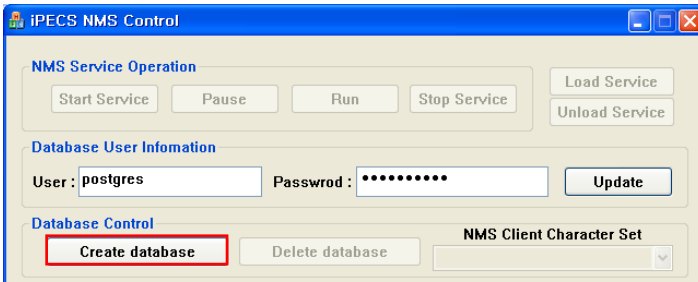
For registration and execution of iPECS-NMS Service, perform the following steps.



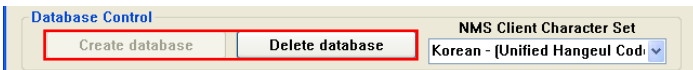
In the iPECS-NMS installation folder (Program Files\WiPECS\WiPECS NMS), locate the 'iPECS_NMS_Control.exe' file and double-click to execute it. (Or, from the Windows Start menu, select iPECS → iPECS NMS → Launch iPECS_NMS_Control.exe to execute it.)



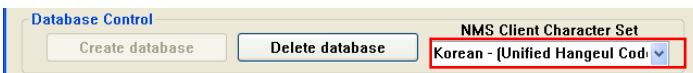
Within the NMS Control screen, enter the User and Password fields using the Superuser Name and Password configured during the installation of the 'PostgreSQL' software. The values 'postgres' and 'postgrespw' were used in this example. Click [Update] when finished making entries.



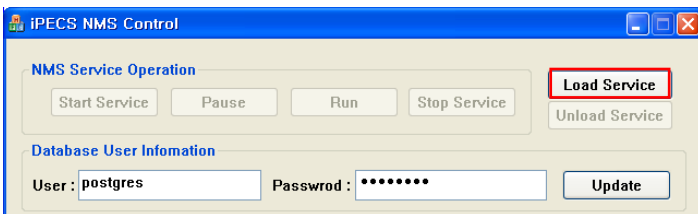
After the two fields are configured, Create Database activates. The NMS local database should be created before registering and executing iPECS-NMS Service. Click the [Create Database] button.



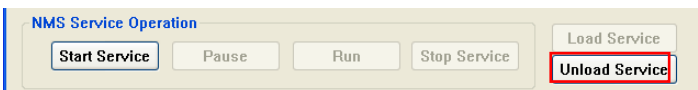
If a local database already exists, the [Delete Database] is present instead of the [Create Database] button. [Delete Database] should be used with caution; when selected, all information stored in the database is permanently removed.



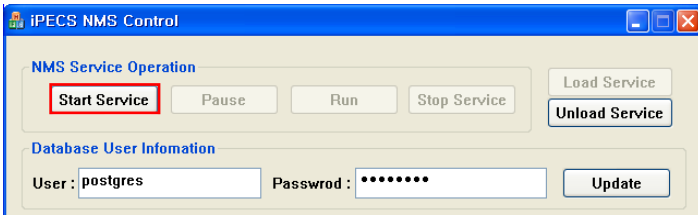
The NMS Client Character Set field normally need not be changed from the default value provided by iPECS-NMS Control. However, in some cases the character set used in the NMS server might not be supported by the PostgreSQL database. If this problem should occur, an error message may appear. Select an appropriate Character set from the drop-down list, as needed.



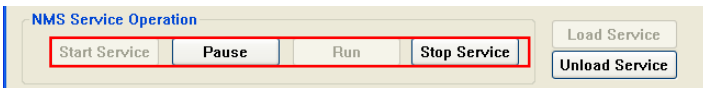
If a local database was successfully created, the [Load Service] button will activate; click [Load Service] to register the iPECS-NMS Service to the Windows Service list.



After the iPECS-NMS Service registers, the [Load Service] button will deactivate, and the [Unload Service] and [Start Service] buttons will activate.



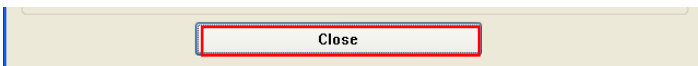
Click [Start Service] to execute the iPECS-NMS Service program as a Windows Service.



When running, the [Start Service] button will deactivate and the [Pause] and [Stop Service] buttons will activate.

Neither [Stop Service] nor [Pause] should be required for normal operation:

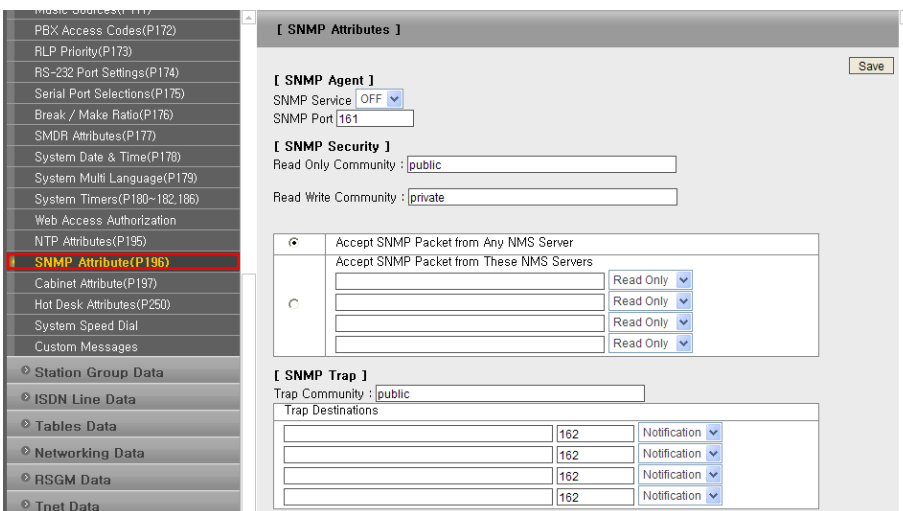
- [Stop Service] terminates iPECS NMS.
- [Pause] temporarily suspends execution of the iPECS-NMS Service program.



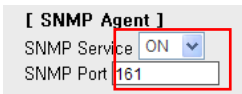
Click [Close] to exit the iPECS-NMS Control program; the control program does not need to be running while the iPECS-NMS Service is in use.

2.3 iPECS System Admin Configuration

Before registering iPECS systems to the iPECS-NMS, NMS-related system admin fields should be configured. After logging-in to iPECS Web Admin, click 'SNMP Attribute (P196)' from the System Data list to enter the NMS configuration page. In iPECS-MG Web Admin, 'SNMP Data' is on the top level menu.

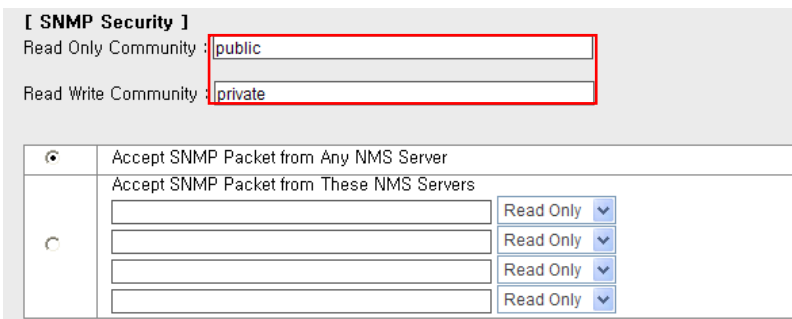


NMS-related system admin screen is categorized into three parts of ‘SNMP Agent’, ‘SNMP Security’ and ‘SNMP Trap’ configurations



SNMP Service field is used for enabling or disabling (ON or OFF) the SNMP agent service running on MFIM(MPB); this field should be set to ‘ON’ for communication with iPECS-NMS using SNMP protocol.

SNMP Port – Standard SNMP port number 161 should be used unless there is a specific reason for changing this port number.



SNMP community and NMS server IP address can be configured; the SNMP community designates a SNMP communication group to which an SNMP message belongs, and is also a logical relationship between the SNMP agent (MFIM/MPB) and SNMP manager (NMS).

- Read Only Community – defines a community string that should be used when SNMP manager (NMS) is trying to read data from the SNMP agent (MFIM/MPB), and its default value is set to ‘public’.
- Read Write Community – is used for both read and write data by the SNMP manager (NMS), and its default value is ‘private’. This value should be the same as set up on the iPECS-NMS community string (default value is ‘private’, but could be changed following installation as needed).
- Accept SNMP Packet from Any NMS Server – if IP Address is not fixed, click to accept SNMP packets from any SNMP manager (or from any IP address), or
- Accept SNMP Packets from These NMS Servers – if IP Address is fixed, click to designate IP addresses to be allowed and the method of data transaction (Read Only / Read Write).

[SNMP Security]
 Read Only Community : public
 Read Write Community : private

<input type="radio"/>	Accept SNMP Packet from Any NMS Server
<input checked="" type="radio"/>	Accept SNMP Packet from These NMS Servers
	150.150.140.82 Read Write
	Read Only
	Read Write
	Read Only
	Read Only

SNMP Trap configuration is for setting the destination IP address to which Trap messages (ex., alarm/fault events) are to be sent from the SNMP agent (MFIM/MPB) and their SNMP community privileges.

NOTE – For IP address of iPECS-NMS server, ‘Read Write’ privilege should be selected.

[SNMP Trap]
 Trap Community : public

Trap Destinations		
150.150.140.82	162	Notification
	162	Notification
	162	Inform
	162	Trap
	162	Notification

Trap Community – designates a Trap communication group to which a Trap message belongs, and is also a logical relationship between the SNMP agent (MFIM/MPB), and SNMP manager (NMS). This value should be same as the Trap community string defined in iPECS-NMS in order for the Trap messages sent from SNMP agent to be accepted by the iPECS-NMS server.

NOTE – Trap communities should be set-up same for all the iPECS systems registered to an iPECS-NMS server (default=public, but could be changed following installation as needed), whereas the SNMP community may be defined with different strings for each iPECS system.

- Trap Destination – is for designating the IP address of the iPECS-NMS server, the Trap port number (default=162), and the Trap type field (Notification, Inform, and Trap).

Notification – defined in SNMPv2c that is sent once without checking the reception of the message.

Inform – similar to Notification, but checks the reception of the message using a Response message sent from the receiving SNMP manager (NMS); messages not transmitting a response will be assumed lost and will be sent again (ex., used in an unstable network where there is packet loss, but may decrease network performance when too many messages are present in the MFIM(MPB)).

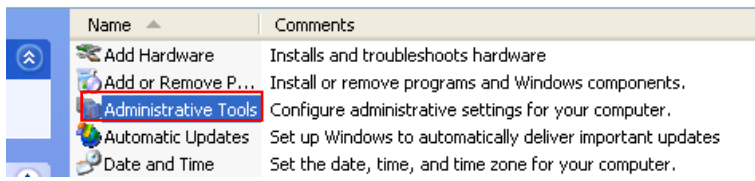
Trap – defined in SNMPv1, but because iPECS-NMS and the SNMP agent on MFIM(MPB) use SNMPv2c, it is not recommended.

After finishing all configurations, click on the [Save] button to save and apply the field values.

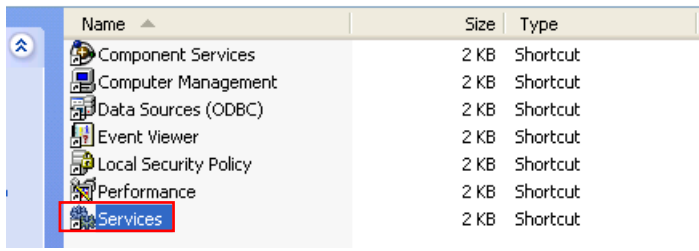
3. Getting Started

3.1 Checking Windows Service Status

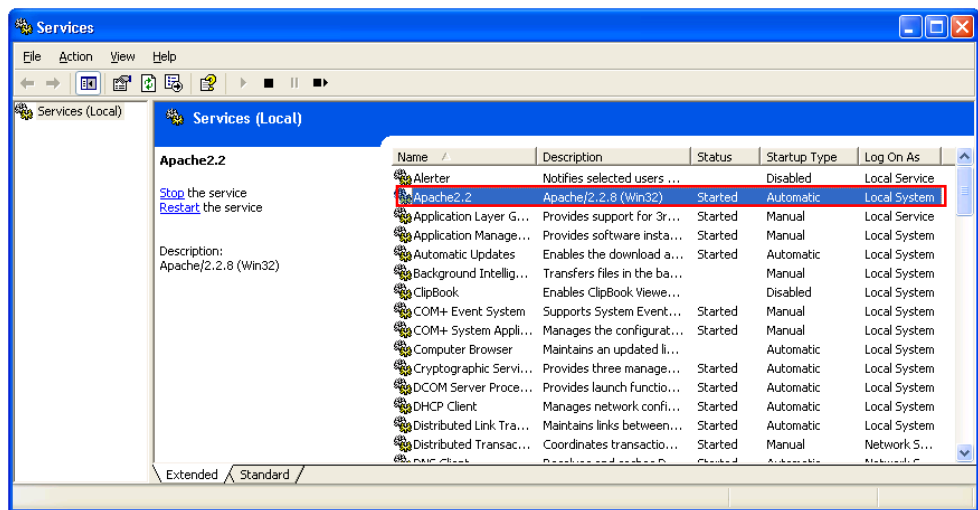
In order for iPECS-NMS to execute properly, verify that Apache HTTP Server, PostgreSQL Database Server, and iPECS-NMS are all running as Windows services. These Windows services may start automatically when the server is restarted, or may be manually controlled using the Windows ‘Administrative Tools’ for services.



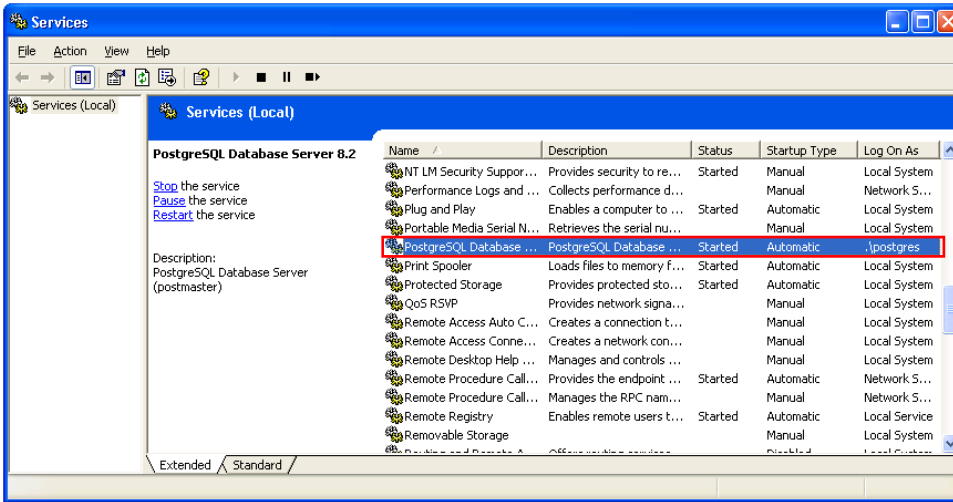
From the Windows Control Panel, double-click on ‘Administrative Tools’.



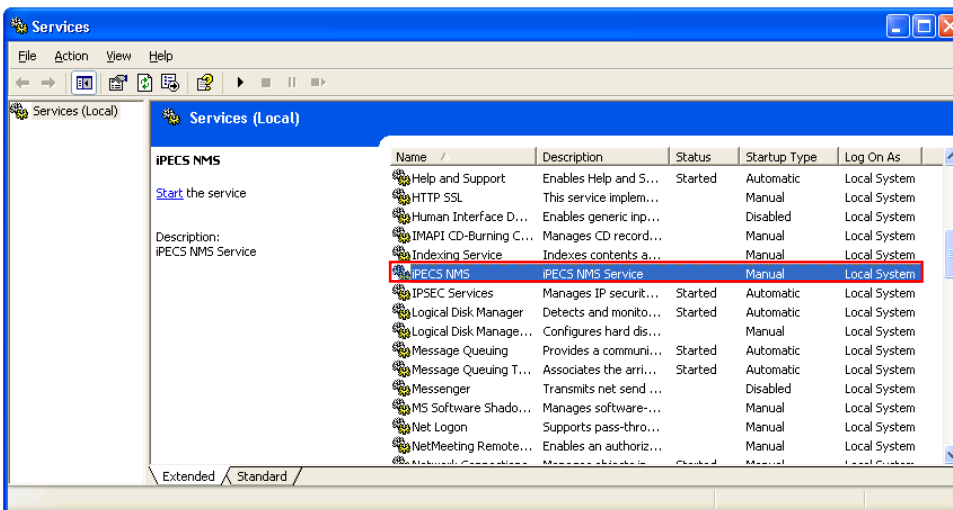
Next, double-click on ‘Services’ in the list of available tools.



On the ‘Services’ window, user may check or modify the status of services. The picture above shows ‘Apache 2.2’ service is in ‘Started’ status, and its startup type is ‘Automatic’.



In the same way, the status of ‘PostgreSQL Database Server’ can be checked, and ‘Log On As’ field shows the account name that was used for log-on to the PostgreSQL database.



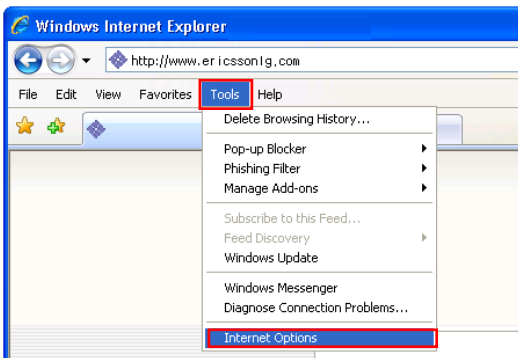
For another example, the captured screen shows that ‘iPECS-NMS’ service is not yet started and its startup type is ‘Manual’. In order to change the status and startup type, double-click on ‘iPECS-NMS’ item to open its ‘Properties’ window. (This example is only for showing how to check and modify the status and startup type of a service. In real situation, the status and startup type field values are set to ‘Started’ and ‘Automatic’, respectively.)

The status of ‘iPECS-NMS Service’ can also be checked and changed by using ‘iPECS-NMS Control’ program as described in ‘iPECS-NMS Software Package Installation’ section.

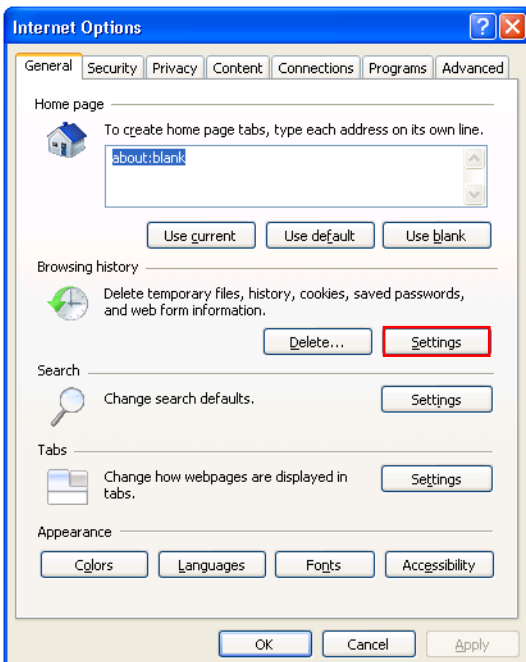
3.2 Accessing iPECS-NMS Server using Web Browser

iPECS-NMS is a Web based application using a Web Browser as the NMS client. Opening your browser and pointing it to the iPECS NMS server automatically opens the NMS client.

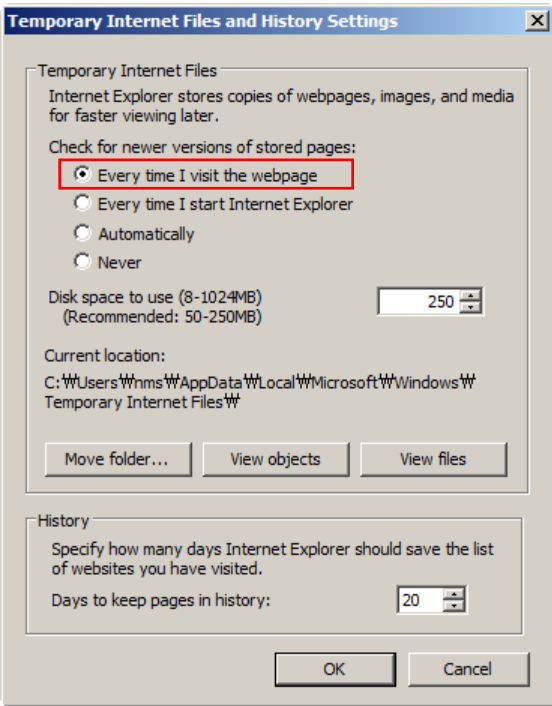
For continual connection between the Web Browser and the NMS Server, set 'Check for newer versions of stored pages' to 'Every time I visit the webpage' on 'Tools → Internet Options → Temporary Internet Files → Settings' or 'Browsing History → Settings' (depending on your browser version).



On the main menu of Web browser, click 'Tools' menu, and then click 'Bowser Options' on the pop-up menu to open 'Internet Options' window.



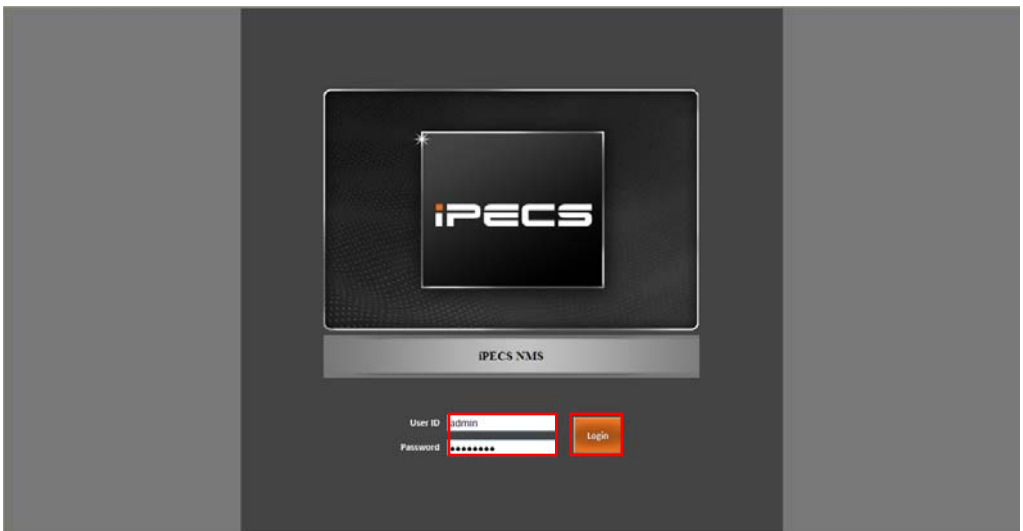
In 'Browsing history' section, click [Settings] button. (Or, if the version of browser has 'Temporary internet files' section, click 'Settings' button in the section.)



7

On the 'Temporary Internet Files and History Settings' window, check if the 'Check for newer version of stored pages' option is set to 'Every time I visit the webpage' time I visit the webpage'. If other option has been set previously, change it to 'Every time I visit the webpage' and then click [OK] button.

To login to the iPECS-NMS, execute the Web browser on the client PC and enter the IP address of the NMS server.



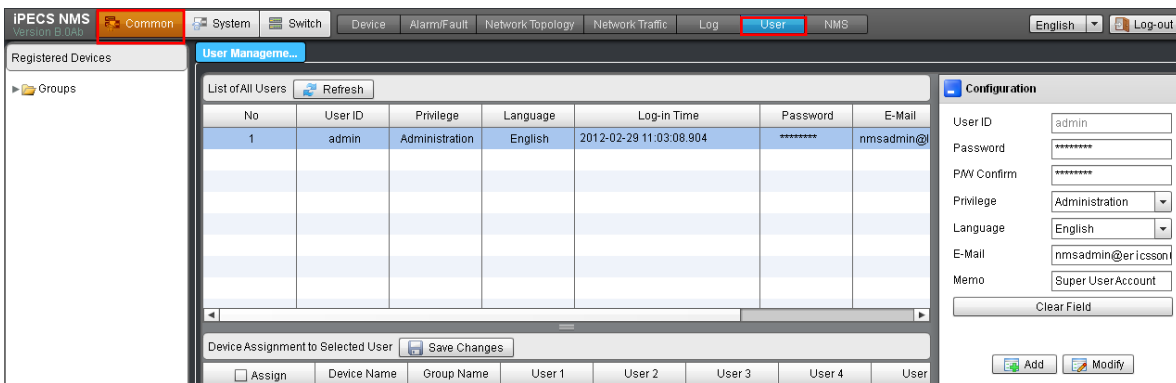
On the iPECS-NMS login page, enter the Admin User ID and Password (ex., admin and default password ipecsnms were used in this document). Then click on the [Login] button.

NOTE—The 'admin' account is the iPECS-NMS Superuser account and cannot be deleted, but the password can be changed.

4. NMS Management

4.1 Modify Superuser Configuration

It is recommended to change the information of the Superuser (admin) account when the Superuser logs in for the first time. For details about configuring user account, please refer to ‘User Management’ section.

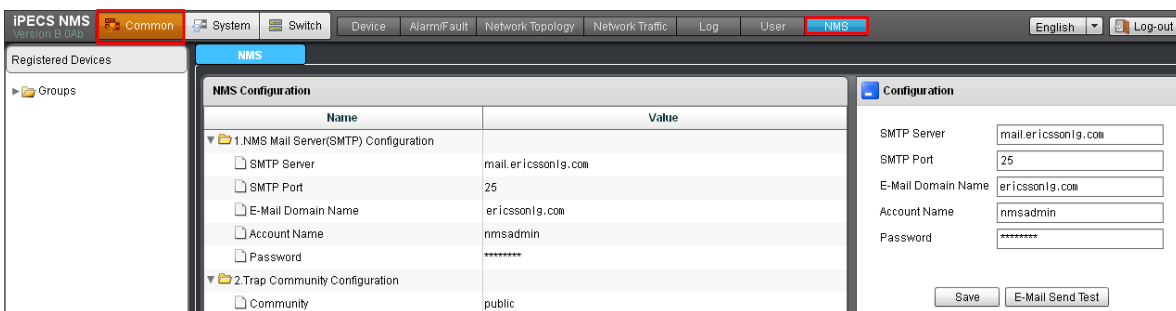


From the NMS Menu, click on the [Common] tab and then [User] sub-menu. If you click the ‘admin’ item from the ‘List of All Users’ then the User information of ‘admin’ will be displayed. The initial password for ‘admin’ (which is ‘ipecsnms’) should be changed for the security of your iPECS-NMS.

After finishing making changes, click on the [Modify] button to apply the information to the Superuser account. To confirm the modification, log out iPECS-NMS (by clicking the [Log Out] button) and log-in again with the new password.

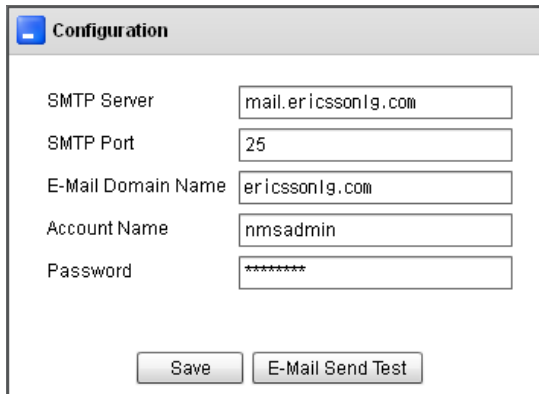
4.2 NMS Server Management

The NMS Server Management screen is used to establish common iPECS NMS characteristics, and can be opened by selecting [Common] on the top-level menu, then [NMS] sub-menu.



4.2.1 NMS Mail Server Configuration

If an alarm or fault event occurs, iPECS NMS server will attempt to send an e-mail to User accounts assigned to receive notification. In order to send an e-mail, NMS server must have an e-mail account on a Simple Mail Transfer Protocol (SMTP) server. While an existing e-mail account could be used, it is recommended a separate iPECS NMS account be created in the e-mail server.



SMTP Server	mail.ericssonlg.com
SMTP Port	25
E-Mail Domain Name	ericssonlg.com
Account Name	nmsadmin
Password	*****

Save E-Mail Send Test

From the the NMS Mail Server (SMTP) Configuration area of the screen, enter the name or IP address of the e-mail server, e-mail domain name, SMTP port, account name and password.

- SMTP Server/Port - if it is not clear what information to input, contact your System Administrator for help.
- E-Mail Domain Name - is the domain name part of an E-Mail address managed on the SMTP server (normally the part of an e-mail address following the '@' symbol).

Click [Save] to store the NMS e-mail account information.

After completing NMS mail server (SMTP) configuration, [E-Mail Send Test] button can be used to check if E-Mail is sent properly using the configuration. The E-Mail is sent to the E-Mail address of currently logged-in user (verify the E-Mail address of the user is configured in 'User Config' of 'User' menu before clicking the [E-Mail Send Test] button).

4.2.2 Trap Community Configuration

The 'Trap Community' is a string that represents the group of SNMP Trap communication. It is used for sending alarm/fault event messages between the NMS and the iPECS System. The same Trap Community string must be set in both the iPECS Web Admin and NMS. On iPECS Web Admin, the trap community can be set in the 'SNMP Attribute (PGM196)' configuration, In case of iPECS-MG Web Admin, the trap community configuration is on 'SNMP Data' menu.

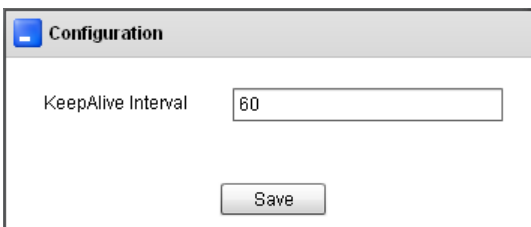


The screenshot shows a configuration window titled "Configuration". Inside, there is a label "Community" followed by a text input field containing the word "public". Below the input field is a "Save" button.

To change the trap community, enter a 4 to 20 character string (default : public) in the Community box and click [Save]. Verify that registered iPECS systems are also configured with the same information.

4.2.3 System KeepAlive Interval Configuration

The iPECS system periodically sends KeepAlive messages to the iPECS NMS for updating the operation and communication status. If the system fails to send a KeepAlive message or it is not received by iPECS NMS for more than 5 minutes, the system is considered off-line. To control traffic, the polling interval can be changed.

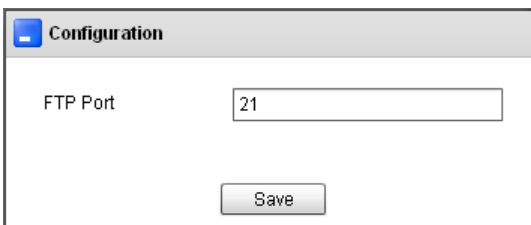


The screenshot shows a configuration window titled "Configuration". Inside, there is a label "KeepAlive Interval" followed by a text input field containing the number "60". Below the input field is a "Save" button.

Enter a value (50-100 sec.) in the box and click [Save].

4.2.4 FTP Port Configuration

In the iPECS NMS, FTP service is working for transferring data. The FTP Service requires a listening TCP/IP port. (Default number is 21)

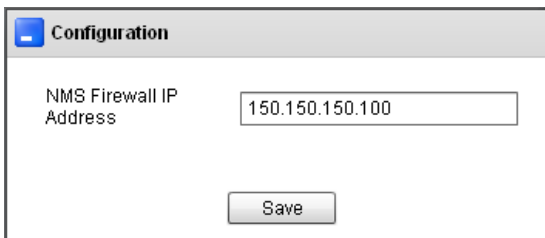


The screenshot shows a configuration window titled "Configuration". Inside, there is a label "FTP Port" followed by a text input field containing the number "21". Below the input field is a "Save" button.

Enter the desired port number in the box and click [Save].

4.2.5 NMS Firewall IP Address Configuration

When the iPECS-NMS is installed behind a NAT server, the fixed IP Address provided by the NAT server must be assigned in this field.

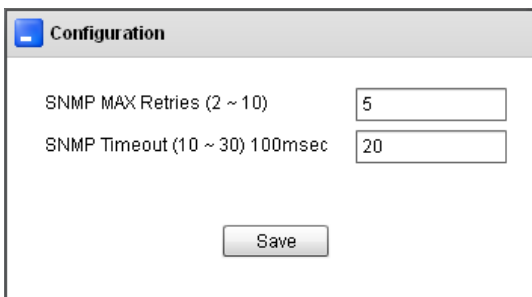


The screenshot shows a configuration window titled "Configuration". It contains a label "NMS Firewall IP Address" followed by a text input field containing the value "150.150.150.100". Below the input field is a "Save" button.

Enter the desired IP address in the box and click [Save].

4.2.6 SNMP Max retries and Timeout Configuration

It is possible that the NMS fails sending SNMP packet to registered system. If sending failure is happened, the NMS retries based on these configurations. The standard unit of timeout is 100ms.



The screenshot shows a configuration window titled "Configuration". It contains two labels: "SNMP MAX Retries (2 ~ 10)" with a text input field containing the value "5", and "SNMP Timeout (10 ~ 30) 100msec" with a text input field containing the value "20". Below the input fields is a "Save" button.

Enter the desired port number in the box and click [Save].

5. Device Management

Device Management provides functions for iPECS system & switch registration and device group management. Up to 500 iPECS devices and 100 device groups can be configured, and the device groups can be configured to have up to 4 sub-level groups under the top most 'Groups' node. Device Web Admin can be accessed directly from iPECS-NMS.

To enter the Device management menu, click [Common] on top-level menu, then [Device] sub-menu.

5.1 Device Configuration

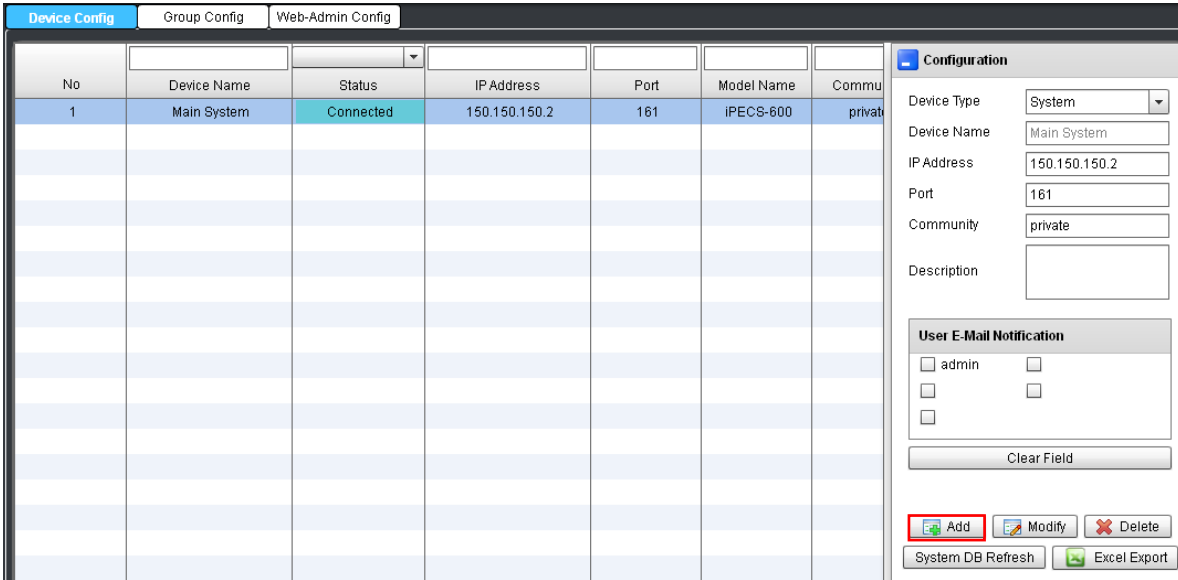
'Device Configuration' provides functions for device registration and E-Mail notification assignment. This page can be accessed by selecting [Device] sub-menu, then clicking [Device Config] tab.

The screenshot displays the iPECS NMS web interface. At the top, there is a navigation bar with tabs: Common, System, Switch, Device (highlighted), Alarm/Fault, Network Topology, Network Traffic, Log, User, and NMS. Below this, there are sub-tabs: Device Config (highlighted), Group Config, and Web-Admin Config. On the left, a sidebar shows 'Registered Devices' with a 'Groups' folder. The main area contains a table with columns: No., Device Name, Status, IP Address, Port, Model Name, and Commu. To the right of the table is a 'Configuration' form. The form includes a 'Device Type' dropdown menu (set to 'System'), text input fields for 'Device Name', 'IP Address', 'Port' (set to 161), and 'Community' (set to private), and a 'Description' text area. Below these is a 'User E-Mail Notification' section with three checkboxes. A 'Clear Field' button is highlighted with a red box. At the bottom of the form are buttons for 'Add', 'Modify', 'Delete', 'System DB Refresh', and 'Excel Export'.

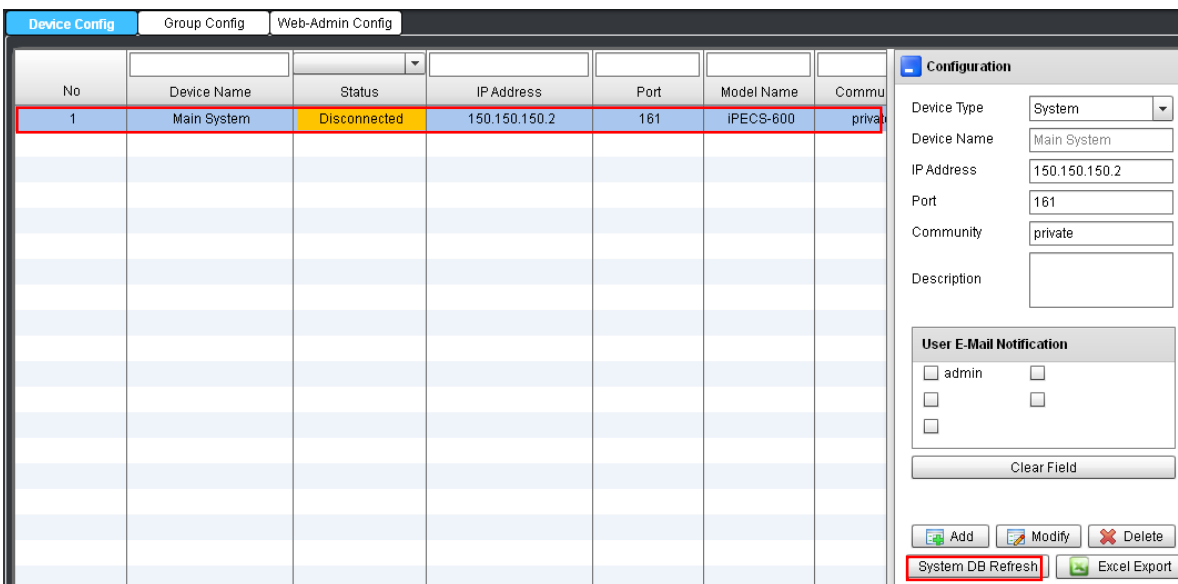
Devices can be added or deleted, and information of a registered device modified. In order to add a new device, first click [Clear Field] button, and then select 'System' or 'Switch' for 'Device Type' field. For each device, alarm/fault E-mail notification is assigned to user accounts. The user account must be assigned to manage the specific system and receive e-mail notifications. Information required for each registered device includes a unique system name (4-20 characters, with no special characters), device IP address, SNMP port number (default is 161, but may be changed), community (4-20 characters, no special characters) and a description field (63 characters). The community field defines the SNMP Read-Write community between the iPECS device and NMS, and must match the Read-Write Community SNMP Attribute, designated in the

iPECS device Web Admin.

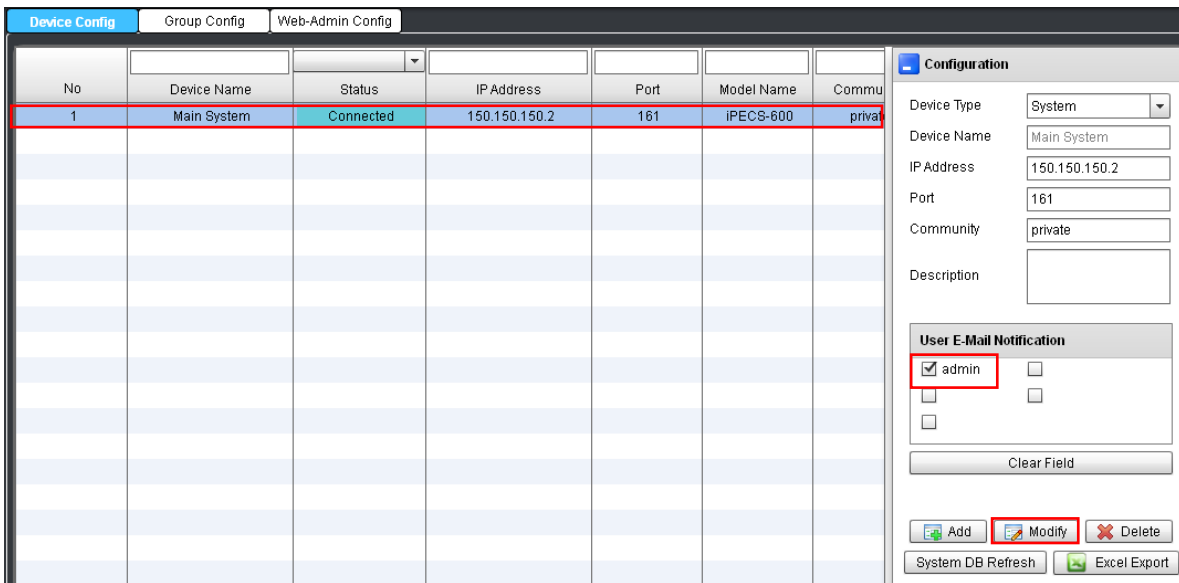
Prior to adding a device registration with iPECS-NMS, the device should be properly configured for SNMP communication, and corresponding license should be installed if required.



After entering device configuration fields, click [Add] button. The device is initially added to the system list with a disconnected status. NMS will contact the device for information exchange. If the connection is successful, the status will change to 'Connected' and NMS will receive basic information from the added device and save it to a local database.



If the device remains disconnected, verify the connection between iPECS-NMS and the iPECS device then click [System DB Refresh] to update the NMS database.



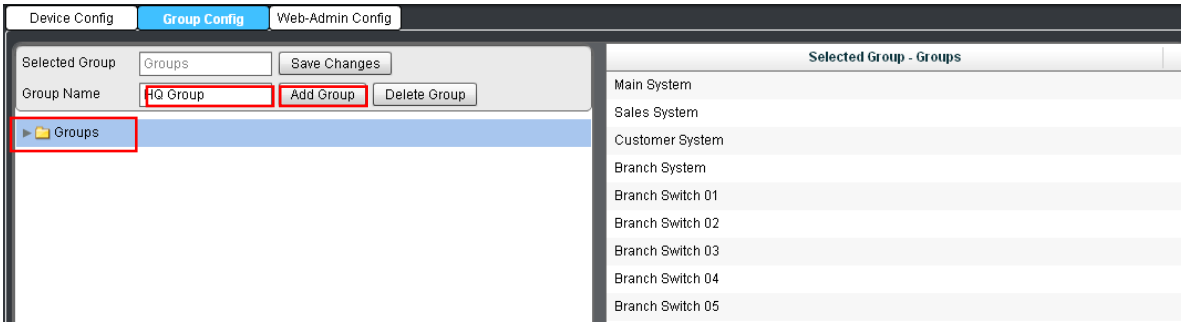
In order to change device information, select a target device from the device list, and change its information. Device name cannot be changed. User E-Mail Notification is for designating where to send alarm/fault notifications related to the device. (For complete E-Mail related configurations, the E-Mail address of ‘admin’ account and NMS mail server (SMTP) settings have to be configured as well.) After modifying device information, click [Modify] button to accept changes. The [Clear Field] button is used to empty all fields (except SNMP Port and Community), and also before entering device information to add a new device.



To delete a registered device, select the target device in device list, and click [Delete] button.

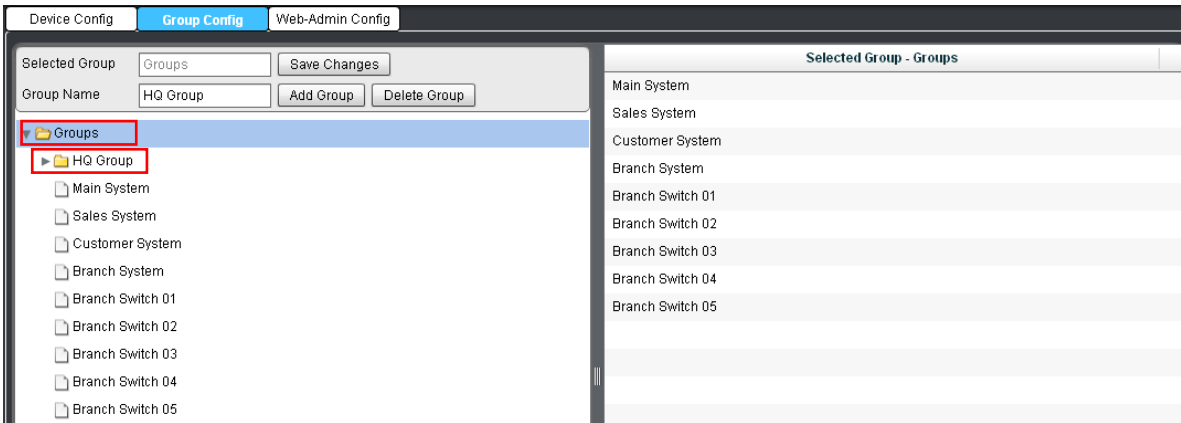
5.2 Device Group Configuration

‘Group Config’ page is used to organize the registered systems into groups for easier management. Up to 100 groups may be defined in a tree with up to 4-level branches. ‘Group Config’ page shows the ‘Device/Group List’ on the left for modifying group configuration and the devices in a selected group on the right panel. This page can be accessed by selecting [Group Config] tab under ‘Device’ sub-menu.

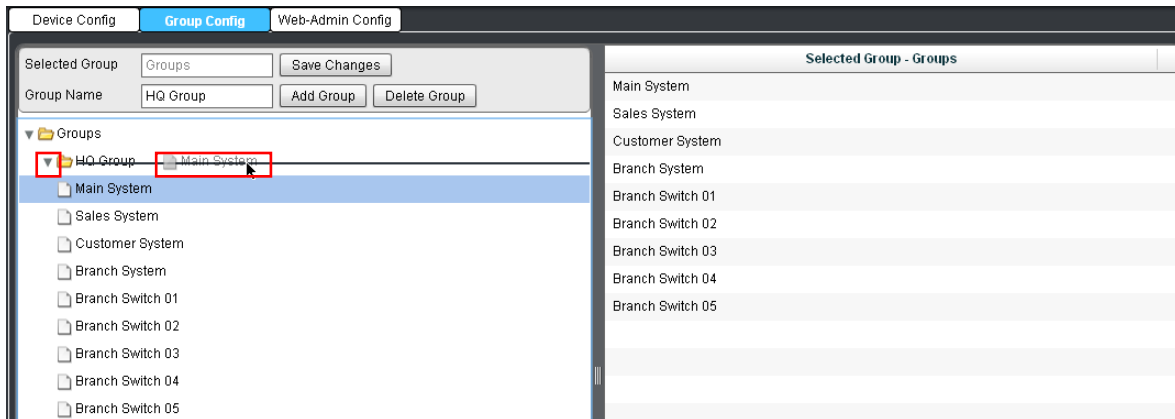


In the initial state, there is no other group than top-level 'Groups', so first select 'Groups' node on 'Device/Group List' and check the name of the selected group is displayed in 'Selected Group' field. Then, enter a unique group name (4 to 20 characters, no special characters) in the 'Group Name' field and click [Add Group] button.

NOTE – Once a group name is created/added, it cannot be changed..

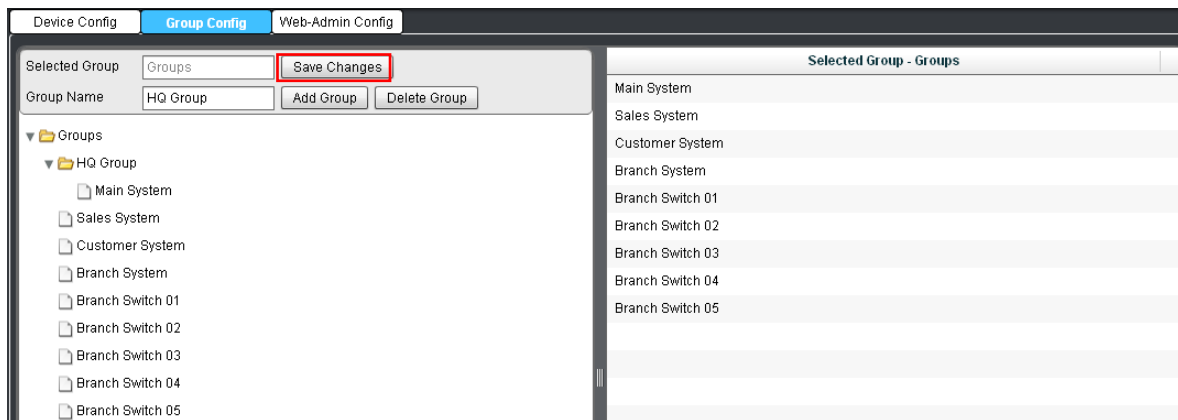


After adding a new group, it can be checked by clicking left arrow button of the 'Groups' node to expand its child nodes. Device groups may have 4-level depth in the tree of nodes.

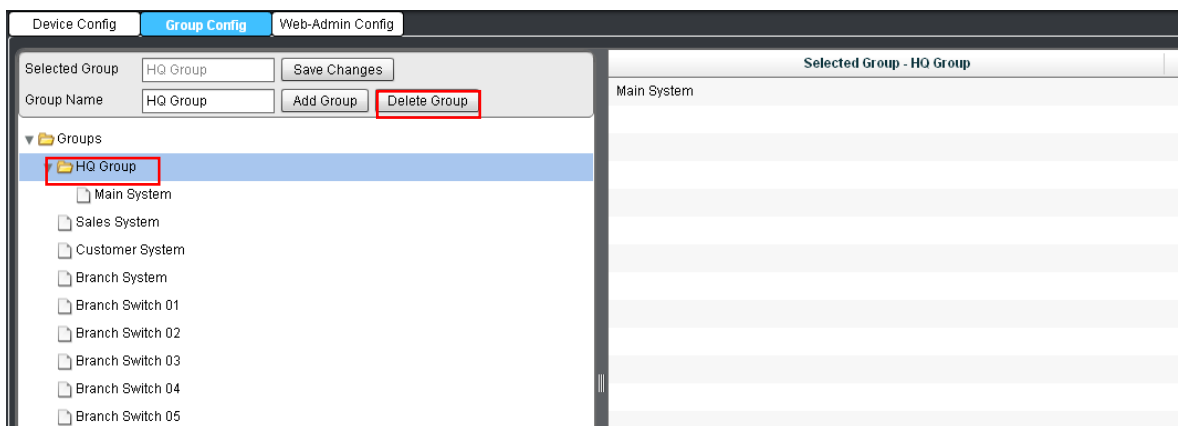


After a new group is added, devices can be assigned to the group as group members. First, click

the left arrow button of the group to make it as ‘expand’ state (pointing downward). Then, drag-and drop a device onto the group position.



After assigning the device to the group, click [Save Changes] button to store the modified group information. Group assignment can be checked by clicking the arrow button on the left of the group, or on the ‘Selected Group’ panel after selecting the group on the ‘Device/Group List’.



In order to remove a device group, select the target group on ‘Device/Group List’ on the left, and then click [Delete Group] button.

5.3 Web Admin Configuration

‘Web Admin Config’ page is used to manage the iPECS system Web Admin passwords and to access the iPECS System Web Admin without the need to manually enter the password. When accessing Web Admin from iPECS-NMS, NMS supplies the password to the system automatically. For iPECS switches, automatic login feature is not supported, and only Web Admin access function is provided. To open ‘Web Admin Config’ page, select [Web Admin Config] tab under ‘Device’ sub-menu.

No	Device Name	Status	IP Address	Model Name	User ID	Passwd
1	Main System	Connected	150.150.150.2	iPECS-600		
2	Sales System	Connected	150.150.131.91	iPECS-50B		
3	Customer System	Connected	192.168.123.85	iPECS-MG300		
4	Branch System	Connected	192.168.123.103	iPECS-1200		***
5	Branch Switch 01	Connected	192.168.123.98	ES-4550G		
6	Branch Switch 02	Connected	192.168.123.99	ES-3026		
7	Branch Switch 03	Connected	192.168.123.100	ES-3024G		
8	Branch Switch 04	Connected	192.168.123.101	ES-2026		
9	Branch Switch 05	Connected	192.168.123.102	ES-2010G		

To configure a password, select a device from the device list, and enter the Web Admin password or user ID & password depending on the type of device. Click [Save] to store the configuration.

No	Device Name	Status	IP Address	Model Name	User ID	Passwd
1	Main System	Connected	150.150.150.2	iPECS-600		
2	Sales System	Connected	150.150.131.91	iPECS-50B		
3	Customer System	Connected	192.168.123.85	iPECS-MG300		
4	Branch System	Connected	192.168.123.103	iPECS-1200		***
5	Branch Switch 01	Connected	192.168.123.98	ES-4550G		
6	Branch Switch 02	Connected	192.168.123.99	ES-3026		
7	Branch Switch 03	Connected	192.168.123.100	ES-3024G		
8	Branch Switch 04	Connected	192.168.123.101	ES-2026		
9	Branch Switch 05	Connected	192.168.123.102	ES-2010G		

To access the Web Admin of a device, click on the Web icon of the target device in device list. This will open the initial Web Admin page of the selected device.

6. User Management

'User Management' provides the means to manage user accounts and assign users to each system to implement management domain for each user. Access control function provides the information of the users currently logged-in to iPECS-NMS, and allows making a selected user to be logged out of iPECS-NMS if needed.

'User Management' page can be viewed by clicking [User] sub-menu under [Common] menu.

6.1 User Configuration

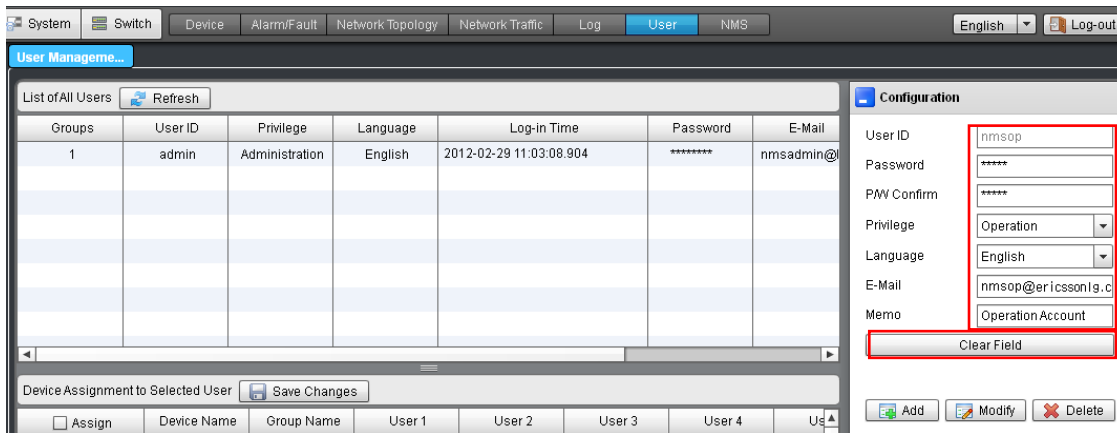
User accounts are managed under the [User] menu. Accounts can be added, modified and deleted, as well as specific iPECS devices may be assigned to an account. Up to a maximum of 100 accounts can be created, and 10 users including 'admin', may access the server simultaneously. It is also possible to assign specific users to each system so that only assigned users can operate on the system.

6.1.1 User Account Configuration

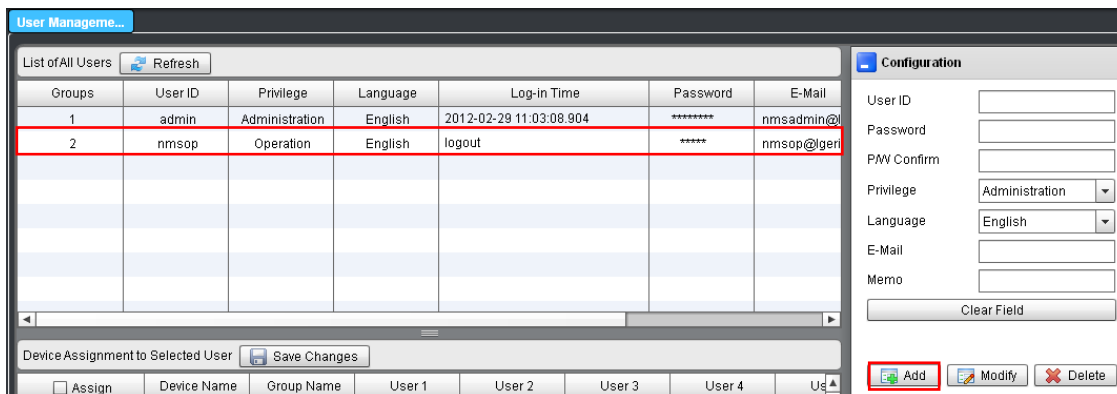
Each User account has an associated unique User ID (4 - 20 characters) and password. Each account has an assigned Privilege. User Account levels (Privileges) available are:

- Administration - allows full access to iPECS NMS server; note the 'admin' account is the superuser account with access to all functions of NMS and information on all systems registered to NMS. This account cannot be deleted, but the password can be changed. If this is a first time installation, for security purposes, it is recommended the 'admin' user account password be changed from the default.
- Operation - allows access to all of the NMS services except for User, NMS or System configurations screens at the Top-level menu.
- Monitoring - allows access to the Device Info, Status and Alarm/Fault screens from the Top-level menu.

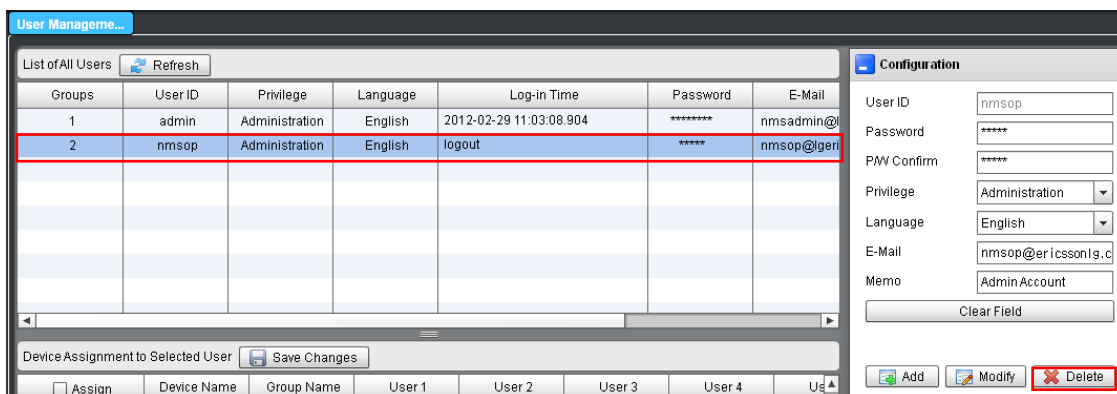
Additionally, the language preference and E-mail address can be entered. Language selection only applies to messages from the iPECS-NMS server and not from other services or Windows. To receive E-mail notification, notification must be assigned in the Device Management screen



In add a new device, first click [Clear Field] button, then enter the desired user ID. User ID allows 4~20 characters of alphabet letters, numbers and underline character (_), and must be unique. 'Password' allows 4~20 characters of letters and numbers (no special characters), and 'Privilege' level can be selected with one of the three levels of 'Administration', 'Operation' and 'Monitoring'. 'Language' can be selected for each user, and this language selection is applied to the texts that iPECS-NMS provides. 'E-Mail' address field should be entered if E-Mail notification of alarm/fault events is to be used. 'Memo' field is for additional descriptions for the user, and up to 63 characters can be entered.



After setting user information, click [Add] button to create the user account, then a new item for the user will appear in the 'List of All Users'.



To modify or delete an account, select the desired account in the 'List of All Users,' change the

necessary user information and click [Modify] button. ‘User ID’ field is not allowed to be changed because it is used as a user identifier in iPECS-NMS.

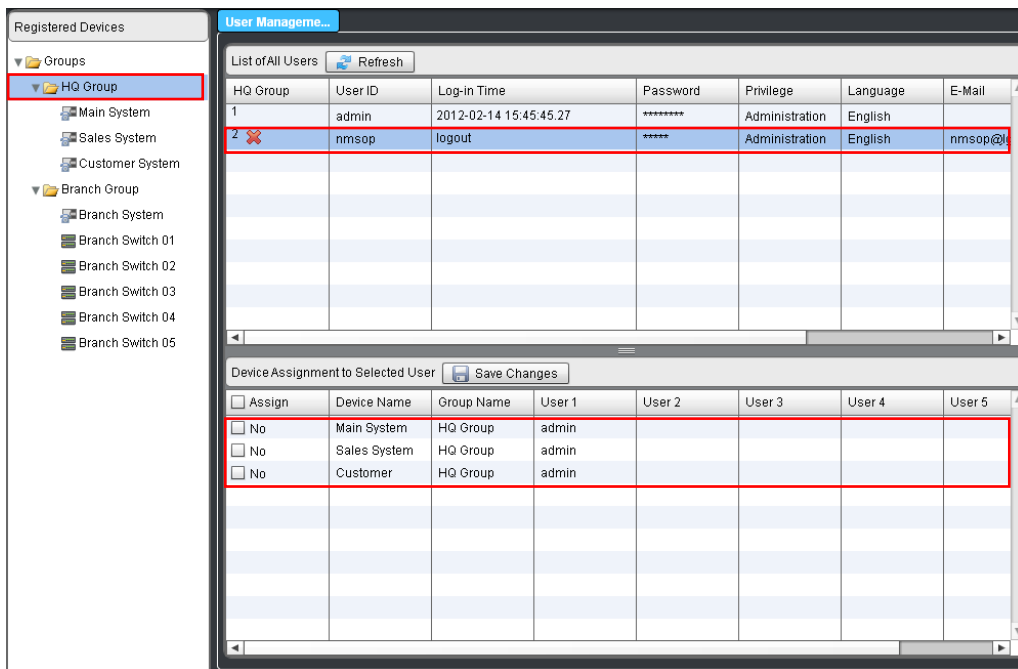
[Clear Field] button is for clearing the values of all the fields except ‘Privilege’ and ‘Language’ fields. This button can also be used to clear existing field values before adding a new user.



In order to remove a user ID, select the user on ‘List of All Users’, and click [Delete] button.

6.1.2 System Assignment to User Account

Each user account may be assigned management and monitoring authority for each registered iPECS device. An account can access information only for authorized devices and a device can have up to five managing user accounts including the ‘admin’ account which can not be modified.



To assign a system to a user account, select the desired system or group from ‘Registered Devices’, then select the account in ‘List of All Users’. ‘Device assignment to Selected User’ window displays the account’s authority for registered devices.

Device Assignment to Selected User

<input checked="" type="checkbox"/> Assign	Device Name	Group Name	User 1	User 2	User 3	User 4	User 5
<input checked="" type="checkbox"/> Yes	Main System	HQ Group	admin	nmsop			
<input checked="" type="checkbox"/> Yes	Sales System	HQ Group	admin	nmsop			
<input checked="" type="checkbox"/> Yes	Customer	HQ Group	admin	nmsop			

In order to assign a device to the selected user, click on the ‘Assign’ check-box to make it changed to ‘Yes’, and click [Save Changes] button. Then, one of the ‘User’ fields will show the currently selected user ID to designate the new user is added to the list of assigned users.

Device Assignment to Selected User

<input type="checkbox"/> Assign	Device Name	Group Name	User 1	User 2	User 3	User 4	User 5
<input type="checkbox"/> No	Main System	HQ Group	admin				
<input type="checkbox"/> No	Sales System	HQ Group	admin				
<input type="checkbox"/> No	Customer	HQ Group	admin				

In order to remove the selected user from the list of assigned users, click on the ‘Assign’ check-box to make it changed to ‘No’, and click [Save Changes] button. Then, currently selected user ID will be removed from the ‘User’ field.

iPECS NMS Version B.04a

Common System Switch **Device** Alarm/Fault Network Topology Network Traffic Log User NMS

Registered Devices

Groups

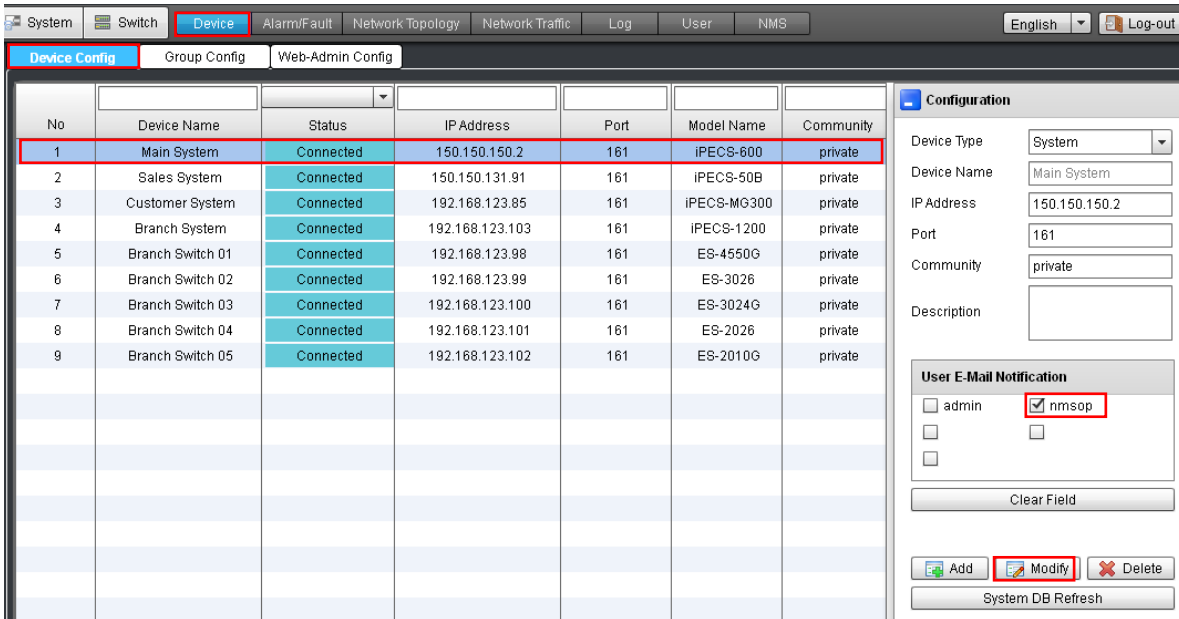
- HQ Group
 - Main System
 - Sales System
 - Customer System

No	Device Name	Status	IP Address	Port	Model Name	Commu
1	Main System	Connected	150.150.150.2	161	iPECS-600	privat
2	Sales System	Connected	150.150.131.91	161	iPECS-50B	privat
3	Customer System	Connected	192.168.123.85	161	iPECS-MG300	privat

To confirm assignment changes, logout and login with the User ID. After login, Systems assigned will be shown in ‘Registered Devices’.

6.1.3 Set E-mail Notification to User Account

After a device is assigned to a user account, the user can receive alarm/fault notification via E-mail. E-mail notification is designated in the [Device Config] tab under ‘Device’ menu.

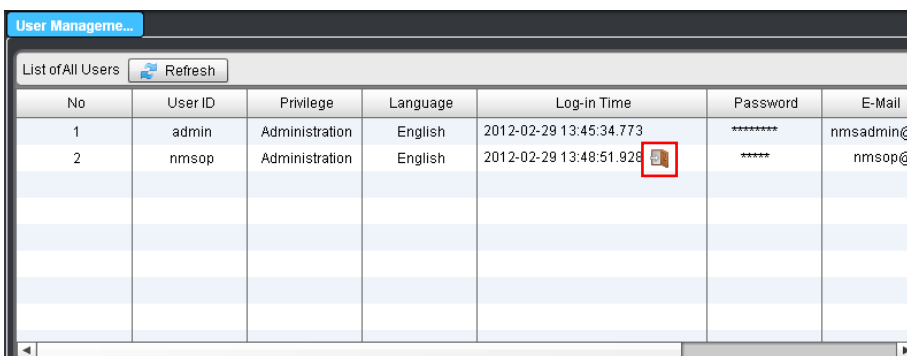


The user accounts, which are assigned as manager, will be displayed in ‘User E-mail Notification’ when a device is selected in the device list. Check user accounts who want to receive e-mail notification and click [Modify] button to save. If an alarm/fault event in the device occurs, the iPECS-NMS will send E-mail to the selected user E-mail addresses configured in user configuration.

NOTE - In order for an e-mail to be sent properly, the Mail (SMTP) Server and the E-mail address of the assigned user should be configured as well.

6.2 User Access Control

‘User Access Control’ provides functions for retrieving the information of currently logged-in users and their login times. And if necessary, specific users can be forced to be logged out of iPECS-NMS by the administrator. The page for this feature is under the [User Management] tab of ‘User’ sub-menu.



On the ‘User Management’ page, currently logged-in users are listed in ‘List of All Users’ with each user’s login time displayed in ‘Log-in Time’ field. If it is needed to force a specific user to be

logged out of iPECS-NMS for some operational reason, click 'Force Log-out' button inside the 'Log-in Time' field.

Then, an NMS warning message is displayed on the user's NMS client screen, and the NMS client becomes logged out of iPECS-NMS automatically.

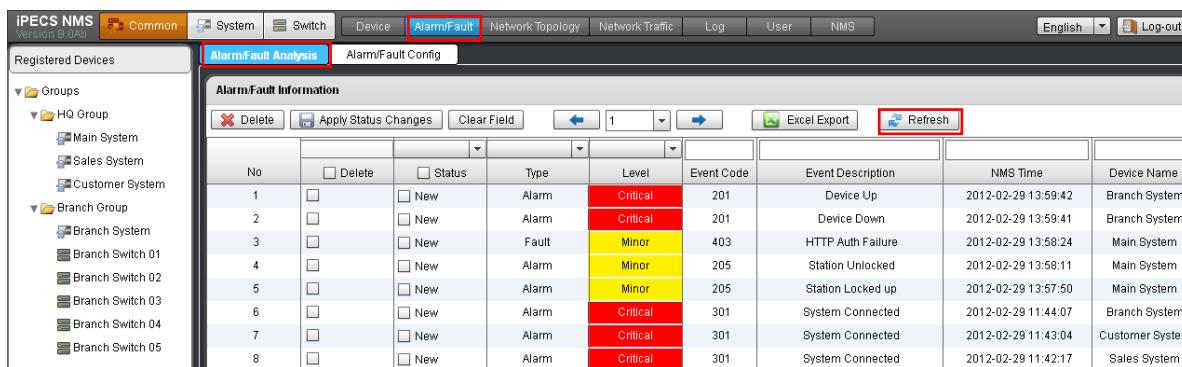
7. Alarm/Fault Management

iPECS NMS receives event notification messages from each registered iPECS device. Event messages are analyzed and, based on Alarm/Fault Configuration, events are logged and stored. If assigned, User accounts with management authority for the iPECS device are immediately notified by E-mail of the event. The iPECS-NMS event log stores up to 10,000 event records for each registered iPECS device. ‘Alarm/Fault Management’ can be entered by selecting [Alarm/Fault] sub-menu under ‘Common’ menu.

7.1 Alarm/Fault Analysis

The Alarm/Fault Analysis includes tools to isolate and search events from registered iPECS devices stored in the NMS event log. Events from a specific device, of a specific type, status and level can be isolated and searched based on event code, location and date. ‘Alarm/Fault Analysis’ page can be accessed by selecting [Alarm/Fault Analysis] tab under ‘Alarm/Fault’ sub-menu.

7.1.1 Event List and Search Fields



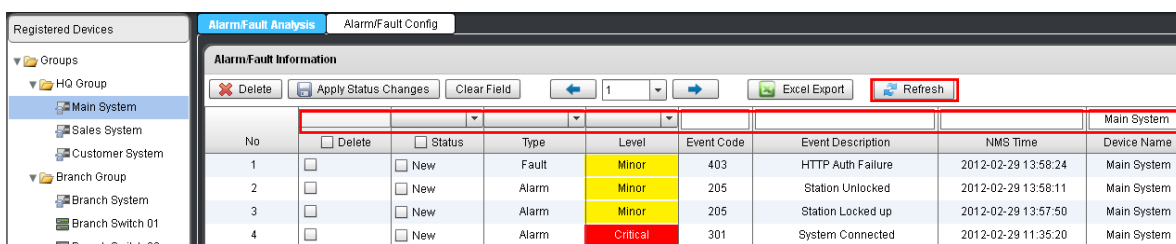
When a device is selected in ‘Registered Devices’, alarm/fault events for the selected device are displayed on the event list, and the event list can be updated by clicking [Refresh] button.

Each event record includes a record number, a delete check box and status check box. The status check box indicates the management status of the record, new or checked. In addition, each record includes fields for the following:

Table Name	Field Name	Description
Event List	Status	The event management status that can be set by NMS user. This field can have two status values of ‘New’ and ‘Checked’. - New : For those events that occurred but not yet

		checked or managed by administrator. - Checked : For those events that have been already checked or managed by administrator.
	Type	The type of the event message received from iPECS device. This field can have one of three event types of 'Information', 'Fault' and 'Alarm'. - Information : Not a problem but an important event to be noticed - Fault : A problem that occurred in iPECS device. For systems, it is a one-time event for which the occurrence and its corresponding clearance are not maintained by MFIM. For switches, it is a problem related to the switch itself. - Alarm : A kind of system fault. For systems, the occurrence and its corresponding clearance are maintained by MFIM. For switches, it is related to the network environment where the switch is operating.
	Level	The level of severity assigned for the event. There are three levels, 'Critical', 'Major' and 'Minor'. - Critical : May cause serious effects on the general operation of the device. - Major : Does not seriously affect the general operation of the whole device, but may cause partial problems or some management/operation is needed to make it work properly. - Minor : Is not an abnormal state of the system, but some management/operation is needed to make it work properly.
	Code	The code of the event message from iPECS device. Refer to '7.3 Types and Definitions of Alarm/Fault Events' for detailed information.
	Event Description	The description of the event message from iPECS device. Refer to '7.3 Types and Definitions of Alarm/Fault Events' for detailed information.
	NMS Time	The time when the event message was received by iPECS-NMS.
	Device Name	The iPECS device name that sent the event message.
	Location	The location (device) where the event occurred.
	Information	Detailed information of the event provided when additional information needs to be specified.

7.1.2 Event Search and Management



Clear all the the search fields above the table header, or after clearing search fields, click

[Refresh] button to retrieve current data. This will load the entire Event Log including all event messages from all registered systems. If a device is selected in ‘Registered Device’, events for the selected device are displayed.

The screenshot shows the 'Alarm/Fault Information' interface with search filters set to 'New', 'Alarm', 'Minor', and '205'. The table contains two rows of event data.

No	<input type="checkbox"/> Delete	<input type="checkbox"/> Status	Type	Level	Event Code	Event Description	NMS Time	Device Name
1	<input type="checkbox"/>	<input type="checkbox"/> New	Alarm	Minor	205	Station Unlocked	2012-02-29 13:58:11	Main System
2	<input type="checkbox"/>	<input type="checkbox"/> New	Alarm	Minor	205	Station Locked up	2012-02-29 13:57:50	Main System

After loading alarm/fault event data, search can be performed with various search conditions. Search fields located above the table header are used for searching specific events. Select combo box fields or enter search values in edit boxes to configure search conditions. Search operation is performed as soon as a search field is modified, and search result is displayed immediately.

The screenshot shows the 'Alarm/Fault Information' interface with the 'Apply Status Changes' button highlighted in red. The table contains four rows of event data.

No	<input type="checkbox"/> Delete	<input type="checkbox"/> Status	Type	Level	Event Code	Event Description	NMS Time	Device Name
1	<input type="checkbox"/>	<input checked="" type="checkbox"/> Checked	Alarm	Critical	201	Device Up	2012-02-29 13:59:42	Branch System
2	<input type="checkbox"/>	<input checked="" type="checkbox"/> Checked	Alarm	Critical	201	Device Down	2012-02-29 13:59:41	Branch System
3	<input type="checkbox"/>	<input type="checkbox"/> New	Fault	Minor	403	HTTP Auth Failure	2012-02-29 13:58:24	Main System
4	<input type="checkbox"/>	<input type="checkbox"/> New	Alarm	Minor	205	Station Unlocked	2012-02-29 13:58:11	Main System

‘Status’ field may be used to designate an event as ‘New’ event that is not yet checked by NMS user or ‘Checked’ event. In order to change the event state, click on the check-box of ‘State’ field to change its state, and then click [Apply Status Changes] button to save and apply the change.

The screenshot shows the 'Alarm/Fault Information' interface with the 'Delete' button highlighted in red. The table contains four rows of event data.

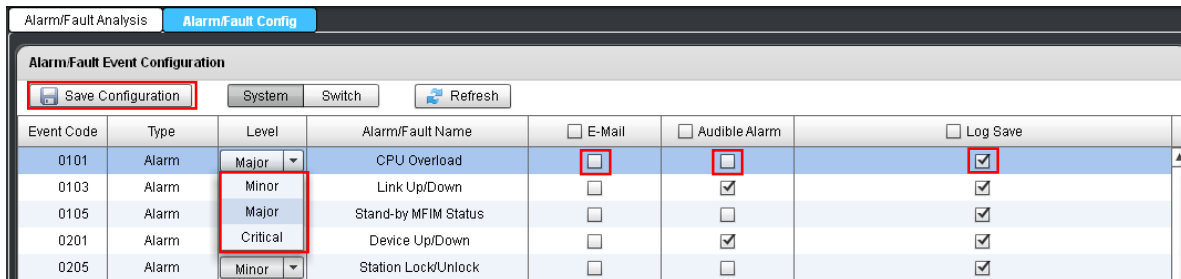
No	<input type="checkbox"/> Delete	<input type="checkbox"/> Status	Type	Level	Event Code	Event Description	NMS Time	Device Name
1	<input checked="" type="checkbox"/>	<input type="checkbox"/> New	Alarm	Critical	201	Device Up	2012-02-29 13:59:42	Branch System
2	<input checked="" type="checkbox"/>	<input type="checkbox"/> New	Alarm	Critical	201	Device Down	2012-02-29 13:59:41	Branch System
3	<input type="checkbox"/>	<input type="checkbox"/> New	Fault	Minor	403	HTTP Auth Failure	2012-02-29 13:58:24	Main System
4	<input type="checkbox"/>	<input type="checkbox"/> New	Alarm	Minor	205	Station Unlocked	2012-02-29 13:58:11	Main System

Similarly, in order to delete an event record, click on the ‘Delete’ check-box of a desired record, then click [Delete] button.

7.2 Alarm/Fault Configuration

‘Alarm/Fault Configuration’ provides the means to enable or disable ‘E-Mail’ notification of alarm/fault events, ‘Audible Alarm’ that alerts NMS client with alarm sound when new alarm/fault

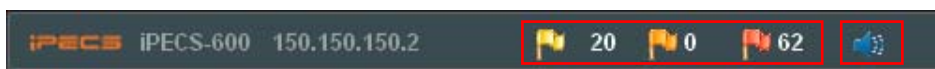
occurs, and ‘Log Save’ option for saving received alarm/fault events into alarm/fault log. The ‘Level’ of alarm/fault events can also be changed from default settings for specific system environment or situation. To access ‘Alarm/Fault Configuration’ page, click [Alarm/Fault Config] tab under ‘Alarm/Fault’ sub-menu.



Each event has a code and is assigned a level of importance, critical, major, or minor. The default level for each event is predefined but can be changed by configuration. Should a specific event code occur, the user accounts assigned management authority for the iPECS device can receive an E-Mail notification. Note that for E-Mail notification, the NMS mail server must be configured on the ‘NMS Management’ page, the user account must be assigned to receive notification in the ‘User Management’ page, and the user account must be assigned to receive notification for the system on the ‘Device Configuration’ page.

To alert a NMS client with an audible alarm when an alarm/fault occurs, check the ‘Audible Alarm’ box of the desired event, and click [Save Configuration] button.

In order to change ‘Log Save’ setting, click on the ‘Log Save’ check-box of desired event, and click [Save] button to save and apply the change. Afterward, selected alarm/fault events will only be saved in alarm/fault log.



Under [System] top-level menu, the information panel is displayed on the upper part of the screen. This panel shows brief information of a device selected from ‘Registered Devices’, and the information for the received alarm/fault events and audible alarm setting is also provided.

The number of alarm/fault events of a selected device is displayed with yellow, orange and red flags for minor, major and critical events, respectively. The speaker icon shows current audible alarm setting for all events, and can also be used to change the setting by clicking the icon which toggles among ‘One Time’, ‘Repeat’ and ‘Disabled’ states. To stop the alarm sound when the audible alarm is set to ‘Repeat’, click the alarm/fault flag, or enter the ‘Alarm/Fault Analysis’ menu.

7.3 Types and Definitions of alarm/Fault Events

Alarm/fault events are classified into two categories of system events (0xxx) and switch events (2xxx). iPECS-NMS logs three types of events, Alarm, Fault and Information. Each event is classified as critical, major or minor and is referenced with a code. Events defined in iPECS-NMS are listed below.

< System Alarm Event >

Code	Name	Type	Level	Location	State	Description
0101	CPU Overload	Alarm	MAJ	MFIM (MPB)	ON	< CPU Overload Occurred > Occurred when CPU usage rate becomes higher than 80%. * Detailed Information : CPU performance availability - "CPU Idle 15%"
					OFF	< CPU Overload Cleared > Occurred when CPU usage rate becomes less than 80%. * Detailed Information : CPU performance availability - "CPU Idle 25%"
0103	Link Up/Down	Alarm	CRI	I/F(#)	ON	< Interface Link Down > Occurred when the status of the network interface (e.g. eth0, eth1, wan0) of MFIM becomes Down. * Detailed Information : Network interface name - "eth0"
					OFF	< Interface Link Up > Occurred when the status of the network interface (e.g. eth0, eth1, wan0) of MFIM becomes Up. * Detailed Information : Network interface name - "eth0"
0105	Stand-by MFIM Status	Alarm	MAJ	MFIM	ON	< Standby MFIM Down > In case of CPU redundancy configuration, this event is occurred when the status of stand-by MFIM becomes Down. The stand-by MFIM is determined to be Down when one or more of the following three conditions are met. 1) The link status of LAN2 is detected to be Down. 2) Stand-by MFIM has not sent redundancy status message longer than 1 minute. 3) The status of call processing

						<p>application of stand-by MFIM is determined to be abnormal.</p> <p>* Detailed Information : The cause of stand-by MFIM status Down</p> <ul style="list-style-type: none"> - "LAN2 POWER DOWN" - "NO STATUS MESSAGE" - "NO APPLICATION MESSAGE" - "CPU REDUNDANCY USAGE ON" (Occurred when administrator enables CPU Redundancy Usage)
					OFF	<p>< Standby MFIM Up ></p> <p>In case of CPU redundancy configuration, this event is occurred when the status of stand-by MFIM becomes Up.</p> <p>* Detail Information : None</p>
0201	Device Up/Down	Alarm	CRI	DEV(#)	ON	<p>< Device Down ></p> <p>Occurred when a device becomes disconnected from MFIM. This event may occur when</p> <ul style="list-style-type: none"> - the device is powered off, - the device is restarted (reset), - the network connection between the device and MFIM is abnormal or not stable, - MFIM does not properly communicate with the device. <p>* Detailed Information : None</p>
					OFF	<p>< Device Up ></p> <p>Occurred when a device becomes connected to MFIM.</p> <p>* Detailed Information : None</p>
0205	Station Lock/Unlock	Alarm	MIN	STA(#)	ON	<p>< Station Locked up ></p> <p>Occurred when a station has gone off-hook under none-conversation state until howler tone is received.</p> <p>* Detailed Information : None</p>
					OFF	<p>< Station Unlocked ></p> <p>Occurred when the locked station becomes on-hook.</p> <p>* Detailed Information : None</p>
0211	SMDR Memory Capacity	Alarm	MAJ	MFIM (MPB)	ON	<p>< SMDR Memory Full Occurred ></p> <p>Occurred when the memory space for SMDR data becomes full. (SMDR Memory Capacity Full is the state that the memory space remains available for less than 50 SMDR records.)</p> <p>* Detailed Information : None</p> <p>* Related Attendant Alarm : SMDR</p>

						BUFFER FULL
					OFF	< SMDR Memory Full Cleared > Occurred when SMDR Memory Capacity Full condition becomes cleared. * Detailed Information : None
0213	VSF Memory Capacity	Alarm	MAJ	DEV(#)	ON	< VSF Memory Full Occurred > Occurred when the memory space of VSF gateway becomes full. * Detailed Information : None * Related Attendant Alarm : VSF WARNING: MEMORY FULL
					OFF	< VSF Memory Full Cleared > Occurred when VSF Memory Capacity Full condition becomes cleared. * Detailed Information : None
0215	License Expired	Alarm	MAJ	MFIM	NONE	<License Expired> When Maintenance License or Demo License is expired, this alarm is occurred.
0216	License Over	Alarm	MAJ	MFIM	NONE	<License Over> When License counts are overed, this alarm is occurred.
0301	System Connectivity	Alarm	CRI	NMS	ON	< System Disconnected > Occurred when the communication between NMS and iPECS system becomes disconnected. NMS determines that the connection between NMS and MFIM is disconnected when it does not receive KeepAlive Trap message from MFIM for 5 minutes. (This may happen when MFIM is powered off, or the network is abnormal or not stable, etc.) * Detailed Information : None
					OFF	< System Connected > Occurred when the connection between NMS and iPECS system is recovered. * Detailed Information : None

< System Fault Event >

Code	Name	Type	Level	Location	State	Description
0401	System Startup	Fault	CRI	MFIM (MPB)	NONE	< System Startup > Occurred when 10 minutes has elapsed after restarting MFIM. (After 10 minutes from restart, MFIM starts device polling, and

						the SNMP agent in MFIM starts working.) * Detailed Information : None
0402	MFIM Switch Over	Fault	MAJ	MFIM	NONE	<p>< MFIM Switch Over Occurred > In case of CPU redundancy configuration, this event is occurred when a switch over between active and stand-by MFIMs happens and so stand-by MFIM becomes active MFIM. The condition for the stand-by MFIM to be switched to active MFIM is as follows.</p> <ol style="list-style-type: none"> 1) The link status of LAN2 is detected to be Down. 2) Active MFIM has not sent redundancy status message longer than 1 minute. 3) The status of call processing application of active MFIM is determined to be abnormal. 4) Active MFIM requests switch-over to stand-by MFIM. (This may happen when administrator forced switch-over using PGM450, or LAN1 of active MFIM becomes down.) <p>* Detailed Information : The cause of switch-over and the direction.</p> <ul style="list-style-type: none"> - "LAN2 POWER DOWN (Master -> Slave)" - "NO STATUS MESSAGE (Master -> Slave)" - "NO APPLICATION MESSAGE (Master -> Slave)" - "REQUEST FROM ASSOCIATED MFIM (Master -> Slave)"
0403	Authentication Failure	Fault	MIN	MFIM (MPB)	NONE	<p>< SNMP Auth Failure > Occurred when the community string of received SNMP message is different from the one configured in MFIM. * Detailed Information : The IP address of the host that sent the SNMP message with invalid community string.</p>
						<p>< HTTP Auth Failure > Occurred when Web Admin is accessed using invalid password. * Detailed Information : The IP address of the host that accessed</p>

						<p>Web Admin using invalid password.</p> <p>< Remote Auth Failure > Occurred when a remote Telnet connection is tried using invalid password. * Detailed Information : The IP address of the host that tried remote connection using invalid password.</p> <p>< Terminal Auth Failure > Occurred when serial terminal login (via RS-232 serial connection or Telnet connection after remote login) is tried using invalid password. * Detailed Information : The IP address of the host that used invalid password, or COM1(Serial).</p> <p>< Keyset Auth Failure > Occurred when Keyset Admin is accessed using invalid password. * Detailed Information : The station number of the station used to access Keyset Admin using invalid password.</p>
0411	Station Capacity	Fault	MIN	MFIM (MPB)	NONE	<p>< Station Capacity Excess Alarm > Occurred when the maximum station capacity has been reached and so additional station device cannot be registered. * Detailed Information : None * Related Attendant Alarm : CAPACITY OVERFLOW STA</p>
0413	CO Line Capacity	Fault	MIN	MFIM (MPB)	NONE	<p>< CO Line Capacity Excess Alarm > Occurred when the maximum CO line capacity has been reached and so additional CO device cannot be registered. * Detailed Information : None * Related Attendant Alarm : CAPACITY OVERFLOW COL</p>
0501	Device Alert	Fault	MAJ	DEV(#)	ON	<p>< DSP Alert Occurred > Occurred when DSP Alert is detected in the DSP of a device. * Detailed Information : DSP Alert code number - "Code 10"</p>
					OFF	<p>< DSP Alert Cleared > Occurred when DSP Alert is</p>

						cleared in the DSP of a device. * Detailed Information : DSP Alert code number - "Code 10"
0503	Device Error	Fault	MAJ	DEV(#)	NONE	< DSP Error Occurred > Occurred when DSP Error happens in the DSP of a device. * Detailed Information : DSP Error code number - "Code 10"
0511	DECT Base Status	Fault	MAJ	DEV(#)	ON	< DECT Base Disconnected > Occurred when the connection between DECT gateway and DECT base is disconnected. This may happen when the cable is not properly connecting DECT gateway and DECT base, or the status of DECT base is not normal. * Detailed Information : Base number - "Base 1"
					OFF	< DECT Base Connected > Occurred when the connection between DECT gateway and DECT base is recovered. * Detailed Information : Base number - "Base 1"
0513	DECT GW Fault	Fault	MAJ	DEV(#)	NONE	< DECT Gateway Fault > Occurred when Base or Chain connections are not stable. This may happen when the connection between DECT gateway and DECT base or the Chain connections between DECT gateways are not stable (so that the connection status keeps changing between connected and disconnected states). * Detailed Information : Base number or Chain - "Base 1" or "Chain" * Related Attendant Alarm : "WTIM BASE FAULT", "WTIM CHAIN FAULT"
0521	Device Line Up/Down	Fault	MAJ	DEV(#)	ON	< Device Line Down > Occurred when the status of T1/E1/PRI line becomes Down. * Detailed Information : None * Related Attendant Alarm : DCOB FAULT
					OFF	< Device Line Up >

						Occurred when the status of T1/E1/PRI line becomes Up. * Detailed Information : None
0523	Gatekeeper Connectivity	Fault	MAJ	DEV(#)	ON	< Gatekeeper Disconnected > Occurred when the connection between H.323 gateway (e.g. VOIM) and Gatekeeper is disconnected. * Detailed Information : None
					OFF	< Gatekeeper Connected > Occurred when the connection between H.323 gateway (e.g. VOIM) and Gatekeeper is recovered. * Detailed Information : None
0525	SIP Proxy Server Connectivity	Fault	MAJ	DEV(#)	ON	< SIP Proxy Disconnected > Occurred when the connection between SIP gateway (e.g. VOIM) and SIP Proxy Server is disconnected. * Detailed Information : None
					OFF	< SIP Proxy Connected > Occurred when the connection between SIP gateway (e.g. VOIM) and SIP Proxy Server is recovered. * Detailed Information : None
0601	Cabinet Fan/Power Failure	Fault	MAJ	CABINET(#) (KSU(#))	ON	< Cabinet Failure Occurred > Occurred when Fan failure or Power failure happens in an iPECS Cabinet. * Detailed Information : The Fan number or Power (PSU) number that caused the failure. - "FAN 1", "POWER 2" * Related Attendant Alarm : CABINET # STS FAULT
					OFF	< Cabinet Failure Cleared > Occurred when the Fan failure or Power failure condition is cleared. * Detailed Information : The Fan number or Power (PSU) number that was recovered from failure. - "FAN 1", "POWER 2"

< System Information Event >

Code	Name	Type	Level	Location	State	Description
0701	System Reset by Admin	System	CRI	MFIM (MPB)	NONE	< System Reset by Admin > Occurred when iPECS system is restarted manually by administrator using Web Admin, Keyset Admin, or Terminal

						<p>Maintenance. (This event is not caused by MFIM power off or reset button on the front panel of MFIM.)</p> <p>* Detailed Information : The cause of the restart (reset)</p> <ul style="list-style-type: none"> - Keyset Admin - Web Admin (Reset System) - Web Admin (Delete Device) - Web Admin (System ID Information Changed) - Web Admin (System IP Information Changed) - Web Admin (CO Gateway Sequence Number Changed) - Maintenance Command
0702	System ID Information Change	System	MAJ	MFIM (MPB)	NONE	<p>< System ID Information Changed ></p> <p>Occurred when administrator changed nation code or numbering plan of a system using Web Admin, Keyset Admin, or Terminal Maintenance.</p> <p>* Detailed Information : Changed information</p> <ul style="list-style-type: none"> - "Nation Code" - "Numbering Plan"
0703	System IP Information Change	System	MAJ	MFIM (MPB)	NONE	<p>< System IP Information Changed ></p> <p>Occurred when IP address information is changed by administrator using Web Admin, Keyset Admin, or Terminal Maintenance.</p> <p>* Detailed Information : Changed Information</p> <ul style="list-style-type: none"> - "MFIM/E IP Address" - "MFIM/E Sub Net Mask" - "Router IP Address" - "System IP Range Start" - "System IP Range End" - "System Sub Net Mask" - "Second System IP Address" - "Second System Net Mask" - "Firewall IP Address" - "MFIM/E LAN2 Master IP Address" - "MFIM/E LAN2 Slave IP Address" - "DNS IP Address"
0704	SNMP Reconfiguration	System	MIN	MFIM (MPB)	NONE	<p>< SNMP Reconfigured ></p> <p>Occurred when SNMP</p>

						configuration information is changed by administrator using Web Admin, or Terminal Maintenance. * Detailed Information : None
0705	Database Initialization	System	MAJ	MFIM (MPB)	NONE	< Database Initialized > Occurred when system database is initialized by administrator using Web Admin, or Keyset Admin. * Detailed Information : Information of initialized database - "Flexible Numbering Plan" - "Station Data" - "CO Line Data" - "System Data" - "Station Group Data" - "ISDN Tables" - "System Timer" - "Toll Tables" - "LCR Data" - "Other Tables" - "Flexible Button" - "Networking Data" - "All Database"
0706	File Upload	System	MIN	MFIM (MPB)	NONE	< File Upload Finished > Occurred when file uploading to MFIM is finished (performed by administrator using Web Admin). * Detailed Information : The result of file upload operation & the name of the uploaded file. - "SUCCESS : GS97ME0As.rom" - "FAIL (DISK SIZE)" - "FAIL (FILE NAME)" - "FAIL (FILE FORMAT)"
0707	Firmware Download	System	MAJ	MFIM (MPB)	ON	< Firmware Download Start > Occurred when MFIM firmware downloading is started. * Detailed Information : None
					OFF	< Firmware Download End > Occurred when MFIM firmware downloading is finished. * Detailed Information : The result of firmware download operation - "SUCCESS" or "FAIL"
0801	Device Registration / Deletion	System	MAJ	DEV(#)	ON	< Device Registered > Occurred when a device is newly registered, or Hot Desk

						user logs in. * Detailed Information : None
					OFF	< Device Unregistered > Occurred when a device is deleted using Device Delete Feature of Web Admin, or Hot Desk user logs out. * Detailed Information : None
0803	Device Service Status	System	MIN	DEV(#)	ON	< Admin Set Device Out-of-Service > Occurred when administrator makes a device into Out-of-Service state using Web Admin. * Detailed Information : None
					OFF	< Admin Set Device I-Service > Occurred when administrator recovers a device from Out-of-Service state using Web Admin. * Detailed Information : None
0805	Device Service Switch Status	System	MAJ	DEV(#)	ON	< Device Switch Service Mode > Occurred when the Normal/Service switch on the front panel of gateway device is moved to Service position. (If a device is in Service mode, no additional calls can be made.) * Detailed Information : None
					OFF	< Device Switch Normal Mode > Occurred when the Normal/Service switch on the front panel of gateway device is moved to Normal position. * Detailed Information : None
0807	Device Firmware Download	System	MAJ	DEV(#)	ON	< Device Firmware Download Start > Occurred when device firmware downloading (from MFIM to device) is started. * Detailed Information : Device firmware version
					OFF	< Device Firmware Download End > Occurred when device firmware downloading is finished. * Detailed Information : The result of device firmware download operation & firmware version. - "SUCCESS : 42Bc" - "FAIL : 42Bc"
0809	CO Line Outgoing Block Status	System	MIN	COL(#)	ON	< CO Blocked by Attendant > Occurred when administrator

						restricts outgoing access to CO/IP lines (using attendant program code 0-7-2). * Detailed Information : None
					OFF	< CO Unblocked by Attendant > Occurred when administrator recovers CO/IP lines from outgoing access restriction. * Detailed Information : None
0811	Device Order Change	System	MAJ	DEV(#)	NONE	< CO Gateway Order Changed > Occurred when administrator changed the order of CO gateways using Web Admin or Keypad Admin. * Detailed Information : None
0812	Station Number Change	System	MAJ	STA	NONE	< Station Logical Number Changed > Occurred when administrator changed station number using Web Admin or Keypad Admin. (Station number can be changed for individual station, station order range, or station number range.) * Detailed Information : Changed station number information - "Station(1) 1000 -> 2000" : for individual station - "Ordering Range 1 ~ 100 -> 2000 ~" : for station order range - "Station Range 1000 ~ 1100 -> 2000 ~" : for station number range
0813	Soft Phone Log In/Out	System	MIN	DEV(#)	ON	< System Reset by Admin > Occurred when iPECS system is restarted manually by administrator using Web Admin, Keypad Admin, or Terminal Maintenance. (This event is not caused by MFIM power off or reset button on the front panel of MFIM.) * Detailed Information : The cause of the restart (reset) - Keypad Admin - Web Admin (Reset System) - Web Admin (Delete Device) - Web Admin (System ID Information Changed) - Web Admin (System IP Information Changed)

						<ul style="list-style-type: none"> - Web Admin (CO Gateway Sequence Number Changed) - Maintenance Command
					OFF	<p>< System ID Information Changed > Occurred when administrator changed nation code or numbering plan of a system using Web Admin, Keyset Admin, or Terminal Maintenance. * Detailed Information : Changed information - "Nation Code" - "Numbering Plan"</p>
0815	Hot Desk Log In/Out	System	MIN	DEV(#)	ON	<p>< System IP Information Changed > Occurred when IP address information is changed by administrator using Web Admin, Keyset Admin, or Terminal Maintenance. * Detailed Information : Changed Information - "MFIM/E IP Address" - "MFIM/E Sub Net Mask" - "Router IP Address" - "System IP Range Start" - "System IP Range End" - "System Sub Net Mask" - "Second System IP Address" - "Second System Net Mask" - "Firewall IP Address" - "MFIM/E LAN2 Master IP Address" - "MFIM/E LAN2 Slave IP Address" - "DNS IP Address"</p>
					OFF	<p>< SNMP Reconfigured > Occurred when SNMP configuration information is changed by administrator using Web Admin, or Terminal Maintenance. * Detailed Information : None</p>
0819	Long Time Call Occurred/Cleared	System	MIN	DEV(#)	ON	<p>< Database Initialized > Occurred when system database is initialized by administrator using Web Admin, or Keyset Admin. * Detailed Information : Information of initialized database</p>

						<ul style="list-style-type: none"> - "Flexible Numbering Plan" - "Station Data" - "CO Line Data" - "System Data" - "Station Group Data" - "ISDN Tables" - "System Timer" - "Toll Tables" - "LCR Data" - "Other Tables" - "Flexible Button" - "Networking Data" - "All Database"
					OFF	<p>< File Upload Finished > Occurred when file uploading to MFIM is finished (performed by administrator using Web Admin).</p> <p>* Detailed Information : The result of file upload operation & the name of the uploaded file.</p> <ul style="list-style-type: none"> - "SUCCESS : GS97ME0As.rom" - "FAIL (DISK SIZE)" - "FAIL (FILE NAME)" - "FAIL (FILE FORMAT)"
0821	PGM Data Save	System	MIN	MFIM (MPB)	NONE	<p>< Firmware Download Start > Occurred when MFIM firmware downloading is started.</p> <p>* Detailed Information : None</p>
0823	Emergency Call	System	MAJ	STA(#)	NONE	<p>< Emergency Call > when Emergency call is dialed, this alarm is occurred.</p>
0825	Bomb Threat	System	CRI	STA(#)	NONE	<p>< Bomb Threat > Occurred when Bomb Threat is occurred.</p>
0827	Bath Alarm	System	MIN	STA(#)	ON	<p>< Bath Alarm Occurred> Occurred when Bath Alarm is on in hotel</p>
					OFF	<p>< Bath Alarm Cleared> Occurred when Bath Alarm is off by manager in hotel</p>

NOTE - iPECS-MG system does not support "Stand-by MFIM Status", "MFIM Switch Over", "DECT GW Fault", "Gatekeeper Connectivity", "SIP Proxy Server Connectivity", "Device Service Status", "Device Service Switch Status", "CO Line Outgoing Block Status", "Long Time Call Occurred/Cleared" events

< Switch Alarm Event >

Code	Name	Type	Level	Location	State	Description
2007	Port Security	Fault	MIN	Switch	NONE	< Port Security > This trap is sent when the port is being intruded. This trap will only be sent when the corresponding setting is enabled.
2013	ATC Broadcast Storm Alarm Fire	Fault	MIN	Switch	NONE	< ATC Broadcast Storm Alarm Fire > When the broadcast traffic is detected as the storm, this trap will be fired.
2014	ATC Broadcast Storm Alarm Clear	Fault	MIN	Switch	NONE	< ATC Broadcast Storm Alarm Clear > When the broadcast storm is detected as the normal traffic, this trap will be fired.
2017	ATC Multicast Storm Alarm Fire	Fault	MIN	Switch	NONE	< ATC Multicast Storm Alarm Fire > When the multicast traffic is detected as the storm, this trap will be fired.
2018	ATC Multicast Storm Alarm Clear	Fault	MIN	Switch	NONE	< ATC Multicast Storm Alarm Clear > When the multicast storm is detected as the normal traffic, this trap will be fired.
2029	Loopback Detection	Fault	MIN	Switch	NONE	< Loopback Detection > This trap will be sent when loopback BPDUs have been detected.
2033	CPU Utilization Rising	Fault	MIN	Switch	NONE	< CPU Utilization Rising > This notification indicates that the CPU utilization has risen from cpuUtiFallingThreshold to cpuUtiRisingThreshold.
2034	CPU Utilization Falling	Fault	MIN	Switch	NONE	< CPU Utilization Falling > This notification indicates that the CPU utilization has fallen from cpuUtiRisingThreshold to cpuUtiFallingThreshold.
2035	Memory Utilization Rising Treshold	Fault	MIN	Switch	NONE	< Memory Utilization Rising Treshold > This notification indicates that the memory utilization has risen from memoryUtiFallingThreshold to memoryUtiRisingThreshold.
2036	Memory Utilization Falling Threshold	Fault	MIN	Switch	NONE	< Memory Utilization Falling Threshold > This notification indicates that the memory utilization has fallen from memoryUtiRisingThreshold to

						memoryUtiFallingThreshold.
2037	IP Filter Inet Reject	Fault	MIN	Switch	NONE	< IP Filter Inet Reject > This trap is sent when an incorrect IP address is rejected by the IP filter.

< Switch Fault Event >

Code	Name	Type	Level	Location	State	Description
2003	Fan Failure	Fault	MIN	Switch	NONE	< Fan Failure > This trap is sent when the fan has failed.
2005	Fan Recover	Fault	MIN	Switch	NONE	< Fan Recover > This trap is sent when fan failure has recovered.
2009	Authentication Failurre	Fault	MIN	Switch	NONE	< Authentication Failurre > This trap will be triggered if authentication is failed.
2011	Authentication Success	Fault	MIN	Switch	NONE	< Authentication Success > This trap will be triggered if authentication is successful.

< Switch Information Event >

Code	Name	Type	Level	Location	State	Description
2021	STP Becom Root Bridge	Fault	MIN	Switch	NONE	< STP Becom Root Bridge > This trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after it has been elected as the new root. When spanning tree algorithm is STP or RSTP, trapMstInstanceId is always 0 and meaningless.
2023	STP Port Enter Forwarding	Fault	MIN	Switch	NONE	< STP Port Enter Forwarding > The trap is sent by a bridge when any of its configured ports transit from Learning state to Forwarding state. When spanning tree algorithm is STP or RSTP, trapMstInstanceId is always 0 and meaningless.
2025	STP Root Port Changed	Fault	MIN	Switch	NONE	< STP Root Port Changed > The trap is sent when the root port of a bridge has changed. When spanning tree algorithm is STP or RSTP, trapMstInstanceId is always 0 and meaningless.
2027	STP Root Bridge Changed	Fault	MIN	Switch	NONE	< STP Root Bridge Changed > The trap will be sent when the root bridge of bridges has changed and the bridge sending

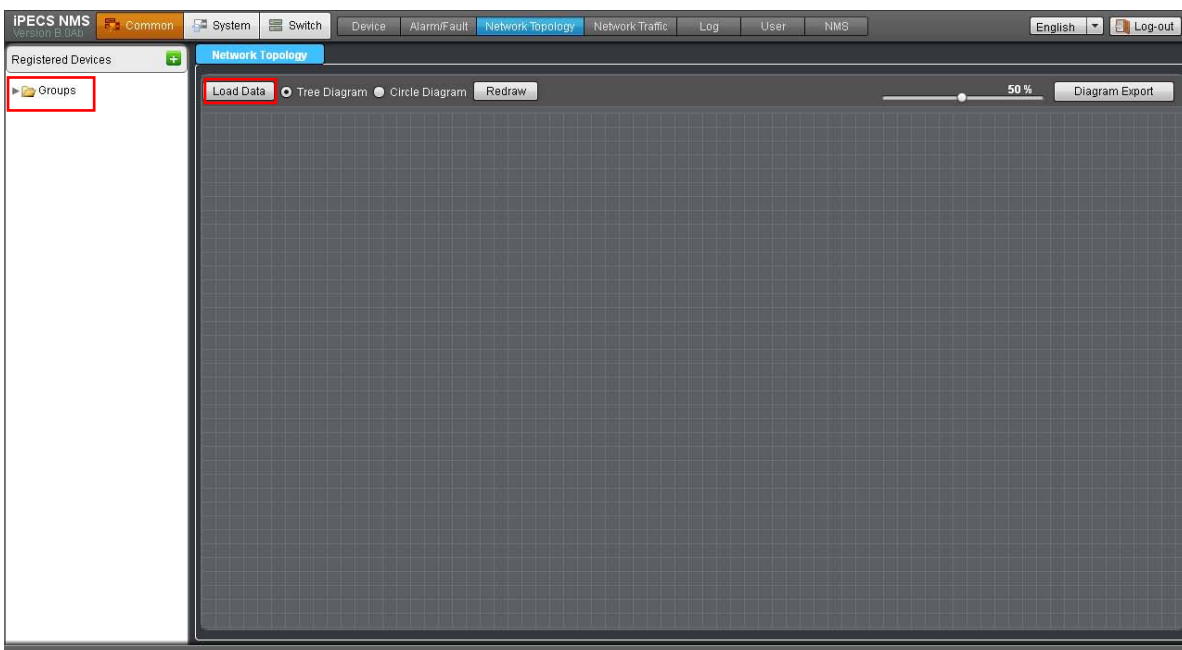
						off the trap is not the root in STP topology. When spanning tree algorithm is STP or RSTP, trapMstInstanceId is always 0 and meaningless.
--	--	--	--	--	--	---

8. Network Topology

'Network Topology' is used to provide topology diagram and LLDP information table by retrieving LLDP (Link Layer Discovery Protocol) MIB (Management Information Base) information from iPECS switches using SNMP (Simple Network Management Protocol). Topology diagram provides brief device information as well as diagram format selection and zooming features. LLDP information table provides detailed information for each local system and the remote devices connected to it. 'Network Topology' page can be viewed by selecting [Topology] sub-menu under 'Common' menu.

8.1 Displaying Topology Diagram

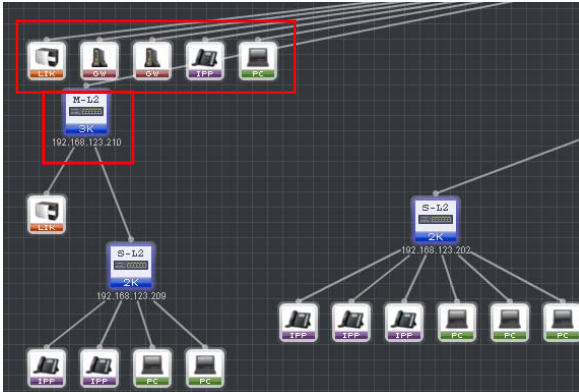
In order to display topology diagram, first select a device or device group in 'Registered Devices', then click [Load Data] button on 'Network Topology' screen.



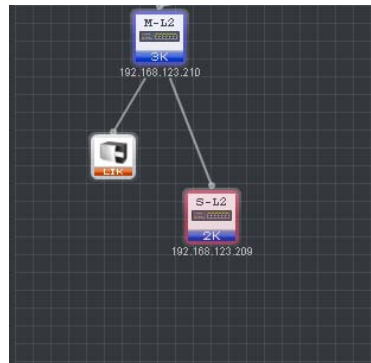
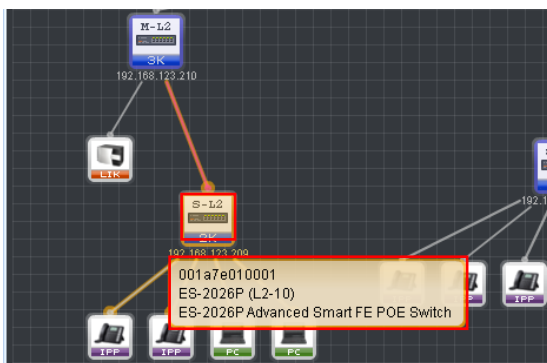
If a device group is selected in 'Registered Devices', LLDP information is retrieved from the member devices of the selected group and its sub-groups. If a device is selected, LLDP information of the selected device is retrieved. After data retrieval is completed, topology diagram is displayed.

8.2 Basic Features of Topology Diagram

Topology diagram provides brief information of each node as well as other basic functions such as hiding branch nodes, changing root node and moving node position.



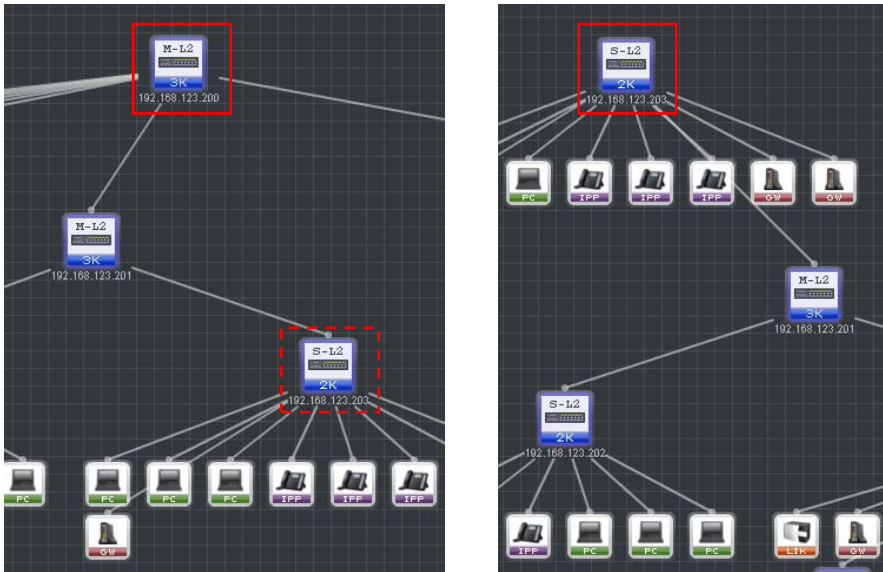
Under an iPECS switch, other devices than switch devices are placed first and then on the next layer, switch devices are displayed.



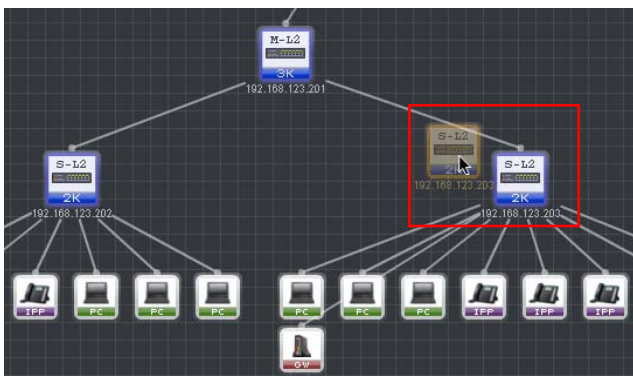
When the mouse pointer is placed on a device node, brief information of the device appears as tooltip displaying chassis ID, device name and device description.

If an iPECS switch node is clicked with left mouse button, all the nodes under the switch node become hidden, and one more click makes the hidden nodes to be displayed again.

When generating topology diagram, iPECS-NMS elects a root node based on the retrieved LLDP MIB information and places it on the top layer. However, the elected root node may be different from the root node the network administrator assigned or the root node on the actual physical topology.



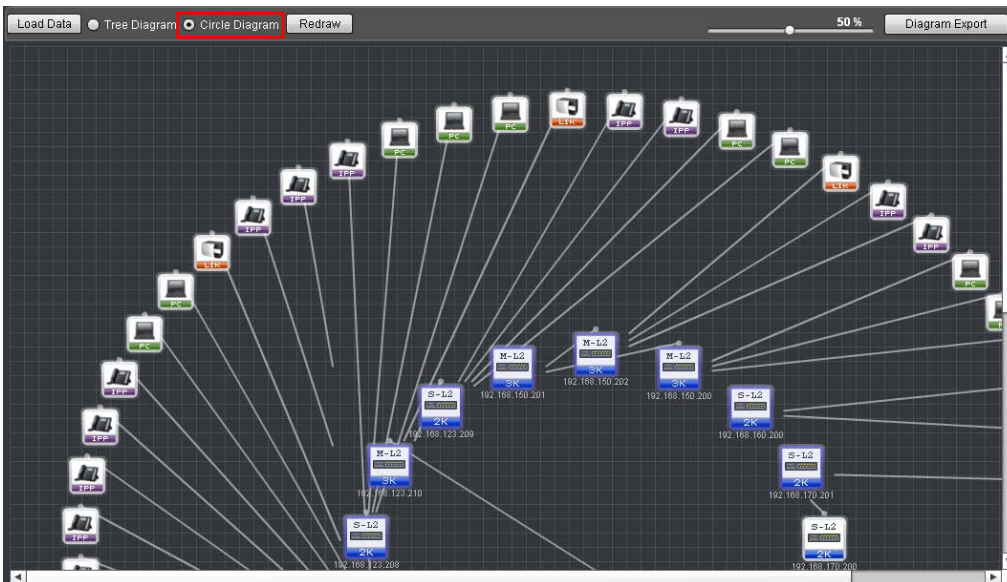
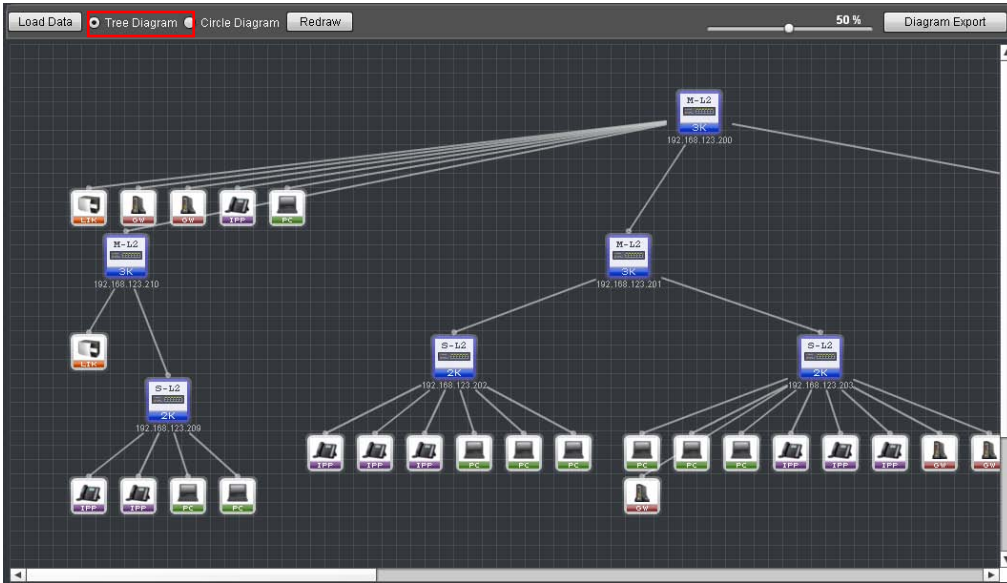
In order to change the root node on the topology diagram, double-click on the iPECS switch node that is to be assigned as a new root node.



In order to move the position of a node on topology diagram, drag-and-drop the node to a desired position using left mouse button.

8.3 Additional Features of Topology Diagram

Topology diagram also provides additional features such as diagram format selection, diagram zooming and diagram export into a picture file.



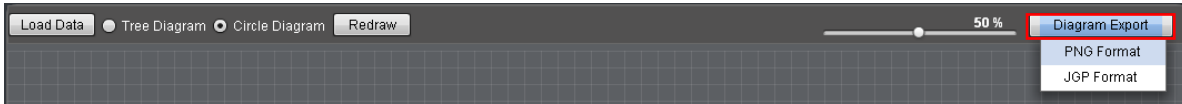
In order to select tree or circle formats, click [Tree Diagram] or [Circle Diagram] radio button, respectively.

Depending on the number of device nodes, it may be convenient to change the size of the topology diagram. In order to change the size, use the 'Diagram Zoom' slider to reduce or enlarge the diagram.

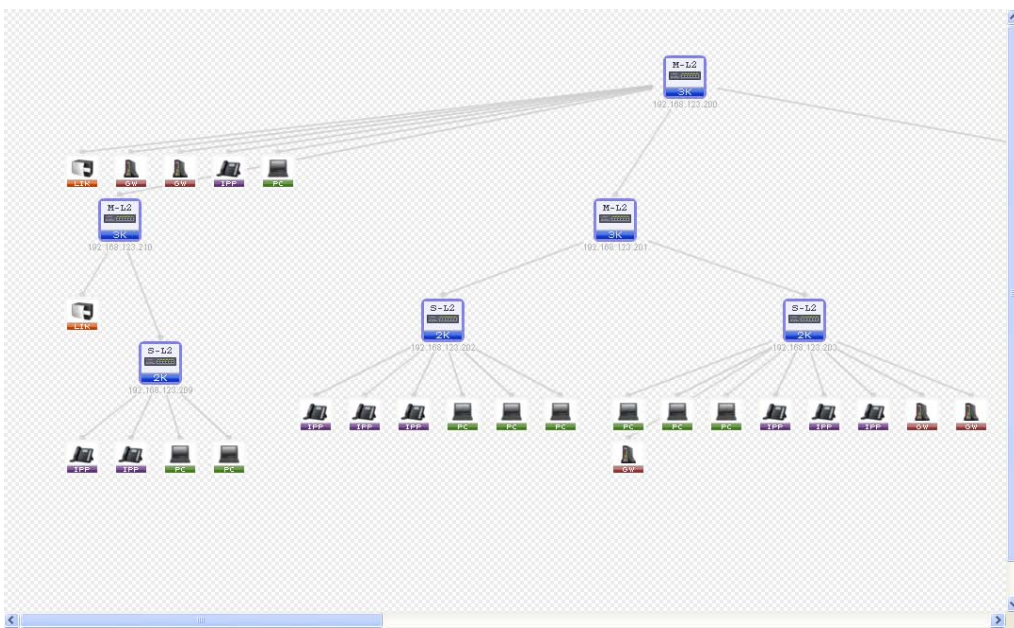


After changing the size of the diagram or moving a node to a different position, it may be needed to display the original diagram iPECS-NMS automatically generated. In this case, the original diagram can be displayed by clicking [Redraw] button.

Diagram export can be used to store the topology diagram automatically generated by iPECS-NMS into PNG or JPG format picture file.



Clicking [Diagram Export] button shows two options of [PNG Format] and [JPG Format]. After selecting a picture format on the menu and entering a file name, the topology diagram automatically generated by iPECS-UDM is stored into a picture file with the given name.



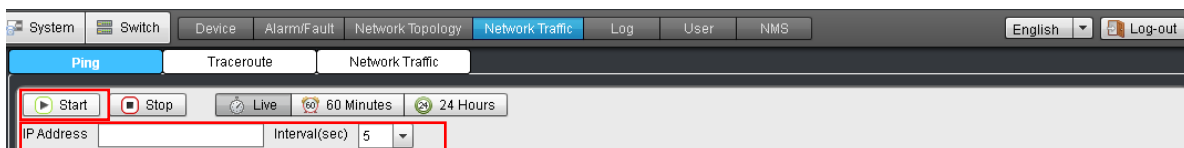
The picture above shows an example of exported topology diagram that is read and displayed by a picture editing application.

9. Network Traffic Monitoring

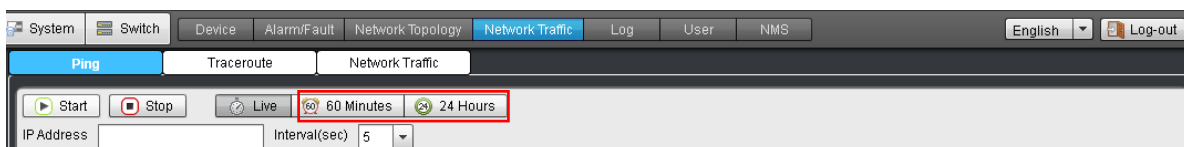
'Network Traffic Monitoring' provides the means to monitor the network traffic and the connection status of a network device. For general network devices, Ping test, Traceroute test, and network traffic monitoring features are provided. The pages for these features can be viewed by clicking [Network Traffic] sub-menu under 'Common' menu.

9.1 Ping Test

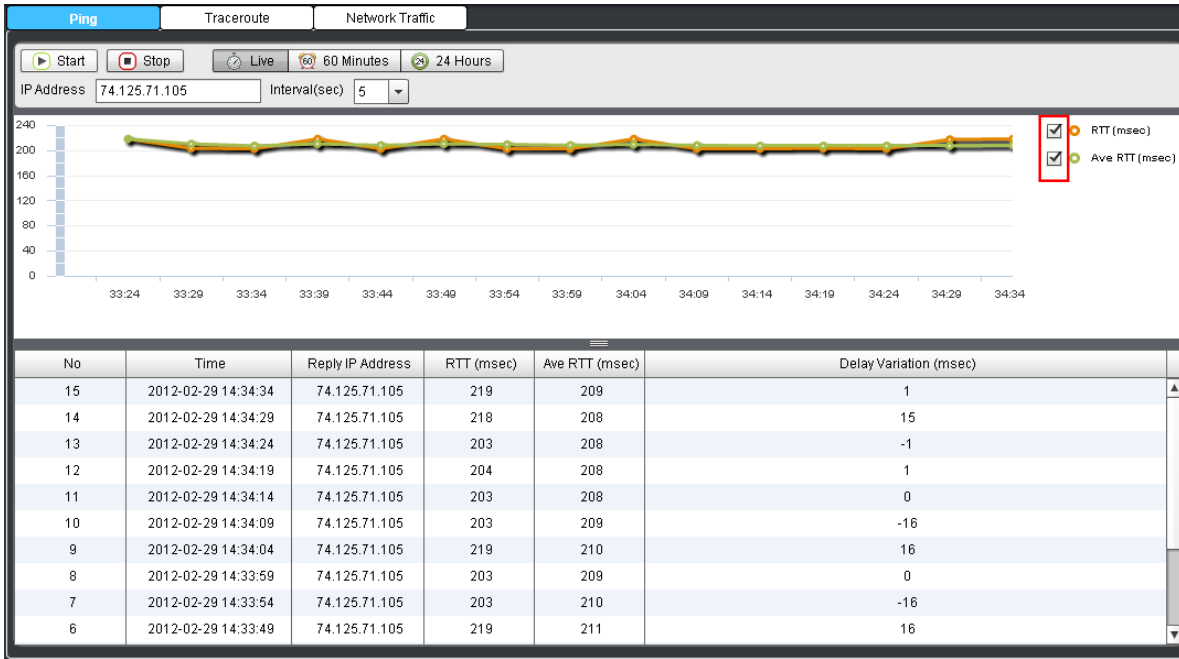
'Ping Test' provides functions to check the connection status and the packet delay time between iPECS-NMS and a general network device, and can be viewed by clicking [Ping] tab under 'Network Traffic' sub-menu.



Before performing Ping test, the IP address of the target network device, and the interval for Ping packet transmission should be configured. For 'Interval' field, one of 5, 10, 20, 30 second options can be selected using the combo-box. After finishing configuration, click [Start] button to initiate Ping test, and [Stop] to finish it. Ping test will be automatically finished without using [Stop] button if the polling count reaches 65545 times.



The graph and table that show the result of Ping test can be displayed in three types of time period such as 'Live Data', 'Last 60 Minutes', and 'Last 24 Hours'. The real-time graph and table are displayed by clicking [Live] button. [60 Minutes] and [24 Hours] buttons are used for displaying the graphs and tables for last 60 minutes and 24 hours from the moment the corresponding button was clicked.



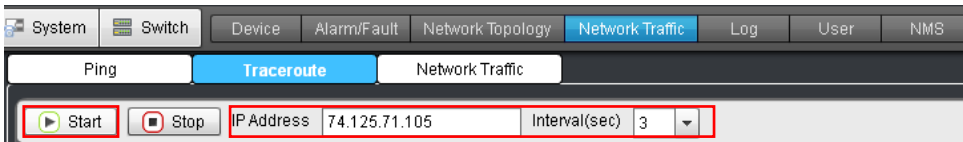
The graph in the picture above shows the changes in RTT (Round-Trip Time), which is the time between the transmission of a Ping packet and the reception of the response packet. RTT is often used to estimate the packet delay time in a network environment. The table below the graph shows the information from the Ping test, and the meanings of the table fields are as follows.

Table Name	Field Name	Description
Live Data	Time	The time when the Ping packet was actually transmitted to the target device. The 'Time' interval may not be exactly same as the 'Interval' value depending on the operational or processing load on the NMS server.
	Reply IP Address	The IP address of the device that responded to the Ping packet sent by iPECS-NMS.
	RTT	Abbreviation of Round-Trip Time. This is the elapsed time until the reception of the response packet to a Ping packet sent by iPECS-NMS.
	Average RTT	The overall average of the RTT values from all the Ping tests calculated since the beginning of the Ping test.
Last 60 Minutes	Time	The time when the Ping packet was actually transmitted to the target device. The 'Time' interval may not be exactly same as the 'Interval' value depending on the operational or processing load on the NMS server.
	Reply IP Address	The IP address of the device that responded to the Ping packet sent by iPECS-NMS.
	RTT	This is the average of the RTT values from the Ping tests for last 1 minute (actually, the time between the previous row and the current row in the table).
	Average RTT	The overall average of the RTT values from all the Ping

		tests calculated since the beginning of the Ping test.
	Delay Variation	The difference in value between the RTT values of the previous row and the current row of the table.
Last 24 Hours	Time	The time when the Ping packet was actually transmitted to the target device. The 'Time' interval may not be exactly same as the 'Interval' value depending on the operational or processing load on the NMS server.
	Reply IP Address	The IP address of the device that responded to the Ping packet sent by iPECS-NMS.
	RTT	This is the average of the RTT values from the Ping tests for last 1 hour (actually, the time between the previous row and the current row in the table).
	Average RTT	The overall average of the RTT values from all the Ping tests calculated since the beginning of the Ping test.
	Delay Variation	The difference in value between the RTT values of the previous row and the current row of the table.

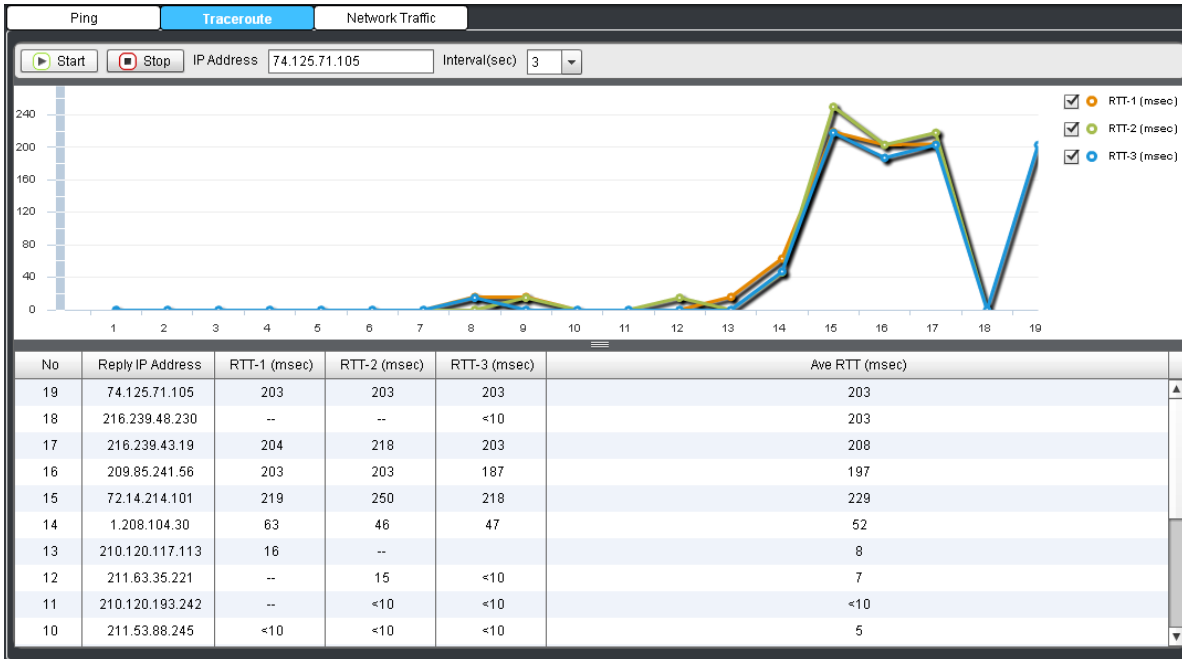
9.2 Traceroute Test

'Traceroute Test' provides functions to check the packet delivery path and packet delay time for each hop to the destination between iPECS-NMS and a general network device, utilizing 'ICMP' message and the TTL field in IP packet header. The page for this feature can be viewed by clicking [Traceroute] tab under 'Network Traffic' sub-menu.



Before performing Traceroute test, the IP address of the target network device and the interval for Traceroute packet transmission should be configured. For 'Interval' field, one of 3, 4, 5 second options can be selected using the combo-box.

After the configuration is completed, Traceroute test can be started by clicking [Start] button. If it is needed to stop the Traceroute test before the completion of the test (before the destination device has been reached), user may click [Stop] button to force the test to be stopped. After a Traceroute test is started, real-time graph and table that show the Traceroute result for each hop to the destination are displayed below.



The graph of Traceroute test shows the changes in RTT (Round-Trip Time) for each hop to the destination, in real-time. RTT is the time between the transmission of a Traceroute packet and the reception of the response packet, and is often used to designate the packet delay time in a network environment.

The table below the graph shows the hops on the path to the destination in sequence, and the RTT from the three trials to the same hop and their average value are displayed together with the 'Reply IP Address' information. The meanings of the table fields are as follows.

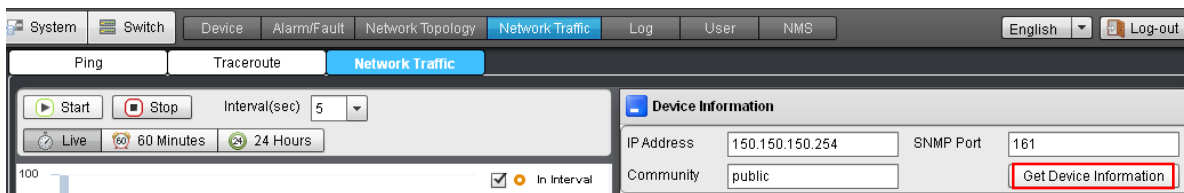
Field Name	Description
Reply IP Address	The IP address of the device that responded with 'ICMP Time Exceeded' message to the Traceroute packet sent by iPECS-NMS. Normally, this is the IP address of a router on the path to the destination or of the target device itself.
RTT-1	This is the elapsed time until the reception of the response packet to the first Traceroute packet to a device on the path to the destination or the target device. (RTT is the abbreviation of Round-Trip Time.)
RTT-2	This is the elapsed time until the reception of the response packet to the second Traceroute packet to a device on the path to the destination or the target device.
RTT-3	This is the elapsed time until the reception of the response packet to the third Traceroute packet to a device on the path to the destination or the target device.
Average RTT	The average of the RTT values from the three Traceroute trials to the same destination.

9.3 Device Network Traffic

'Device Network Traffic' provides functions to retrieve network device information and its interface configuration/status, and to monitor the real-time network traffic of the device using

SNMP messages. The page for this feature can be viewed by clicking [Network Traffic] tab under ‘Network Traffic’ sub-menu.

‘Device Network Traffic’ has two functional parts. ‘Device Information’ on the right is to retrieve and display general device information and network interface information, and ‘Device Traffic’ on the left is to present graph and table of real-time network traffic information. These two parts are functionally separated, but because ‘Device Traffic’ part can be working based on the information retrieved in ‘Device Information’, ‘Device Information’ part should always be configured and executed first.



In order to retrieve device information, the ‘IP Address’, ‘SNMP Port’, and SNMP ‘Community’ information should be entered. For ‘SNMP Port’ field, the standard SNMP port number ‘161’ can usually be used, but if the target device uses different port number for SNMP communication, that port number should be entered. For ‘Community’ field, ‘public’ can usually be used for general network devices, but if the target device uses different SNMP community string, that string should be entered. After the configuration is finished, general device information and its interface information can be retrieved and displayed by clicking [Get Device Information] button.

Device Information

IP Address: 150.150.150.254 SNMP Port: 161
 Community: public

Description: Cisco Internetwork Operating System Software
 IOS (tm) s72033_rp Software (s72033_rp-PK9SV-M), Versio
 12.2(17d)SXB5, RELEASE SOFTWARE (fc1)
 Technical Support: http://www.cisco.com/techsupport
 Copyright (c) 1986-2004 by cisco Systems, Inc.
 Compiled Fr

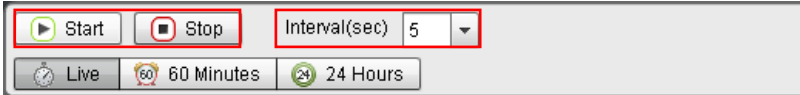
Name: NEW_6509
 UpTime: 1724941024
 Packet forward: 1
 Default TTL: 255

Interface Info.	Admin St.	Oper Stat.	Mac Address	MTU	Speed
GigabitEthernet2/1	Up	Up	0001c9b06e78	1500	10000000
GigabitEthernet2/2	Up	Up	0001c9b06e79	1500	10000000
GigabitEthernet2/3	Up	Up	0001c9b06e7a	1500	10000000
GigabitEthernet2/4	Up	Up	0001c9b06e7b	1500	10000000
GigabitEthernet2/5	Down	Down	0001c9b06e7c	1500	10000000
GigabitEthernet2/6	Down	Down	0001c9b06e7d	1500	10000000
GigabitEthernet2/7	Up	Down	0001c9b06e7e	1500	10000000

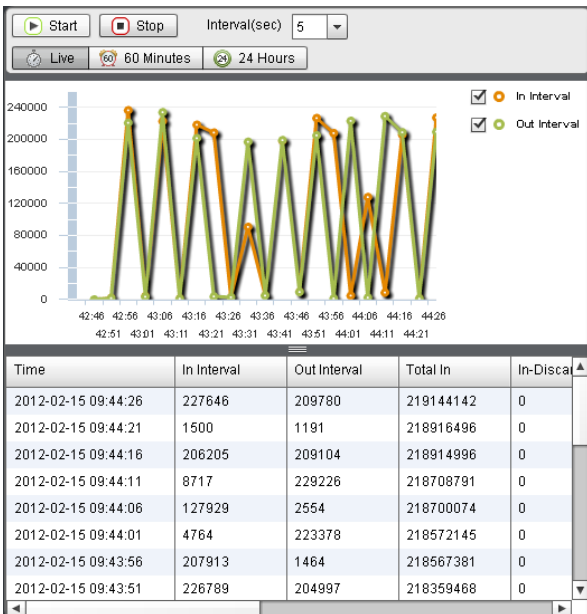
‘Device Information’ displays gneral information of the target network device, and the table below shows the device’s network interface information. The meanings of the fields are as follows.

Table Name	Field Name	Description
Device Information	Description	A textual description of the entity. This value normally includes the full name and version identification of the system's hardware type, software operating-system, and networking software.
	Name	An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.
	Up Time	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
	No. of Interface	The number of network interfaces (regardless of their current state) present on the device.
	Packet Forward	The indication of whether this entity is acting as an IP router in respect to the forwarding of datagrams received by, but not addressed to, this entity.
	Default TTL	The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.
Interface Information	Interface Info.	A textual string containing information about the interface. This string normally includes the name of the manufacturer, the product name and the version of the interface hardware/software.
	Admin Status	The desired state of the interface. The 'Testing' state indicates that no operational packets can be passed. When a managed device initializes, all interfaces start with 'Admin Status' in the 'Down' state. As a result of either explicit management action or per configuration information retained by the managed device, 'Admin Status' is then changed to either the 'Up' or 'Testing' states (or remains in the 'Down' state).
	Oper Status	The current operational state of the interface. The 'Testing' state indicates that no operational packets can be passed. If 'Admin Status' is 'Down' then 'Oper Status' should be 'Down'. If 'Admin Status' is changed to 'Up' then 'Oper Status' should change to 'Up' if the interface is ready to transmit and receive network traffic. It should remain in the 'Down' state if and only if there is a fault that prevents it from going to the 'Up' state. It should remain in the 'Not Present' state if the interface has missing (typically, hardware) components.
	MAC Address	The interface's address at its protocol sub-layer. For example, for an 802.x interface, this object normally contains a MAC address. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.
	MTU	The size of the largest packet which can be sent/received on the interface, specified in octets. For interfaces that are used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.
	Speed	An estimate of the interface's current bandwidth in bits

		per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. For a sub-layer which has no concept of bandwidth, this object should be zero.
--	--	---



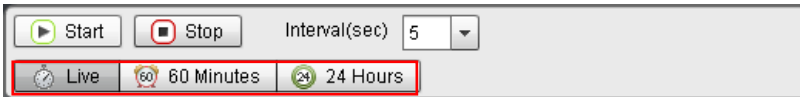
In order to monitor real-time network traffic of the target device, the interval for polling network traffic data should be configured. For 'Interval' field, one of 5, 10, 20, 30 second options can be selected using the combo-box. After finishing configuration, click [Start] button to initiate traffic monitoring, and [Stop] to finish it. Traffic monitoring will be automatically finished without using [Stop] button if the polling count reaches 65545 times.



The graph in the picture above shows in real time the number of incoming and outgoing packets that occurred during the polling interval, and the traffic table shows the traffic data occurred within the interval as well as the accumulated traffic data. The meanings of the table fields are as follows.

Field Name	Description
In-Interval	The number of packets received during the time period configured in 'Interval' field.
Out-Interval	The number of packets transmitted during the time period configured in 'Interval' field.
Total In	The total number of input datagrams received from interfaces, including those received in error.
In-Discard	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were

	discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.
In-Error	The number of input datagrams discarded due to errors in their IP headers, the use of unknown or unsupported protocol, or invalid IP address to be received at this device.
Total Out	The total number of IP datagrams which local IP user protocols (including ICMP) supplied to IP in requests for transmission, and the datagrams for which this device was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
Out-Discard	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).
Out-Error	The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which the device cannot route because all of its default routers are down.
Time	The time when iPECS-NMS retrieved traffic information from the target device. The 'Time' interval may not be exactly same as the 'Interval' value depending on the operational or processing load on the NMS server.



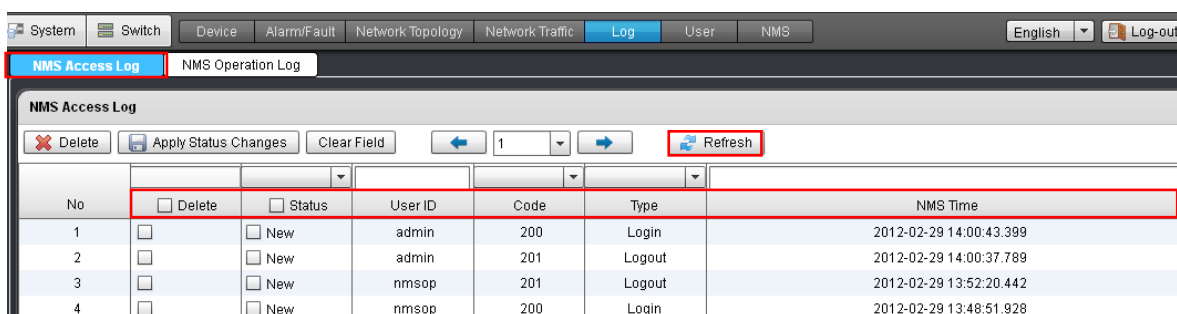
The graph and table that show the result of network traffic polling can be displayed in three types of time period such as 'Live Data', 'Last 60 Minutes', and 'Last 24 Hours'. The real-time graph and table are displayed by clicking [Live] button. [60 Minutes] and [24 Hours] buttons are used for displaying the graphs and tables for last 60 minutes and 24 hours from the moment the corresponding button was clicked.

10. Log & History Management

‘Log & History Management’ is for checking and managing the access & operation history of iPECS-NMS, and provides ‘NMS Access Log’ and ‘NMS Operation Log’ for the management of the history data. The pages for these features can be viewed by clicking [Log] tab under ‘Common’ sub-menu.

10.1 NMS Access Log

‘NMS Access Log’ provides means to store the access history of iPECS-NMS as log data, and to search and manage the access log. The page for this feature can be viewed by clicking [NMS Access Log] tab under ‘Log’ sub-menu.

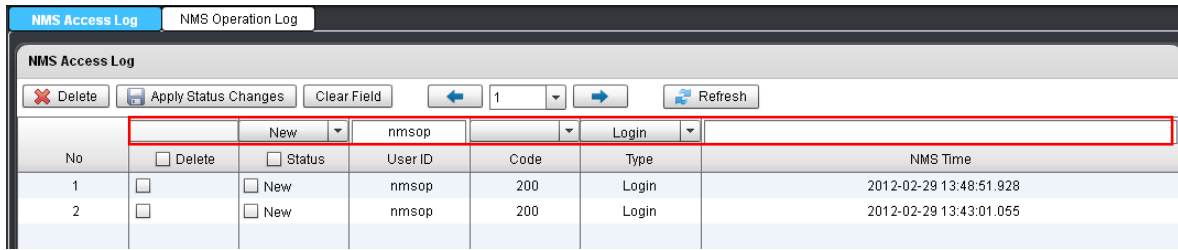


NMS access log data are displayed when entering ‘NMS Access Log’ page. In order to refresh the log data, click [Refresh] button. Search fields located above the table header are used for searching specific logs.

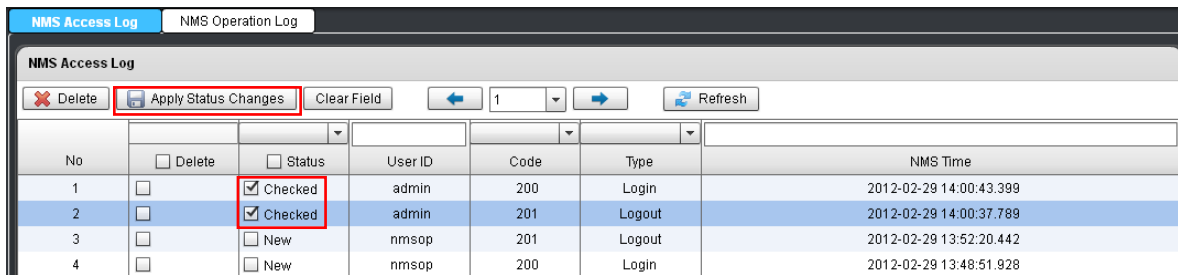
The types and meanings of the search fields are as follows.

Table Name	Field Name	Description
NMS Access Log	Status	- New : Indicates the log record has not been checked by the administrator. When login or logout event happens on iPECS-NMS, new log record is generated and stored with ‘New’ status. - Checked : Means the log record has been checked by the administrator. After a new record is checked by the administrator, the status of the item is to be manually changed to ‘Checked’ status and saved.
	User ID	This field is for entering target User ID to be used for searching.
	Code (Type)	This field is for entering the code number of target log type, and the meanings of the codes are as follows. - 200 (Login) : User logged in to iPECS-NMS

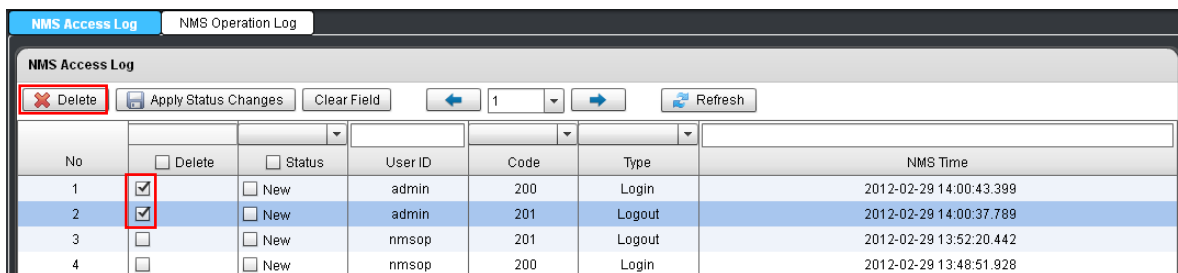
		- 201 (Logout) : User logged out from iPECS-NMS
	NMS Time	This field is for entering the time or time range when the login/logout events happened.



After loading access log data, search can be performed with various search conditions. Select combo box fields or enter search values in edit boxes to configure search conditions. Search operation is performed as soon as a search field is modified, and search result is displayed immediately.



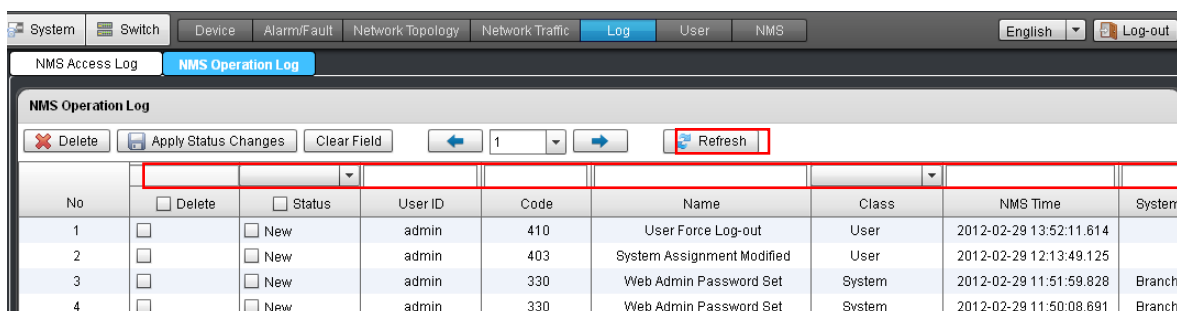
In order to change the status of a log item to 'New' or 'Checked' status, user may click on the check-box in 'Status' field of the target item. Then, click [Apply Status Changes] button to save and apply the change of status.



In order to delete a target log item, select the item by clicking the check-box in 'Delete' field, and then click [Delete] button to delete the selected item.

10.2 NMS Operation Log

‘NMS Operation Log’ provides means to store the NMS operation history as log data, and to search and manage the operation log. The page for this feature can be viewed by clicking [NMS Operation Log] tab under ‘Log’ sub-menu.



NMS operation log data are displayed when entering ‘NMS Operation Log’ page. In order to refresh the log data, click [Refresh] button. Search fields located above the table header are used for searching specific logs.

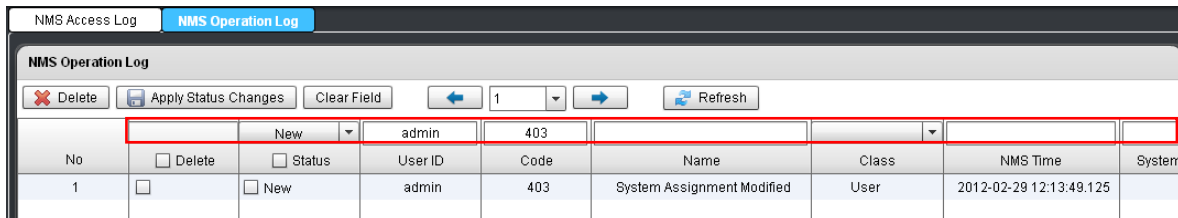
The types and meanings of the search fields are as follows.

Table Name	Field Name	Description
NMS Operation Log	Status	- New : Means the log item has been newly stored and has not been checked by the administrator. When an operational event happens on iPECS-NMS, new log item is generated and stored with ‘New’ status. - Checked : Means the log item has already been checked by the administrator. After a new item is checked by the administrator, the status of the item is supposed to be manually modified to ‘Checked’ status and saved.
	User ID	This field is for entering target User ID to be used for searching.
	Code	This field is for entering the code number of target operation type. The meanings of the codes are defined in the table below.
	Class	- System : Operations related to system management. - User : Operations related to user management. - NMS : Operations related to NMS management. - Alarm/Fault : Operations related to alarm/fault management - Call Statistics : Operations related to call statistics
	NMS Time	This field is for entering the time or time range when the operational events happened.
	System Name	This field is for entering the name of the system on which the operation is performed.

The table of operation codes that designate the operations done by users is shown below.

Operation Class	Code	Name
System	300	(Reserved)
	310	System Added

	311	System Deleted
	312	System Modified
	320	System Group Added
	321	System Group Deleted
	322	System Group Modified
	330	Web Admin Password Set
	331	Web Admin Started
	340	Firmware Upgrade
	341	Firmware Upgrade Cancel
	350	System DB Upload
	351	System DB Upload Cancel
	352	System DB Scheduled Backup
	353	System DB Scheduled Backup Cancel
	360	Prompt Upload
	361	Prompt Upload Cancel
	362	Individual Upload
	363	Individual Upload Cancel
	370	System Greeting Upload
	371	System Greeting Upload Cancel
	372	Individual Greeting Upload
	373	Individual Greeting Upload Cancel
User	400	User Added
	401	User Deleted
	402	User Modified
	403	System Assignment Modified
	410	User Force Log-out
NMS	500	Mail Server Set
	501	External Link Set
	502	KeepAlive Interval Set
	503	NHIC NMS Service Set
	504	Trap Community Set
Alarm/Fault	600	Log Item Checked
	601	Log Item Deleted
	602	Alarm Notification Set
Call Statistics	700	Traffic Configuration Set
	701	SMDR Data Set



After loading operation log data, search can be performed with various search conditions. Select combo box fields or enter search values in edit boxes to configure search conditions. Search operation is performed as soon as a search field is modified, and search result is displayed immediately.

The screenshot shows the 'NMS Operation Log' interface. At the top, there are tabs for 'NMS Access Log' and 'NMS Operation Log'. Below the tabs, there are buttons for 'Delete', 'Apply Status Changes', 'Clear Field', and 'Refresh'. A table below contains log entries with columns: No, Delete, Status, User ID, Code, Name, Class, NMS Time, and System. In the table, the 'Status' column for rows 1 and 2 has 'Checked' selected, and the 'Apply Status Changes' button is highlighted with a red box.

No	<input type="checkbox"/> Delete	<input type="checkbox"/> Status	User ID	Code	Name	Class	NMS Time	System
1	<input type="checkbox"/>	<input checked="" type="checkbox"/> Checked	admin	410	User Force Log-out	User	2012-02-29 13:52:11.614	
2	<input type="checkbox"/>	<input checked="" type="checkbox"/> Checked	admin	403	System Assignment Modified	User	2012-02-29 12:13:49.125	
3	<input type="checkbox"/>	<input type="checkbox"/> New	admin	330	Web Admin Password Set	System	2012-02-29 11:51:59.828	Branch
4	<input type="checkbox"/>	<input type="checkbox"/> New	admin	330	Web Admin Password Set	System	2012-02-29 11:50:08.691	Branch

In order to change the status of a log item to 'New' or 'Checked' status, user may click on the check-box in 'Status' field of the target item. Then, click [Apply Status Changes] button to save and apply the change of status.

The screenshot shows the 'NMS Operation Log' interface. At the top, there are tabs for 'NMS Access Log' and 'NMS Operation Log'. Below the tabs, there are buttons for 'Delete', 'Apply Status Changes', 'Clear Field', and 'Refresh'. A table below contains log entries with columns: No, Delete, Status, User ID, Code, Name, Class, NMS Time, and System. In the table, the 'Delete' column for rows 1 and 2 has checkboxes selected, and the 'Delete' button is highlighted with a red box.

No	<input type="checkbox"/> Delete	<input type="checkbox"/> Status	User ID	Code	Name	Class	NMS Time	System
1	<input checked="" type="checkbox"/>	<input type="checkbox"/> New	admin	410	User Force Log-out	User	2012-02-29 13:52:11.614	
2	<input checked="" type="checkbox"/>	<input type="checkbox"/> New	admin	403	System Assignment Modified	User	2012-02-29 12:13:49.125	
3	<input type="checkbox"/>	<input type="checkbox"/> New	admin	330	Web Admin Password Set	System	2012-02-29 11:51:59.828	Branch
4	<input type="checkbox"/>	<input type="checkbox"/> New	admin	330	Web Admin Password Set	System	2012-02-29 11:50:08.691	Branch

In order to delete a target log item, select the item by clicking the check-box in 'Delete' field, and then click [Delete] button to delete the selected item.

11. System Information

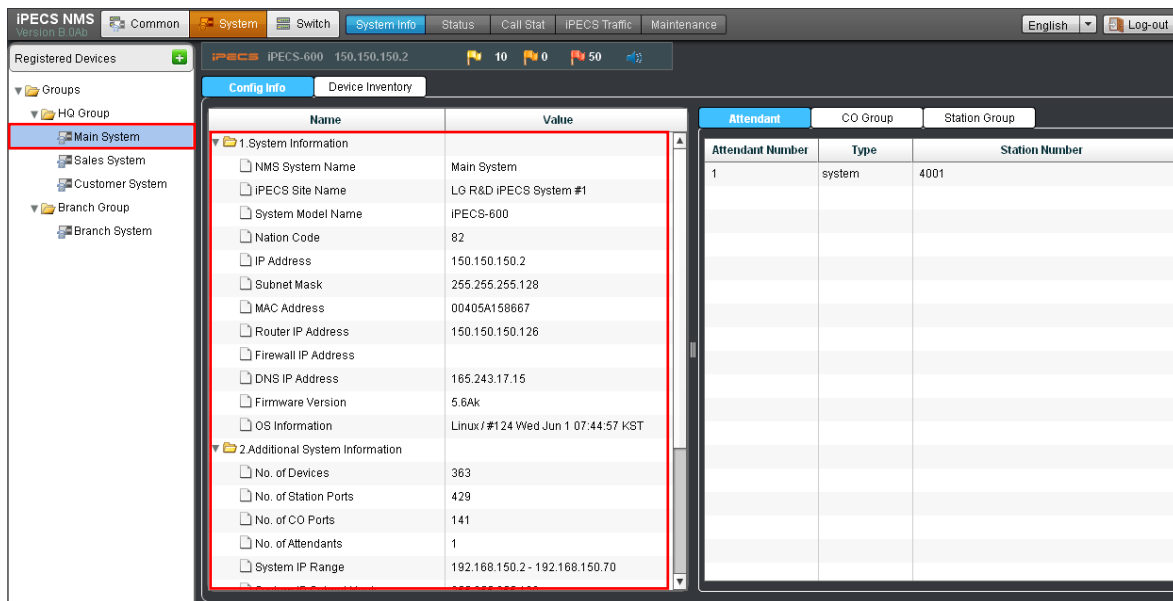
The System Information page gives basic information on the system selected in ‘Registered Devices’, including Attendant, CO Group, and Station Group information. It also provides device inventory information that shows a summary of System capacity and component devices. The pages for these features can be viewed by clicking [System Info] sub-menu under ‘System’ menu.

11.1 System Configuration Information

‘System Configuration Information’ provides system information summary and attendant, CO group & station group information of a selected system. The page for this feature can be viewed by clicking [Config Info] tab under ‘System Info’ sub-menu.

11.1.1 System Information Summary

‘System Information Summary’ provides basic configuration information (e.g. network address, firmware version, etc.) of a system selected in ‘Registered Devices’.



The information provided in ‘System Information Summary’ is grouped into two lists of ‘System Information’ and ‘Additional System Information’. The types of list fields and their meanings are as follows.

List Name	Field Name	Description
System Information	NMS System Name	The name of the system configured in iPECS-NMS when registering the system to iPECS-NMS.
	iPECS Site Name	'Site Name' field value of iPECS Web Admin (PGM 100).
	System Model Name	The model name of the system.
	Nation Code	The nation code of the system.
	IP Address	The IP address of MFIM(MPB).
	Subnet Mask	The subnet mask of MFIM(MPB).
	MAC Address	The MAC address of MFIM(MPB).
	Router IP Address	The router IP address of MFIM(MPB).
	Firewall IP Address	'Firewall IP Address' field value of iPECS-LiK Web Admin (PGM 102). If this address is configured, it means an NAT router exists in front of MFIM.
	DNS IP Address	The DNS IP address of MFIM(MPB).
	Firmware Version	The firmware version of MFIM(MPB).
	OS Information	The OS build information of MFIM(MPB).
Additional System Information	NO. of Devices	Number of iPECS devices that are registered to the system.
	NO. of Station Ports	Number of station device ports that are registered to the system.
	NO. of CO Ports	Number of CO device ports that are registered to the system.
	NO. of Attendants	Number of attendants (system attendant and main attendant)
	System IP Range	A range of IP addresses that are automatically assigned to local mode iPECS devices by the system. Normally, private IP addresses are used.
	System IP Subnet Mask	The subnet mask that is applied together with the System IP Addresses.
	2 nd System IP Address	Another IP address (in addition to System IP Address) that is to be used for direct communication among iPECS devices in local network segment.
	2 nd System IP Subnet Mask	The subnet mask that is applied together with the 2 nd System IP Address.
	System Codec Type	The audio codec type configured in iPECS-LiK Web Admin (PGM 161). This codec type is commonly used for voice calls unless different codec type is asserted for specific devices using PGM 132 (Board Base Attributes).
	MFIM DiffServ Code Point	The DSCP (DiffServ Code Point) value used for setting packet priority by DiffServ Pre-Tagging. In some cases, this value may be used as IP ToS (Type of Service) value.
	Auto IP Assign	This field designates if iPECS system automatically assigns IP address to local mode devices.
	CPU Redundancy Usage	This field designates if MFIM is configured to use CPU redundancy function.
T-Net Enable	This field designates if MFIM is configured to use T-Net (Transparent Networking) function.	

For iPECS-MG system, some additional system information such as 'No. of Attendants', 'System IP Range', 'System IP Subnet Mask', '2nd System IP Address', '2nd System IP Subnet Mask', 'System Codec Type', 'Auto IP Assign', 'CPU Redundancy Usage' are not provided.

11.1.2 Attendant, CO Group & Station Group Information

Selecting the [Attendant], [CO Group] or [Station Group] displays the associated page view with basic information on the specific characteristic of the iPECS system selected in ‘Registered Devices’.

Attendant		
Attendant Number	Type	Station Number
1	system	4001

Attendant information is displayed by clicking [Attendant] tab. It shows attendant number, attendant type, and attendant’s station number as a table. Attendant type can have one of two values of ‘system’ and ‘main’. For iPECS–MG, attendant types are ‘attendant’ and ‘night attendant’.

CO Group	
Group Number	CO Line Number
0	55,62,63,101,106,107
1	1,2,3,4,142,143,144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159,160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175,176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263,264,265,266,267,268,269,270,271,272,273,274,275,276,277,278,279,280,281,282,283,284,285,286,287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307,308,309,310,311,312,313,314,315,316,317,318,319,320,321,322,323,324,325,326,327,328,329,330,331,332,333,334,335,336,337,338,339,340,341,342,343,344,345,346,347,348,349,350,351,352,353,354,355,356,357,358,359,360,361,362,363,364,365,366,367,368,369,370,371,372,373,374,375,376,377,378,379,380,381,382,383,384,385,386,387,388,389,390,391,392,393,394,395,396,397,398,399,400

CO group information is displayed by clicking [CO Group] tab. It shows group number and its CO line numbers as a table. For iPECS–MG, group members of outgoing and incoming CO groups are displayed.

Station Group			
Group Number	Type	Pick-Up	Station Number
*620	ACD	On	4631,4637,4638,4639
*621	VSF-VM	Off	
*623	Ring	Off	3052,3053,3054,3055,3056,3063,3064,3065,3066,3074,3075,3076,3077,3078
*624	Ring	Off	4644,3105,3501

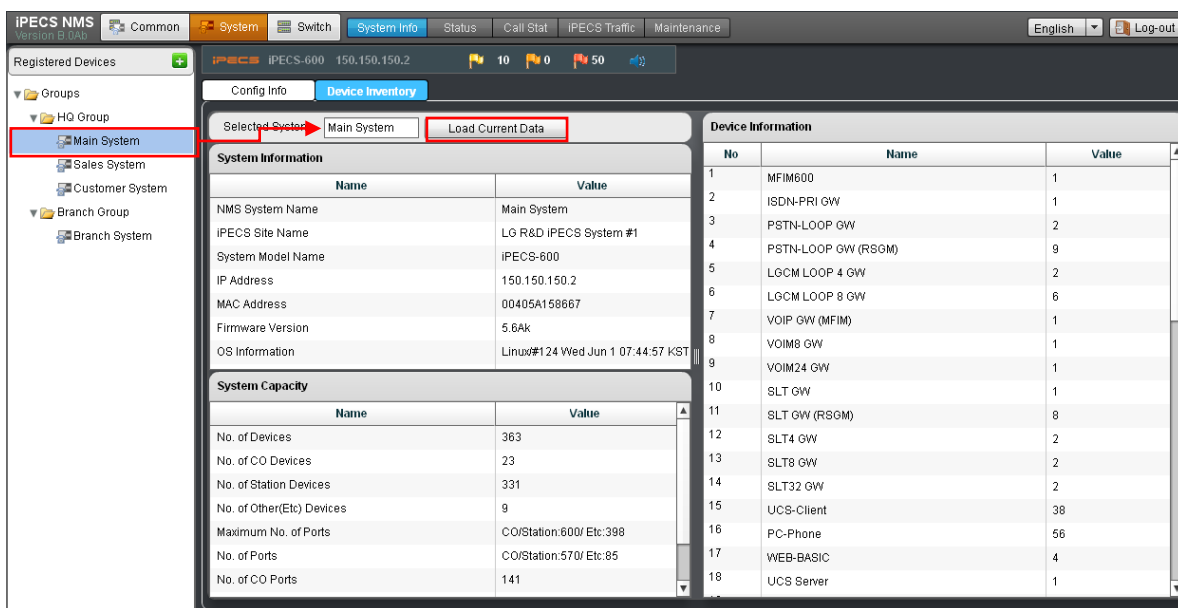
Station group information is displayed by clicking [Station Group] tab. It shows group number, group type, pick-up attribute and group members. Group type field can have Circular, Terminal, ACD, Ring, External VM, Pick-up, VSF-VM, UMS-VM, NET-VM or UCS. For iPECS–MG, group types are Terminal, Circular, Ring, Longest Idle, Voice Mail.

11.2 Device Inventory Information

‘Device Inventory Information’ provides overall system capacity and device inventory information of a selected system or system group. The page for this feature can be viewed by clicking [Device Inventory] tab under ‘System Info’ sub-menu.

11.2.1 System Device Inventory

‘System Device Inventory’ is the device inventory information of one system. In order to retrieve and display system device inventory information, enter ‘Device Inventory’ page by clicking [Device Inventory] tab, select a target system in ‘Registered Devices’, and click [Load Current Data] button.



‘System Information’ table shows the system name, address, and firmware version information, and ‘System Capacity’ table shows the number of devices and channels (ports) of the selected system. ‘Device Information’ shows the list of devices of the system and the number of modules of the corresponding device type. The table fields and their meanings are as follows.

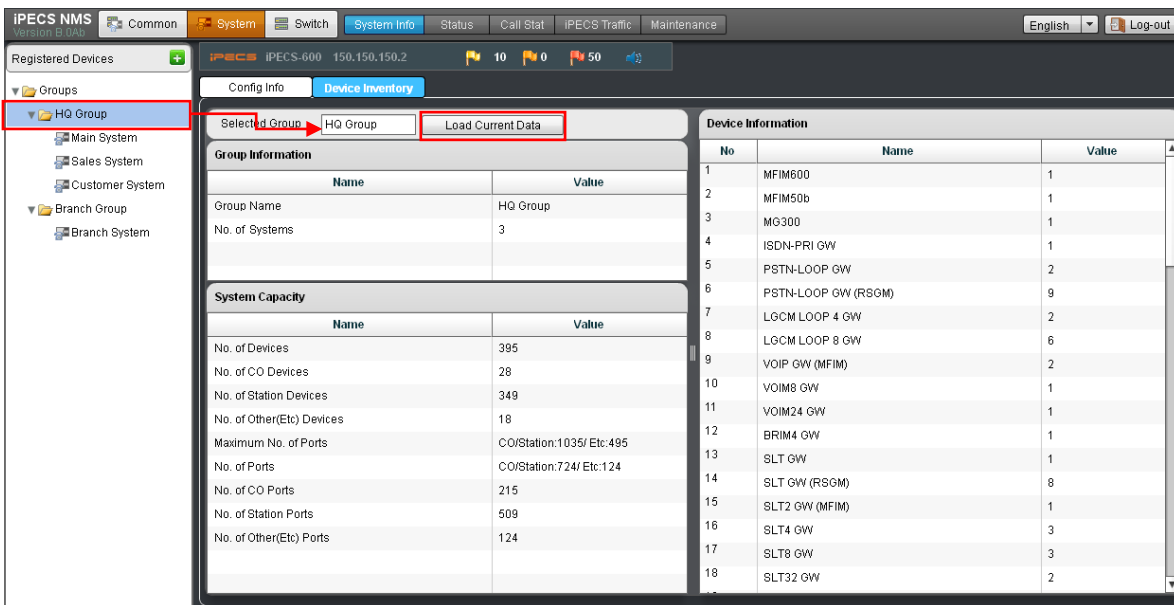
Table Name	Field Name	Description
System Information	NMS System Name	The name of the system configured when registering the system to iPECS-NMS.
	iPECS Site Name	‘Site Name’ field value of iPECS Web Admin (PGM 100).
	System Model Name	The model name of the system.
	IP Address	The IP address of MFIM(MPB).
	MAC Address	The MAC address of MFIM(MPB).
	Firmware Version	The firmware version of MFIM(MPB).
	OS Information	The OS build information of MFIM(MPB).
System Capacity	No. of Devices	Number of iPECS devices that are registered to the system.
	No. of CO Devices	Number of CO devices that are registered to the system.

	No. of Station Devices	Number of station devices that are registered to the system.
	No. of Other(Etc.) Devices	Number of other (etc.) devices that are registered to the system.
	Maximum No. of Ports	Maximum number of device ports that can be registered to the system.
	No. of Ports	Number of device ports that are registered to the system.
	No of CO Ports	Number of CO device ports that are registered to the system.
	No. of Station Ports	Number of station device ports that are registered to the system.
	No. of Other(Etc.) Ports	Number of other (etc.) device ports that are registered to the system.
Device Information	(Device Type Name)	Number of modules of each device type.

- ‘No. of Other(Etc.) Ports’ is based on the number of other (etc.) device ports managed internally by MFIM for device registration and operations. So, the number may be different from the total number of other (etc.) device ports shown in ‘Device Based Status’. In other words, ‘No. of Other(Etc.) Ports’ includes all the internal ports reserved by the system.

11.2.2 System Group Device Inventory

‘System Group Device Inventory’ is the device inventory information of a system group and its sub-groups. In order to retrieve and display system group device inventory information, enter ‘Device Inventory’ page by clicking [Device Inventory] tab, select a target system group in ‘Registered Devices’, and click [Load Current Data] button, then the device inventory information of the selected system group and its sub-groups will be displayed as a list of table fields.



‘Group Information’ table shows the system group name, and the number of systems that belong to the system group and its sub-groups, and ‘System Capacity’ table shows the number of devices and channels (ports) of the selected system group and its sub-groups. ‘Device Information’ shows the list of devices of the system group and its sub-groups, and the number of modules of the corresponding device type. The table fields and their meanings are as follows.

Table Name	Field Name	Description
Group Information	Group Name	The name of the system group configured when creating the system group in iPECS-NMS.
	No. of Systems	The number of systems of the system group and its sub-groups.
System Capacity	No. of Devices	The number of iPECS devices that are registered to the system group and its sub-groups.
	No. of CO Devices	The number of CO devices that are registered to the system group and its sub-groups.
	No. of Station Devices	The number of station devices that are registered to the system group and its sub-groups.
	No. of Other (Etc.) Devices	The number of other (etc.) devices that are registered to the system group and its sub-groups.
	Maximum No. of Ports	The maximum number of device ports that can be registered to the system group and its sub-groups.
	No. of Ports	The number of device ports that are registered to the system group and its sub-groups.
	No. of CO Ports	The number of CO device ports that are registered to the system group and its sub-groups.
	No. of Station Ports	The number of station device ports that are registered to the system group and its sub-groups.
	No. of Other(Etc.) Ports	The number of other (etc.) device ports that are registered to the system group and its sub-groups.
Device Information	(Device Type Name)	Number of modules of each device type.

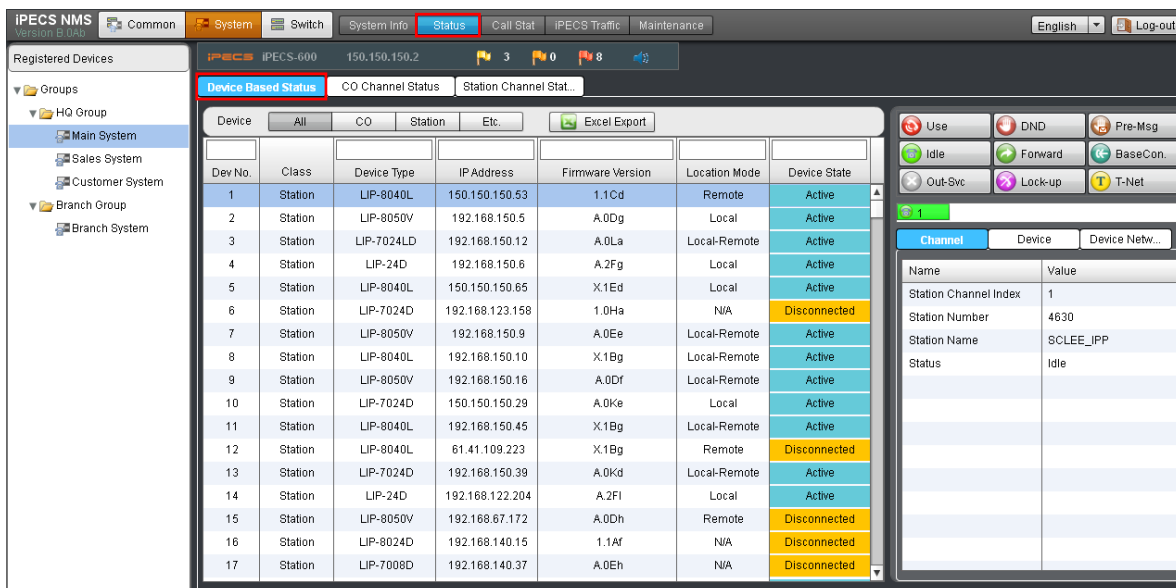
- ‘No. of Other(Etc.) Ports’ is based on the number of other (etc.) device ports managed internally by MFIM for device registration and operations. So, the number may be different from the total number of other (etc.) device ports shown in ‘Device Based Status’. In other words, ‘No. of Other(Etc.) Ports’ includes all the internal ports reserved by the system.

12. System Configuration and Status

‘System Configuration and Status’ provides detailed information of the device type selected in ‘Registered Devices’ and real-time status of devices and channels. The pages for these features can be viewed by clicking [Status] sub-menu under ‘System’ menu.

12.1 Device Based Status

‘Device Based Status’ provides the configuration information of each device of a device type (‘CO’, ‘Station’, ‘Etc.’) selected in ‘Registered Devices’ as well as the real-time status information of devices and their channels. The page for this feature can be viewed by clicking [Device Based Status] tab under ‘Status] sub-menu.



The device list in the middle of ‘Device Based Status’ screen displays the configuration and real-time status of each device. On the right side is the section for displaying the information of selected device and its channels with real-time channel status. At the top of the section, there is the icon legend box that shows the title of each status icon and its color. Below the box are the channel status block for displaying status icons for all the channels of a selected device, ‘Channel Information’ of a selected channel, and ‘Device Information’ & ‘Device Network Information’ of a selected device. The information fields of ‘Device Information’ and ‘Device Network Information’ are updated when a device is selected, and ‘Channel Information’ fields are displayed after a channel is selected.

Device Based Status						
CO Channel Status		Station Channel Stat...				
Device	All	CO	Station	Etc.	Excel Export	
Dev No.	Class	Device Type	IP Address	Firmware Version	Location Mode	Device State
1	Station	LIP-8040L	150.150.150.53	1.1Cd	Remote	Active
2	Station	LIP-8050V	192.168.150.5	A.0Dg	Local	Active
3	Station	LIP-7024LD	192.168.150.12	A.0La	Local-Remote	Active
4	Station	LIP-24D	192.168.150.6	A.2Fg	Local	Active

The main section of the window is a listing of all of the devices of the specific type (CO, Station, Etc.) and the state of the device. The device list includes:

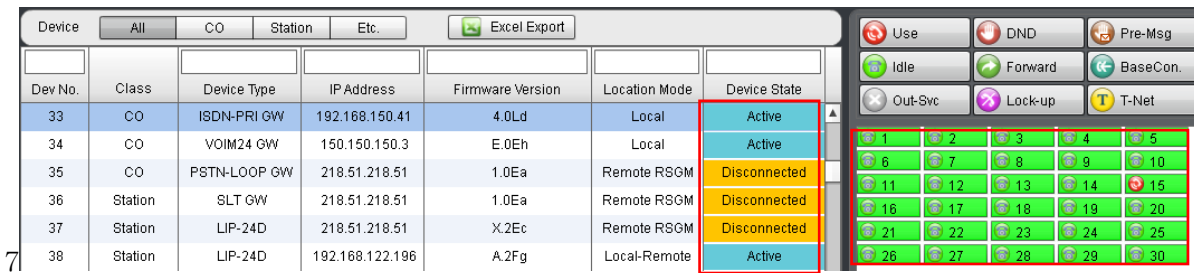
Table Name	Field Name	Description
Device List	Dev No.	Dev No. is the device sequence number on iPECS Web Admin, and is assigned by MFIM to each registered iPECS device with a unique sequence number.
	Class	Classification of the device and may have Station, CO, VSF, MISC or UCS Server.
	Device Type	The name of the device type.
	IP Address	IP address of the device.
	Firmware Version	Firmware version of the device.
	Location Mode	Location of a device configured when registering the device to the system. There are four location modes of Local, Remote, Local-Remote, and Remote RSGM.
	Device State	Device State shows the operation and registration status of a device. The states are 'Disconnected', 'Registering', 'Active', 'T-Net', 'Downloading', 'Out-of Service' and 'N/A'.

Channel	Device	Device Netw...
Name	Value	
Dev No.	1	
Device Type	LIP-8040L	
Firmware Version	1.1Cd	
CPU Type	TI1050	
Number of Channels	1	
Device Class/Order	STA1	
Service Switch	Normal	
Remarks	532f573220efbfbdcdbdef bfbdc3b6	

Channel	Device	Device Netw...
Name	Value	
IP Address	150.150.150.53	
MAC Address	001a7ea34909	
NAPT IP Address		
Location Mode	Remote	
ARP Usage	on	
Reg. Signal Type	unicast	
T-Net Reg. Type	Not T-Net	
Zone Number		

The table fields of 'Channel Information' are different for each device type, while the fields of 'Device Information' and 'Device Network Information' are same for all device types. The types and meanings of information fields are as follows.

Table Name	Field Name	Description
Device Information	Dev No.	Device No. is the device sequence number on iPECS Web Admin, and is assigned by MFIM to each registered iPECS device with a unique sequence number.
	Device Type	The name of the device type.
	Firmware Version	Firmware version of the device.
	CPU Type	CPU type of the device
	Number of Channels	The number of channels of the device
	Device Class/Order	Devices are grouped by their functionality to make 'Device Class', and the classes are 'CO Gateway', 'Station', 'MISC Gateway', 'VSF Gateway', 'MCIM Gateway', 'WTIM Gateway', 'UCS Server' and 'Not Defined'. 'Order' is the order of the device within its device class.
	Service Switch	The position of the service switch on the front panel of gateway device. The value can be 'Normal' or 'Service'.
Remarks	The 'Remark' field value of 'System & Device IP Address (PGM 102~103)' on iPECS Web Admin. This field is for additional information of each device entered by system administrator. For iPECS-MG, this field is not supported.	
Device Network Information	IP Address	IP address of the device
	MAC Address	MAC address of the device
	NAPT IP Address	This is the WAN side IP address translated by NAPT router where the remote mode device is installed behind the NAPT router
	Location Mode	Location of a device configured when registering the device to the system. There are four location modes of Local, Remote, Local-Remote, and Remote RSGM. For iPECS-MG, internal slot number is displayed.
	ARP Usage	The 'ARP' field value of 'System & Device IP Address (PGM 102~103)' on iPECS Web Admin. If this field is set to 'ON', ARP protocol is used to get MAC address for the packet exchange between local mode device and MFIM. If this is set to 'OFF', the MAC address information exchanged during registration process is used instead of using ARP protocol.
	Reg. Signal Type	Local mode devices can utilize either of multicast or unicast signaling for device registration. Multicast signaling supports automatic configuration and registration feature for Plug&Play of local mode devices. Remote and local-remote devices always use unicast signaling.
	T-Net Reg. Type	This field shows the T-Net configuration and registration status of a device, and the values are 'Not T-Net', 'T-Net Registered', 'T-Net Register Failed', 'LM-Registered' and 'LM-Register Failed'.
	Zone Number	The zone number to which the device belongs. Device zone number is configured using 'Device Zone Number (PGM 436)' on iPECS Web Admin. For iPECS-MG, this field is not supported.

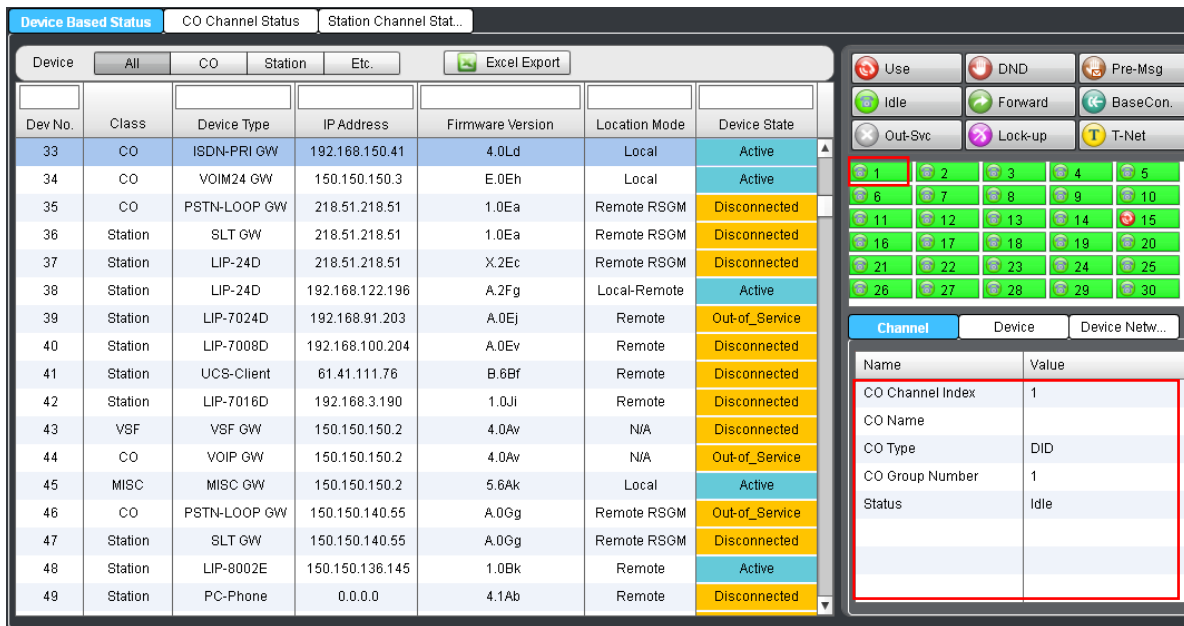


The status values of ‘Device Status’ of device list and ‘Channel Status’ of channel status block are commonly used for all types of devices, and the types and meanings of the values are as follows. (In case of DECT gateway, ‘Channel Status’ designates the connection status between DECT gateway and DECT base. If DECT base is connected to DECT gateway, the status displays ‘BaseCon’, and if disconnected, it displays ‘Out-Svc’.)

Field Name	Field Value	Description
Device Status	Disconnected	Previously registered device becomes disconnected from the system, and currently not working.
	Registering	Device registration is proceeding, and not yet completed.
	Active	Device is registered and working properly.
	T-Net	Device on LM is registered to CM through T-Net.
	Downloading	Firmware (software) upgrade is proceeding, and not yet completed.
	Out-of Service	iPECS administrator made the device into out-of-service state using iPECS Web Admin.
	N/A	Undefined state
Channel Status	Use	The channel is in use for conversation, seizure, or on other busy state.
	DND	The channel is on ‘Do Not Disturb’ state.
	Pre-Msg	The channel is on ‘Preselected Message’ state.
	Idle	The channel is not in use.
	Forward	The channel is on ‘Call Forwarding’ state.
	BaseCon.	DECT Base is connected to DECT gateway
	Out-Svc	The channel is out of service, or DECT base is not connected to DECT gateway.
	Lock-up	The station device of the channel is locked up after long off-hook time under non-conversational state.
	T-Net	The device of the channel is registered to CM through T-Net

12.1.1 CO Device Status

‘CO Device Status’ provides detailed information of CO device/channel information and real-time device/channel status information.



‘Channel Information’ on the right side of the page displays detailed information of a device channel selected in channel status block. The types and meaning of the information fields are as follows.

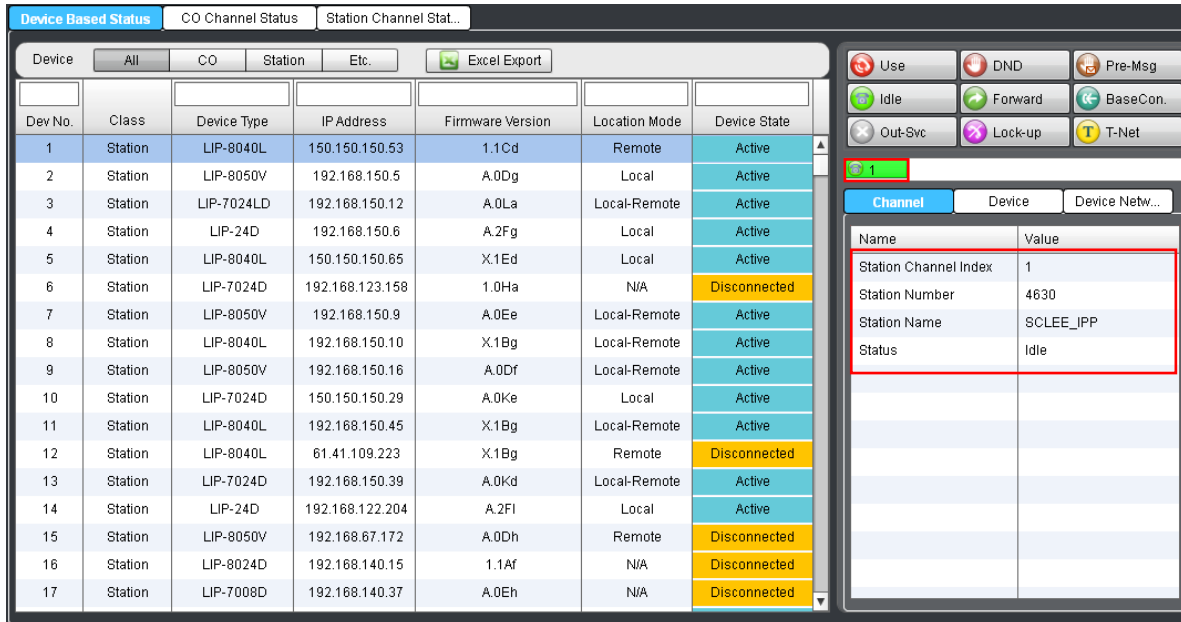
Table Name	Field Name	Description
CO Channel Information	CO Channel Index	This index number is assigned to the channels of ‘CO’ type devices. It also has the meaning of CO line number.
	CO Name	Name of the CO channel that is configured in ‘CO Name Assign’ field of ‘CO/IP Attribute (PGM 140~142)’ on iPECS Web Admin.
	CO Type	CO type of the channel that has one of the values of ‘Normal’, ‘DID’ or ‘TIE’.
	CO Group Number	CO group number to which the CO channel belongs.
	Status	Status of the CO channel

For iPECS-MG, the types and meaning of the fields are as follows.

Table Name	Field Name	Description
CO Channel Information	CO Channel Index	This index number is assigned to the channels of ‘CO’ type devices. It also has the meaning of CO line number.
	CO Line Type (Mode)	CO line type and incoming/outgoing mode of the channel, which may have ‘Incoming’, ‘Outgoing’, ‘Both’.
	CO Service Type	CO type of the channel that has one of the values of ‘Normal’, ‘DID’.
	CO Group Number	CO group number to which the CO channel belongs.
	Status	Status of the CO channel
	Tenant Number	Tenant number to which the CO channel belongs.
	Zone Number	Zone number to which the CO channel belongs.

12.1.2 Station Device Status

‘Station Device Status’ provides detailed information of station device/channel configuration and real-time device/channel status information.

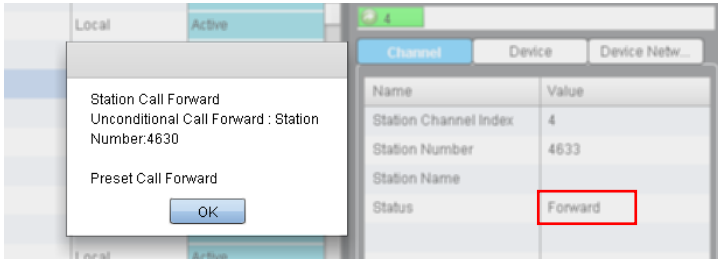


‘Channel Information’ displays detailed information of a device channel selected in channel status block. The types and meaning of the information fields are as follows.

Table Name	Field Name	Description
Station Channel Information	Station Channel Index	This index number is assigned to the channels of ‘Station’ type devices.
	Station Number	The station number of the channel.
	Station Name	Name of the station channel that is configured in ‘Station Name Display’ on iPECS Web Admin.
	Status	Status of the station channel (refer to ‘Channel State’ table)

For iPECS-MG, the types and meaning of the fields are as follows.

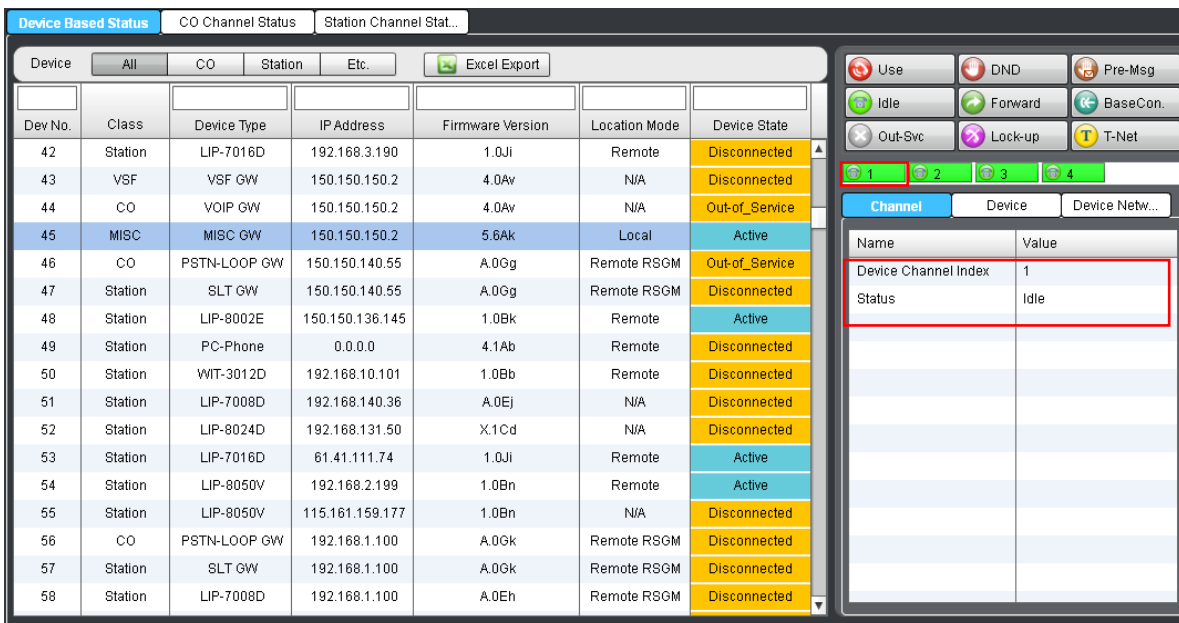
테이블 명	필드 명	의미
Station Channel Information	Station Type	Station type of the channel.
	Tenant Number	Tenant number of the channel.
	Zone Number	Zone number of the channel
	Prime Number	The extension number used as prime number for the channel.
	Hot Desk Login Number	The extension number of hot desk if the hot desk is logged in on the channel.



If the station or CO status is ‘Forward’, the forward configuration can be displayed by clicking on the ‘Status’ field.

12.1.3 Other (Etc.) Device Status

‘Other (Etc.) Device Status’ provides device/channel configuration and real-time device/channel status information of the other devices than CO or station devices.



‘Channel Information’ displays detailed information of a channel selected in channel status block. The types and meaning of the information fields are as follows.

Table Name	Field Name	Description
Other (Etc.) Channel Information	Device Channel Index	This index number is assigned to the channels of other devices than ‘CO’ or ‘Station’ type devices. ‘Etc.’ type channels maintain separate index numbering sequence for different type of devices.
	Status	Status of the device channel (refer to ‘Channel State’ table)

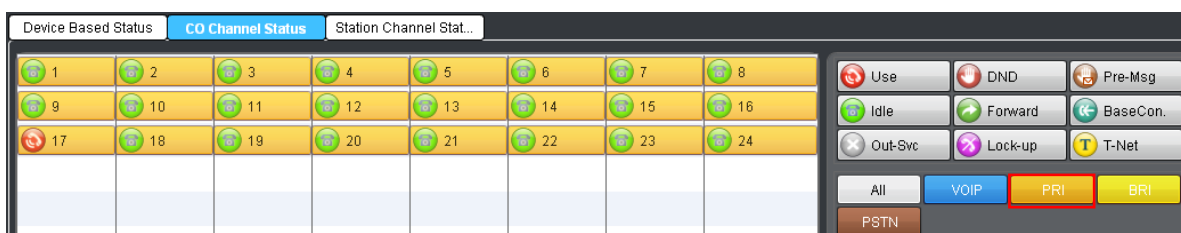
If a BRIB of iPECS-MG is used for both extension and trunk, that BRIB is displayed in ‘Other (Etc.) Channel Information’.

12.2 CO Channel Status

The main section of the CO channel Status view shows all CO channels registered to the iPECS system selected in ‘Registered Devices’. Each channel of all CO/IP devices (PSTN, PRI, BRI, and VoIP modules) is represented graphically with icons indicating the real-time status of the channel. The right side of the screen shows the channel information and the Device and Network Information for the highlighted CO channel as in the Device Based Status view. To open this page, click [CO Channel Status] tab under ‘Status’ sub-menu.



‘Channel Information’ on the right side of the page displays detailed information of a channel selected in channel status list in the middle, and ‘Device Information’ and ‘Device Network Information’ display their corresponding device information. The information fields of ‘Device Information’ and ‘Device Network Information’ are updated when a channel of the device is selected, and ‘Channel Information’ fields are displayed after the channel is selected. Each channel status button displays the status of the channel as well as the corresponding CO device type. Channel status is displayed using the nine icons shown in the icon legend box, and the CO device type is displayed with the four colors to designate the types of ‘VOIP’, ‘PRI’, ‘BRI’, and ‘PSTN’.



In order to show the CO channels of a specific CO type, click the corresponding CO type button, and to show all the CO channels again, click [All] button.

12.3 Station Channel Status

The main section of the ‘Station channel Status’ view shows all station channels registered to the iPECS system selected in ‘Registered Devices’. Each channel of all stations is represented graphically with icons indicating the real-time status of the channel. The right-side of the screen shows the channel information and the Device and Network Information charts for the highlighted station channel as in the Device Based Status view. To open this page, click [Station Channel Status] tab under ‘Status’ sub-menu.



‘Channel Information’ on the right side of the page displays detailed information of a channel selected in channel status list in the middle, and ‘Device Information’ and ‘Device Network Information’ display their corresponding device information. The information fields of ‘Device Information’ and ‘Device Network Information’ are updated when a channel of the device is selected, and ‘Channel Information’ fields are displayed after the channel is selected. Each channel status button displays the status of the channel as well as the corresponding station device type. Channel status is displayed using the nine icons shown in the icon legend box, and the station device type is displayed with the seven colors shown at the top of the screen to designate the seven types of ‘IP-Phone’, ‘SoftPhone’, ‘SLT’, ‘DKT’, ‘DECT’, ‘DSS’ and ‘SIP’. For iPECS-MG, ‘ISDN’ type is added to the station device types.

The screenshot displays the 'Station Channel Sta...' tab in the iPECS NMS interface. It features a table of station channels and a control panel on the right.

3161	3162	3163	3164	3165	3166	3167	3168
3207	3208	3209	3210	3211	FFFF	FFFF	FFFF

The control panel on the right includes the following buttons:

- Use (red icon)
- DND (red icon)
- Pre-Msg (orange icon)
- Idle (green icon)
- Forward (green icon)
- BaseCon. (blue icon)
- Out-Svc (grey icon)
- Lock-up (purple icon)
- T-Net (yellow icon)
- All (white icon)
- IP-Phone (blue icon)
- SoftPhone (green icon)
- SLT (yellow icon)
- DKT (red icon)
- DECT (orange icon)
- DSS (brown icon)
- SIP (purple icon)

In order to show the station channels of a specific station type, click the corresponding station type button, and to show all the station channels again, click [All] button.

13. System Call Statistics

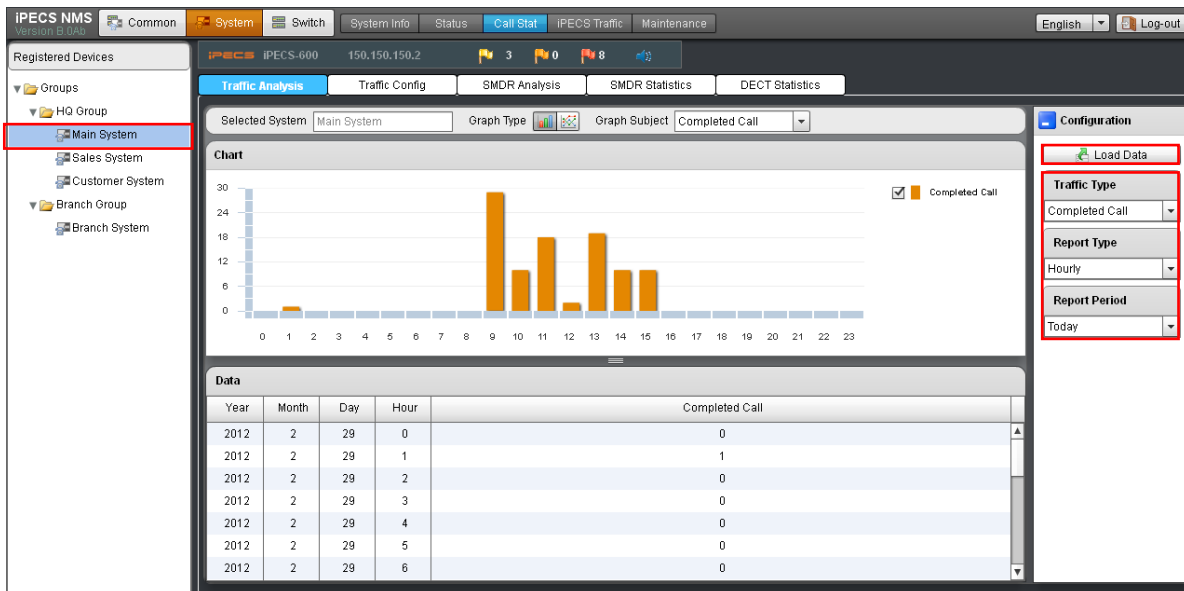
‘Call Statistics’ provides functions to analyze statistic information from call traffic and SMDR (Station Message Detail Recording) data, and also provides DECT statistics information. The pages for these features can be viewed by clicking [Call Stat] sub-menu under ‘System’ menu.

13.1 Call Traffic Analysis

‘Call Traffic Analysis’ provides the call traffic statistics of iPECS system in tabular and graphical format. There are some differences between call traffic information of iPECS-LiK system and that of iPECS-MG system. The Call Traffic Analysis page will be changed according to the system selected in ‘Registered Devices’. ‘Call Traffic Analysis’ page can be viewed by clicking [Traffic Analysis] tab under ‘Call Stat’ sub-menu.

13.1.1 iPECS-LiK System Traffic Analysis

For iPECS-LiK system, call traffic information for each traffic type of attendant call, completed call, CO group call, and voice mail service request are provided.



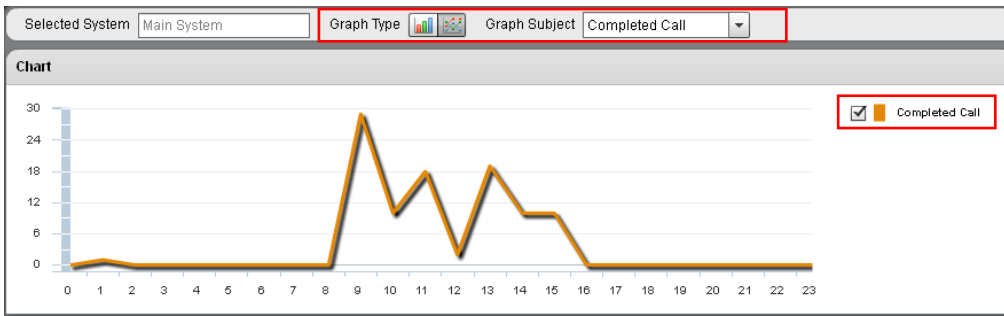
In order to load call traffic data, ‘Selected System’, ‘Report Type’, and ‘Report Period’ should be selected. For ‘Attendant’ or ‘CO Group’ in ‘Traffic Type’ field, attendant list or CO group list is additionally provided as ‘Graph Subject’ and one of them should be selected. After configuration, click [Load Data] button to retrieve call traffic data of the selected conditions. The types and meaning of the information fields are as follows.

Table Name	Field Name	Description
Traffic Type	Attendant	Selected for loading call traffic data of a specific attendant calls, and attendant list is provided for the selection of a specific attendant as an additional parameter.
	Completed Call	Selected for loading call traffic data of completed calls, and additional parameter selection is not needed.
	CO Group	Selected for loading call traffic data of a specific CO group calls, and CO group list is provided for the selection of a specific CO group as an additional parameter.
	Voice Mail	Selected for loading service request information of voice mail, and additional parameter selection is not needed.
Report Type	Daily	Selected for loading daily traffic information. If 'Daily Report' is configured in 'Traffic Configuration' for the selected system, 'Last 7 Days' and 'Last 4 Weeks' traffic data can be retrieved that has been stored since the configuration was made.
	Hourly	Selected for loading hourly traffic information. For this type of report, 'Today' and 'Yesterday' can only be selected on 'Report Period' because hourly traffic information is not accumulated on a daily basis.
Report Period	Today	Selected for loading call traffic data of the day ('today'). Both 'Daily' and 'Hourly' report types are available for this type of period.
	Yesterday	Selected for loading call traffic data of the previous day ('yesterday'). Both 'Daily' and 'Hourly' report types are available for this type of period.
	Last 7 Days	Selected for loading call traffic data for last 7 days. This choice becomes available (enabled) when 'Daily' report type is selected, and the traffic information that has been stored since the 'Daily Report' configuration was made is to be retrieved.
	Last 4 Weeks	Selected for loading call traffic data for last 4 weeks. This choice becomes available (enabled) when 'Daily' report type is selected, and the traffic information that has been stored since the 'Daily Report' configuration was made is to be retrieved.

After loading call traffic data, corresponding graph and table are displayed. The types and meanings of the table fields of each traffic type are as follows.

Table Name	Field Name	Description
Attendant	Year	The year of the date when the traffic data of the item has been accumulated.
	Month	The month of the date when the traffic data of the item has been accumulated.
	Day	The day of the date when the traffic data of the item has been accumulated.
	Hour	The hour of the traffic data item, and it has meaning only when 'Report Type' is set to 'Hourly'.
	Total-C	Total number of calls, except group & recalls, routed to the attendant.
	Ans-C	Total number of calls answered during the Analysis period.

	Abdn-C	Total number of calls abandoned before answer by the attendant (does not include calls abandoned while on hold).
	Held-C	Total number of calls placed on hold by the attendant.
	H-Abdn	Total number of calls abandoned while on hold.
	Avail-T	Total time the attendant was available to handle new calls between one call and the next one.
	Talk-T	Total time the attendant was active on calls.
	Held-T	Total time the attendant had calls on hold.
	NoAns-D	Average time calls were ringing or in queue for the attendant before abandoned.
Completed Call	Ans-D	Average time calls rang before answer by the attendant.
	Year	The year of the date when the traffic data of the item has been accumulated.
	Month	The month of the date when the traffic data of the item has been accumulated.
	Day	The day of the date when the traffic data of the item has been accumulated.
	Hour	The hour of the traffic data item, and it has meaning only when 'Report Type' is set to 'Hourly'.
CO Group	Completed Call	Number of completed calls.
	Year	The year of the date when the traffic data of the item has been accumulated.
	Month	The month of the date when the traffic data of the item has been accumulated.
	Day	The day of the date when the traffic data of the item has been accumulated.
	Hour	The hour of the traffic data item, and it has meaning only when 'Report Type' is set to 'Hourly'.
	CO Group	CO/IP group number.
	Total Seizure	Total number of times CO/IP lines in the group were used for any call.
	In-Seizure	Total number of incoming calls answered for CO/IP lines in the group.
	Out-Seizure	Total number of outgoing calls attempted on CO/IP lines in the group.
	Grp-Overflow	Total number of times group-overflow had been occurred.
Voice Mail	All-CO-Busy	Total time that all CO/IP lines in the group were simultaneously busy.
	Year	The year of the date when the traffic data of the item has been accumulated.
	Month	The month of the date when the traffic data of the item has been accumulated.
	Day	The day of the date when the traffic data of the item has been accumulated.
	Hour	The hour of the traffic data item, and it has meaning only when 'Report Type' is set to 'Hourly'.
	Requested	Total number of voice mail service requests including both cases of service success and denial.
Denied	Total number of denied voice mail service requests.	



After loading call traffic data, various types of graphs can be display by changing the selection of ‘Graph Type’ and ‘Graph Subject’. The selection change is applied to the graph at the moment the selection is made. The items in ‘Graph Subject’ change according to the selection of ‘Traffic Type’ (Attendant, Completed Call, CO Group, Voice Mail), and ‘Graph Component’ changes according to the selection of ‘Graph Subject’. This dependency is summarized below.

Traffic Type	Graph Subject	Description	Graph Component
Attendant	Total Call	Calls routed to the attendant (except group & recalls)	Total Call
	Held Call	Calls held by the attendant	Abandoned Call
			Held-Abandoned
	Call Time	Call times for each attendant status (talk, held, idle)	Available Time between Calls
Talk Time			
Held Time			
Answer Delay	Delay time for answered or unanswered calls	Answer Delay	
		No-Answer Delay	
Completed Call	Completed Call	Number of completed calls	Completed Call
CO Group	CO Group Usage	Number of line seizures of the group for each type (total, incoming, outgoing, overflow)	Total Seizure
			Incoming Seizure
			Outgoing Seizure
	All CO Busy	Total time that all CO/IP lines in the group were simultaneously busy	All CO Busy
Voice Mail	Voice Mail	Number of voice mail (VSF/VMIM) requests/denials	Requested
			Denied

13.1.2 iPECS-MG System Traffic Analysis

For iPECS-MG system, call traffic information for extensions and trunks are provided. Before loading call traffic data, ‘Selected System’, ‘Report Type’, ‘Report Period’, ‘Statistics Type’ and ‘Direction’ should be configured, and depending on the ‘Statistics Type’, additional fields may need to be configured. The types and meanings of the fields are as follows.

Table Name	Field Name	Description
Traffic Type	Station	Selected to retrieve data for incoming or outgoing station calls. Available statistics type is ‘Tenant’.
	CO	Selected to retrieve data for incoming or outgoing CO calls. Available statistics types are ‘Call Type’ and ‘CO Group’.

Report Type	Daily	Selected for loading daily traffic information. If 'Daily Report' is configured in 'Traffic Configuration' for the selected system, 'Last 7 Days' and 'Last 4 Weeks' traffic data can be retrieved that has been stored since the configuration was made.
	Hourly	Selected for loading hourly traffic information. 'Today' and 'Yesterday' can only be selected on 'Report Period' because hourly traffic information is not accumulated on a daily basis.
Report Peirod	Today	Selected for loading call traffic data of the day ('today'). Both 'Daily' and 'Hourly' report types are available for this type of period.
	Yesterday	Selected for loading call traffic data of the previous day ('yesterday'). Both 'Daily' and 'Hourly' report types are available for this type of period.
	Last 7 Days	Selected for loading call traffic data for last 7 days. This choice becomes available (enabled) when 'Daily' report type is selected, and the traffic information that has been stored since the 'Daily Report' configuration was made is to be retrieved..
	Last 4 Weeks	Selected for loading call traffic data for last 4 weeks. This choice becomes available (enabled) when 'Daily' report type is selected, and the traffic information that has been stored since the 'Daily Report' configuration was made is to be retrieved.
Statistics Type	Tenant	Selected to retrieve station statistics for each tenant. (Additional input field : Tenant number)
	Call Type	Selected to retireve statistics data for CO call types.
	CO Group	Selected to retrieve statistics data for each CO group. (Additional input field : Co group number)
Direction	Outgoing	Selected to retrieve data for outgoing call from station or CO. For Station Report, 'Station → CO' or 'Local' can be selected as the additional direction information. For CO Report, 'Station → CO' or 'CO → CO' can be selected.
	Incoming	Selected to retrieve data for incoming call to station or CO. For Station Report, 'CO → Station' or 'Local' can be selected as the additional direction information. For CO Report, 'CO → Station' or 'CO → CO' can be selected.

Table fields for each combination of traffic type and direction are as follows.

Traffic Type / Direction	Field Name	Description
Station / Outgoing	Year	The year when the traffic data was logged
	Month	The month when the traffic data was logged
	Day	The day when the traffic data was logged
	Hour	The hour when the traffic data was logged. This column is only meaningful If the Hourly Report Period is selected.
	DROPCALL	Total number of dropped calls in conversation
	HOLD	Sum of the connection holding time of each call
	AVGHOLD	Average holding time
	CCRATE(%)	Call Completing Rate. CCRATE is calculated by the following

		formula. CCRATE = ANSER / ATTEMPT * 100 (%)
	TRAFFIC (Erlang)	Traffic density. Erlang is calculated by the following formula. Erlang = (Average Hold Time x Total Number of Calls) / 3600 second
	ATTEMPT	Total number of calls attempted by calling station (off-hook)
	NTR	Total number of calls translating called number
	ALERT	Total number of calls sending ring to called station
	ANSWER	Total number of calls answered by called station
	RELEASE	Total number of calls completed (on-hook)
Station / Incoming	Year	The year when the traffic data was logged
	Month	The month when the traffic data was logged
	Day	The day when the traffic data was logged
	Hour	The hour when the traffic data was logged. This column is only meaningful If the Hourly Report Period is selected.
	DROPCALL	Total number of dropped calls in conversation
	HOLD	Sum of the connection holding time of each call
	AVGHOLD	Average holding time
	CCRATE(%)	Call Completing Rate. CCRATE is calculated by the following formula. CCRATE = ANSER / ATTEMPT * 100 (%)
	TRAFFIC (Erlang)	Traffic density. Erlang is calculated by the following formula. Erlang = (Average Hold Time x Total Number of Calls) / 3600 second
	ATTEMPT	Total number of calls ringing to called station
	ANSWER	Total number of calls answered by called station
	RELEASE	Total number of calls completed (on-hook)
CO / Outgoing	Year	The year when the traffic data was logged
	Month	The month when the traffic data was logged
	Day	The day when the traffic data was logged
	Hour	The hour when the traffic data was logged. This column is only meaningful If the Hourly Report Period is selected.
	DROPCALL	Total number of dropped calls in conversation
	HOLD	Sum of the connection holding time of each call
	AVGHOLD	Average holding time
	CCRATE(%)	Call Completing Rate. CCRATE is calculated by the following formula. CCRATE = ANSER / ATTEMPT * 100 (%)
	TRAFFIC (Erlang)	Traffic density. Erlang is calculated by the following formula. Erlang = (Average Hold Time x Total Number of Calls) / 3600 second
	ATTEMPT	Total number of calls seizing a CO
	ALERT	Total number of calls attempting alerting to called CO
	ANSWER	Total number of calls answered by called station
RELEASE	Total number of calls completed	
CO / Incoming	Year	The year when the traffic data was logged
	Month	The month when the traffic data was logged
	Day	The day when the traffic data was logged
	Hour	The hour when the traffic data was logged. This column is only

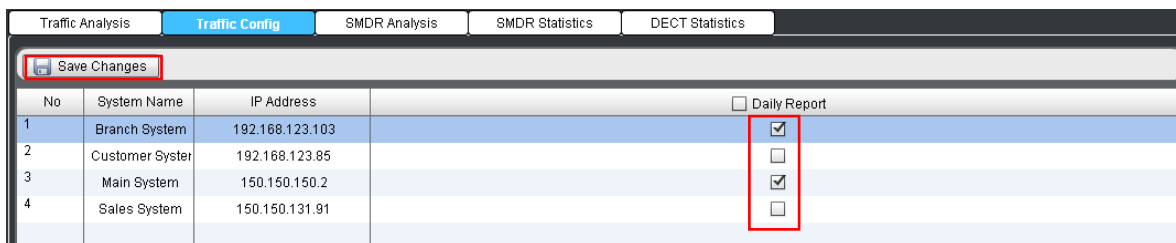
		meaningful If the Hourly Report Period is selected.
	DROPCALL	Total number of dropped calls in conversation
	HOLD	Sum of the connection holding time of each call
	AVGHOLD	Average holding time
	CCRATE(%)	Call Completing Rate. CCRATE is calculated by the following formula. CCRATE = ANSER / ATTEMPT * 100 (%)
	TRAFFIC (Erlang)	Traffic density. Erlang is calculated by the following formula. Erlang = (Average Hold Time x Total Number of Calls) / 3600 second
	ATTEMPT	Total number of calls attempting a call
	NTR	Total number of calls translating called number
	ALERT	Total number of calls sending ring to called station
	ANSWER	Total number of calls answered by called station
	RELEASE	Total number of calls completed

There are five types of graph subjects such as ‘Dropped Call’, ‘Hold Time’, ‘Call Completion Rate’, ‘Traffic Density (Erlang)’ and ‘Call State’. Graph Components varies depending on the graph subject selection as follows.

Graph Subject	Graph component
DROPCALL	DROPCALL
HOLD(sec)	HOLD
	AVGHOLD
CCRATE(%)	CCRATE(%)
TRAFFIC(Erl)	TRAFFIC(Erl)
Call State	ATTEMPT
	NTR
	ALERT
	ANSWER
	RELEASE

13.2 Call Traffic Configuration

iPECS-NMS may be configured to automatically retrieve and store call traffic data (‘Daily Report’ data of ‘Traffic Analysis’) on daily basis. ‘Call Traffic Configuration’ is for configuring this daily collection of call traffic data, and its configuration page can be viewed by clicking [Traffic Config] tab under ‘Call Stat’ sub-menu.

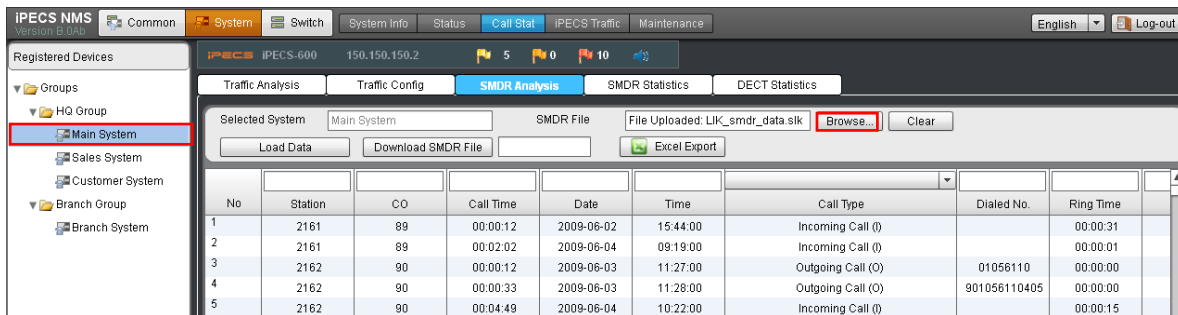


To enable retrieval and storage of traffic statistics, click the check box in the ‘Daily Report’ field

of the desired system. After configuration, click [Save Changes] to save and apply selections.

13.3 SMDR Analysis

‘SMDR Analysis’ provides the means to analyze SMDR data downloaded from a registered iPECS system applying various search and sort operations. The page for this feature can be viewed by clicking on the [SMDR Analysis] tab under the ‘Call Stat’ sub-menu.

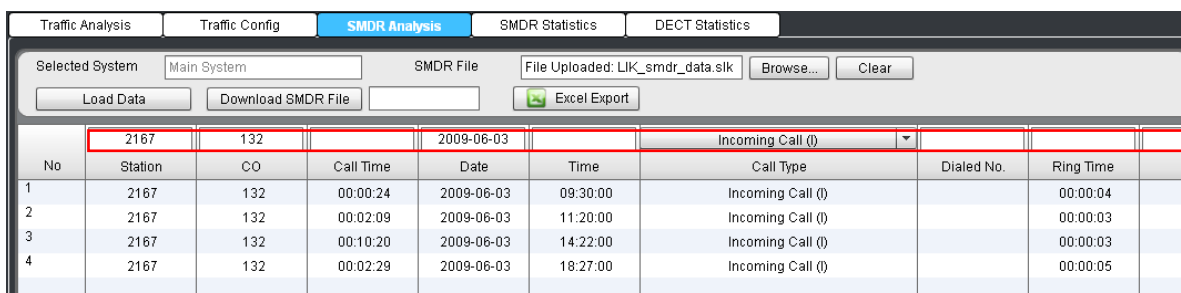


The field values of ‘Selected System’ and ‘SMDR File’ are configured and the corresponding data is loaded in ‘SMDR Analysis’ menu. Statistics graph and table provided in ‘SMDR Statistics’ menu are based on the loaded data from ‘SMDR Analysis’.

The target system for SMDR analysis should be selected first by clicking the system in ‘Registered Devices’, and the selected system will be displayed in ‘Selected System’ field. Then, ‘SMDR File’ field should be set by clicking [Browse ...] button to select an SMDR file. SMDR data is read from the file into iPECS-NMS local database when the SMDR file is selected.



By clicking [Load Data] button, SMDR file can be downloaded from the selected system and stored into iPECS-NMS local database..



After reading the SMDR file data into the local database, iPECS-NMS may perform search operation using the search options corresponding to each SMDR column field. The resulting SMDR records are displayed in the SMDR data list.

The type and meaning of ‘Call Type’ field is as follows.

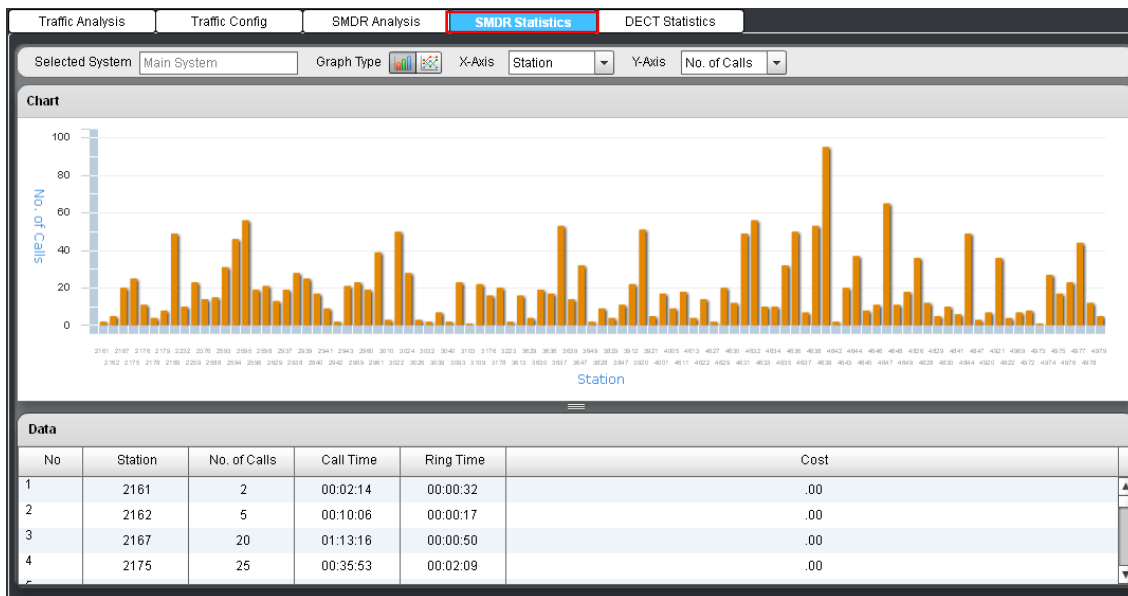
Field Type	Field Value	Description
Normal Calls	Incoming Call (I)	Incoming call to iPECS system from external caller
	Transfer of Incoming Call (t)	Incoming call to iPECS system was answered, and then transferred
	Outgoing Call (O)	Outgoing call from iPECS system
	Transfer of Outgoing Call (T)	Outgoing call was answered, and the caller transferred the call
	Station Call (E)	Calls between iPECS system extensions
Abandoned Calls	When Ringing to a Station (R)	While a station was ringing for an incoming call, the caller dropped the call before the station answers
	When Ringing to a Station Group (G)	While a station group was ringing for an incoming call, the caller dropped the call before the station answers
	When under (Transfer) Hold State (H)	The call was dropped while it was placed in hold state (including transfer hold)

After loading the SMDR file data, search operations can be performed afterwards with various search conditions. When modifying a search field value, new search is performed immediately and the result is displayed in the SMDR data list.

By clicking [Download SMDR File] button, SNMR file can be downloaded from the selected system and stored in the user’s PC.

13.4 SMDR Statistics

‘SMDR Statistics’ provides additional presentations of the results from the most recent SMDR Analysis. Results are provided in graphical and tabular formats. After completing an analysis, this page can be viewed by clicking [SMDR Statistics] tab under ‘Call Stat’ sub-menu.

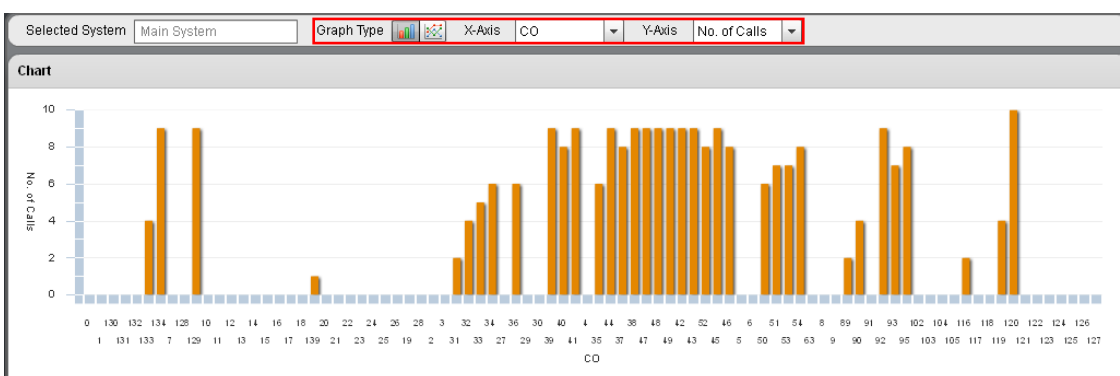


‘SMDR Statistics’ provides graphs and tables based on the data from the SMDR data from ‘SMDR

Analysis’, and so if data search was performed in ‘SMDR Analysis’, the search result will be used for the graphs and tables of ‘SMDR Statistics’.

‘Selected System’ field cannot be changed here, but just show the system configured and used in ‘SMDR Analysis’. (These fields can only be changed in ‘SMDR Analysis’ menu.)

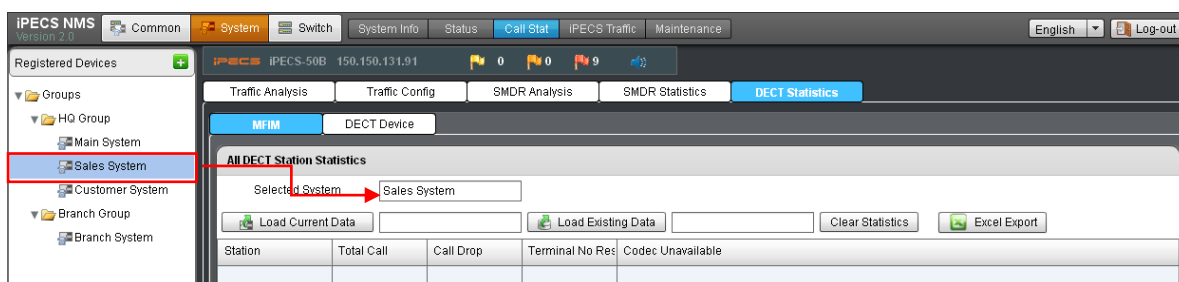
The combo-box and left/right arrow buttons in ‘Table Page’ can be used to select a specific page, and ‘Line Graph’ and ‘Column Graph’ icons are for changing the type of graph. Graphs and tables are generated based on the selection of X-Axis component (Station, CO, Date, Time). Graph is drawn for the Y-Axis component (No of Calls, Call Time, Ring Time, Cost) of the selected X-Axis component, and table shows all the Y-Axis components for the X-Axis component.



If user wants to generate various combinations of graphs and tables, click one of the X-Axis component buttons (‘Station’, ‘CO’, ‘Data’, ‘Time’) and then one of the Y-Axis component buttons (‘No of Calls’, ‘Call Time’, ‘Ring Time’, ‘Cost’). When the selection is changed, the result is displayed immediately in the graph and table.

13.5 DECT Statistics

The DECT Statistics screen provides DECT statistics information such as traffic, call, end-of-call, cell, RF access, and station statistics of a DECT device as well as the statistics information for all the DECT stations registered to an MFIM(MPB). The pages for this feature can be viewed by clicking [DECT Statistics] tab under ‘Call Stat’ sub-menu.



DECT statistics can be classified into two parts. One is the statistics information collected and managed by MFIM(MPB), and provides statistics information for all the DECT stations registered to the MFIM(MPB). The other one is the statistics information collected and managed by each DECT device (WTIM or WTIB), and provides various statistics information such as traffic, call, end-of-call, cell, RF access, station statistics of a DECT device.

As the first step, the target system for DECT statistics should be selected using 'Registered Devices', and then either of [MFIM] or [DECT Device] can be selected in order to specify whether the information collected by MFIM(MPB) or the information from DECT device is to be used for data retrieval.

The types and meanings of the statistics information provided by 'MFIM(MPB) Statistics' and 'DECT Device Statistics' are as follows.

Table Name	Field Name	Description
MFIM Statistics	All DECT Station Statistics	This provides the statistics data of the number of total and abnormal calls for all the DECT stations registered to an MFIM(MPB). The statistics data are collected and managed by MFIM(MPB).
DECT G/W Statistics	Traffic Statistics	This provides the statistics data of the wireless hold time and traffic density of a DECT device.
	Call Statistics	This provides the statistics data of incoming and outgoing calls for each cell.
	End-of-Call Statistics	This provides the statistics data of normal and abnormal end of calls for each cell.
	Cell Statistics	This provides the statistics data of the frequency usage for each slot of a selected cell.
	RF Access Statistics	This provides the statistics data of channel access, handover, and their loads (%) for each cell.
	Station Statistics	This provides the information for normal & abnormal end of calls and the last cell where a DECT station has been most recently located.

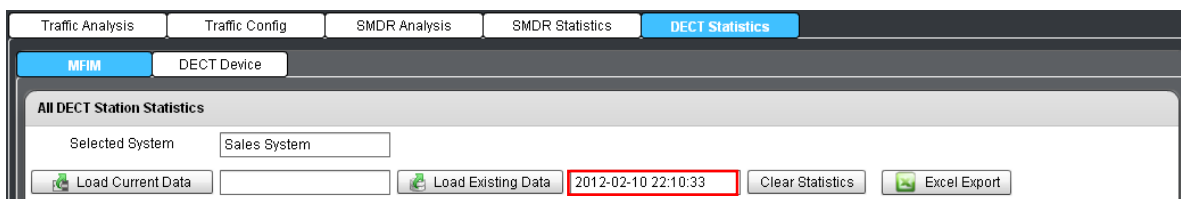
'MFIM(MPB) Statistics' information is retrieved directly from MFIM(MPB) because its data are collected and managed in MFIM(MPB). However, because 'DECT Device Statistics' data are collected in each DECT device, the data should be sent from DECT device to MFIM(MPB) and then retrieved from MFIM(MPB) to iPECS-NMS, which causes some processing delay. All the statistics information received from MFIM(MPB) is stored into NMS local database, and then presented to NMS users as tables of statistics information.

After storing the statistics data into NMS local database, NMS user can utilize the information previously stored in the database in order to get the last referenced data (with minimal processing

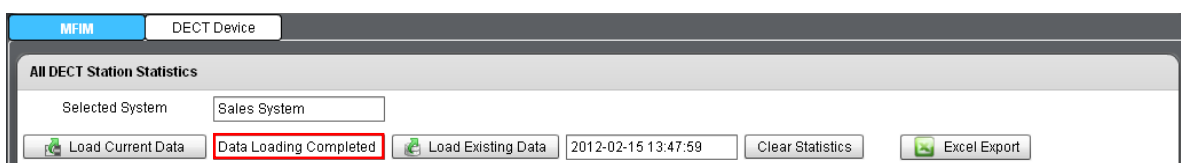
delay). Or, if the current statistics information is needed, all the data can be retrieved again, stored into NMS local database, and then presented to NMS users.

13.5.1 MFIM(MPB) Statistics

‘MFIM(MPB) Statistics’ information is collected and managed in MFIM(MPB), and provides the statistics of total number of calls and abnormal calls for all the DECT stations registered to the MFIM(MPB).



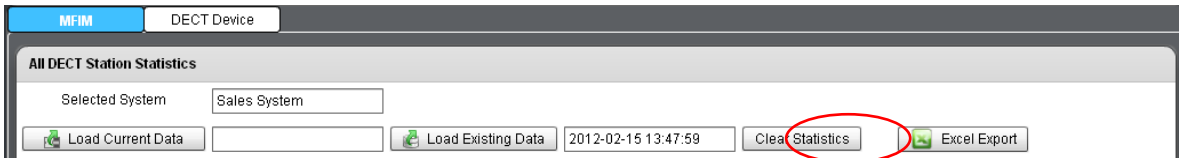
After selecting a system in ‘Registered Devices’ and clicking [MFIM] tab, check if ‘Statistics Time’ field on the right shows a date and time. The ‘Statistics Time’ field value means the date and time when MFIM(MPB) statistics information was retrieved from MFIM(MPB) and stored into NMS local database. So, if this field shows a date and time, the statistics data previously stored in NMS local database can be retrieved by clicking [Load Existing Data] button. If this field is blank, it means there is no previously stored MFIM(MPB) statistics data in NMS local database. In this case, current MFIM(MPB) statistics data may be retrieved from MFIM(MPB) by clicking [Load Current Data] button. The received data will be stored in NMS local database and then presented to NMS user as a table of statistics information.



After clicking on the [Load Current Data] button, current MFIM(MPB) Statistics information is sent to iPECS–NMS, stored in NMS local database, and then presented to the NMS user as a statistics table. While in process, the ‘Loading Status’ field on the left displays the current status of the procedure. The types and meanings of the status messages are as follows.

Loading Status	Description
MFIM(MPB) Data Requested	The first step that designates the data request state from iPECS–NMS to MFIM(MPB) for MFIM(MPB) statistics data.

Loading Data (NMS ← MFIM(MPB))	The second step that designates the state of the transmission of MFIM(MPB) statistics data from MFIM(MPB) to iPECS-NMS.
Data Loading Completed	The last step that designates the completion of the transmission of MFIM(MPB) statistics data, and the storage of the data into NMS local database.



MFIM(MPB) statistics data can be cleared to '0' and statistics data accumulation re-started from the beginning, by clicking on the [Clear Statistics] button. Because this does not remove the statistics data currently stored in NMS local database, the NMS user is still able to retrieve statistics data from NMS local database by clicking [Load Existing Data] button.

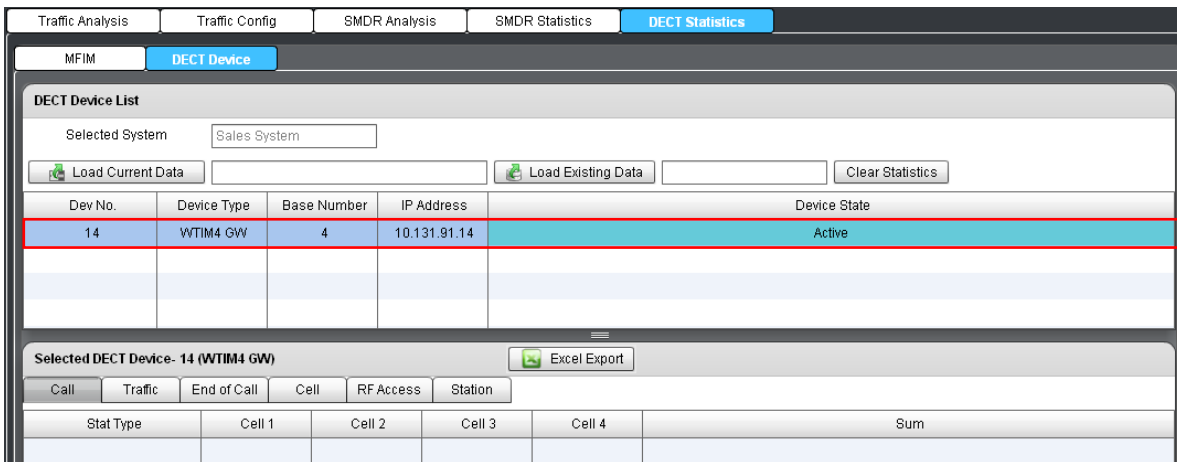
< All DECT Station Statistics >

'All DECT Station Statistics' provides the statistics of total number of calls and abnormal calls for all the DECT stations registered to the MFIM(MPB). The meaning of each table field is as follows.

Field Name	Description
Total Call	Total number of calls including both normal and abnormal calls.
Call Drop	Number of call drops caused by power-off or disconnection of wireless channel. (The figure inside the parentheses designates the proportion (%) of call drops to the total number of calls)
Terminal No Response	Counted when a DECT station cannot receive an incoming call (no response for signaling messages) due to power-off or other reasons. (The figure inside the parentheses designates the proportion (%) of no responses to the total number of calls)
Codec Unavailable	Counted when a call cannot be made because all the codec channels of a DECT device are already used for other calls. (The figure inside the parentheses designates the proportion (%) of codec unavailable cases to the total number of calls) iPECS-MG system does not support this field.

13.5.2 DECT Device Statistics

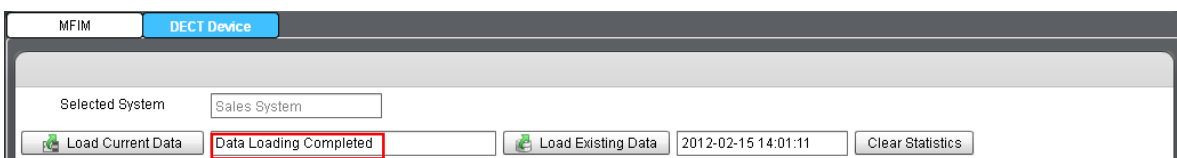
'DECT Device Statistics' information is collected and managed in each DECT device, and provides various statistics information such as traffic, call, end-of-call, cell, RF access, station statistics of a DECT device.



After selecting the system in ‘Registered Devices’ and the [DECT Device] tab to be selected, click on the target DECT device in the list of DECT devices registered to the selected system.



‘Statistics Time’ field on the right means the date and time when DECT Device Statistics information was retrieved and stored into NMS local database. So, if this field shows a date and time, the statistics data previously stored in NMS local database can be retrieved by clicking [Load Existing Data] button. If this field is blank, it means there is no previously stored DECT Device Statistics data in NMS local database. In this case, current DECT Device Statistics data can be retrieved from MFIM(MPB) by clicking [Load Current Data] button. The received data will be stored in NMS local database and then presented to NMS user as tables of statistics information.

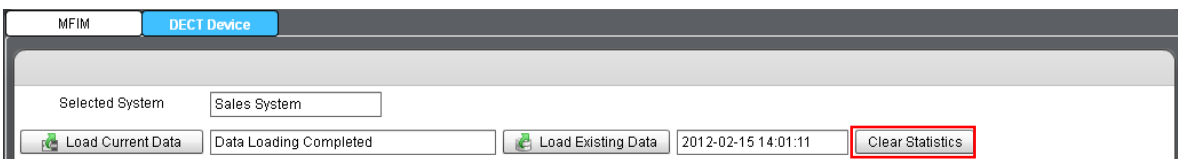


After clicking [Load Current Data] button, current DECT Device Statistics information is sent to iPECS-NMS, stored in NMS local database, and then presented as statistics tables. This needs additional procedure and takes relatively longer time than retrieving existing data directly from NMS local database using [Load Existing Data] button. So, in order to give more information about the steps of information retrieval process, ‘Loading Status’ field on the left displays the current status of the procedure. The types and meanings of the status messages are as follows.

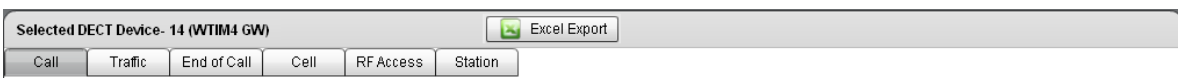
Loading Status	Description
DECT Data Requested	The first step that designates the data request state from iPECS-NMS to MFIM(MPB) for DECT Device statistics data.
Loading Data (MFIM(MPB) ← WTIM(WTIB))	The second step that designates the state of the transmission of DECT Device statistics data from DECT device to MFIM(MPB).
Data Loaded to MFIM(MPB)	The third step that designates the completion of the transmission of DECT Device statistics from DECT device, and the storage of the data into a memory space in MFIM(MPB).
Loading Data (NMS ← MFIM(MPB))	The fourth step that designates the state of the transmission of DECT Device statistics data from MFIM(MPB) to iPECS-NMS.
Data Loading Completed	The last step that designates the completion of the transmission of DECT Device statistics data from MFIM(MPB), and the storage of the data into NMS local database.

During the statistics data request and transmission, it is possible to receive an error caused by problems in network communication or in the DECT device itself. The types and meanings of the error messages are as follows.

Loading Error	Description
No Data in MFIM(MPB)	The data transmission from DECT device to MFIM(MPB) has not been properly performed due to the internal problem of the DECT device.
Invalid Data from DECT	Malformed or invalid data message has been sent from DECT device.
Data Not Available	DECT device had not been properly registered to MFIM(MPB) when the statistics data were requested to the DECT device.



If it is needed to clear DECT Device statistics data into '0' and start statistics data accumulation from the beginning, user may click [Clear Statistics] button to initialize the accumulated statistics data in DECT device. Because this does not remove the statistics data currently stored in NMS local database, NMS user is still able to retrieve statistics data from NMS local database by clicking [Load Existing Data] button.



'DECT Device Statistics' provides various statistics information such as traffic, call, end-of-call,

cell, RF access, station statistics of a DECT device. This information can be retrieved by clicking [Load Existing Data] or [Load Current Data] button. Each type of statistics information can be presented by clicking one of the 'DECT Device Statistics Type' tab corresponding to the type of statistics information.

< DECT Device Call Statistics >

'DECT Device Call Statistics' table is displayed by clicking 'Call' tab menu in 'DECT Device Statistics Type', and provides the statistics data of incoming and outgoing calls for each cell.

Selected DECT Device- 14 (WTIM4 GW) Excel Export					
Call	Traffic	End of Call	Cell	RF Access	Station
Stat Type	Cell 1	Cell 2	Cell 3	Cell 4	Sum
Incoming	0	0	0	0	0
Outgoing	0	0	0	0	0
Total	0	0	0	0	0

This table shows statistics data for 'Incoming' calls, 'Outgoing' calls, and the 'Total' number of calls. The meanings of the table fields are as follows. (The table fields can have values between 0~99999, and if the value exceeds the maximum value, FFFFF will be displayed to indicate overflow.)

Field Name	Description
Incoming	Number of incoming calls to DECT stations in the cell.
Outgoing	Number of outgoing calls from DECT stations in the cell.
Total	Sum of incoming and outgoing calls.

< DECT Device Traffic Statistics >

'DECT Device Traffic Statistics' table is displayed by clicking 'Traffic' tab in 'DECT Device Statistics Type', and provides the statistics data of the wireless hold time and traffic density of a DECT device.

Selected DECT Device- 14 (WTIM4 GW) Excel Export					
Call	Traffic	End of Call	Cell	RF Access	Station
Stat Type	Value				
Total No. of calls with hold time	0				
Total Hold Time (Sec)	0				
MAXimum Call Time (Sec)	0				
MINimum Call Time (Sec)	0				
Average Hold Time (Sec)	0				
Traffic Density (ERLANG)	0				

This table shows statistics data for 'Total No. of Calls with Hold Time', 'Total Hold Time', 'Maximum Call Time', 'Minimum Call Time', 'Average Hold Time', and Traffic Density (ELANG)'.

The meanings of the table fields are as follows. (The time fields in the table can have values between 0~999999999 in the unit of seconds, and if the value exceeds the maximum value, FFFFFFFF will be displayed to indicate overflow.)

Field Name	Description
Total Number of Calls with Hold Time	Total number of calls for which wireless connections were completely made.
Total Hold Time	Sum of the wireless connection holding time of each call.
Maximum Call Time	The longest wireless holding time among all the calls made on the DECT device. (The time for failed calls is not counted.)
Minimum Call Time	The shortest wireless holding time among all the calls made on the DECT device. (The time for failed calls is not counted.)
Average Hold Time	Average wireless holding time.
Traffic Density (ERLANG)	Traffic density of the DECT device. Erlang is calculated by the following formula. Erlang = (Average Hold Time x Total Number of Calls) / 3600 second

< DECT Device End of Call Statistics >

‘DECT Device End of Call Statistics’ table is displayed by clicking ‘End of Call’ tab menu in ‘DECT Device Statistics Type’, and provides the statistics data of normal and abnormal end of calls for each cell.

Stat Type	Cell 1	Cell 2	Cell 3	Cell 4	Sum
Normal Call	0	0	0	0	0
Abnormal Call	0	0	0	0	0
Call Fail	0	0	0	0	0
MSG Error	0	0	0	0	0
No Subs.	0	0	0	0	0
No RF Channel	0	0	0	0	0

This table shows statistics data for ‘Normal Call’, ‘Abnormal Call’ (‘Call Fail’, ‘MSG Error’, ‘No Subs.’, ‘No RF Channel’), and ‘No Response’. The meanings of the table fields are as follows. (The table fields can have values between 0~99999, and if the value exceeds the maximum value, FFFFF will be displayed to indicate overflow.)

Field Name	Description
Normal Call	Number of calls that were released normally.
Abnormal Call	Number of calls that were released abnormally. This type is assorted into four sub-types such as Call Fail, MSG Error, No Subs., No RF Channel.
Call Fail	Number of call releases caused by disconnection of wireless channels, timer expiration, etc.

MSG Error	Number of call releases caused by signaling message error.
No Subs.	Number of call releases caused by trying to make call to non-subscribed wireless terminal.
No RF Channel	Number of call releases due to no available RF channel.
No Response	Number of call releases caused by no signaling response from wireless terminal. ('No Response' does not provide statistics data counted for each cell.)
Total	Sum of Normal Call, Abnormal Call, and No Response field values.

< DECT Device Cell Statistics >

'DECT Device Cell Statistics' table is displayed by clicking 'Cell' tab in 'DECT Device Statistics Type', and provides the statistics data of the frequency usage for each slot of a selected cell.

Selected DECT Device - 14 (WTIM4 GW)							
Excel Export							
Call	Traffic	End of Call	Cell	RF Access	Station		
Cell 1	Cell 2	Cell 3	Cell 4				
Stat Type	Slot 0	Slot 2	Slot 4	Slot 6	Slot 8	Slot A	Sum
Freq 0	0	0	0	0	0	0	0
Freq 1	0	0	0	0	0	0	0
Freq 2	0	0	0	0	0	0	0
Freq 3	0	0	0	0	0	0	0
Freq 4	0	0	0	0	0	0	0

This table shows statistics data of the frequency usage for each slot of a selected cell, and the cell can be selected by clicking on the target cell in the list of cells. The meanings of the table fields are as follows. (The table fields can have values between 0~99999, and if the value exceeds the maximum value, FFFFF will be displayed to indicate overflow.)

Field Name	Description
Freq	Number of access to the frequency channel of the slot.
Sum	Number of wireless channel access to the slot over all the frequency numbers.

< DECT Device RF Access Statistics >

'DECT Device RF Access Statistics' table is displayed by clicking 'RF Access' tab menu in 'DECT Device Statistics Type', and provides the statistics data of channel access, handover, and their loads (%) for each cell.

Selected DECT Device - 14 (WTIM4 GW)					
Excel Export					
Call	Traffic	End of Call	Cell	RF Access	Station
Stat Type	Cell 1	Cell 2	Cell 3	Cell 4	Sum
CH ACCESS	0	0	0	0	0
Load (%)	0.00	0.00	0.00	0.00	0.00
Handover	Cell 1	Cell 2	Cell 3	Cell 4	Sum
IntraCell	0	0	0	0	0
Load (%)	0.00	0.00	0.00	0.00	0.00

This table shows statistics data for channel access, handover, and their load (%) information, and the handover statistics is subdivided into IntraCell, InterCell, InterCHO, IA-IR CHO, and IA-IA CHO statistics. The meanings of the table fields are as follows.

(The ‘Load (%)’ fields are displayed in the unit of percent, and the other table fields can have values between 0~999999, and if the value exceeds the maximum value, FFFFFFFF will be displayed to indicate overflow.)

Field Name	Description
CH Access	Number of wireless channel access to a cell
{CH Access} Load (%)	Proportion (%) of wireless channel access to a cell to all wireless connections including handover.
IntraCell	Number of BHOs (Bearer Handover) occurred within a cell.
InterCell	Number of BHOs (Bearer Handover) occurred among cells.
InterCHO	Number of CHOs (Connection Handover) occurred among DECT device.
IA-IR CHO	Number of CHOs (Connection Handover) occurred among the cells of a DECT device.
IA-IA CHO	Number of CHOs (Connection Handover) occurred within a cell of a DECT device.
{Handover} Load (%)	Proportion (%) of wireless handovers (within a cell or among cells) to all wireless connections.
Total (%)	Sum of the handover load values.

(In the table above, BHO is the abbreviation of Bearer HandOver, and means a type of handover occurred in MAC layer. CHO is the abbreviation of Connection HandOver, and mean a type of handover occurred in DLC (Data Link Control) layer that is above MAC layer.)

< DECT Device Station Statistics >

‘DECT Device Station Statistics’ table is displayed by clicking ‘Station’ tab menu in ‘DECT Device Statistics Type’, and provides the information for normal & abnormal end of calls and the last cell where a DECT station has been most recently located.

Selected DECT Device- 14 (WTIM4 GW)				
Call	Traffic	End of Call	Cell	RF Access
Station				
Station	Last Cell	Normal Call	Abnormal Call	Terminal No Response
1050	1	0	0	0
1051	1	0	0	0
-				
Sum	-	0	0	0

This table shows statistics data for ‘Last Cell’, ‘Normal Call’, ‘Abnormal Call’ and ‘No Response’ for each station. The meanings of the table fields are as follows. (The table fields can have values between 0~999999, and if the value exceeds the maximum value, FFFFFFFF will be displayed to

indicate overflow.)

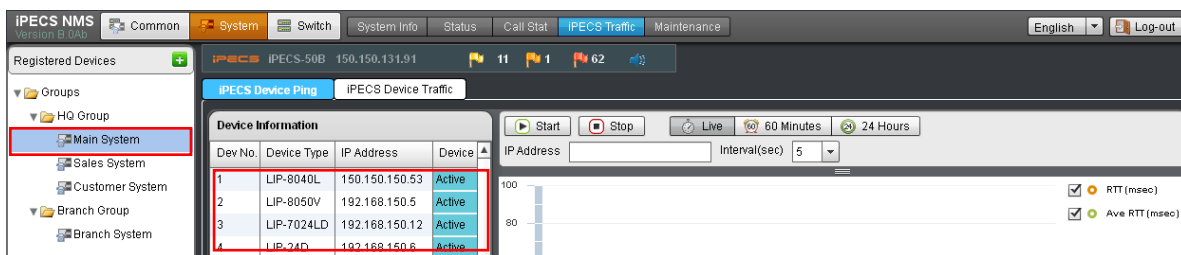
Field Name	Description
Last Cell	The last cell where a DECT station was most recently located
Normal Call	Number of calls that were released normally
Abnormal Call	Number of calls that were released abnormally
No Response	Number of call releases caused by no signaling response from DECT station.
Sum	Sum of the column values over all the DECT stations in the table

14. System Device Traffic Monitoring

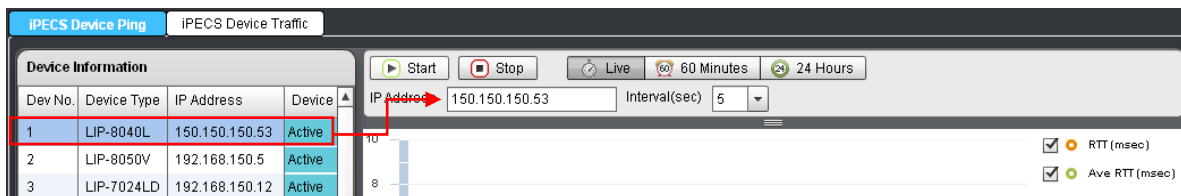
‘System Device Traffic Monitoring’ provides the means to monitor the network traffic and the connection status of an iPECS device. Ping test and traffic monitoring features are provided. The pages for these features can be entered by clicking [iPECS Traffic] sub-menu under ‘system’ menu.

14.1 iPECS Device Ping Test

‘iPECS Device Ping Test’ provides functions to check the connection status and the packet delay time between MFIM(MPB) and an iPECS device that is registered to the MFIM(MPB). This operation is performed by the Ping message implemented in iPECS protocol. The page for this feature can be viewed by clicking [iPECS Device Ping] tab under ‘iPECS Traffic’ sub-menu.



Before executing ‘iPECS Device Ping Test’, the target iPECS device to be tested should be selected. When an iPECS system is selected in ‘Registered Devices’, registered iPECS devices are displayed in ‘Device Information’ table. (This function does not support the internal slot devices of iPECS-MG system)



The target device can be selected in ‘Device Information’ by clicking on the device item. After the selection is made, the IP address of the selected device is displayed in ‘IP Address’ field. (If the target device is located behind an NAPT router, ‘NAPT IP’ value will also be displayed.)

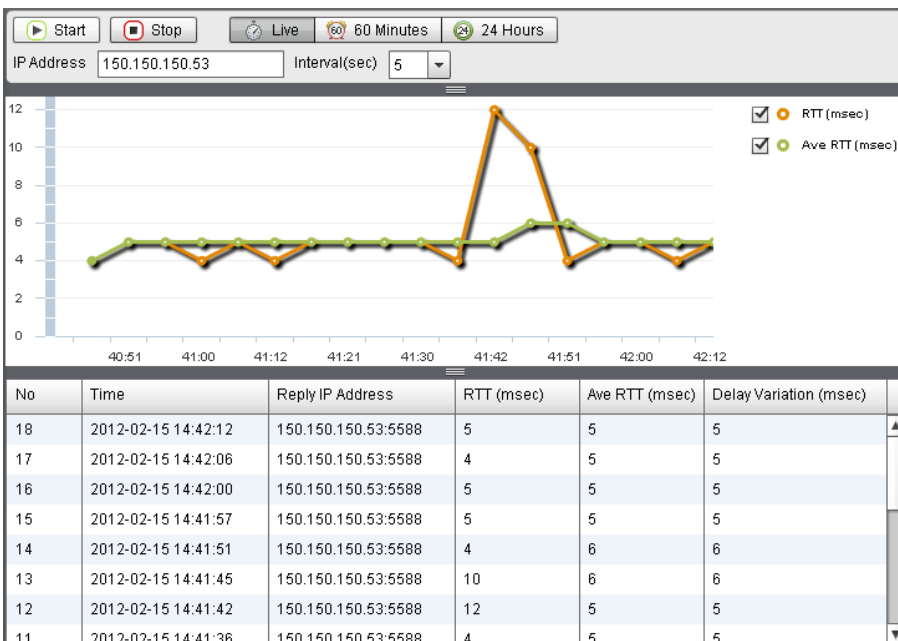
IP Address:
 Interval(sec):

Before starting Ping test, the interval for Ping packet transmission should be configured. For 'Interval' field, one of 5, 10, 20, 30 second options can be selected using the combo-box. After finishing configuration, click [Start] button to initiate Ping test, and [Stop] to finish it. Ping test will be automatically finished without using [Stop] button if the polling count reaches 65545 times.

iPECS Device Ping Test is different from the Ping test for general network device (9.1 Ping Test) in that the Ping packet is sent from MFIM(MPB) to the target device (rather than sent from iPECS-NMS). Therefore, 'iPECS Device Ping Test' can be used to check the network connection and packet delay time between MFIM(MPB) and the target iPECS device.

IP Address:
 Interval(sec):

The graph and table that show the result of Ping test can be displayed in three types of time period such as 'Live Data', 'Last 60 Minutes', and 'Last 24 Hours'. The real-time graph and table are displayed by clicking [Live] button. [60 Minutes] and [24 Hours] buttons are used for displaying the graphs and tables for last 60 minutes and 24 hours from the moment the corresponding button was clicked.

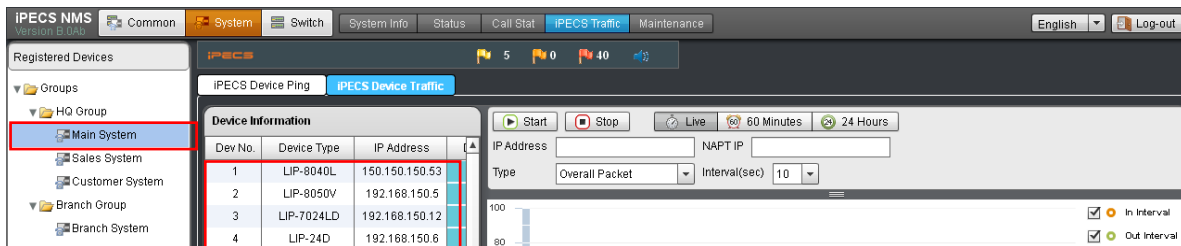


The graph in the picture above shows the changes in RTT (Round-Trip Time), which is the time between the transmission of a Ping packet and the reception of the response packet. RTT is often used to estimate the packet delay time in a network environment. The table below the graph shows the information from the Ping test, and the meanings of the table fields are as follows.

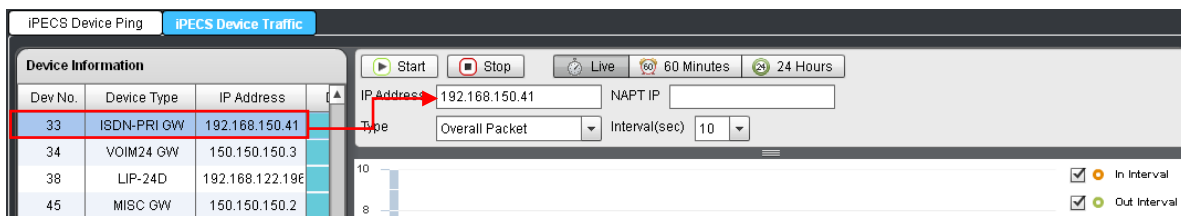
Table Name	Field Name	Description
Live Data	Time	The time when iPECS-NMS retrieved Ping test result from MFIM(MPB). The 'Time' interval may not be exactly same as the 'Interval' value depending on the operational or processing load on the NMS server.
	Reply IP Address	The IP address of the device that responded to the Ping packet sent by MFIM(MPB).
	RTT	Abbreviation of Round-Trip Time. This is the elapsed time until the reception of the response packet to a Ping packet sent by MFIM(MPB).
	Average RTT	The overall average of the RTT values from all the Ping tests calculated since the beginning of the Ping test.
	Delay Variation	The difference in value between the RTT values of the previous row and the current row of the table.
Last 60 Minutes	Time	The time when iPECS-NMS retrieved Ping test result from MFIM(MPB). The 'Time' interval may not be exactly same as the 'Interval' value depending on the operational or processing load on the NMS server.
	Reply IP Address	The IP address of the device that responded to the Ping packet sent by MFIM(MPB).
	RTT	This is the average of the RTT values from the Ping tests for last 1 minute (actually, the time between the previous row and the current row in the table).
	Average RTT	The overall average of the RTT values from all the Ping tests calculated since the beginning of the Ping test.
	Delay Variation	The difference in value between the RTT values of the previous row and the current row of the table.
Last 24 Hours	Time	The time when iPECS-NMS retrieved Ping test result from MFIM(MPB). The 'Time' interval may not be exactly same as the 'Interval' value depending on the operational or processing load on the NMS server.
	Reply IP Address	The IP address of the device that responded to the Ping packet sent by MFIM(MPB).
	RTT	This is the average of the RTT values from the Ping tests for last 1 hour (actually, the time between the previous row and the current row in the table).
	Average RTT	The overall average of the RTT values from all the Ping tests calculated since the beginning of the Ping test.
	Delay Variation	The difference in value between the RTT values of the previous row and the current row of the table.

14.2 iPECS Device Network Traffic

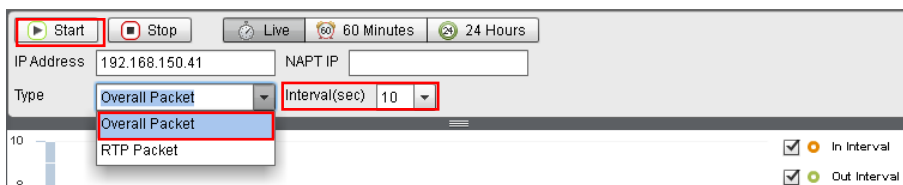
‘iPECS Device Network Traffic’ provides functions to monitor the real-time network traffic of the selected iPECS device. The page for this feature can be viewed by clicking [iPECS Device Traffic] tab under ‘iPECS Traffic’ sub-menu. (This feature can only be applied to the gateways and IP-Phones developed for and after iPECS Phase 4, and VOIU/VOIB of iPECS-MG. In case of VSF and UVMU, ‘RTP Packet’ is not supported)



Before executing ‘iPECS Device Network Traffic’ monitoring, the target iPECS device to be tested should be selected. When an iPECS system is selected in ‘Registered Devices’, registered iPECS devices are displayed in ‘Device Information’ table. (This function does not support the internal slot devices of iPECS-MG system)

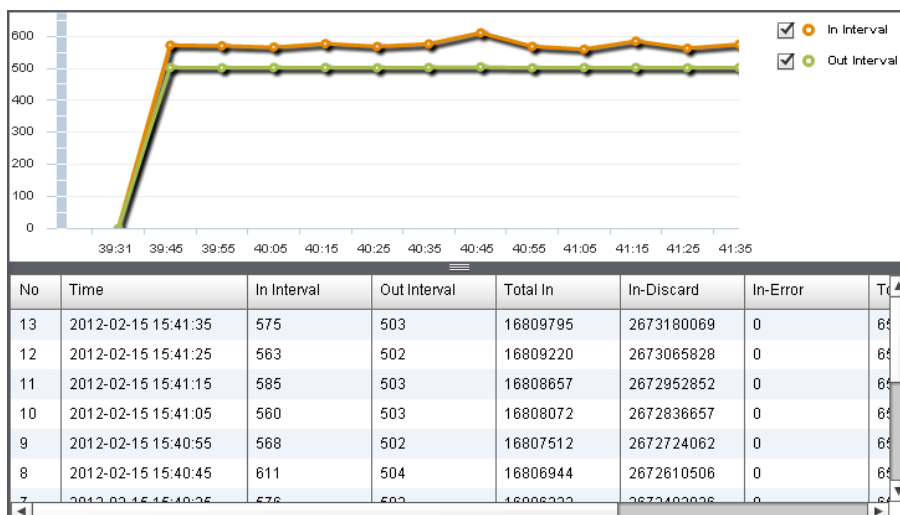


The target device can be selected in ‘Device Information’ by clicking on the device item. After the selection is made, the IP address of the selected device is displayed in ‘IP Address’ field. (If the target device is located behind an NAPT router, ‘NAPT IP’ value will also be displayed.)



Before starting traffic monitoring, the interval for traffic polling should be configured. For ‘Interval’ field, one of 10, 20, 30 second options can be selected using the combo-box. For ‘Type’ field, either of ‘Overall Packet’ or ‘RTP Packet’ can be selected. ‘Overall Packet’ means all type of

transmitted or received packets, and ‘RTP Packet’ means media packets such as voice or video packets delivered using RTP. After finishing configuration, click [Start] button to initiate traffic monitoring, and [Stop] to finish it. Traffic monitoring will be automatically finished without using [Stop] button if the polling count reaches 65545 times.



The graph shows in real-time the number of incoming and outgoing packets that occurred during the polling interval, and the traffic table shows the traffic data occurred within the interval as well as the accumulated traffic data. The meanings of the table fields are as follows.

Table Name	Field Name	Description
Overall Packet	In-Interval	The number of overall packets received during the time period configured in ‘Interval’ field of ‘Polling Configuration & Operation’.
	Out-Interval	The number of overall packets transmitted during the time period configured in ‘Interval’ field.
	Packets In	The number of overall packets received at the selected device.
	Bytes In	The number of bytes for all the packets received at the selected device.
	ErrPackets In	The number of input packets discarded due to packet errors.
	Packets Out	The number of overall packets transmitted from the selected device.
	Bytes Out	The number of bytes for all the packets transmitted from the selected device.
	ErrPackets Out	The number of outgoing packets discarded due to problems at the network device driver.
RTP Packet	In-Interval	The number of overall packets received during the time period configured in ‘Interval’ field.
	Time	The time when iPECS-NMS retrieved RTP traffic information of the target device from MFIM(MPB). The ‘Time’ interval may not be exactly same as the

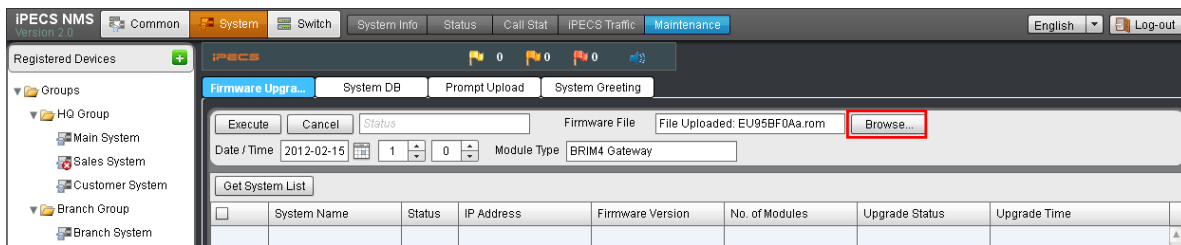
		'Interval' value depending on the operational or processing load on the NMS server.
	In-Interval	The number of RTP packets received during the time period configured in 'Interval' field.
	Out-Interval	The number of RTP packets transmitted during the time period configured in 'Interval' field.
	Packets In	The number of RTP packets received at the selected device, and those packets may include audio and/or video packets for media communication.
	Packets Out	The number of RTP packets transmitted from the selected device, and those packets may include audio and/or video packets for media communication.

15. System Maintenance

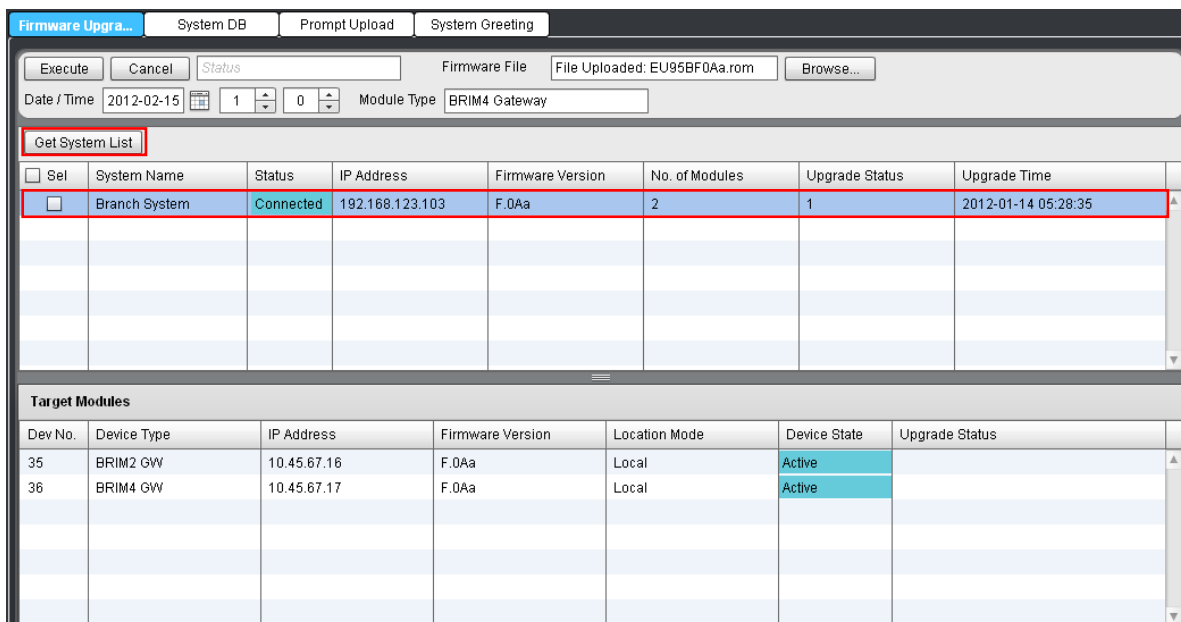
‘System Maintenance’ provides functions for device firmware upgrade and upload/download of system database, system greetings & prompts. The pages for these features can be viewed by clicking [Maintenance] sub-menu under ‘system’ menu.

15.1 Firmware Upgrade

‘Firmware Upgrade’ is used to upgrade firmware for a specific type of iPECS devices of selected systems at a designated time. From ‘Maintenance’ sub-menu, click [Firmware Upgrade] tab.



Click on the [Browse...] button to select a firmware file to use for upgrading device firmware. Then, the file name will be displayed in the ‘Firmware File’ field and ‘Module Type’ field will display the type of the device that can be upgraded using the selected firmware file.



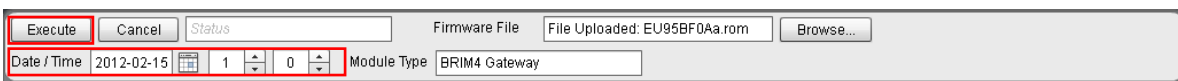
When [Get System List] button is clicked, the systems to which the upgradable devices are

registered will be listed in the 'System List' table. The upgradable modules that are registered to a specific system will be listed in 'Target Modules' when clicking on the system in the 'System List'. ('Target Modules' does not display MFIM(MPB) items when upgrading MFIM(MPB) firmware.) 'System List' and 'Target Modules' tables display detailed information of the systems and target devices. The types and meanings of the table fields are as listed in the following table.

Table Name	Field Name	Description
System List	System Name	The name of the system configured when registering to iPECS-NMS.
	IP Address	The IP address of MFIM(MPB) that is the main call processing module of iPECS system.
	Firmware Version	The firmware version of MFIM(MPB).
	Status	The connection (communication) status between iPECS-NMS and iPECS system.
	No. of Modules	The number of devices that can be upgraded with the selected firmware file.
	Upgrade Status	Upgrade Status shows the process status of firmware upgrade of the system, and includes the status values of 'Connecting FTP', 'Transferring by FTP', 'Transferring by HTTP', 'Upgrade MFIM(MPB)', 'Upgrading Device', 'Finished', and 'Failed'. In normal cases, the status will display 'Connecting FTP' when the firmware upgrade is started, and the FTP connection is made between NMS server and MFIM(MPB). After the FTP connection is established, the status changes to 'Transferring by FTP' and the firmware file is transferred from NMS server to MFIM(MPB). After the file transfer is completed, the status becomes 'Upgrading MFIM(MPB)' or 'Upgrading Device' and performs the firmware upgrade for MFIM(MPB) or target devices. When firmware upgrade is finished, the displays as 'Finished' status. NOTE - 'Transferring by HTTP' status may be shown when firmware upgrade is being performed by Web Admin.
	Upgrade Time	When the firmware upgrade for the system is finished.
Target Modules	Dev. No.	Device Number is the device sequence number on iPECS Web Admin.; a unique number is assigned to each registered device.
	Device Type	The type of the device
	IP Address	The IP address of the device
	Firmware Version	The firmware (software) version of the device
	Location Mode	Location of the device that was configured when the device was registered on system (For iPECS-LiK system, Local, Remote, Local-Remote, and Remote RSGM. iPECS-MG system displays only Internal Slot).
	Device Status	Device Status shows the operation and registration status of the device (Disconnect, Active, T-Net, Downloading, Out-of-Service and N/A).
	Upgrade Status	Upgrade Status shows the process status of firmware upgrade of the device (Ready, Started, Transferring,

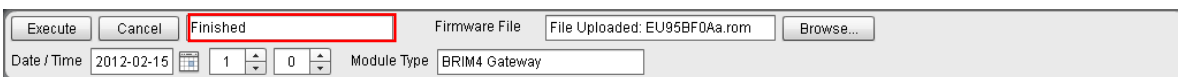
		<p>Transfer Completed, Success, and Failed.</p> <p>In normal cases, the status of all the target devices will display 'Ready' when the firmware upgrade for the system is started. After the firmware upgrade is started for each device, the firmware file is transferred to the device under 'Transferring' status. After the firmware transfer is completed, the status changes to 'Transfer Completed', and then becomes 'Success' when the firmware upgrade is finished.</p>
--	--	---

Because a system can be configured for one firmware upgrade at a time, only the systems that are not already scheduled for other firmware upgrade can be selected in 'System List'.



In order to schedule a firmware upgrade at a specific date and time, configure the target date and time for firmware upgrade in 'Date/Time' field, and then click on the [Execute] button. The firmware upgrade will be automatically started at the designated date and time for the selected systems. If the 'Date/Time' field is configured with the current date/time or a past date/time, the firmware upgrade will immediately start after clicking on the [Execute] button.

If the [Cancel] button is clicked while the firmware upgrade is in process for multiple systems, the schedules for waiting systems can only be canceled, and the systems that are performing firmware upgrade at that moment proceed the firmware upgrade to the end and finish their upgrade procedure.



The 'Status' field on the left shows the overall process status of the firmware upgrade for all the selected systems (Transferring to NMS, Scheduled, Upgrading, and Finished).

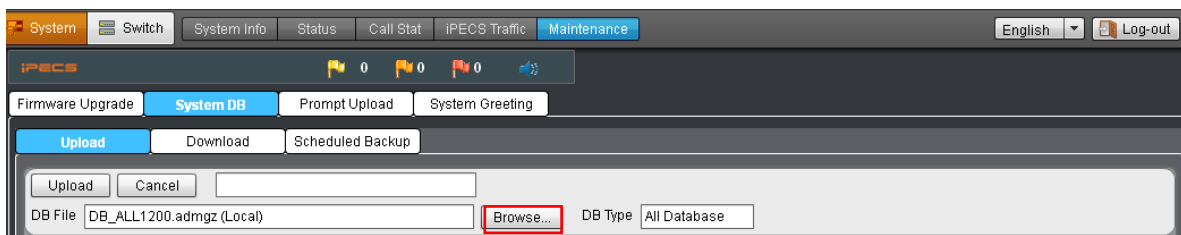
'Transferring to NMS' designates the status of the transferring firmware file from the NMS client browser to NMS server; this is performed immediately after clicking on the [Execute] button. After firmware file transfer to NMS server is completed, the 'Status' will change to 'Scheduled' if the 'Date/Time' field is configured with future date and time, or will change to 'Upgrading' if the firmware upgrade is started after the current time has exceeded the date and time configured in the 'Date/Time' field. When the firmware upgrade for all selected systems is finished, the 'Status' field will display 'Finished' to show that the overall firmware upgrade procedure is finished.

15.2 System DB Management

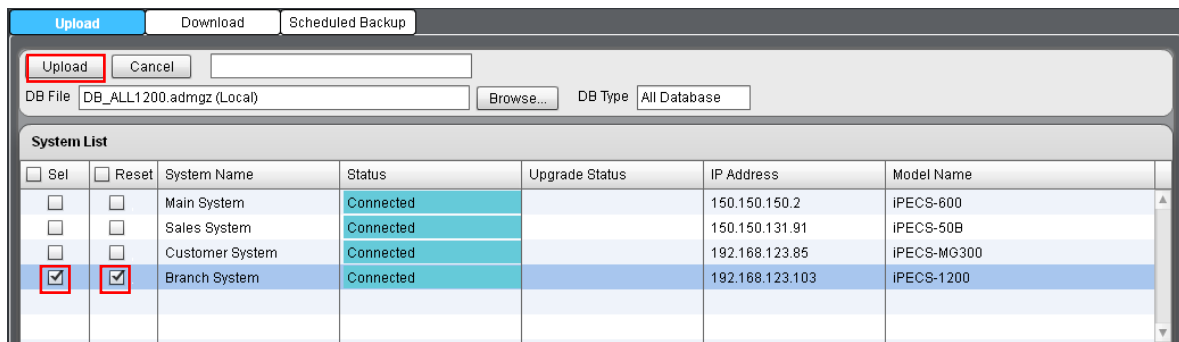
‘System DB Management’ provides the means to upload or download system a DB file to/from the iPECS system, and also periodically backup the system database to the NMS server. The pages for these features can be located by clicking on the [System DB] tab under ‘Maintenance’ sub-menu.

15.2.1 System DB Upload

‘System DB Upload’ function is for uploading a system DB file stored in the NMS client PC or in the NMS server to selected iPECS systems. The page for this function can be opened by clicking on the [Upload] tab under ‘System DB’.

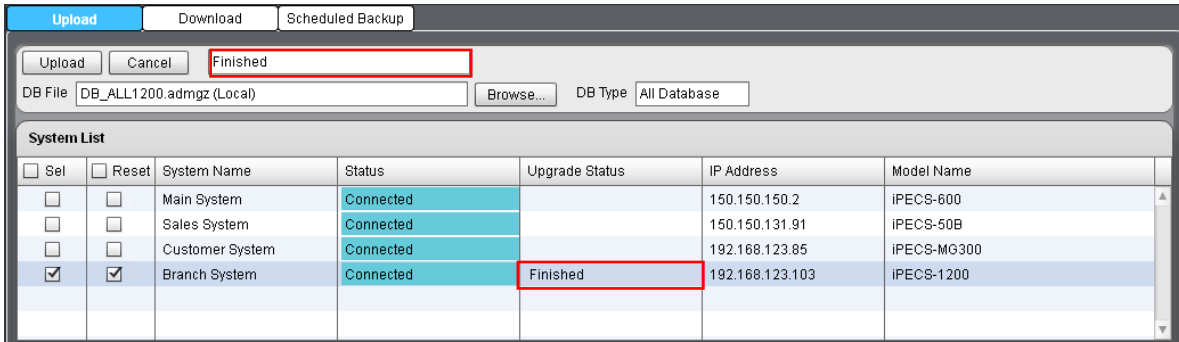


In order to upload a system DB file stored in the NMS user’s PC to the iPECS system, the system DB file should be selected first. Click [Browse...] button to select the system DB file, then the selected file name is displayed in the ‘DB File’ field. The appended string ‘(Local)’ means that the file is selected from the NMS user’s PC. The ‘DB Type’ field displays the type of the selected system DB file.



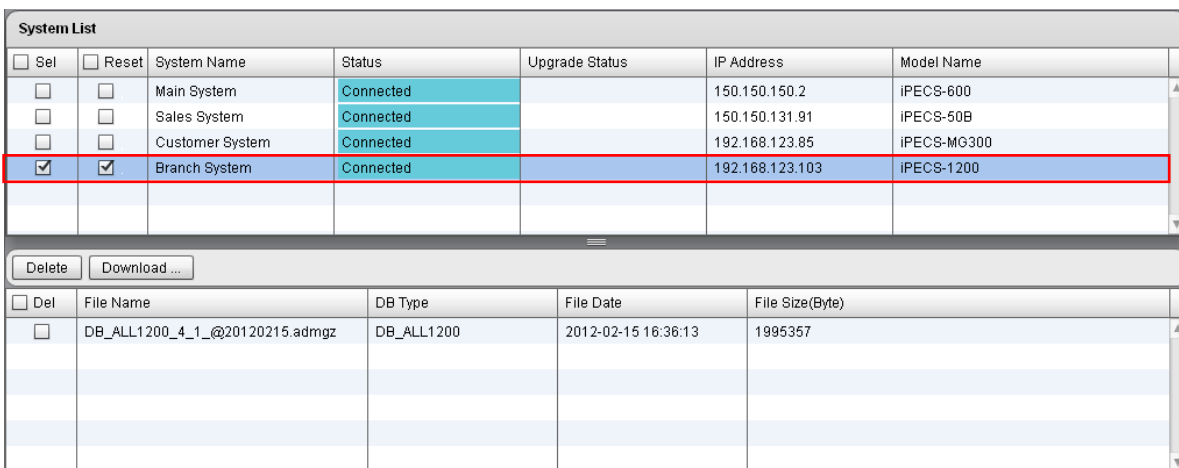
After a system DB file is selected, the check-boxes of the systems that can be uploaded with the selected file become enabled, and for other systems that cannot accept the selected file, the check-boxes become disabled.

Select the ‘Sel’ check-boxes of the systems to be uploaded with the selected DB file. If system reset is needed after completing system DB upload, click the ‘Reset’ check-boxes of those systems as well. After completing the configuration, click [Upload] button to start the system DB upload process.

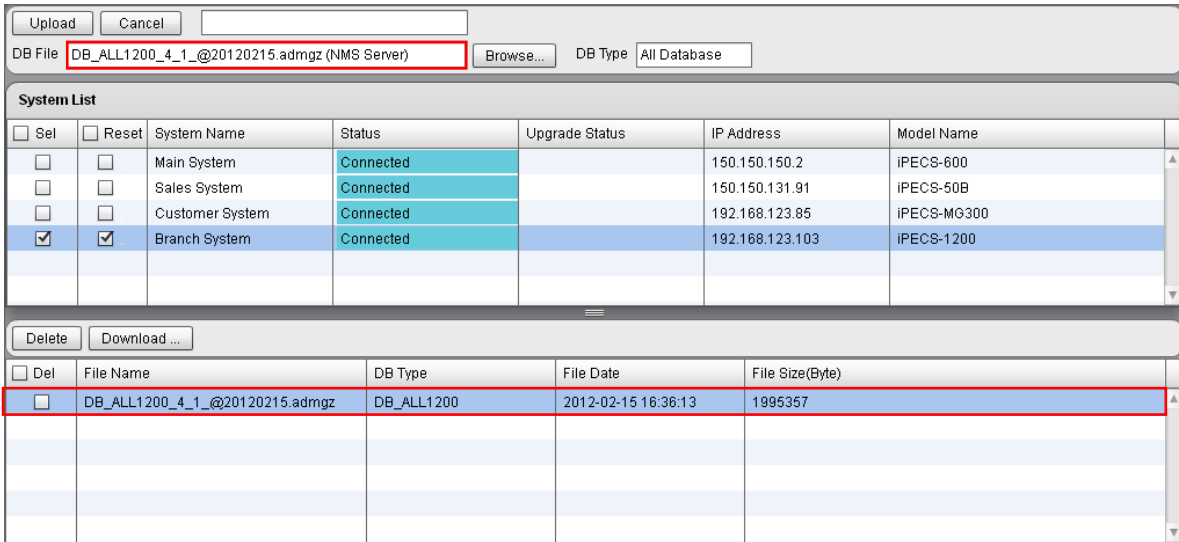


After the upload process is initiated, the system DB file is transferred to the NMS server first, and then uploaded to selected systems. As the upload process is proceeding, the status string of the ‘Status’ edit-box changes from ‘File transferring to NMS’ to ‘Uploading’. and when the uploads for all the selected systems are completed, it displays ‘Finished’. The ‘Upload Status’ field in system list displays ‘Transferring by FTP (xx%)’ (‘xx’ is the rate of file transfer process) after file upload for a specific system is started. Then it displays ‘Updating’ when file transfer is finished and the transferred system DB file is applied to the iPECS system database. After applying the system DB file, the ‘Upload Status’ changes to ‘Finished’.

Some types of system DB files such as ‘All Database’ require iPECS system reset to complete applying the uploaded DB file. Therefore, in this case, the ‘Reset’ check-box should be selected so that the iPECS system can be automatically restarted after uploading and applying the system DB file.

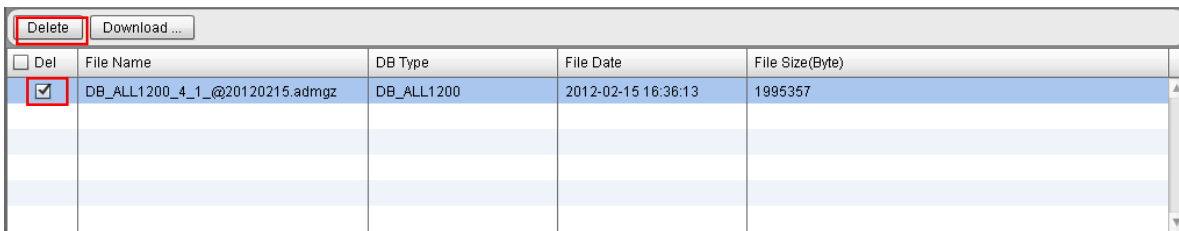


In the case that ‘All Database’ files are backed-up in NMS server using the ‘Scheduled Backup’ feature, a system DB backup file can be uploaded to the iPECS system. Before performing this, select a system that has been configured to use ‘Scheduled Backup’ from the system list to check if the system DB file to be uploaded has been backed-up in the NMS server.

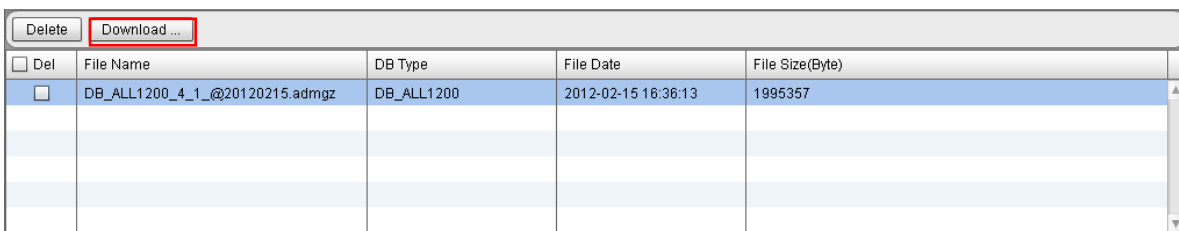


When a system DB file is selected for uploading in the ‘System DB in NMS Server’, the selected file name is displayed in ‘DB File’ field. The appended string ‘(NMS Server)’ means that the file is selected from the backup files stored in NMS server. After DB file is selected, select the ‘Sel’ check-boxes of the systems to be uploaded with the selected DB file. If system reset is needed after completing system DB upload, selected ‘Reset’ check-boxes of those systems as well. After finishing all the configurations, click on the [Upload] button to start the system DB upload process.

Selecting target systems needs to be done carefully especially when uploading ‘All Database’ file as well as other types of system DB files so that improper or unwanted systems are not to be selected and uploaded by mistake.



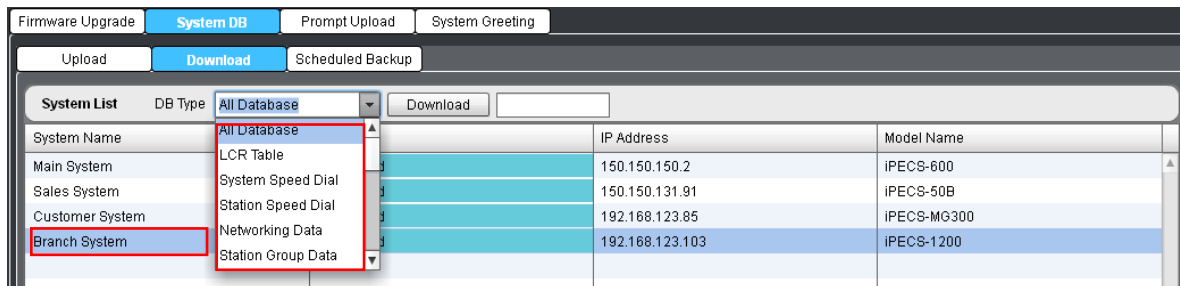
In order to delete system DB files stored in NMS server, select the ‘Del’ check-boxes of the files to be deleted, and then click [Delete] button.



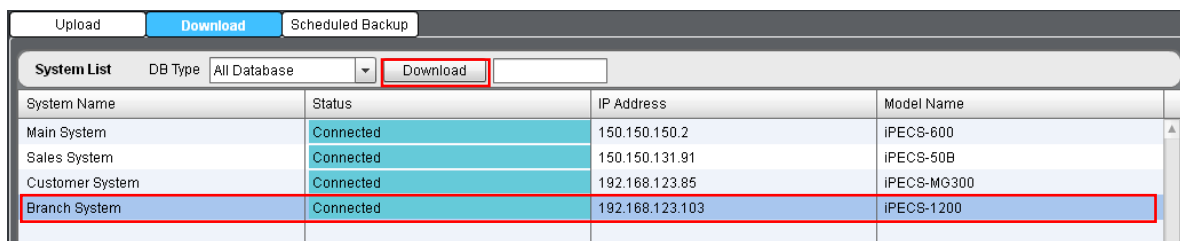
In order to download a system DB file stored in NMS server into NMS user’s PC, select the system DB file to be downloaded, and then click [Download...] button.

15.2.2 System DB Download

'System DB Download' function is for downloading system DB file of selected iPECS system into the NMS client PC. The page for this function can be opened by clicking on the [Download] tab under 'System DB'.



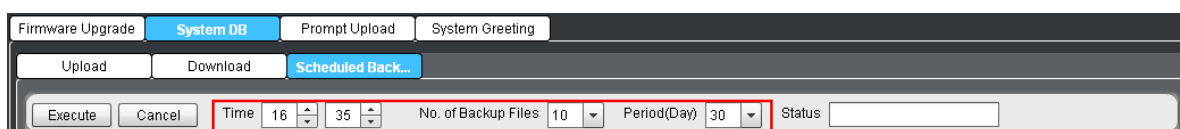
At first, select the type of system DB to be downloaded using the combo-box in 'DB Type' field (refer to the iPECS System manual for details and explanation of each database type).



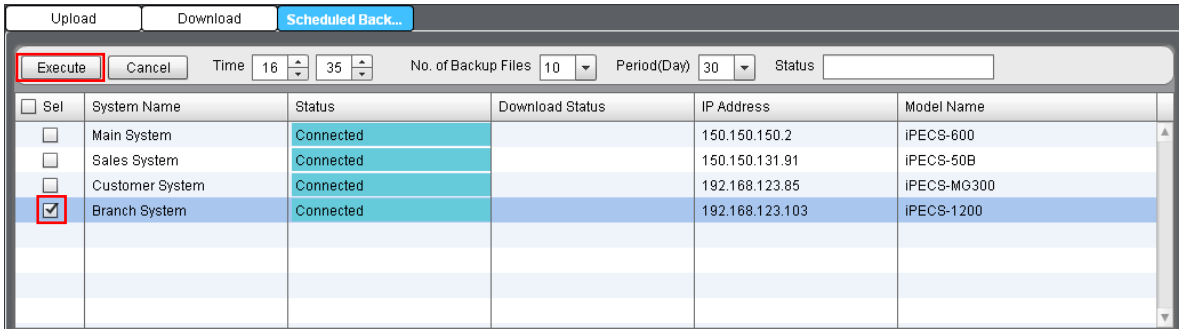
After selecting a system from which the DB file is to be downloaded, click [Download] button to start downloading the system DB file to NMS user's PC.

15.2.3 System DB Scheduled Backup

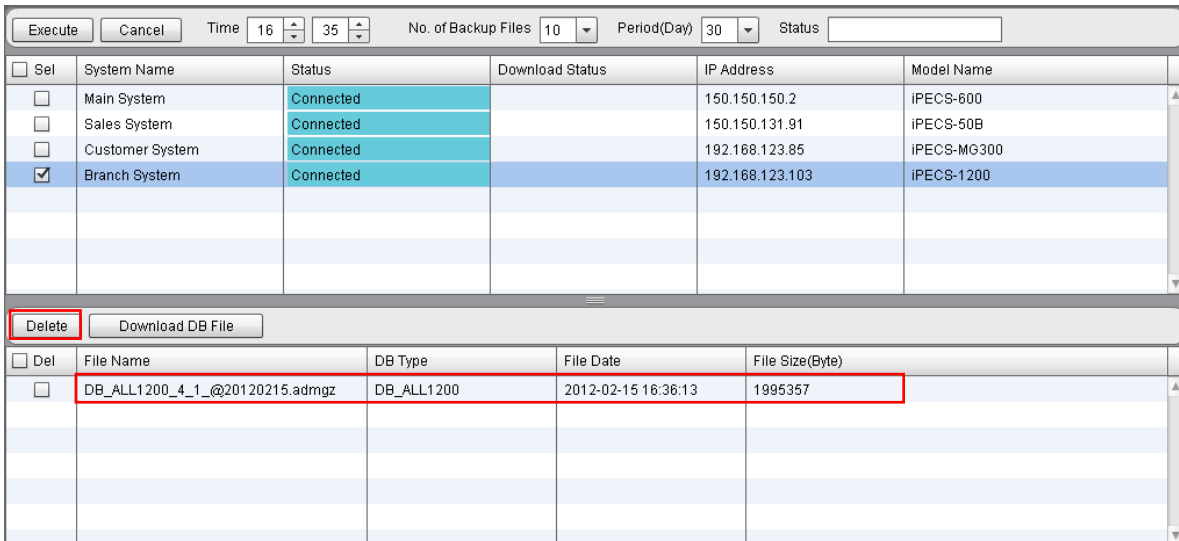
'System DB Scheduled Backup' function is for automatic downloading of 'All Database' DB files of selected iPECS systems with predefined backup period. The downloaded backup files are stored in the NMS server. The page for this function can be opened by clicking on the [Scheduled Backup] tab under 'System DB'.



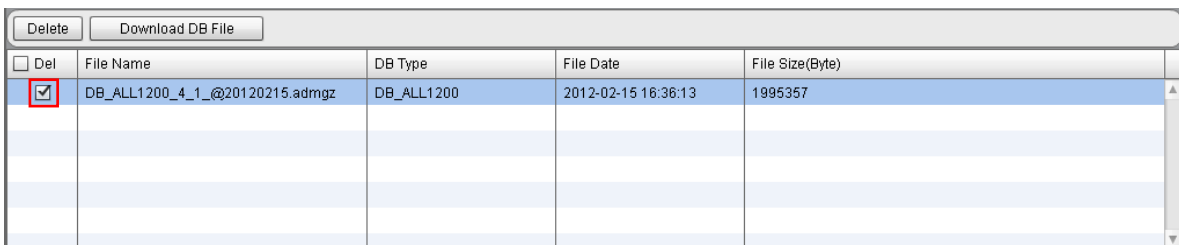
In the 'Time' field, configure the backup time when 'All Database' file is downloaded to NMS server, and in 'Period (Day)' field, the backup period in days. 'No. of Backup Files' is for setting the maximum number of backup files stored in NMS server per system. After this number of files has been backed-up, the oldest file is deleted when new system DB file is downloaded.



Select the check-boxes of the systems from which 'All Database' files are to be backed-up, and then click [Execute] button. Afterwards, 'All Database' files are downloaded from the selected systems and stored in NMS server periodically when the configured period and time has come. The maximum number of backup files per system follows the number in the 'No. of Backup Files' field.



After the DB file backup is performed, selecting a system in system list shows the 'All Database' files downloaded to NMS server in 'System DB in NMS Server'.



In order to delete system DB files stored in NMS server, select the 'Del' check-boxes of the files to be deleted, and click [Delete] button.

Del	File Name	DB Type	File Date	File Size(Byte)
<input type="checkbox"/>	DB_ALL1200_4_1_@20120215.admgz	DB_ALL1200	2012-02-15 16:36:13	1995357

In order to download a system DB file stored in NMS server into the NMS user’s PC, click on the system DB file to be downloaded, and click [Download DB File] button.

15.3 Prompt Upload

‘Prompt Upload’ provides the means to upload entire or individual prompt files to VSF (Voice Store-and-Forward) of selected iPECS system. The page for this feature can be viewed by clicking [Prompt Upload] tab under ‘Maintenance’ sub-menu. In case of UVMU of iPECS UCP supports ‘entire/ Individual Prompt Upload’. In case of AAFU of iPECS-MG system, ‘Individual Prompt Upload’ function is not supported.

* This feature applies only to VSF inside iPECS-LiK MFIM and to AAFU inside iPECS-MG MPB and to UVMU inside iPECS UCP, and does not support to VMIM of iPECS-LiK and AAIB/VMIB of iPECS-MG.

15.3.1 Entire Prompt Upload

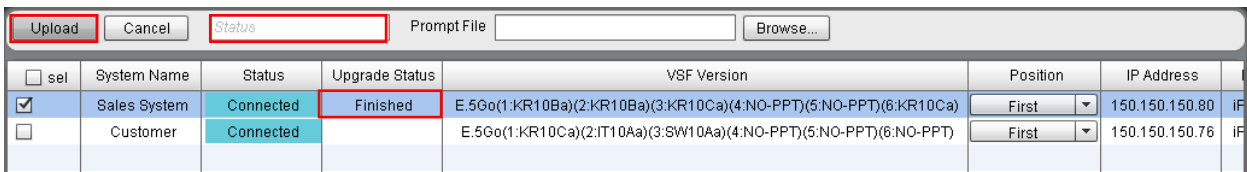
‘Entire Prompt Upload’ function is for uploading an entire prompt file to VSF (AAFU,UVMU) of selected iPECS system.



In order to upload an entire prompt file stored in NMS user’s PC to the VSF (AAFU,UVMU) of iPECS system, the prompt file should be selected first. Select a target prompt file by clicking [Browse...] button, then the selected file name is displayed in ‘Prompt File’ field. The name of entire prompt file must have the file extension of ‘rom’ as in ‘xxxxx.rom’.

sel	System Name	Status	Upgrade Status	VSF Version	Position	IP Address
<input checked="" type="checkbox"/>	Sales System	Connected		E.5Go(1:KR10Ca)(2:KR10Ba)(3:KR10Ca)(4:NO-PPT)(5:NO-PPT)(6:KR10Ca)	First	150.150.150.80
<input type="checkbox"/>	Customer	Connected		E.5Go(1:KR10Ca)(2:IT10Aa)(3:SW10Aa)(4:NO-PPT)(5:NO-PPT)(6:NO-PPT)	First	150.150.150.76

Select the check-box of the target system to be uploaded with the entire prompt file, and select the position of the prompt in VSF (AAFU,UVMU) with ‘Position’ combo-box.

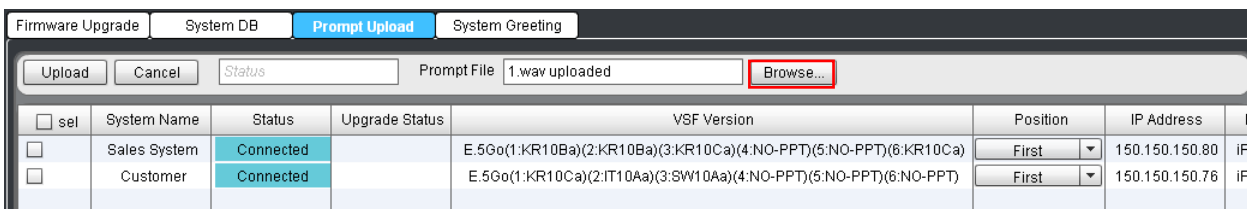


After completing the configuration, click [Upload] button to start prompt file upload process.

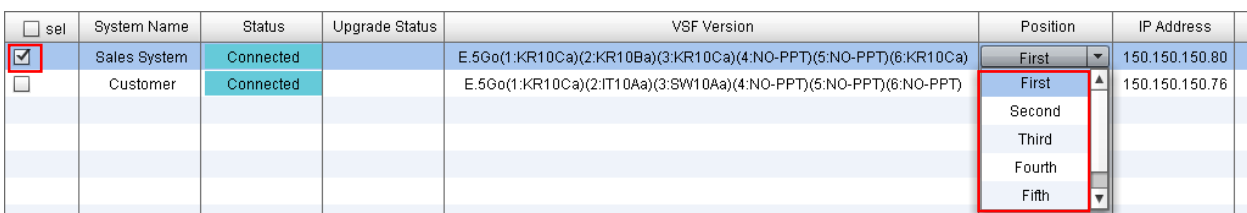
After the upload process is initiated, the prompt file is transferred to NMS server first, and then uploaded to the selected systems. As the upload process is proceeding, the status string in ‘Status’ edit-box changes from ‘File transferring to NMS’ to ‘Uploading’, and when the uploads for all the selected systems are completed, it displays ‘Finished’. The ‘Upload Status’ field in system list displays ‘Transferring by FTP (xx%)’ (‘xx’ is the rate of file transfer process) after file upload for a specific system is started. Then it displays ‘Updating’ when file transfer is finished and the transferred prompt file is applied to VSF (AAFU,UVMU). After the prompt file is applied, the ‘Upload Status’ changes to ‘Finished’.

15.3.2 Individual Prompt Upload

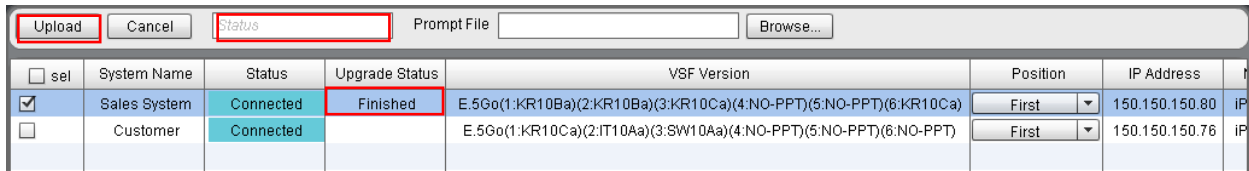
‘Individual Prompt Upload’ function is for uploading an individual prompt file to the VSF of the selected iPECS-LiK system and the UVMU of the selected iPECS UCP system. (This function does not support iPECS-MG.)



In order to upload an individual prompt file stored in the NMS user’s PC to the VSF, the prompt file has to be selected first. Select a target prompt file by clicking on the [Browse...] button; the selected file name is displayed in ‘Prompt File’ field. The individual prompt file must have the ‘wav’ file extension (ex., xxx.wav). Here, ‘xxx’ is the prompt number of the file, and can have the value of 1 ~255. In addition to the ‘wav’ file format, the file should be encoded with G.711 μ-Law (or CCITT μ-Law) at 8kHz sampling rate.



Select the check-box of the target system to which the individual prompt file is to be uploaded, and select the position of the prompt in VSF with the ‘Position’ combo-box.



After completing the configuration, click [Upload] button to start prompt file upload process.

After the upload process is initiated, the prompt file is transferred to NMS server first, and then uploaded to the selected systems. As the upload process is proceeding, the status string in ‘Status’ edit-box changes from ‘File transferring to NMS’ to ‘Uploading’. and when the uploads for all the selected systems are completed, it displays ‘Finished’. The ‘Upload Status’ field in system list displays ‘Transferring by FTP (xx%)’ (‘xx’ is the rate of file transfer process) after file upload for a specific system is started. Then it displays ‘Updating’ when file transfer is finished and the transferred prompt file is applied to VSF. After the prompt file is applied, the ‘Upload Status’ changes to ‘Finished’.

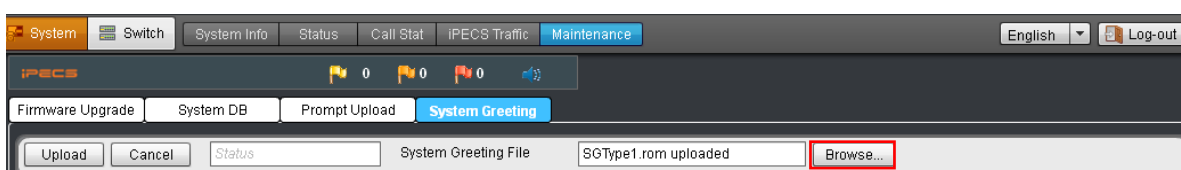
15.4 System Greeting Management

‘System Greeting Management’ provides the means to upload/download all or individual system greeting files to/from the VSF (Voice Store-and-Forward) of selected iPECS-LiK system or to/from the AAFU of selected iPECS-MG system or to/from the UVMU of selected iPECS UCP system. The page for this feature can be viewed by clicking [System Greeting] tab under ‘Maintenance’ sub-menu.

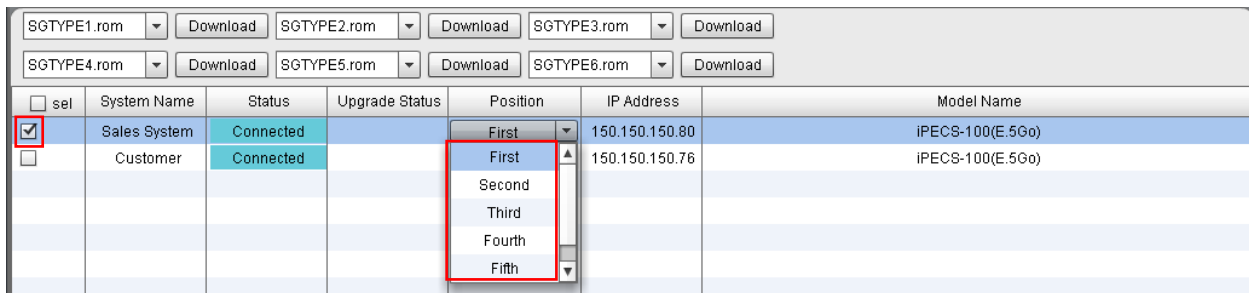
* This feature applies only to VSF inside iPECS-LiK MFIM and to AAFU inside iPECS-MG MPB and to UVMU inside iPECS UCP, and is not applicable to VMIM of iPECS-LiK and AAIB/VMIB of iPECS-MG.

15.4.1 Entire System Greeting Management

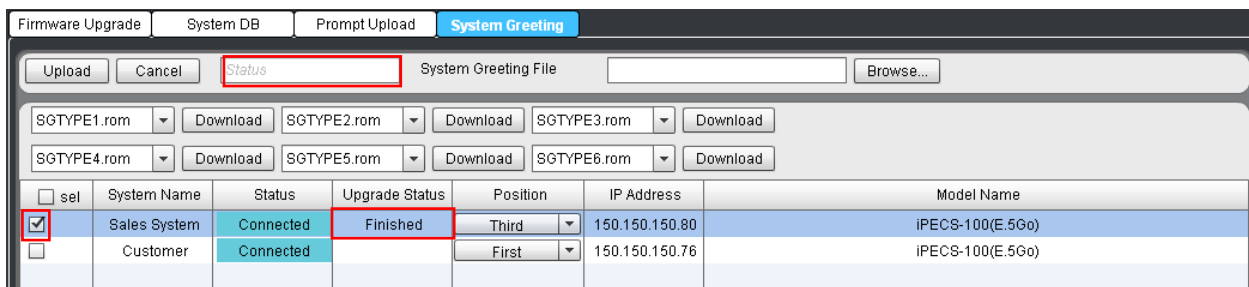
‘Entire System Greeting Management’ function is for uploading/downloading entire system greeting file to/from the VSF (AAFU,UVMU) of selected iPECS system.



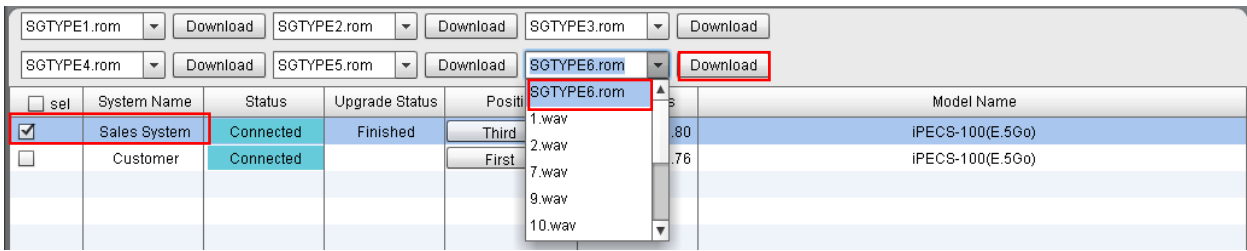
In order to upload an entire system greeting file stored in NMS user’s PC to VSF (AAFU,UVMU) of the iPECS system, the system greeting file has to be selected first. Select a system greeting file by clicking on the [Browse...] button, then the selected file name is displayed in the ‘System Greeting File’ field. The system greeting file must have the ‘rom’ file extension (ex., ‘SGTYPEx.rom’). Here, ‘x’ is the position of the system greeting in VSF (AAFU,UVMU), and can have the value of 1~3. However, this position value does not have meaning when executing the upload process.



Select the check-box of the target system to be uploaded with the entire system greeting file, and select the position of the system greeting in VSF (AAFU,UVMU) using the ‘Position’ combo-box.



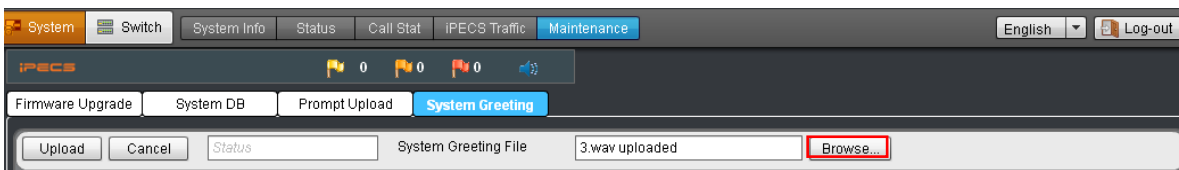
After completing the configuration, click [Upload] button to start the system greeting upload process. After the upload process is initiated, the system greeting file is transferred to the NMS server first, and then uploaded to selected systems. As the upload process is proceeding, the status string in the ‘Status’ edit-box changes from ‘File transferring to NMS’ to ‘Uploading’, and when the uploads for all the selected systems are completed, it displays ‘Finished’. The ‘Upload Status’ field in the system list displays ‘Transferring by FTP (xx%)’ (‘xx’ is the rate of file transfer process) after file upload for a specific system is started. The field will display ‘Updating’ when file transfer is finished and the transferred system greeting file will be applied to VSF (AAFU,UVMU). After the system greeting file is applied, the ‘Upload Status’ changes to ‘Finished’.



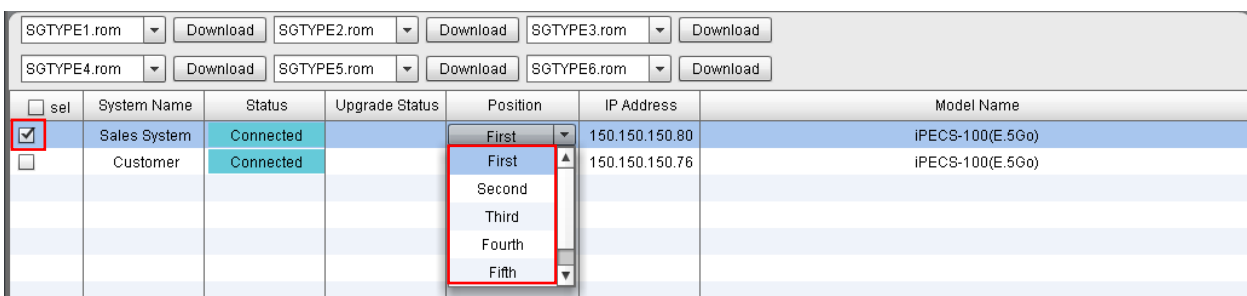
The entire system greeting file stored in VSF (AAFU,UVMU) can be downloaded to the NMS user’s PC. In system list, click on the system from which entire system greeting file is to be downloaded, then entire system greeting files of each position are displayed in the corresponding combo-boxes. Select a file of the format ‘SGTYPEx.rom’ using the combo-box, and click [Download] button on the right to download the file into NMS user’s PC.

15.4.2 Individual System Greeting Management

‘Individual System Greeting Management’ function is for uploading/downloading individual system greeting files to/from the VSF (AAFU,UVMU) of a selected iPECS system.

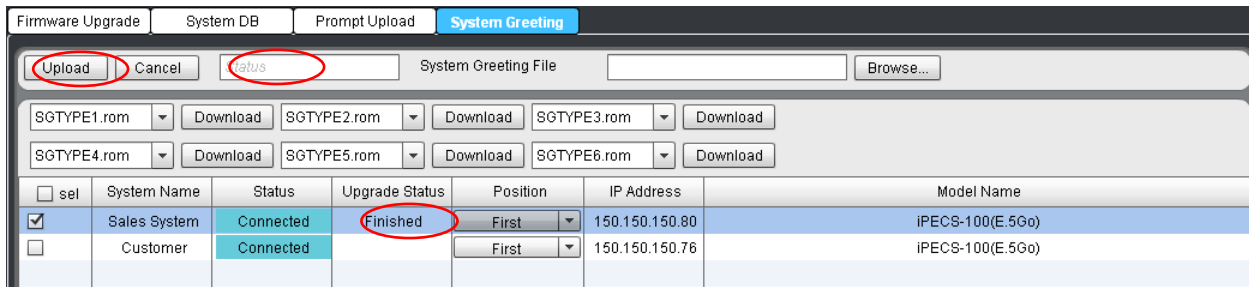


In order to upload an individual system greeting file stored in the NMS user’s PC to the VSF (AAFU,UVMU) of the iPECS system, the system greeting file has to be selected first. Select a target system greeting file by clicking on the [Browse...] button, then the selected file name is displayed in the ‘System Greeting File’ field. The name of individual system greeting file must have the ‘wav’ file extension (Ex., ‘yy.rom’ or ‘x_yy.wav’). Here, ‘x’ is the position of the system greeting in VSF (AAFU,UVMU), and can have the value of 1~3. However, this position value does not have meaning when executing the upload process. ‘yy’ is the individual system greeting number, and can have the value of 1~72. In addition, the file should be encoded with G.711 μ-Law (or CCITT μ-Law) at 8kHz sampling rate.

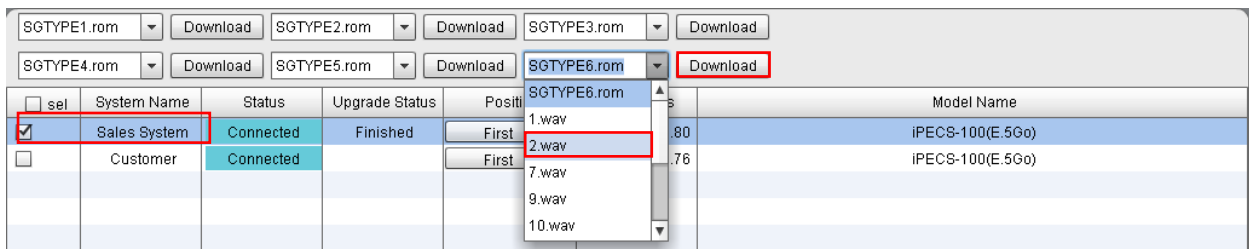


Click on the check-box of the target system to be uploaded with the individual system greeting

file, and select the position of the system greeting in VSF (AAFU,UVMU) using the 'Position' combo-box.



After completing the configuration, click [Upload] button to start the system greeting upload process. After the upload process is initiated, the system greeting file is transferred to the NMS server first, and then uploaded to selected systems. As the upload process is proceeding, the status string in the 'Status' edit-box changes from 'File transferring to NMS' to 'Uploading', and when the uploads for all the selected systems are completed, it displays 'Finished'. The 'Upload Status' field in the system list displays 'Transferring by FTP (xx%)' ('xx' is the rate of file transfer process) after file upload for a specific system is started. The field will display 'Updating' when file transfer is finished and the transferred system greeting file will be applied to VSF (AAFU). After the system greeting file is applied, the 'Upload Status' changes to 'Finished'.



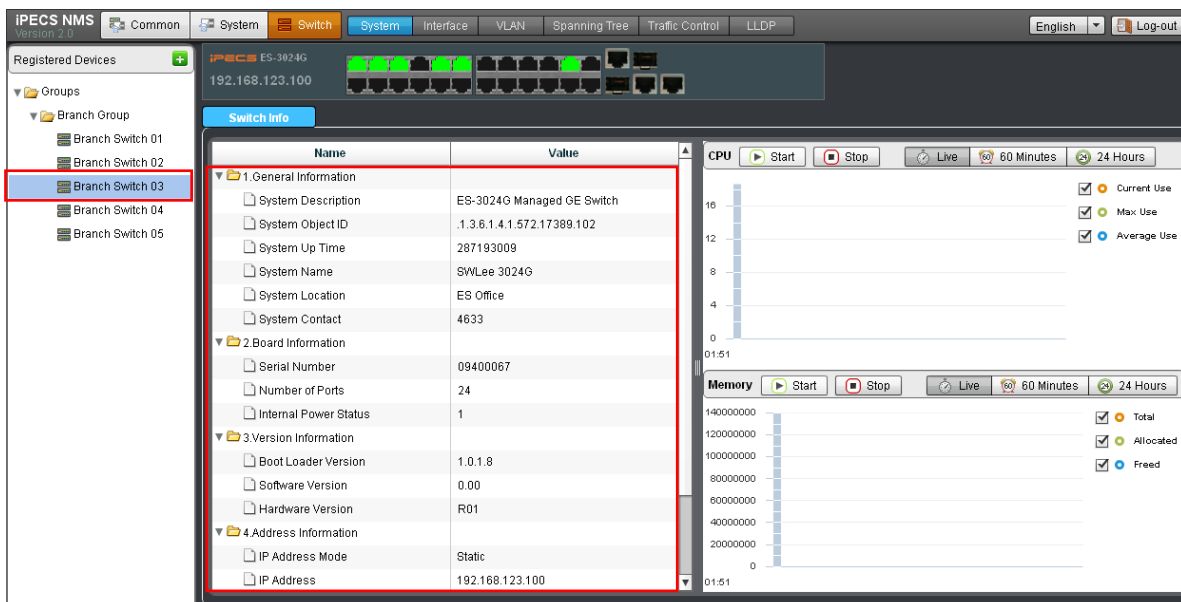
The individual system greeting file stored in VSF (AAFU,UVMU) can be downloaded to the NMS user's PC. In system list, click on the system from which individual system greeting file is to be downloaded, then individual system greeting files of each position are displayed in the corresponding combo-boxes. Select a file of the format '*.wav' using the combo-box, and click [Download] button on the right to download the file into NMS user's PC.

16. Switch Information

‘Switch Information’ is used for checking device information such as general switch information, board & version information and network address information. Real-time monitoring functions for CPU and memory usage information are also provided. The page for this feature can be viewed by clicking [System] sub-menu under ‘Switch’ menu.

16.1 Device Information

‘Device Information’ provides general information, board & version information and address information of a switch selected in ‘Registered Devices’.



16.1.1 General Information

‘General Information’ shows the information for system description, system object ID, system up time, system name, system location and system contact of a device selected ‘Registered Devices’.

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
General Information	System Description	Brief description of device type.
	System Object ID	MIB II object ID for switch’s network management subsystem.
	System Up Time	Length of time the management agent has been up.

	System Name	Name assigned to the switch system.
	System Location	Specifies the switch location.
	System Contact	Contact information of the administrator responsible for the switch.

16.1.2 Board Information

'Board Information' shows the information for serial number, number of ports, internal power status of a device selected in 'Registered Devices'.

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Board Information	Serial Number	The serial number of the switch.
	Number of Ports	Number of built-in ports.
	Internal Power Status	Displays the status of the internal power supply.

16.1.3 Version Information

'Version Information' shows the information for boot loader version, software version and hardware version of a device selected in 'Registered Devices'.

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Version Information	Software Version	Version number of runtime code.
	Boot Loader Version	Version number of loader code.
	Hardware Version	Hardware version of the main board.

16.1.4 Address Information

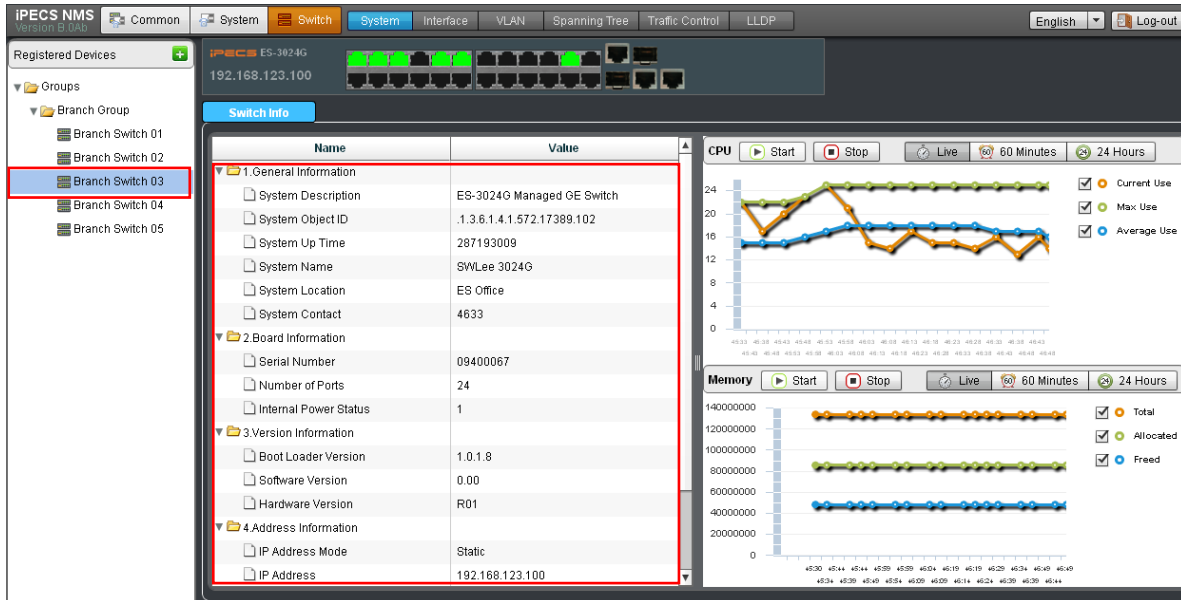
'Address Information' shows the information for IP address mode, IP address, subnet mask, gateway IP address and MAC address of a device selected in 'Registered Devices'.

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Address Information	IP Address Mode	Specifies whether IP functionality is enabled via manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP).
	IP Address	IP address assigned to the switch
	Subnet Mask	This mask identifies the host address bits used for routing to specific subnets.
	Gateway IP Address	IP address of the gateway router
	MAC Address	The physical layer address for this switch.

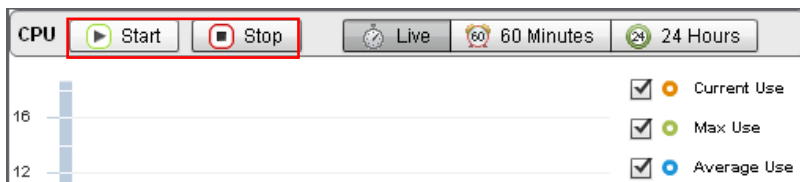
16.2 CPU and Memory Usage Information

‘CPU and Memory Usage Information’ provides CPU and memory usage information of a switch selected in ‘Registered Devices’.

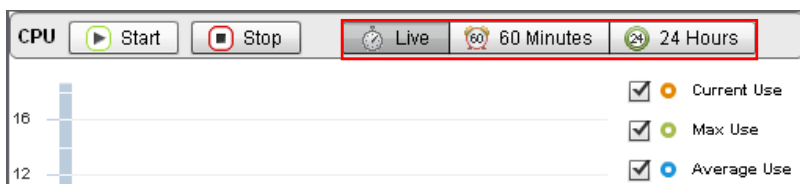


16.2.1 CPU Usage Information

‘CPU Usage Information’ shows CPU usage information in graph format for a switch selected in ‘Registered Devices’.

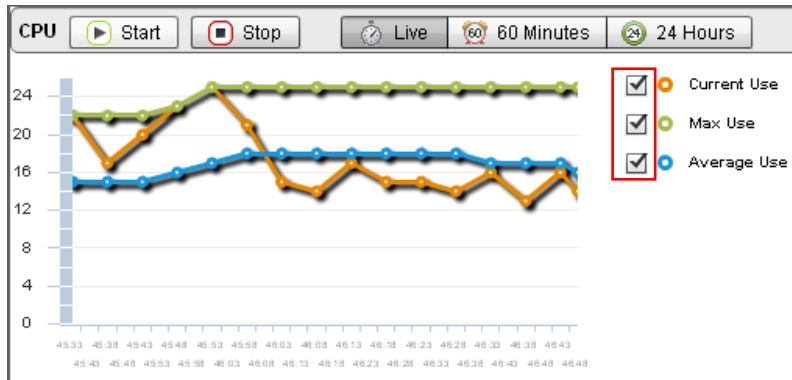


To display CPU usage information, click [Start] button to initiate data display, and [Stop] to finish it. CPU usage display will be automatically finished without using [Stop] button if the polling count reaches 65545 times.



The graph that shows the CPU usage can be displayed in three types of time period such as ‘Live

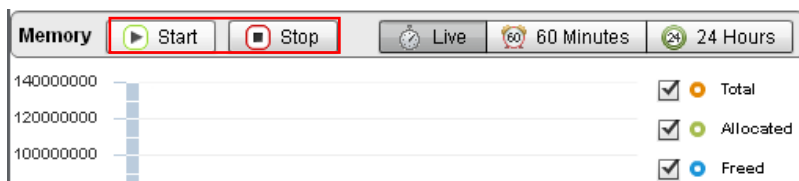
Data', 'Last 60 Minutes' and 'Last 24 Hours'. The real-time graph is displayed by clicking [Live] button. [60 Minutes] and [24 Hours] buttons are used for displaying the graph for last 60 minutes and 24 hours from the moment the corresponding button was clicked.



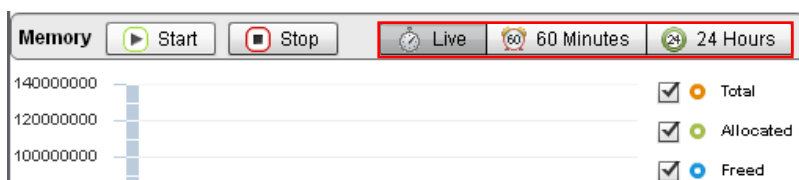
By using the check boxes on the right side, graphs for 'Current Use', 'Max Use' and 'Average Use' can be selectively displayed.

16.2.2 Memory Usage Information

'Memory Usage Information' shows memory usage information in graph format for a switch selected in 'Registered Devices'.

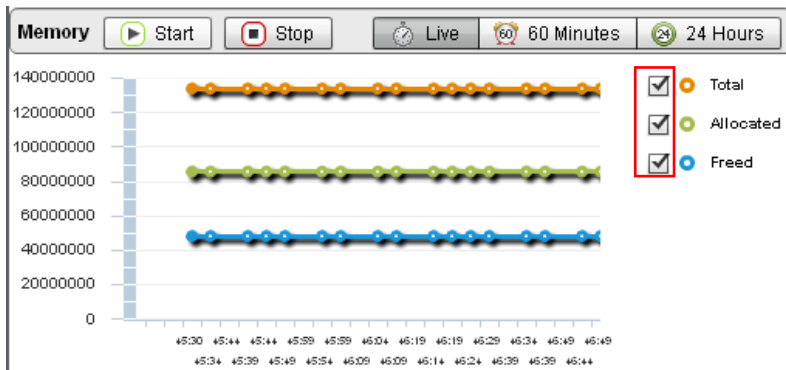


To display memory usage information, click [Start] button to initiate data display, and [Stop] to finish it. Memory usage display will be automatically finished without using [Stop] button if the polling count reaches 65545 times.



The graph that shows the memory usage can be displayed in three types of time period such as 'Live Data', 'Last 60 Minutes' and 'Last 24 Hours'. The real-time graph is displayed by clicking

[Live] button. [60 Minutes] and [24 Hours] buttons are used for displaying the graph for last 60 minutes and 24 hours from the moment the corresponding button was clicked.



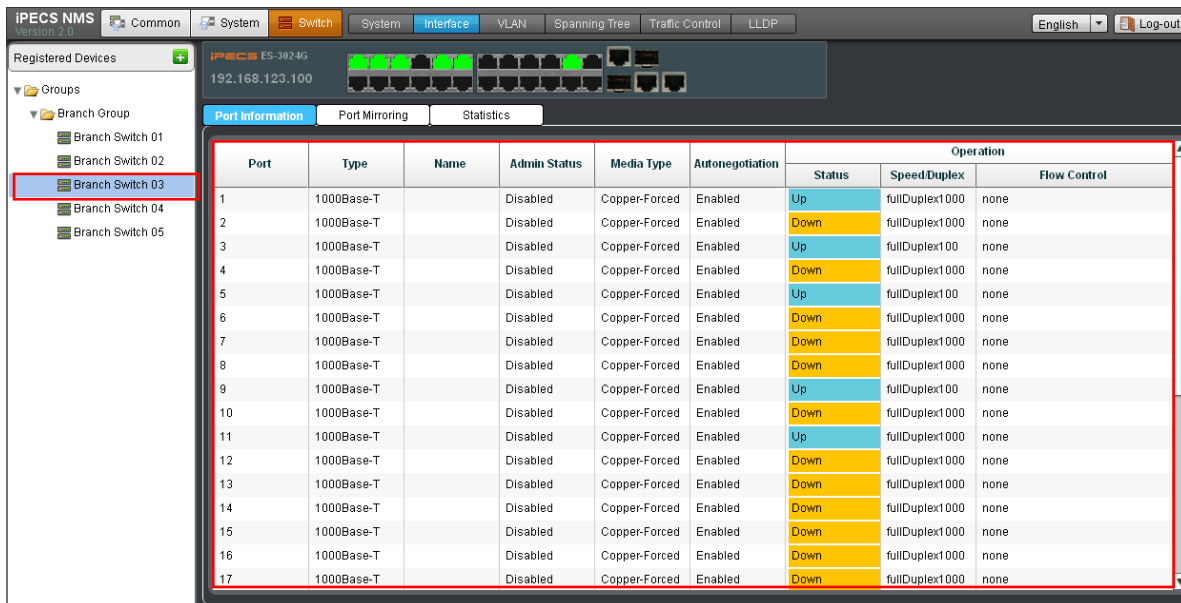
By using the check boxes on the right side, graphs for 'Total', 'Allocated' and 'Freed' can be selectively displayed.

17. Switch Interface Information

‘Switch Interface Information’ provides interface information of a registered switch such as port information, port mirroring information and statistics information. The pages for these features can be viewed by clicking [Interface] sub-menu under ‘Switch’ menu.

17.1 Port Information

‘Port Information’ shows port information of a selected switch such as port type, name admin status, media type, autonegotiation and operational information. The page for this feature can be viewed by clicking [Port Information] tab under ‘Interface’ sub-menu.

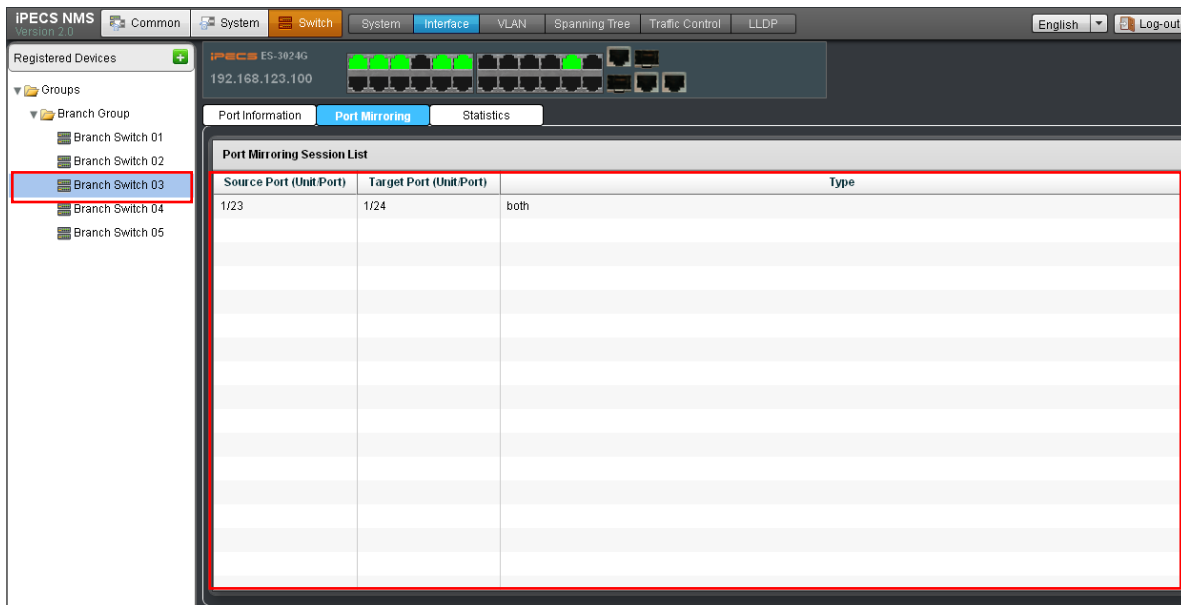


The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Port Information	Type	Indicates the port type. (e.g. 100Base-TX, 1000Base-T, 100Base SFP, 1000Base SFP)
	Name	Interface label.
	Admin Status	Shows if the port is enabled or disabled.
	Media Type	Media type used. (e.g. Copper-Forced, SFP-Forced, SFP-Preferred-Auto)
	Autonegotiation	Shows if auto-negotiation is enabled or disabled.
	Operation Status	Shows the status of the link (e.g. Up, Down)
	Speed/Duplex	Shows the current speed and duplex mode.
	Flow Control	Shows if flow control is enabled or disabled.

17.2 Port Mirroring Information

‘Port Mirroring Information’ shows port mirroring configuration information of a switch selected in ‘Registered Devices’. The page for this feature can be viewed by clicking [Port Mirroring] tab under ‘Interface’ sub-menu.

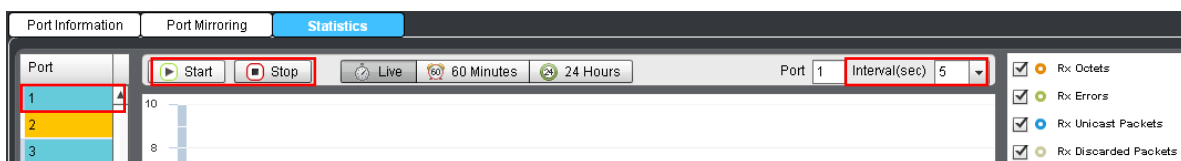


The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Port Mirroring	Source Port (Unit/Port)	The port whose traffic will be monitored.
	Target Port (Unit/Port)	The port that will mirror the traffic on the source port.
	Type	Shows which traffic to mirror to the target port (e.g. Rx, Tx, Both)

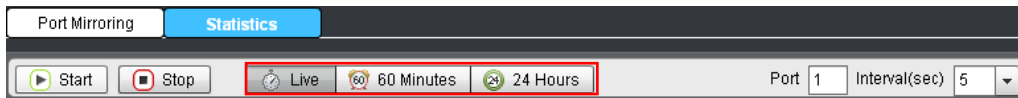
17.3 Port Statistics Information

‘Port Statistics Information’ shows the traffic statistics information of a selected switch port with graph and table. The page for this feature can be viewed by clicking [Statistics] tab under ‘Interface’ sub-menu.

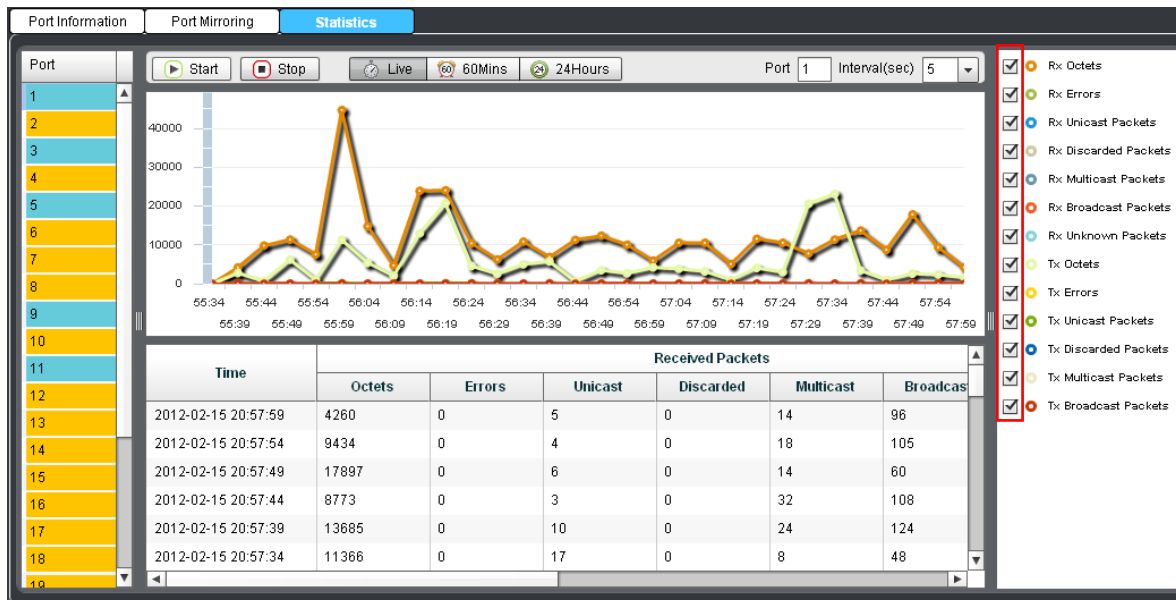


Before displaying port statistics information, a target port and the polling interval should be configured. A target port can be selected using the ‘Port’ list on the left. For ‘Interval’ field, one of

5, 10, 20, 30 second options can be selected using the combo-box. After finishing configuration, click [Start] button to initiate displaying port statistics information, and [Stop] to finish it. Port statistics display will be automatically finished without using [Stop] button if the polling count reaches 65545 times.



The graph that shows the port statistics information can be displayed in three types of time period such as 'Live Data', 'Last 60 Minutes' and 'Last 24 Hours'. The real-time graph is displayed by clicking [Live] button. [60 Minutes] and [24 Hours] buttons are used for displaying the graph for last 60 minutes and 24 hours from the moment the corresponding button was clicked.



By using the check boxes on the right side, graphs can be selectively displayed for various types of network traffic.

Below the graph is the table that shows the data of the port statistics information. The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Port Statistics	Rx Octets	The total number of octets received on the interface, including framing characters.
	Rx Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
	Rx Unicast	The number of subnetwork-unicast packets delivered to a

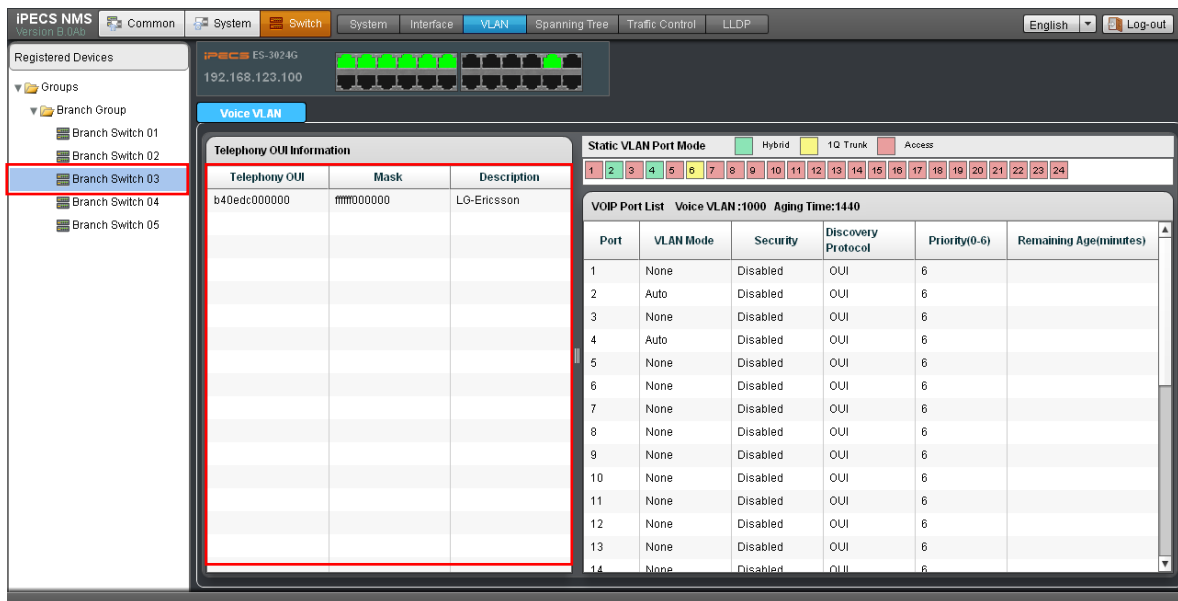
Packets	higher-layer protocol.
Rx Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Rx Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Rx Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Rx Unknown Packets	The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.
Tx Octets	The total number of octets transmitted out of the interface, including framing characters.
Tx Errors	The number of outbound packets that could not be transmitted because of errors.
Tx Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Tx Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Tx Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Tx Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

18. Switch VLAN Information

‘Switch VLAN Information’ provides Voice VLAN information configured for a selected switch such as telephony OUI information, VoIP port information and static VLAN port mode. The page for these features can be viewed by clicking [VLAN] sub-menu under ‘Switch’ menu.

18.1 Telephony OUI Information

‘Telephony OUI Information’ shows telephony OUI information configured in a switch selected in ‘Registered Devices’. OUI (Organizationally Unique Identifier) uniquely identifies a network equipment vendor or manufacturer, and corresponds to the first 3 octets of MAC address. A configured switch checks sender’s MAC address of a packet to see if its OUI part matches with the telephony OUI value. If it matches, the switch determines that the packet is sent from a VoIP device.



The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Telephony OUI Information	Telephony OUI	Specifies MAC address or MAC address range
	Mask	Identifies a range of MAC addresses. Selecting a mask of FF-FF-FF-00-00-00 identifies all devices with the same OUI (the first three octets). Other masks restrict the MAC address range. Selecting FF-FF-FF-FF-FF-FF specifies a single MAC address.
	Description	User-defined text that identifies the VoIP devices.

18.2 Static VLAN Port Mode

‘Static VLAN Port Mode’ shows the type of VLAN membership for a port of a selected switch, and may have ‘Hybrid’, ‘1Q Trunk’ or ‘Access’.

Static VLAN Port Mode																							
Hybrid						1Q Trunk						Access											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Static VLAN Port Mode	Hybrid	Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
	1Q Trunk	Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN.
	Access	Specifies the port to operate as an untagged interface. The port transmits and receives untagged frames on a single VLAN only.

18.3 VoIP Port Information

‘VoIP Port Information’ shows Voice VLAN configuration information of a port of a selected switch such as VLAN mode, security, discovery protocol, priority and remaining age.

VoIP Port List Voice VLAN:1000 Aging Time:1440					
Port	VLAN Mode	Security	Discovery Protocol	Priority(0-6)	Remaining Age(minutes)
1	None	Disabled	OUI	6	
2	Auto	Disabled	OUI	6	
3	None	Disabled	OUI	6	
4	Auto	Disabled	OUI	6	
5	None	Disabled	OUI	6	
6	None	Disabled	OUI	6	
7	None	Disabled	OUI	6	
8	None	Disabled	OUI	6	
9	None	Disabled	OUI	6	
10	None	Disabled	OUI	6	
11	None	Disabled	OUI	6	
12	None	Disabled	OUI	6	
13	None	Disabled	OUI	6	
14	None	Disabled	OUI	6	

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
VoIP Port Information	VLAN Mode	Specifies if the port will be added to the Voice VLAN when VoIP traffic is detected. - None : The Voice VLAN feature is disabled on the port. The port will not detect VoIP traffic or be added to

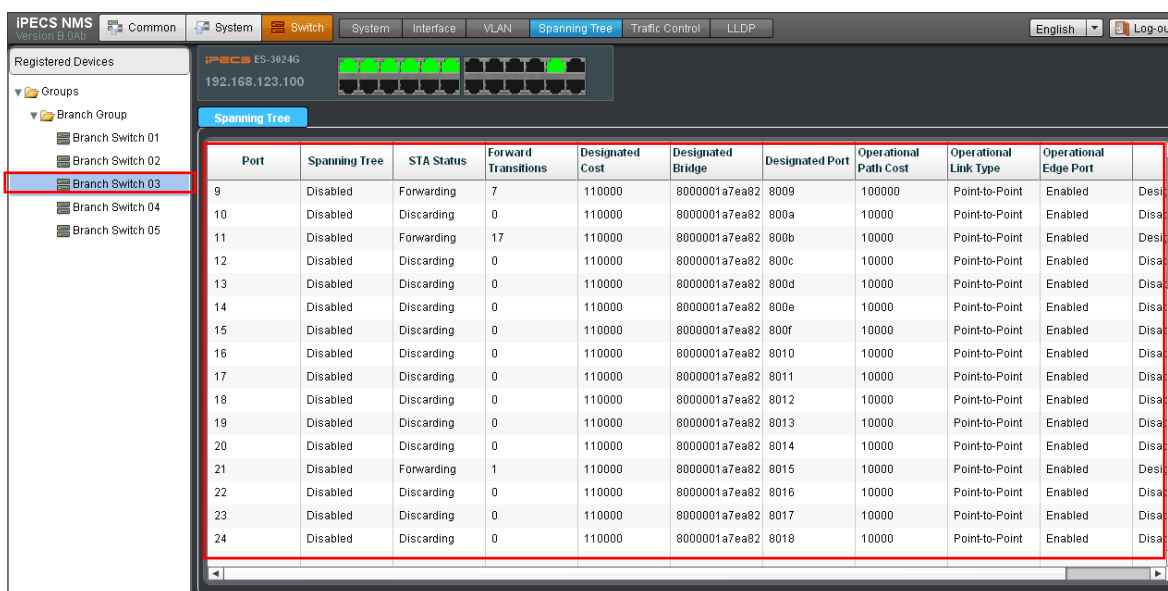
		<p>the Voice VLAN.</p> <ul style="list-style-type: none"> - Auto : The port will be added as a tagged member to the Voice VLAN when VoIP traffic is detected on the port. - Manual : The Voice VLAN feature is enabled on the port, but the port must be manually added to the Voice VLAN.
	Security	<p>Specifies security filtering that discards any non-VoIP packets received on the port that are tagged with the voice VLAN ID.</p> <p>VoIP traffic is identified by source MAC addresses configured in the Telephony OUI list, or through LLDP that discovers VoIP devices attached to the switch.</p>
	Discovery Protocol	<p>Specifies a method to use for detecting VoIP traffic on the port.</p> <ul style="list-style-type: none"> - OUI : Traffic from VoIP devices is detected by the OUI of the source MAC address. MAC address OUI numbers must be configured in the Telephony OUI list so that the switch recognizes the traffic as being from a VoIP device. - LLDP : Uses LLDP (IEEE 802.1AB) to discover VoIP devices attached to the port. LLDP checks that the 'telephone bit' in the system capability TLV is turned on.
	Priority	<p>Specifies a CoS priority for port traffic on the Voice VLAN. The priority of any received VoIP packet is overwritten with the new priority when the Voice VLAN feature is active for the port.</p>
	Remaining Age (minutes)	<p>Number of minutes before this entry is aged out.</p>

19. Switch Spanning Tree Information

‘Switch Spanning Tree Information’ provides STP/RSTP status and configuration information of a registered switch. The pages for these features can be viewed by clicking [Spanning Tree] sub-menu under ‘Switch’ menu.

19.1 Spanning Tree Information

‘Spanning Tree Information’ shows STP/RSTP information of a switch selected in ‘Registered Devices’ such as spanning tree enable/disable status, STA status, forward transitions, designated cost, designated bridge, designated port, operational path cost, operational link type, operational edge port and port role.



The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Spanning Tree Information	Spanning Tree	Shows if STA has been enabled on this interface.
	STA Status	Displays current state of this port within the Spanning Tree. - Discarding : Port receives STA configuration messages, but does not forward packets. - Learning : Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses. - Forwarding : Port forwards packets, and continues learning addresses.

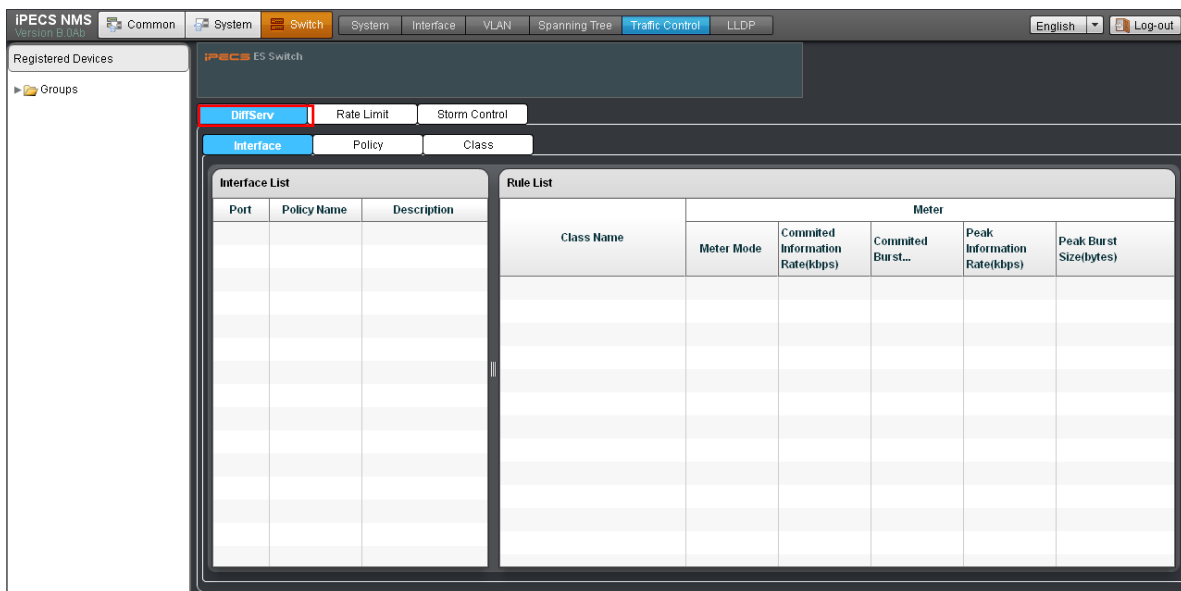
	Forward Transitions	The number of times this port has transitioned from the Learning state to the Forwarding state.
	Designated Cost	The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
	Designated Bridge	The bridge priority and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
	Designated Port	The port priority and number of the port on the designated bridging device through which this switch must communicate with the root of the Spanning Tree.
	Operational Path Cost	The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
	Operational Link Type	The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection..
	Operational Edge Port	This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration (i.e., true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
	Port Role	Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (i.e., root port), connecting a LAN through the bridge to the root bridge (i.e., designated port), is the MSTI regional root (i.e., master port), or is an alternate or backup port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (i.e., disabled port) if a port has no role within the spanning tree.

20. Switch Traffic Control Information

‘Switch Traffic Control Information’ provides traffic control information of a registered switch such as DiffServ information, rate control information and storm control information. The pages for these features can be viewed by clicking [Traffic Control] sub-menu under ‘Switch’ menu.

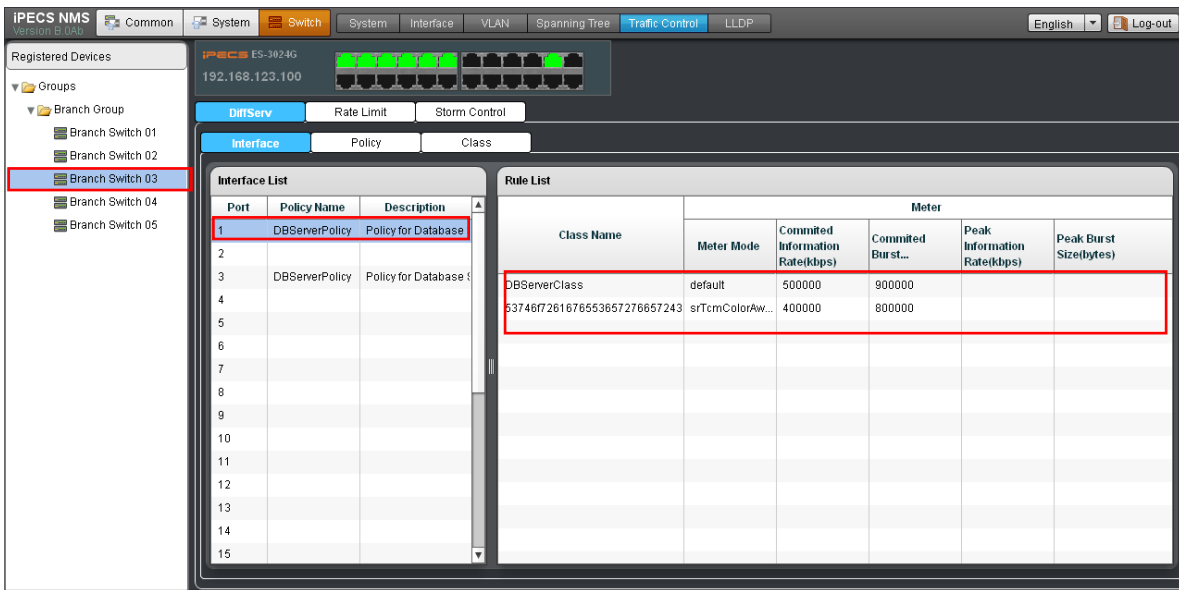
20.1 DiffServ Information

‘DiffServ Information’ provides DiffServ configuration information of a switch selected in ‘Registered Devices’ such as interface information, policy information and class information. The pages for these features can be viewed by clicking [DiffServ] tab under ‘Traffic Control’ sub-menu.



20.1.1 Interface Information

‘Interface Information’ shows diffServ configuration information for each interface of selected switch. This view is comprised of ‘Interface List’ panel and ‘Rule List’ panel. This page can be viewed by clicking [Interface] tab under ‘DiffServ’.



When a switch is selected in ‘Registered Devices’, port list of the switch is displayed in ‘Interface List’ with the fields of ‘Policy Name’ and ‘Description’. The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Interface List	Port	Port number of a switch selected in ‘Registered Devices’
	Policy Name	Name of policy map. (A policy map is used to group one or more class map statements, modify service tagging, and enforce bandwidth policing. A policy map can then be bound by a service policy to one or more interfaces.)
	Description	A brief description of a policy map.

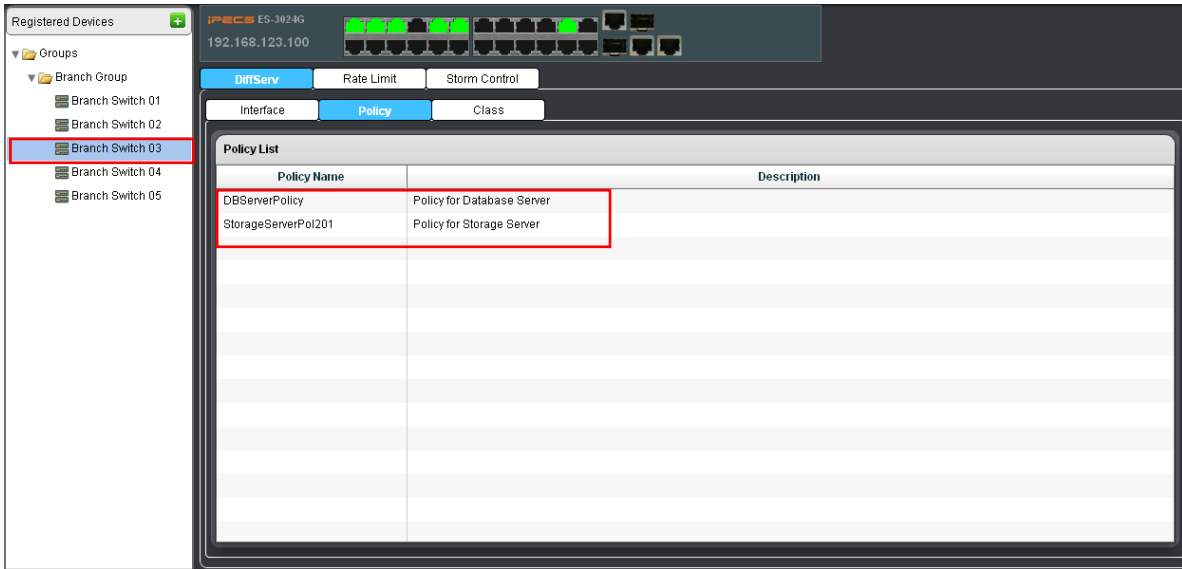
When a policy is selected in ‘Interface List’, the rules related to the policy are displayed in ‘Rule List’ on the right. The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Rule List	Class Name	Name of a class map that defines a traffic classification upon which a policy can act.
	Action	This attribute is used to set an internal QoS value for matching packets. - Set CoS : Configures the service provided to ingress traffic by setting an internal CoS value for a matching packet (as specified in rule settings for a class map). (0-7) - Set PHB : Configures the service provided to ingress traffic by setting the internal per-hop behavior for a matching packet (as specified in rule settings for a class map). (0~7) - Set IP DSCP : Configures the service provided to ingress traffic by setting an IP DSCP value for a

		matching packet (as specified in rule settings for a class map). (0~63)
	Meter Mode	Shows one of the following policing methods, and may have 'Flow', 'SRTCM-Color-Aware', 'SRTCM-Color-Blind', 'TRTCM-Color-Aware' or 'TRTCM-Color-Blind'.
	Committed Information Rate	Rate in kilobits per second. (Range: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower) The rate cannot exceed the configured interface speed.
	Committed Burst Size	Burst in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)
	Exceeded Burst Size	Burst in excess of committed burst size. (Range: 4000-16000000 at a granularity of 4k bytes) The burst size cannot exceed 16 Mbytes.
	Peak Information Rate	Rate in kilobits per second. (Range: 64-10000000 kbps at a granularity of 64 kbps or maximum port speed, whichever is lower) The rate cannot exceed the configured interface speed.
	Peak Burst Size	Burst size in bytes. (Range: 4000-16000000 at a granularity of 4k bytes)
	Conform	Specifies that traffic conforming to the maximum rate (CIR) will be transmitted without any change to the DSCP service level. - Transmit : Transmits in-conformance traffic without any change to the DSCP service level.
	Exceed	Specifies whether traffic that exceeds the maximum rate (CIR) but is within the peak information rate (PIR) will be dropped or the DSCP service level will be reduced. - Set IP DSCP : Decreases DSCP priority for out of conformance traffic. (0~63). - Drop : Drops out of conformance traffic.
	Violate	Specifies whether the traffic that exceeds the peak information rate (PIR) will be dropped or the DSCP service level will be reduced. - Set IP DSCP : Decreases DSCP priority for out of conformance traffic. (0~63). - Drop : Drops out of conformance traffic.

20.1.2 Policy Information

'Policy Information' shows traffic policy information configured in the switch selected in 'Registered Devices'. This page can be viewed by clicking [Policy] tab under 'DiffServ'.

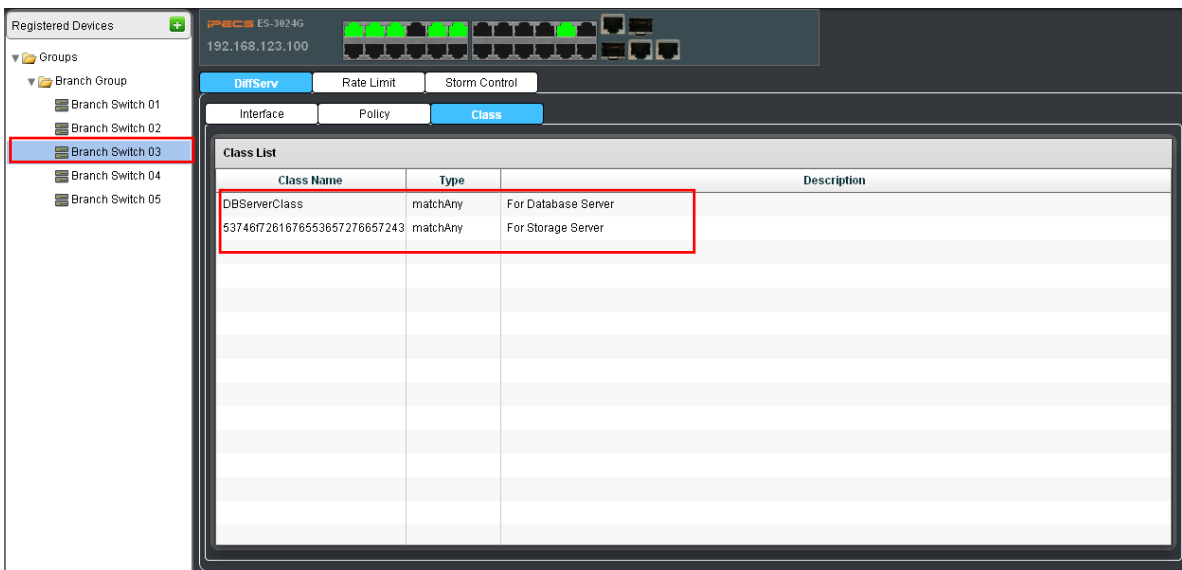


When a switch is selected in 'Registered Devices', the name and description of the traffic policy configured in the switch are displayed. The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Policy List	Policy Name	Name of policy map.
	Description	A brief description of the traffic policy.

20.1.3 Class Information

'Class Information' shows class map information configured in the switch selected in 'Registered Devices'. This page can be viewed by clicking [Class] tab under 'DiffServ'.

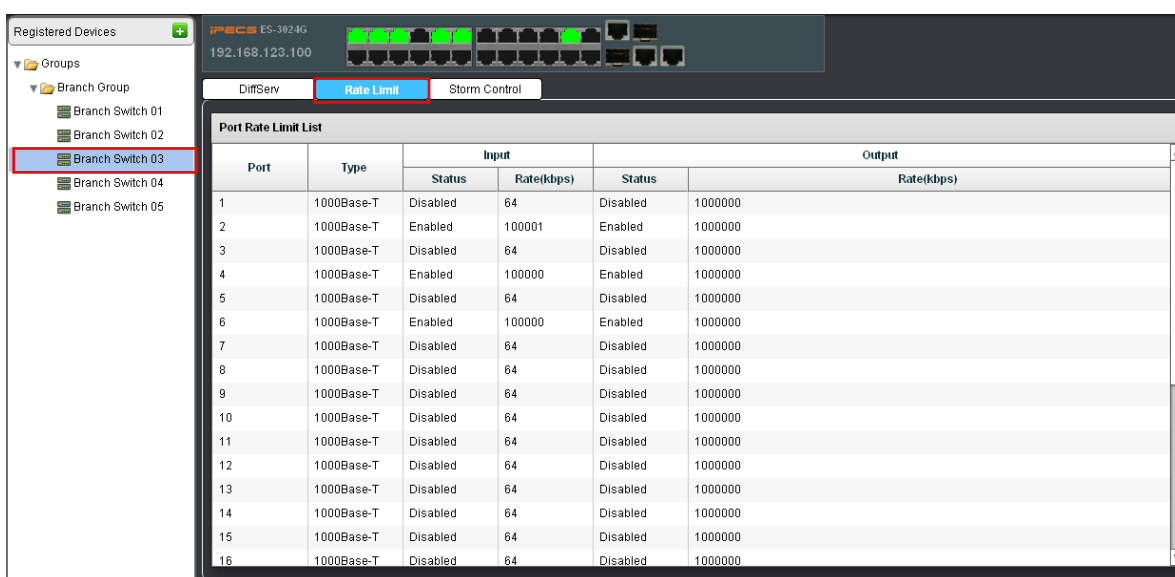


When a switch is selected in 'Registered Devices', the name, type and description of the class map configured in the switch are displayed. The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Class List	Class Name	Name of the class map.
	Type	Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
	Description	A brief description of the class map.

20.2 Rate Limit Information

‘Rate Limit Information’ shows the rate limit configuration information of a switch selected in ‘Registered Devices’. This page can be viewed by clicking [Rate Limit] tab under ‘Traffic Control’ sub-menu.

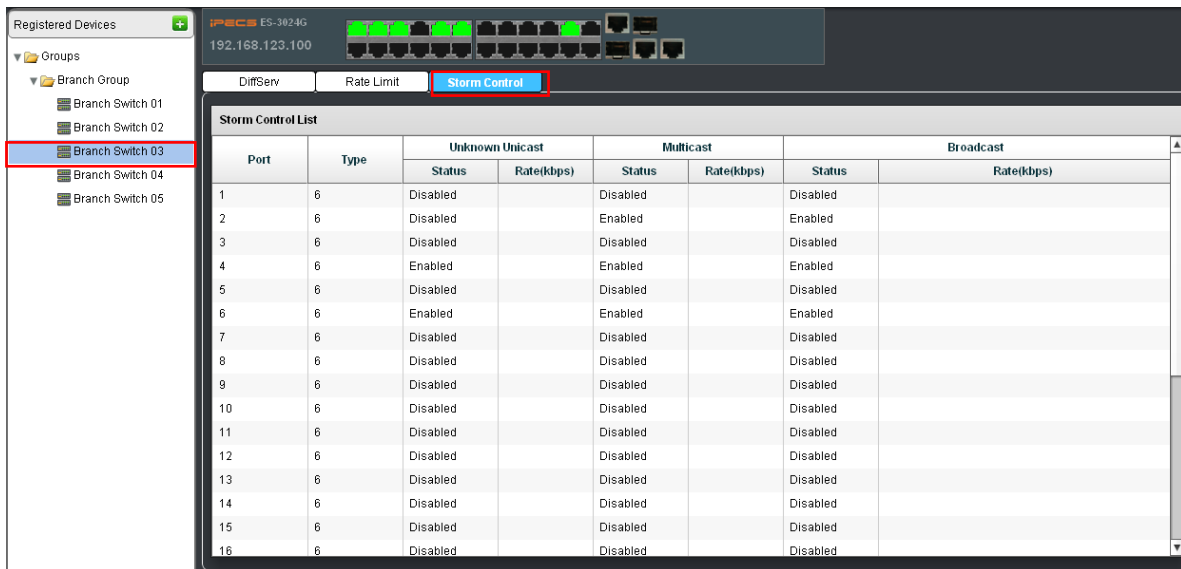


When a switch is selected in ‘Registered Devices’, rate limit configuration information for each port is displayed in ‘Port Rate Limit List’ such as port type, input & output status and rate. The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
Port Rate Limit List	Type	Indicates the port type. (e.g. 100Base-TX, 1000Base-T, or SFP)
	Input Status	Shows enable/disable status of the rate limit for input.
	Input Rate	Shows the rate limit level for input. (64 - 100,000 kbits per second for Fast Ethernet ports; 64 - 1,000,000 kbits per second for Gigabit Ethernet ports)
	Output Status	Shows enable/disable status of the rate limit for output.
	Output Rate	Shows the rate limit level for output. (64 - 100,000 kbits per second for Fast Ethernet ports; 64 - 1,000,000 kbits per second for Gigabit Ethernet ports)

20.3 Storm Control Information

‘Storm Control Information’ shows the storm control configuration information of a switch selected in ‘Registered Devices’. This page can be viewed by clicking [Storm Control] tab under ‘Traffic Control’ sub-menu.



When a switch is selected in ‘Registered Devices’, storm control configuration information for each port is displayed in ‘Storm Control List’ such as port type, status & rate of unknown unicast, multicast and broadcast. The types and meanings of the table fields are as follows.

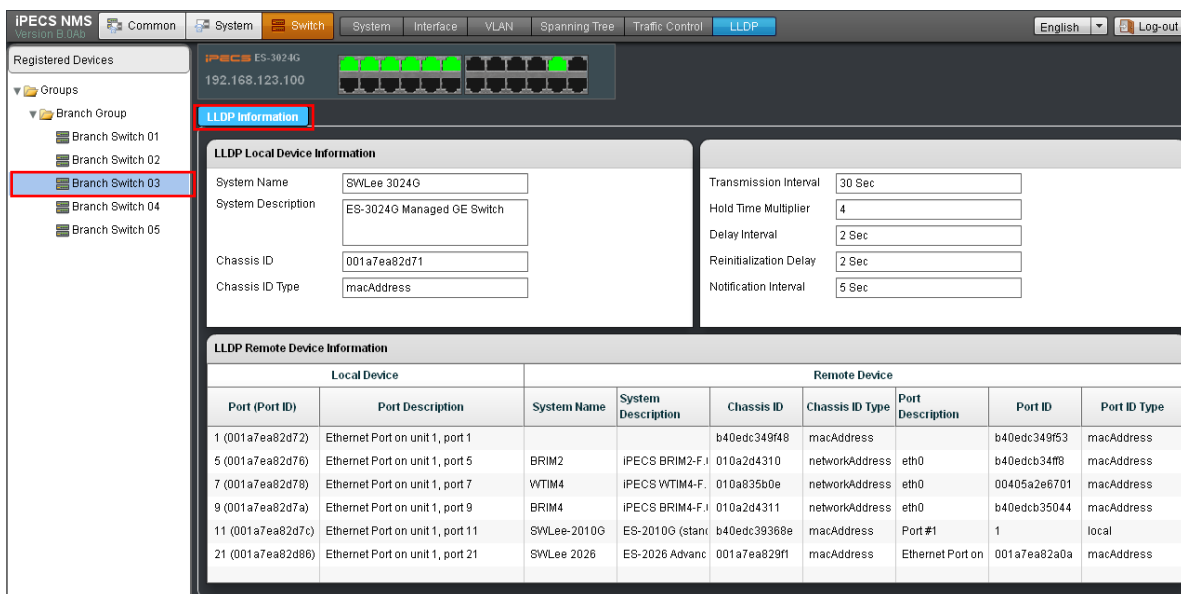
Table Name	Field Name	Description
Storm Control List	Type	Indicates interface type. (e.g. 100Base-TX, 1000Base-T, or SFP)
	Unknown Unicast Status	Specifies enable/disable status of storm control for unknown unicast traffic.
	Unknow Unicast Rate	Threshold level for unknown unicast as a rate; i.e., kilobits per second. (64-100000 Kbps for Fast Ethernet ports, 64-1000000 Kbps for Gigabit Ethernet ports)
	Multicast Status	Specifies enable/disable status of storm control for multicast traffic.
	Multicast Rate	Threshold level for multicast as a rate; i.e., kilobits per second. (64-100000 Kbps for Fast Ethernet ports, 64-1000000 Kbps for Gigabit Ethernet ports)
	Broadcast Status	Specifies enable/disable status of storm control for broadcast traffic.
	Broadcast Rate	Threshold level for broadcast as a rate; i.e., kilobits per second. (64-100000 Kbps for Fast Ethernet ports, 64-1000000 Kbps for Gigabit Ethernet ports)

21. Switch LLDP Information

‘Switch LLDP Information’ provides LLDP device information and configuration information of a registered switch. LLDP device information shows information for both LLDP local device information and LLDP remote device information. The page for this feature can be viewed by clicking [LLDP] sub-menu under ‘Switch’ menu.

21.1 LLDP Device Information

‘LLDP Device Information’ retrieves LLDP MIB information from a switch selected in ‘Registered Devices’, and provides ‘LLDP Local Device Information’, ‘LLDP Configuration Information’ and ‘LLDP Remote Device Information’. The page for this feature can be viewed by clicking [LLDP Information] tab under ‘LLDP’ sub-menu.



21.1.1 LLDP Local Device Information

‘LLDP Local Device Information’ shows LLDP information of the switch itself selected in ‘Registered Devices’ such as system name, system description, chassis ID and chassis ID type.

LLDP Local Device Information	
System Name	SWLee 3024G
System Description	ES-3024G Managed GE Switch
Chassis ID	001a7ea82d71
Chassis ID Type	macAddress

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
LLDP Local Device Information	System Name	A string that indicates the system’s administratively assigned name.
	System Description	A textual description of the network entity.
	Chassis ID	An octet string indicating the specific identifier for the particular chassis in this system.
	Chassis ID Type	Used to indicate the type of component being referenced by the chassis ID field. (e.g. chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local)

21.1.2 LLDP Configuration Information

‘LLDP Configuration Information’ shows the LLDP configuration information of a switch selected in ‘Registered Devices’ such as transmission interval, hold time multiplier, delay interval, reinitialization delay and notification interval.

LLDP Configuration Information	
Transmission Interval	30 Sec
Hold Time Multiplier	4
Delay Interval	2 Sec
Reinitialization Delay	2 Sec
Notification Interval	5 Sec

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
LLDP Configuration Information	Transmission Interval	Shows the periodic transmit interval for LLDP advertisements. (5-32768 seconds) This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤ 65536, and Transmission Interval ≥ (4 * Delay Interval)
	Hold Time Multiplier	Shows the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (2-10)

		<p>The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.</p> <p>TTL in seconds is based on the following rule: $(\text{Transmission Interval} * \text{Holdtime Multiplier}) \leq 65536$.</p>
	Delay Interval	<p>Shows a delay between the successive transmission of advertisements initiated by a change in local LLDP MIB variables. (1-8192 seconds)</p> <p>The transmit delay is used to prevent a series of successive LLDP transmissions during a short period of rapid changes in local LLDP MIB objects, and to increase the probability that multiple, rather than single changes, are reported in each transmission.</p> <p>This attribute must comply with the rule: $(4 * \text{Delay Interval}) \leq \text{Transmission Interval}$</p>
	Reinitialization Delay	<p>Shows the delay before attempting to reinitialize after LLDP ports are disabled or the link goes down. (1-10 seconds)</p> <p>When LLDP is re-initialized on a port, all information in the remote systems LLDP MIB associated with this port is deleted.</p>
	Notification Interval	<p>Shows the allowed interval for sending SNMP notifications about LLDP MIB changes. (5-3600 seconds)</p> <p>This parameter only applies to SNMP applications which use data stored in the LLDP MIB for network monitoring or management. Information about changes in LLDP neighbors that occur between SNMP notifications is not transmitted. Only state changes that exist at the time of a notification are included in the transmission.</p>

21.1.3 LLDP Remote Device Information

‘LLDP Remote Device Information’ shows the LLDP information of the remote devices connected to the switch selected in ‘Registered Devices such as system name & description, chassis ID, chassis ID type, port description, port ID and port ID type.

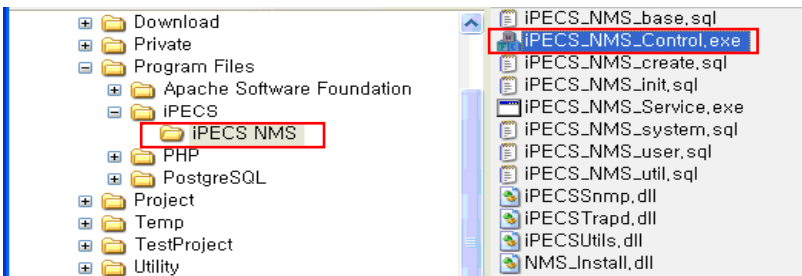
LLDP Remote Device Information								
Local Device		Remote Device						
Port (Port ID)	Port Description	System Name	System Description	Chassis ID	Chassis ID Type	Port Description	Port ID	Port ID Type
1 (001a7ea82d72)	Ethernet Port on unit 1, port 1			b40edc349f48	macAddress		b40edc349f53	macAddress
5 (001a7ea82d76)	Ethernet Port on unit 1, port 5	BRIM2	IPECS BRIM2-F.	010a2d4310	networkAddress	eth0	b40edcb34f8	macAddress
7 (001a7ea82d78)	Ethernet Port on unit 1, port 7	WTIM4	IPECS WTIM4-F.	010a835b0e	networkAddress	eth0	00405a2e6701	macAddress
9 (001a7ea82d7a)	Ethernet Port on unit 1, port 9	BRIM4	IPECS BRIM4-F.	010a2d4311	networkAddress	eth0	b40edcb35044	macAddress
11 (001a7ea82d7c)	Ethernet Port on unit 1, port 11	SWLee-2010G	ES-2010G (stanc	b40edc39368e	macAddress	Port #1	1	local
21 (001a7ea82d86)	Ethernet Port on unit 1, port 21	SWLee 2026	ES-2026 Advanc	001a7ea829f1	macAddress	Ethernet Port on	001a7ea82a0a	macAddress

The types and meanings of the table fields are as follows.

Table Name	Field Name	Description
LLDP Remote Device Information	Local Device	The local device (selected in 'Registered Devices') to which a remote LLDP-capable device is attached. This field includes port number, port ID and port description.
	System Name	A string that indicates the remote system's assigned name.
	System Description	A textual description of the remote system.
	Chassis ID	An octet string indicating the specific identifier for the particular chassis in the remote system.
	Chassis ID Type	Used to indicate the type of component being referenced by the chassis ID field. (e.g. chassisComponent, interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, local)
	Port Description	A string that indicates the port's description.
	Port ID	A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
	Port ID Type	Indicates the basis for the identifier that is listed in the Port ID field. (e.g. interfaceAlias, portComponent, macAddress, networkAddress, interfaceName, agentCircuitId, local)

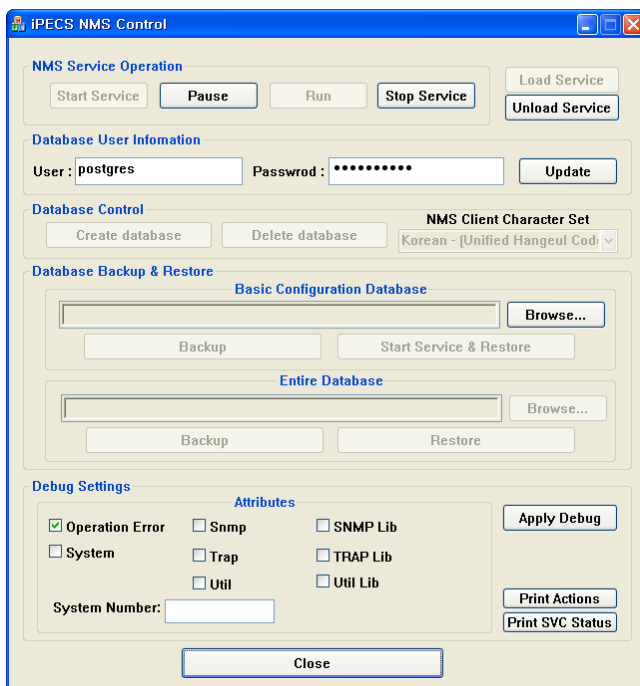
22. NMS Local Database Backup & Restore

The iPECS NMS Control program registers iPECS-NMS Service to the Windows Service list and manages the NMS database and program operation. Using the control program, the NMS database can be backed up to a user defined folder and, if needed later, the NMS database can be restored. The control program permits Basic Backup & Restore operation that backs up configuration information and log data, and Entire Backup & Restore includes all the information stored in the local database



The first step in the basic backup and restore operation is to find and open the iPECS-NMS Control program. The iPECS_MNS-Control.exe program should be located under the iPECS-NMS folder in the iPECS folder located in the Program Files directory.

When located, double click on the program to open the control window. (Or, from the Windows Start menu, select iPECS > iPECS NMS > Launch iPECS_NMS_Control.exe to execute it.)



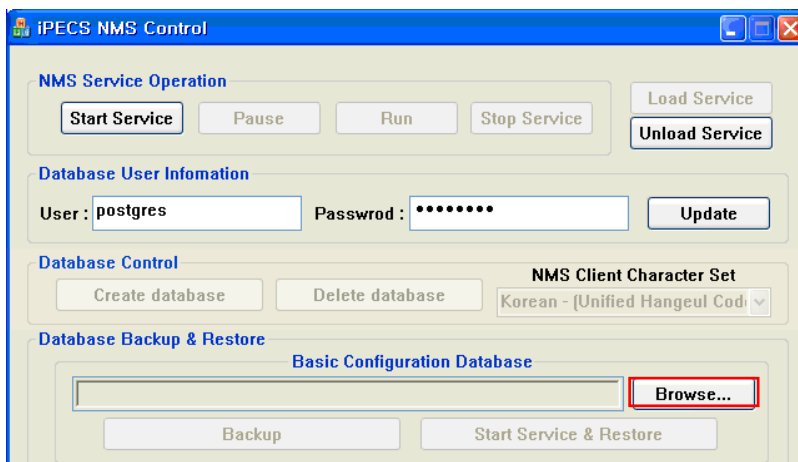
Backup & restore for both Basic and Entire Databases should be performed after the iPECS-NMS Service stops running, by clicking [Stop Service]. However, in case it is not possible to stop iPECS NMS Service (operational reason), Basic Backup can be performed while iPECS-NMS Service is operating, but the changed information during the backup process may not be applied to the database backup file.

22.1 Backup & Restore Basic Configuration Database

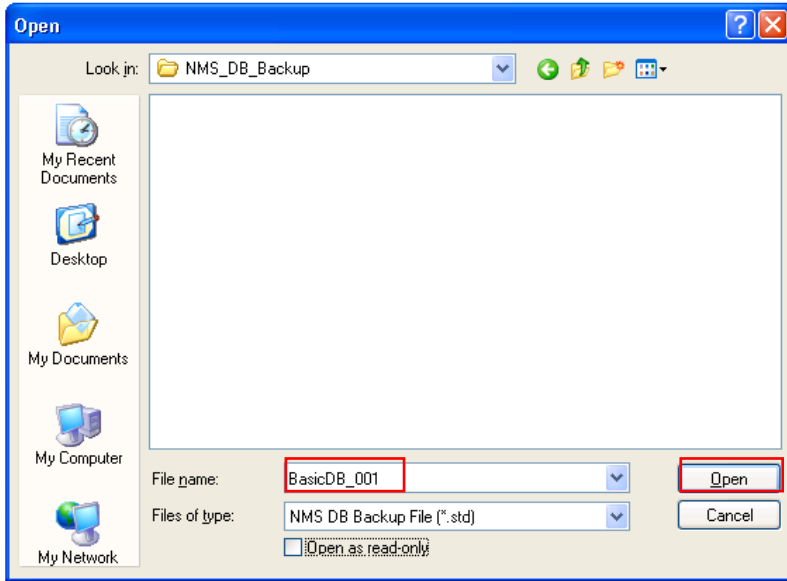
‘Basic Configuration Database’ means the configuration data set by administrator and log data. This includes the configuration information of ‘System Management’, ‘User Management’, ‘NMS Management’, and the log data of ‘Alarm/Fault Management’ and ‘Log Management’.

22.1.1 Basic Configuration Database Backup

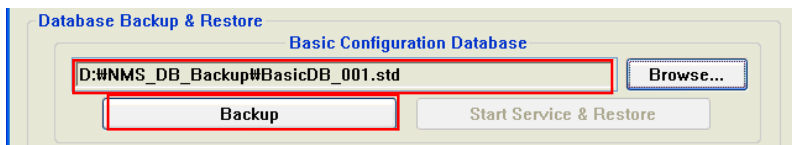
It is recommended and desirable to perform Basic Configuration Database backup after stopping ‘iPECS-NMS Service’ by clicking [Stop Service] button. However, if it is not possible to stop ‘iPECS-NMS Service’ for operational reason, the next step for configuring backup file name can be performed without stopping ‘iPECS-NMS Service’. (However, if the content of NMS local database is changed during the backup process, the changed information may not be applied to the database backup file.)



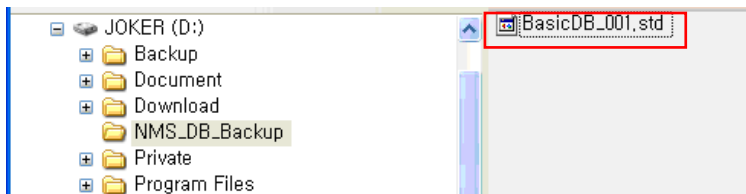
After ‘iPECS-NMS Service’ is stopped, [Start Service] button becomes enabled. Click [Browser...] button to open a file open window and enter a backup file name.



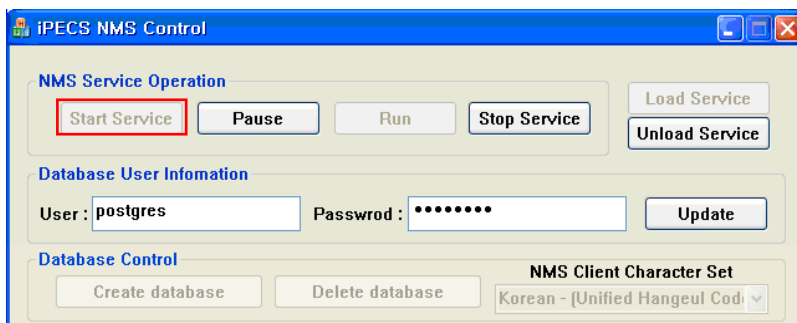
On file open window, browse to a target folder for storing the backup file, and then enter a file name in the 'File name' field. (The file extension of Basic Configuration Database backup file is 'std'.)



After a backup file name is entered, click [Backup] button to start database backup.



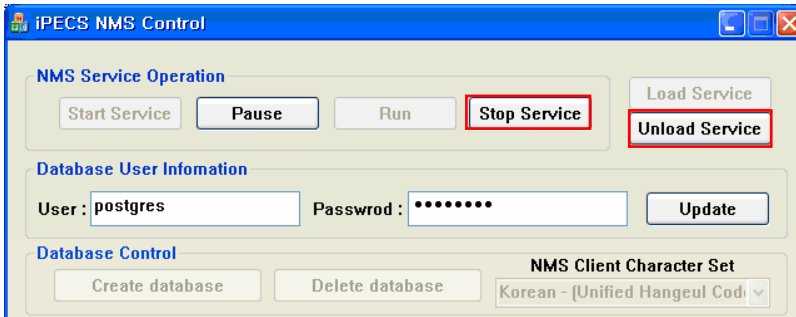
After the operation is finished, the backup file is created in the target folder.



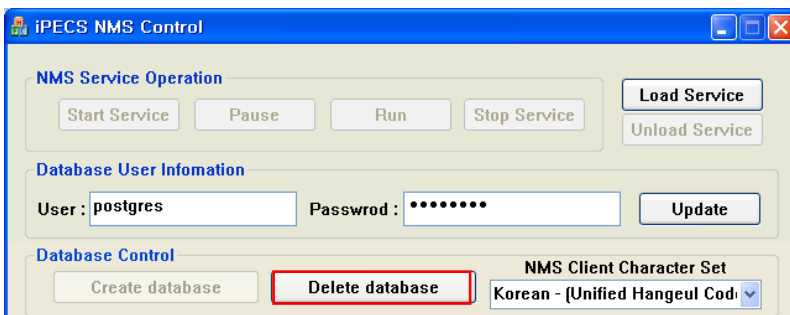
After checking the creation of the database backup file, click [Start Service] button to start 'iPECS-NMS Service' again.

22.1.2 Basic Configuration Database Restore

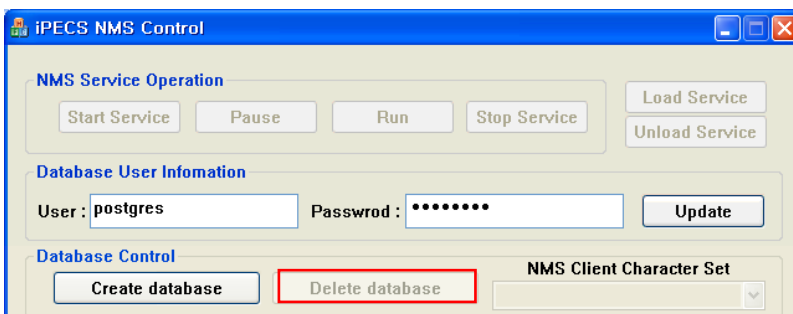
Before restoring Basic Configuration Database, delete current local database and create a new one, then database backup file can be restored on the newly created database.



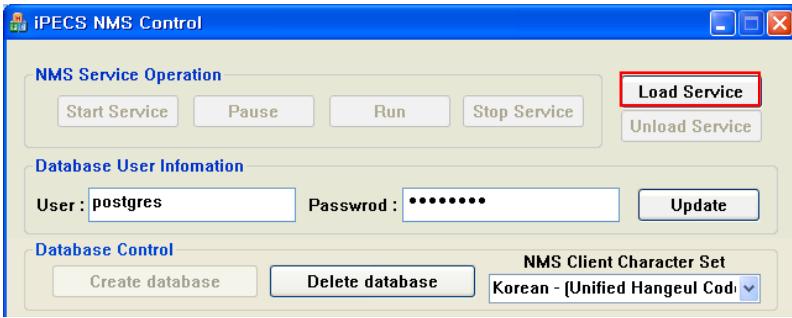
If 'iPECS-NMS Service' is in running status, click [Stop Service] button to stop running 'iPECS-NMS Service', and then click [Unload Service] button to unregister 'iPECS-NMS Service' from Windows Service list. (If [Unload Service] button is clicked before clicking [Stop Service] button, it will stop 'iPECS-NMS Service' first, and then unregister it from Windows Service list. So, this does the same thing as clicking [Stop Service] and [Unload Service] in sequence.)



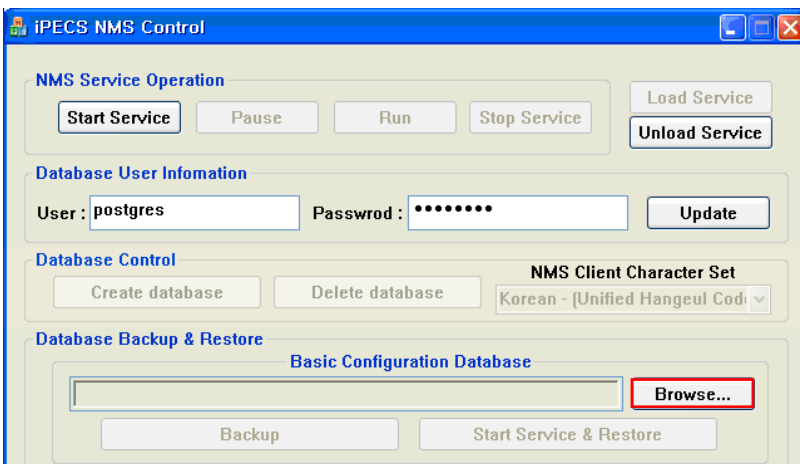
When [Delete Database] button becomes enabled after 'iPECS-NMS Service' is unregistered, click [Delete Database] button to delete existing NMS local database.



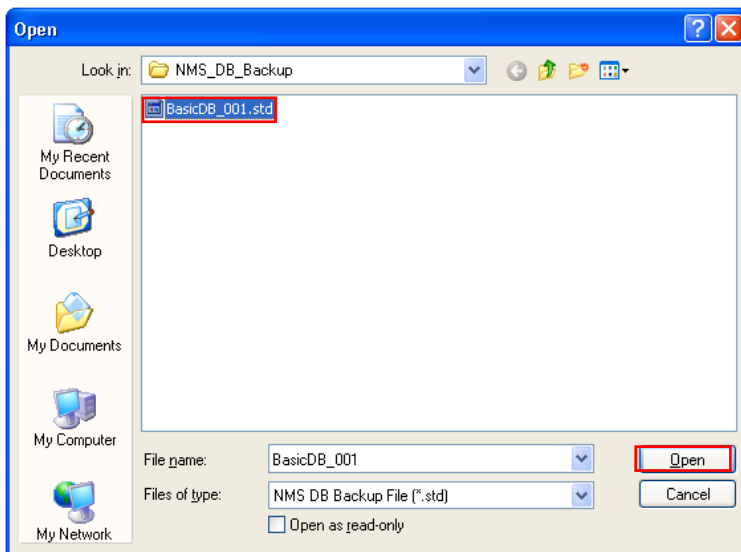
After the local database is deleted, click [Create Database] button to create a new local database.



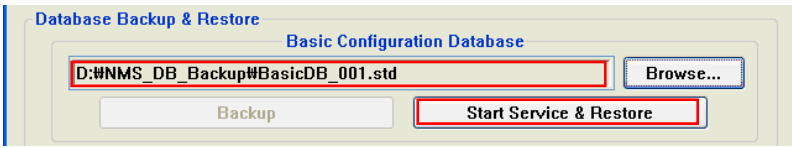
After the database creation is finished, [Load Service] button becomes enabled. Click [Load Service] button to register 'iPECS-NMS Service' to Windows Service list again.



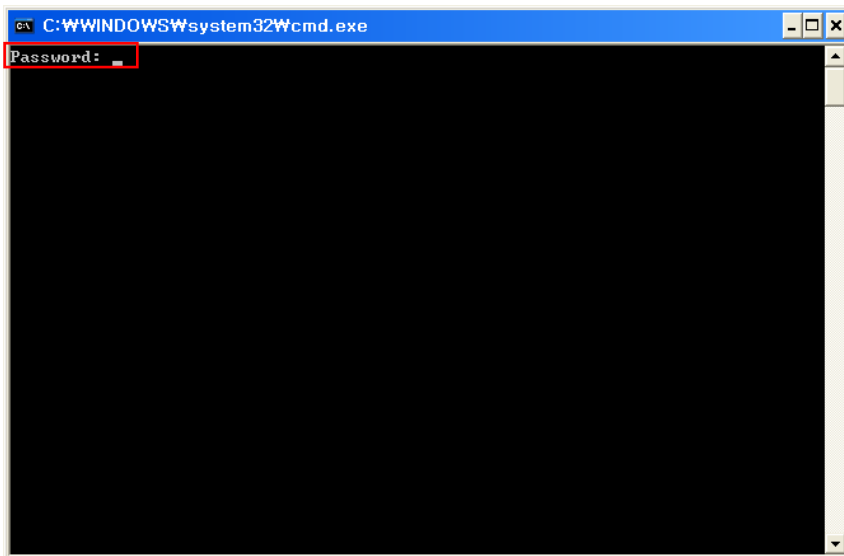
Now, it is ready to restore local database from previously saved backup file for 'Basic Configuration Database'. In order to select the target backup file, click [Browse...] button in 'Basic Configuration Database' group.



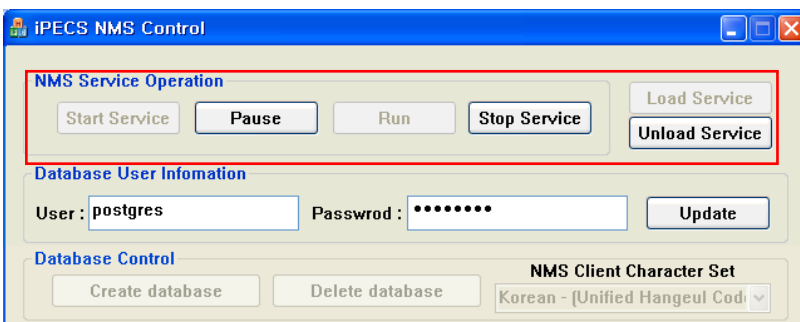
Select the target backup file, and click [Open] button.



After selecting a database backup file, click [Start Service & Restore] button to start restoring Basic Configuration Database. (Before the restoration, a DOS command prompt window that asks 'PostgreSQL' user account password appears. So, check the account password configured during 'PostgreSQL' installation procedure before clicking [Start Service & Restore] button.)



If a DOS command prompt window appears, enter the database account password and press 'Enter' key. (This password is actually same as the value of 'Password' field in 'Database User Information' group.)



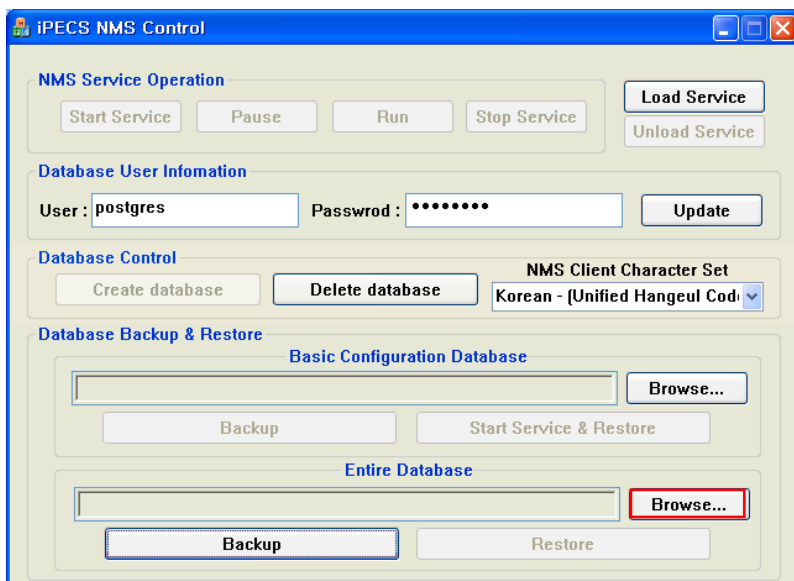
After finishing database restoration, 'iPECS-NMS Service' gets into running status. Click [Close] button to close 'iPECS-NMS Control' program.

22.2 Backup & Restore Entire Database

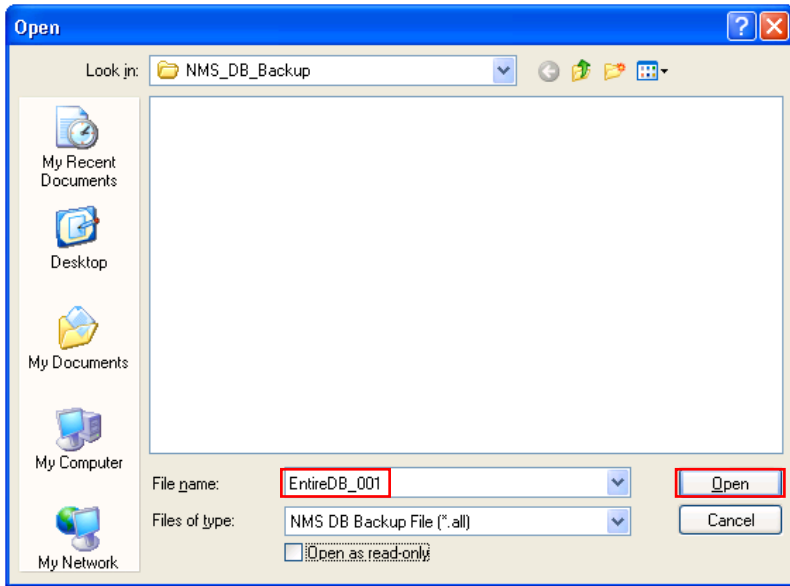
'Entire Database' means all the data stored in local database, and it includes all the detailed information received & stored while communicating with MFIM in addition to the information of Basic Configuration Database.

22.2.1 Entire Database Backup

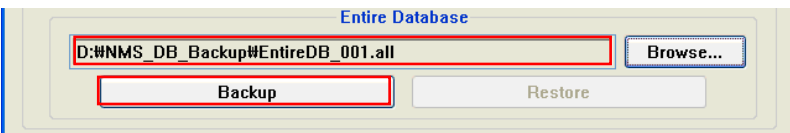
Before starting Entire Database backup, 'iPECS-NMS Service' should be stopped and then unregistered from Windows Service list. Therefore, if 'iPECS-NMS Service' is in running status, click [Stop Service] button to stop running 'iPECS-NMS Service' and then click [Unload Service] button to unregister 'iPECS-NMS Service' from Windows Service list. (If [Unload Service] button is clicked before clicking [Stop Service] button, it will stop 'iPECS-NMS Service' first, and then unregister it from Windows Service list. So, this does the same thing as clicking [Stop Service] and [Unload Service] in sequence.)



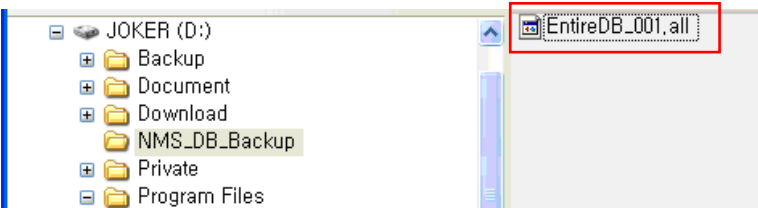
After 'iPECS-NMS Service' is stopped and unregistered, [Browse...] button in 'Entire Database' group becomes enabled. Click [Browser...] button to open a file open window and enter a backup file name.



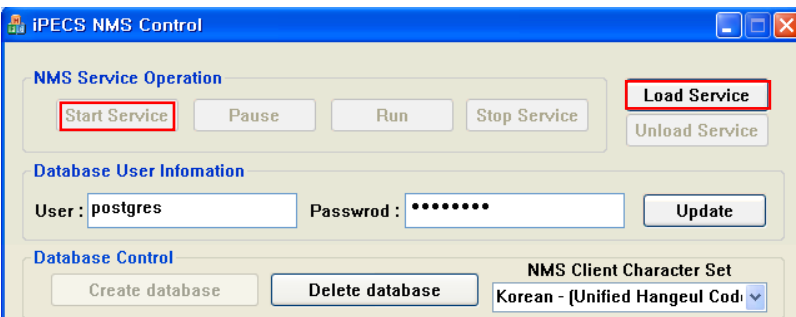
On file open window, browse to a target folder for storing the backup file, and then enter a file name in the 'File name' field. (The file extension of Entire Database backup file is 'all'.)



After a backup file name is configured, click [Backup] button to start database backup.



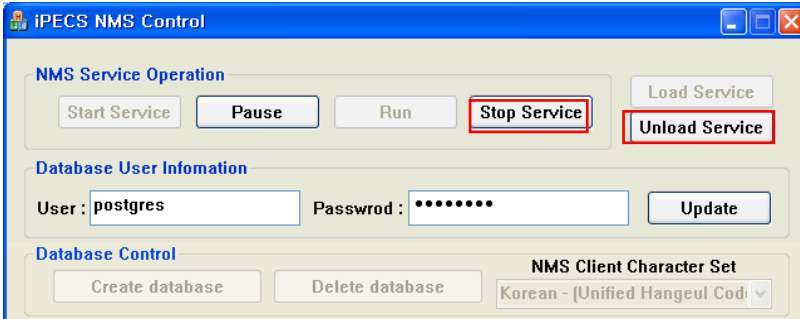
After the operation is finished, the backup file is created in the target folder.



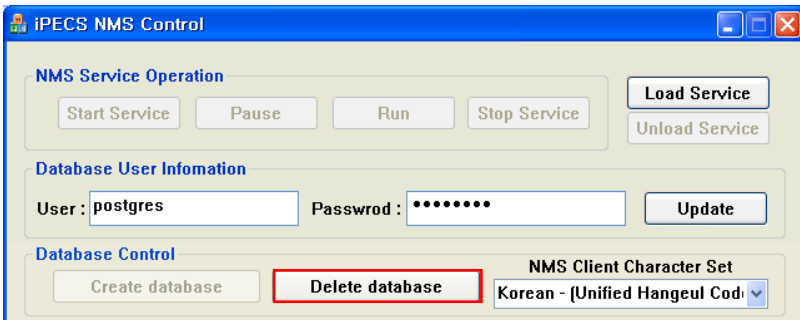
After checking the creation of the database backup file, click [Load Service] button to register 'iPECS-NMS Service' to Windows Service list, and then [Start Service] button to start 'iPECS-NMS Service' again.

22.2.1 Entire Database Restore

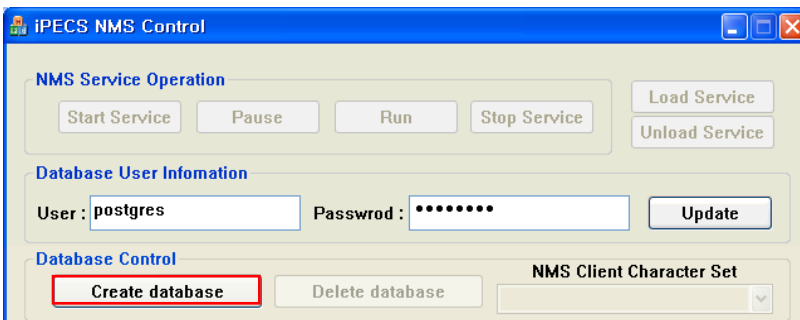
Before restoring Entire Database, delete current local database and create a new one. Then, database backup file can be restored on newly created database.



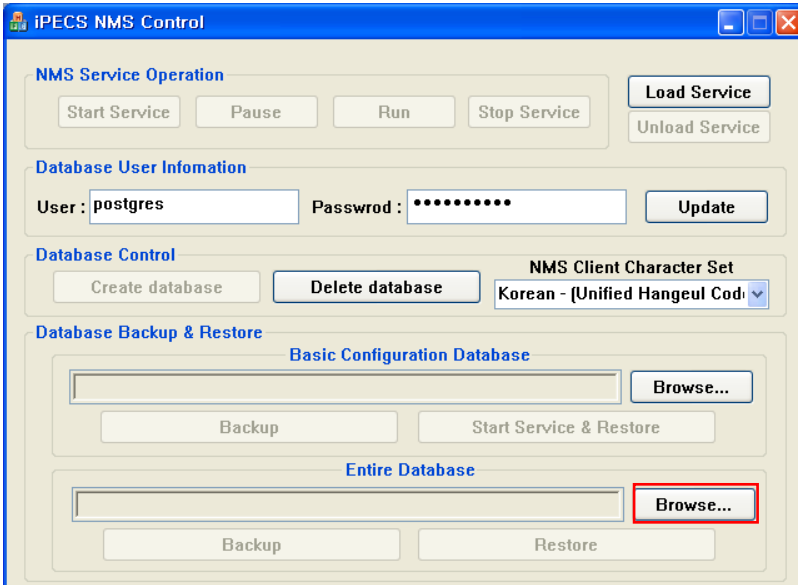
If 'iPECS-NMS Service' is in running status, click [Stop Service] button to stop running 'iPECS-NMS Service', and then click [Unload Service] button to unregister 'iPECS-NMS Service' from Windows Service list. (If [Unload Service] button is clicked before clicking [Stop Service] button, it will stop 'iPECS-NMS Service' first, and then unregister it from Windows Service list. So, this does the same thing as clicking [Stop Service] and [Unload Service] in sequence.)



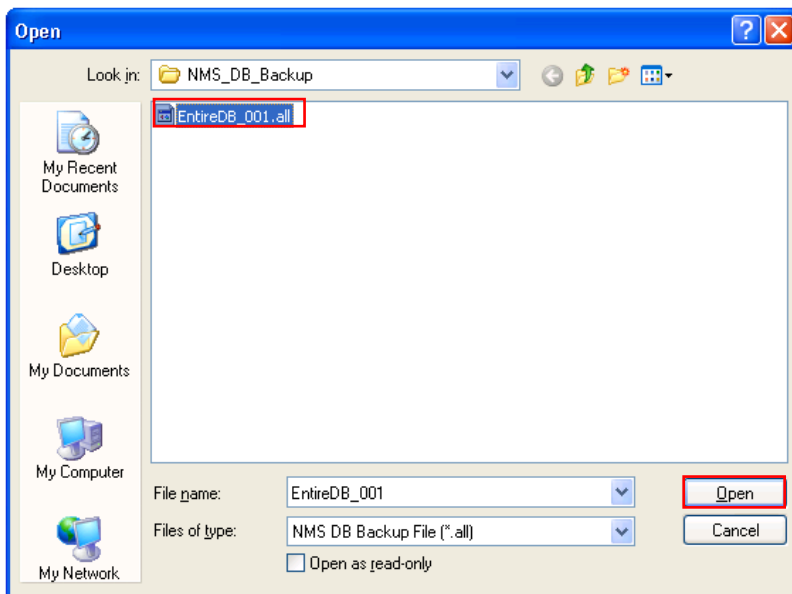
When [Delete Database] button becomes enabled after 'iPECS-NMS Service' is unregistered, click [Delete Database] button to delete existing NMS local database.



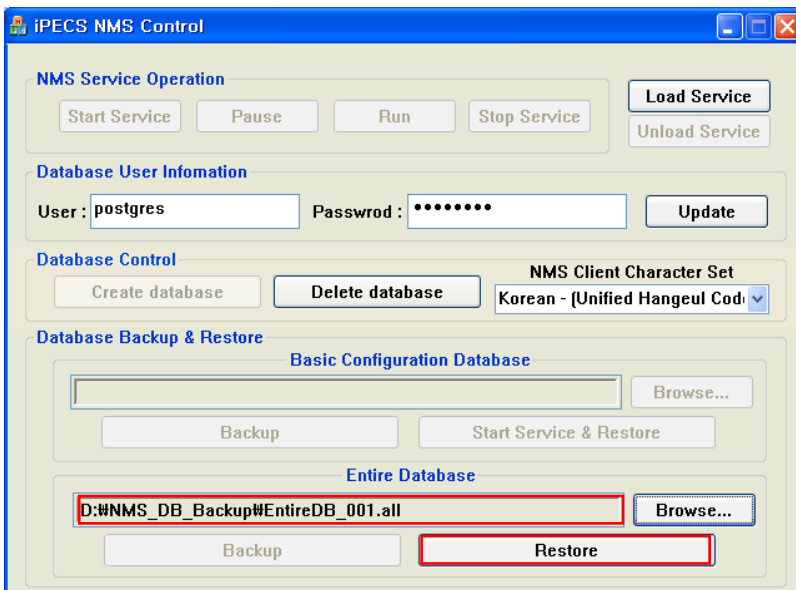
After the local database is deleted, click [Create Database] button to create a new local database.



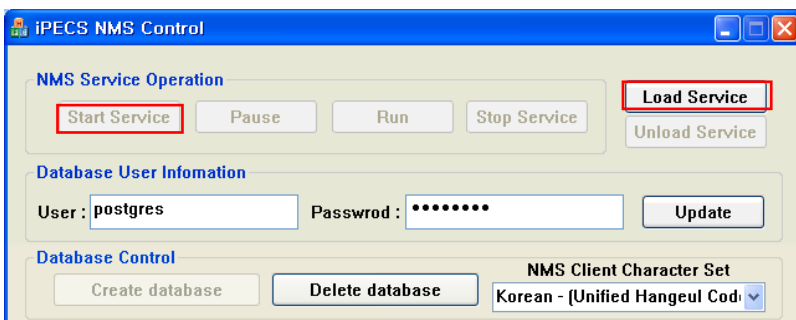
Now, it is ready to restore local database from previously saved backup file for 'Entire Database'. In order to select the target backup file, click [Browse...] button in 'Entire Database' group.



Select the target backup file, and click [Open] button.



After selecting a database backup file, click [Restore] button to start restoring Entire Database.



After finishing database restoration, click [Load Service] button to register 'iPECS-NMS Service' to Windows Service list, and then [Start Service] button to start 'iPECS-NMS Service' again.

The contents of this document are subject to revision without notice due to continued progress in methodology design and manufacturing. Ericsson-LG Enterprise shall have no liability for any error or damage of any kind resulting from the use of this document.

Posted In Korea

www.ericssonlg-enterprise.com
© Ericsson-LG Enterprise Co., Ltd. 2008