Baicells CloudCore 7.3

Configuration & Network Administration Guide

CloudCore System – Version 7.3
CloudCore OMC – Version 7.3.5
CloudCore BOSS – Version 7.3.5

March 2022

Version 2.02

About This Document

This document describes the mainstream applications used for configuring and administering the Baicells network components and subscriber information. The scope includes the Baicells System module, CloudCore Operations Management Console (OMC), and Business and Operation Support System (BOSS) modules. The target audience is network administrators who are responsible for managing the operator's CloudCore account, the eNodeBs (eNBs), eNBs that support Citizens Broadband Radio Service (CBRS) which needs integration with Spectrum Access System (SAS) for spectrum access, Customer Premise Equipment (CPEs), and the subscribers and service plans.

New in This Release

The following updates are provided in this release:

- Updated for CloudCore version 7.3 features, improvements, and GUI changes.

Related Documents

Understanding how the Baicells technical documentation is structured will help you know where to find the information you need. Below are some notes about where to find related configuration information:

- This guide covers only the Baicells CloudCore apps. Versions before CloudCore v6.2 and document v1.03 published December 2020 also covered the equipment GUIs. You can now find those GUIs covered in the *eNodeB Configuration Guide* and the *CPE Configuration Guide*, respectively.
- Information specific to two-carrier eNBs such as Nova436Q, Nova246, and Neutrino430, is in the *Carrier Aggregation & Dual Carrier (Split Mode) Configuration Guide*.
- For eNB HaloB operation, refer to the *HaloB User Guide*.
- How to configure eNBs to operate in CBRS SAS mode can be found in the *SAS Deployment Guide*.

Additionally, terms used in this document or related to LTE are listed in alphabetical order and described in *Acronyms & Abbreviations*. Please refer to the Baicells website (Baicells.com > Resources > *Documents*) for all installation guides, user manuals, and other customer documents.

Copyright Notice

Disclaimer

All products, services, and features bought from Baicells Technologies are subject to the constraints of the company's business contract and terms. All or part of the products, services, or features described in this document might not be your specific Baicells network. Unless stated in the contract, Baicells Technologies does not make any explicit or default statement or guarantee about the contents of this document.

Unless stated otherwise, this document serves only as a user guide, and all descriptions/information/suggestions mean no guarantee, neither explicit nor implicit.

The information in this document is subject to change at any time without notice. For more information, please consult with a Baicells technical engineer or the support team. Refer to the “Contact Us” section.

Revision Record

Date	Version	Description	SMEs/Contributors	Authors/Editors
14-Mar-2022	V2.02	Updated for CloudCore version 7.3 features, improvements, and GUI changes, and incorporated SME and peer review feedback	Yunfeng Jiang, Blake Volk	Angelin Selvaraj Jocelyn Watson
1-Nov-2021	V2.01	Updated for CloudCore version 7.1 features, improvements, and GUI changes, and incorporated SME and peer review feedback	Yunfeng Jiang, Warren Lai, Seng Tang, Blake Volk	Jocelyn Watson Catherine Philley Kathy Clark
17-Jun-2021	V2.0	Updated for CloudCore version 7.0 features, improvements, and GUI changes, and incorporated SME and peer review feedback	Nitisha Potti, Yunfeng Jiang, Kathy Clark, Jesse Raasch, Wu Junfeng	Jocelyn Watson Sharon Redfoot
7-Mar-2021	V1.04	Updated to CC 6.3 and refreshed with SME feedback	Nitisha Potti, Wu Junfeng	Jocelyn Watson Sharon Redfoot
11-Dec-2020	V1.03	Added SME feedback	Yunfeng Jiang	Jocelyn Watson Sharon Redfoot
18-Nov-2020	V1.02	Updated content to CC OMC v6.2.8, BOSS v6.2.3	Nitisha Potti, Wu Junfeng, Yang Yanan	Jocelyn Watson Sharon Redfoot
8-Sep-2020	V1.01	This is a new document for Baicells CloudCore System/OMC/BOSS releases: • CloudCore System version: 6.1.3 • CloudCore OMC version: 6.0.5.1 • CloudCore BOSS version: 6.1.3	Nitisha Potti, Yang Yanan	Jocelyn Watson Sharon Redfoot

Resources

- **Documentation** - Baicells product data sheets, technical manuals, and a list of acronyms and abbreviations can be found at baicells.com > Resources > *Documents*.
- **Support** - Open a support ticket, process an RMA, and the Support Forum are at Baicells.com > *Support*

Contact Us

Baicells Technologies	
Address	5700 Tennyson Pkwy, #300, Plano, TX 75024, USA
Phone	+1-888-502-5585
Email	*sales_na@baicells.com* or *support_na@baicells.com*
Website	*www.baicells.com*

Table of Contents

1 INTRODUCTION 1
2 CLOUDCORE 2
2.1 CLIENT COMPUTER REQUIREMENTS 2
2.2 GETTING STARTED 2
2.2.1 Sign up for CloudCore Account 2
2.2.2 CloudCore Users 4
2.2.3 CloudCore GUI Layout 5
2.2.4 GUI Icons 6
2.2.5 CloudCore Software Structure 7
2.3 SYSTEM 8
2.3.1 Billing Menu 8
2.3.2 Invoice 11
2.3.3 System 12
2.4 OMC 21
2.4.1 Dashboard Menu 21
2.4.2 eNB Menu 27
2.4.3 CPE Menu 86
2.4.4 Alarm Menu 116
2.4.5 Performance Menu 123
2.4.6 Advance Menu 132
2.4.7 System Menu 134
2.5 BOSS 139
2.5.1 Overview 139
2.5.2 Subscription Menu 139
2.5.3 Network Menu 149
2.5.4 System Menu 158

List of Figures

FIGURE 1-1: STANDARD BAICELLS LTE NETWORK 1
FIGURE 2-1: CLOUDCORE WEB PAGE 3
FIGURE 2-2: SIGN UP FIELDS 3
FIGURE 2-3: DEFAULT CLOUD USER GROUPS 4
FIGURE 2-4: DEFAULT OMC AND BOSS USER GROUPS 4
FIGURE 2-5: CLOUDCORE MODULES 5
FIGURE 2-6: CLOUDKEY 5
FIGURE 2-7: WELCOME DROP-DOWN MENU 5
FIGURE 2-8: HOME PAGE (OMC DASHBOARD) 6
FIGURE 2-9: CLOUDCORE SOFTWARE STRUCTURE 7
FIGURE 2-10: SYSTEM MENU 8
FIGURE 2-11: BILLING MENU 8
FIGURE 2-12: ADD CREDIT CARD 9
FIGURE 2-13: UPCOMING INVOICE 9
FIGURE 2-14: STRIPE PAYMENT 10
FIGURE 2-15: OVERDUE INVOICE EXAMPLE 10
FIGURE 2-16: INVOICE STATISTIC[S] TAB 11
FIGURE 2-17: LIST TAB 12
FIGURE 2-18: SYSTEM MENU 12
FIGURE 2-19: ADMIN USER 13
FIGURE 2-20: ROLE SET 14
FIGURE 2-21: USER GROUP 14
FIGURE 2-22: ADD USER GROUP 15
FIGURE 2-23: USER TAB 16
FIGURE 2-24: RESET PASSWORD 16
FIGURE 2-25: ADD ADMINISTRATIVE USER 17
FIGURE 2-26: ADMIN USER SETUP EXAMPLE 18
FIGURE 2-27: LOGS 18
FIGURE 2-28: SECURITY SETTING 20
FIGURE 2-29: OMC MENU 21
FIGURE 2-30: DASHBOARD 22
FIGURE 2-31: ALARM ICONS 23
FIGURE 2-32: QUICK LINKS 23
FIGURE 2-33: ACTIVE ALARM PANE 24
FIGURE 2-34: ACTIVE ALARM PANE - PIE CHART DISPLAY OPTIONS 25
FIGURE 2-35: ACTIVE ALARM PANE - 24-HOUR TIME PERIOD 26
FIGURE 2-36: ACTIVE ALARM PANE - FULL CALENDAR MONTH 26
FIGURE 2-37: DASHBOARD STATISTICS 27
FIGURE 2-38: ENB MENU 28
FIGURE 2-39: ENB > MONITOR - TABLE TAB GENERAL LAYOUT 28
FIGURE 2-40: ENB > MONITOR - MAP TAB GENERAL LAYOUT 29

FIGURE 2-41: TABLE TAB FIELDS 29
FIGURE 2-42: ENB > MONITOR TABLE TAB 30
FIGURE 2-43: DISPLAY SETTINGS 31
FIGURE 2-44: OPERATIONS 37
FIGURE 2-45: INFORMATION (LEFT SIDE AND MIDDLE) 39
FIGURE 2-46: GRAPHS (RIGHT SIDE) 40
FIGURE 2-47: BASIC TAB 41
FIGURE 2-48: NETWORK TAB 42
FIGURE 2-49: LTE TAB 43
FIGURE 2-50: ENB TAB 43
FIGURE 2-51: QUICK SETTINGS TAB 44
FIGURE 2-52: NETWORK TAB 44
FIGURE 2-53 LTE TAB (1 OF 4) 45
FIGURE 2-54: LTE TAB (2 OF 4) 46
FIGURE 2-55: LTE TAB (3 OF 4) 47
FIGURE 2-56: LTE TAB (4 OF 4) 47
FIGURE 2-57: BTS TAB (1 OF 3) 48
FIGURE 2-58: BTS TAB (2 OF 3) 48
FIGURE 2-59: BTS TAB (3 OF 3) 48
FIGURE 2-60: REBOOT 49
FIGURE 2-61: RESET CONFIGURATION 49
FIGURE 2-62: LOGS 50
FIGURE 2-63: ACTIONS 51
FIGURE 2-64: MULTI-DEVICE OPERATIONS 51
FIGURE 2-65: MAP TAB VIEW 52
FIGURE 2-66: OPTIONAL INFORMATION VIEW 52
FIGURE 2-67: INFORMATION PANE 53
FIGURE 2-68: MAP DISPLAY FILTERS 53
FIGURE 2-69: DISPLAY TAB 54
FIGURE 2-70: MAINTENANCE 55
FIGURE 2-71: MML MENU 55
FIGURE 2-72: MML TAB 56
FIGURE 2-73: MML SCRIPT 58
FIGURE 2-74: ENB CONFIGURATION 59
FIGURE 2-75: IMPORT 59
FIGURE 2-76: EXPORT 60
FIGURE 2-77: CHANGE ENB PASSWORD 61
FIGURE 2-78: TASK LIST OPERATIONS 62
FIGURE 2-79: DEVICES TAB 62
FIGURE 2-80: REBOOT 62
FIGURE 2-81: CREATE A REBOOT TASK 64
FIGURE 2-82: RECURRING REBOOT 65
FIGURE 2-83: ADVANCED QUERY SEARCH 65

FIGURE 2-84: CREATING RECURRING REBOOT TASK 66
FIGURE 2-85: RECURRING REBOOT DEVICES LIST 67
FIGURE 2-86: LOGS 67
FIGURE 2-87: NEW DEVICE LOG TASK 68
FIGURE 2-88: EXECUTE TYPE 69
FIGURE 2-89: NEW ALARM LOG TASK 70
FIGURE 2-90: RESULTS OF THE ALARM LOG 70
FIGURE 2-91: EXCEPTION LOGS 71
FIGURE 2-92: EVENT LOGS 72
FIGURE 2-93: ENB > UPGRADE LANDING PAGE 73
FIGURE 2-94: ENB > UPGRADE > UPGRADE & ROLLBACK 73
FIGURE 2-95: ENB > UPGRADE > FILE 74
FIGURE 2-96: TASK LIST 75
FIGURE 2-97: DEVICE LIST 76
FIGURE 2-98: UPGRADE FROM THE OMC UPGRADE MESSAGES 77
FIGURE 2-99: INVENTORY 78
FIGURE 2-100: DEVICE 78
FIGURE 2-101: ADD GROUP 79
FIGURE 2-102: REGISTER ENB IN OMC 80
FIGURE 2-103: IMPORT ENB INFORMATION 81
FIGURE 2-104: BASIC LICENSE 82
FIGURE 2-105: BACKUP & RESTORE LANDING PAGE 83
FIGURE 2-106: ENB DEVICES 83
FIGURE 2-107: IMPORT FILE 84
FIGURE 2-108: TASK LIST 85
FIGURE 2-109: DEVICE LIST 85
FIGURE 2-110: CPE MENU 86
FIGURE 2-111: CPE > MONITOR GENERAL LAYOUT 86
FIGURE 2-112: CPE MONITOR – TABLE TAB (1 OF 3) 87
FIGURE 2-113: CPE MONITOR – TABLE TAB (2 OF 3) 88
FIGURE 2-114: CPE MONITOR – TABLE TAB (3 OF 3) 88
FIGURE 2-115: CPE MONITOR MAP TAB 89
FIGURE 2-116: CPE OPERATIONS 92
FIGURE 2-117: CPE MONITOR INFORMATION (LEFT SIDE) 93
FIGURE 2-118: CPE MONITOR INFORMATION – GRAPHS (RIGHT SIDE, 1 OF 2) 94
FIGURE 2-119: CPE MONITOR INFORMATION – GRAPHS (RIGHT SIDE, 2 OF 2) 94
FIGURE 2-120: DIAGNOSTIC 95
FIGURE 2-121: DOWNLOADTEST 95
FIGURE 2-122: UPLOADTEST 96
FIGURE 2-123: PINGTEST 96
FIGURE 2-124: TRACEROUTE 97
FIGURE 2-125: SETTINGS 98
FIGURE 2-126: REBOOT 99

FIGURE 2-127: CHANGE PASSWORD 99
FIGURE 2-128: DISPLAY 100
FIGURE 2-129: CPE MONITOR ADD A DEVICE 101
FIGURE 2-130: MAINTENANCE 101
FIGURE 2-131: REBOOT 102
FIGURE 2-132: NEW TASK 102
FIGURE 2-133: OPERATIONS 103
FIGURE 2-134: CONFIGURE 103
FIGURE 2-135: TASK AND DEVICE LIST 104
FIGURE 2-136: PCI LOCK 105
FIGURE 2-137: NEW PCI LOCK TASK (ENB TAB) 106
FIGURE 2-138: NEW PCI LOCK TASK (CPE TAB) 107
FIGURE 2-139: ADVANCED QUERY FIELDS 108
FIGURE 2-140: CHANGE PASSWORD 108
FIGURE 2-141: NEW CHANGE PASSWORD TASK 109
FIGURE 2-142: DEVICE LOG 110
FIGURE 2-143: NEW DEVICE LOG TASK 111
FIGURE 2-144: ACCESS LOG 111
FIGURE 2-145: CPE > UPGRADE 112
FIGURE 2-146: NEW CPE UPGRADE TASK 113
FIGURE 2-147: DEVICE 114
FIGURE 2-148: ADD CPE DEVICE GROUP, ADD CPE(S) 115
FIGURE 2-149: QUICK MOVE TO DEVICE GROUP 115
FIGURE 2-150: ALARM MENU 116
FIGURE 2-151: ALARM MENU - GENERAL LAYOUT 116
FIGURE 2-152: VIEW TAB 117
FIGURE 2-153: OPERATIONS 117
FIGURE 2-154: ALARM DETAIL 117
FIGURE 2-155: CHART VIEW OF TOP 10 ALARMS (BY DEVICE) 118
FIGURE 2-156: CHART VIEW OF TOP 10 ALARMS (BY DEVICE GROUP) 119
FIGURE 2-157: CHART VIEW OF TOP 10 ALARMS (BY ALARM ID) 120
FIGURE 2-158: ADD NEW ALARM TEMPLATE 121
FIGURE 2-159: ALARM FILTER 121
FIGURE 2-160: ADD NEW ALARM FILTER TEMPLATE 122
FIGURE 2-161: OPERATIONS 123
FIGURE 2-162: LIBRARY 123
FIGURE 2-163: PERFORMANCE MENU 124
FIGURE 2-164: KPI VIEW TABLE FORMAT 124
FIGURE 2-165: KPI VIEW CHART FORMAT 125
FIGURE 2-166: FILTER KPI VIEW 125
FIGURE 2-167: ADD NEW KPI TEMPLATE 126
FIGURE 2-168: KPI MEAS 127
FIGURE 2-169: DOWNLOAD XML FILES 128

FIGURE 2-170: KPI MGMT STANDARD LTE KPI EXAMPLE 129
FIGURE 2-171: KPI MGMT, CUSTOM KPI EXAMPLE 130
FIGURE 2-172: NEW KPI ALARM TEMPLATE 131
FIGURE 2-173: RESULTS 132
FIGURE 2-174: ADVANCE MENU 132
FIGURE 2-175: PLUG-AND-PLAY ENB DISPLAY 133
FIGURE 2-176: NEW PLUG AND PLAY TASK 134
FIGURE 2-177: OMC SYSTEM MENU 134
FIGURE 2-178: RESOURCES 135
FIGURE 2-179: SETTINGS 136
FIGURE 2-180: OMC OPERATION LOGS 136
FIGURE 2-181: BACKUP 137
FIGURE 2-182: RESTORE 138
FIGURE 2-183: LICENSE 138
FIGURE 2-184: UPDATE LICENSE 139
FIGURE 2-185: BOSS MENU 139
FIGURE 2-186: ADVANCED QUERY FILTER 140
FIGURE 2-187: SUBSCRIPTION MENU 140
FIGURE 2-188: OPERATIONS DETAIL 141
FIGURE 2-189: NEW SUBSCRIPTION (1 OF 2) 143
FIGURE 2-190: NEW SUBSCRIPTION (2 OF 2) 143
FIGURE 2-191 ADD SUBSCRIPTION BY COPYING AND MODIFYING AN EXISTING SUBSCRIPTION ..... **ERROR! BOOKMARK NOT DEFINED.**
FIGURE 2-192: IMPORT USER 145
FIGURE 2-193: RECORDS 146
FIGURE 2-194: EXPORT 146
FIGURE 2-195: BULK CHANGES 147
FIGURE 2-196: CHANGE CUSTOMER 148
FIGURE 2-197: BOSS NETWORK MENU 149
FIGURE 2-198: SIM CARD 149
FIGURE 2-199: SIM CARD LIST 150
FIGURE 2-200: SIM CARD IMPORT 150
FIGURE 2-201: IMPORT BY ACTIVATION CODE 151
FIGURE 2-202: ACTIVATION CODE EXAMPLE 151
FIGURE 2-203: IMPORT BY FILE 152
FIGURE 2-204: SIM CARDS 152
FIGURE 2-205: EXPORT IMSI FILE 153
FIGURE 2-206: SERVICE PLANS 153
FIGURE 2-207: NEW SERVICE PLAN 155
FIGURE 2-208: FLOW PACKAGE 156
FIGURE 2-209: ROAMING CONFIGURATION/VIEW ROAMING OPERATOR 157
FIGURE 2-210: ADD OPERATOR TO ROAM 157
FIGURE 2-211: SYSTEM MENU 158
FIGURE 2-212: LOGS 158

List of Tables

TABLE 2-1: CLIENT REQUIREMENTS 2
TABLE 2-2: ICONS 6
TABLE 2-3: ENB > MONITOR FIELDS 31
TABLE 2-4: ENB > MONITOR GRAPHS 35
TABLE 2-5: PRODUCT TYPES / SOFTWARE STREAMS 57
TABLE 2-6: EXECUTE MODES 59
TABLE 2-7: CPE > MONITOR FIELDS 89
TABLE 2-8: SCAN MODES 98

1 Introduction

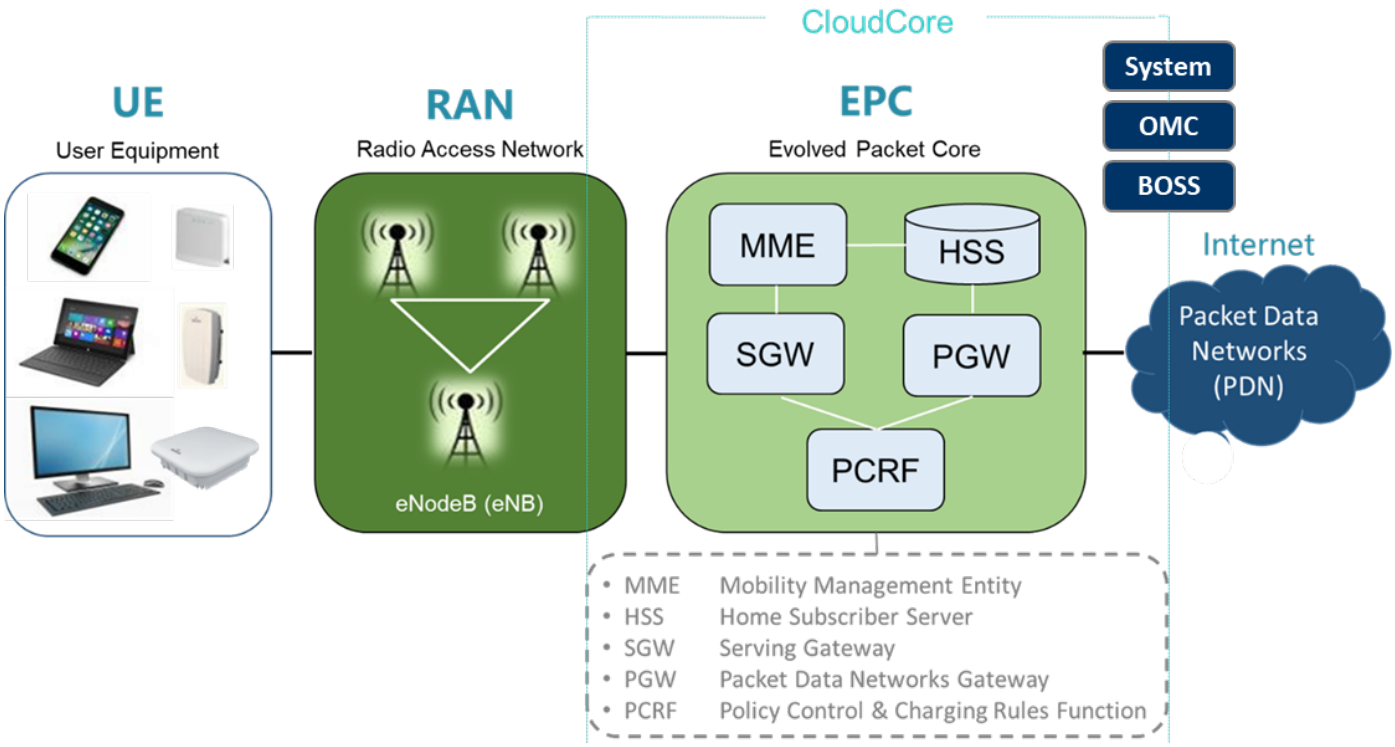
The Baicells products give network operators the ability to offer solutions in rural outdoor, urban outdoor, commercial indoor, unlicensed, and licensed, and a wide variety of vertical opportunities for subscribers using LTE-based broadband wireless access. In a standard configuration, the key components include Customer Premise Equipment (CPE), eNodeB (eNB) radio access network equipment, and cloud-based core functions and network/subscriber management applications (Figure 1-1). A subscriber connects a laptop, tablet, or other smart devices through the CPE - *aka* User Equipment (UE) - connecting wirelessly to an eNB. The eNB communicates with the LTE backhaul network.

The available operations, administration, and management (OAM) applications include an eNB GUI, a CPE GUI, the Baicells CloudCore Operations Management Console (OMC), and the Baicells CloudCore Business and Operation Support System (BOSS). The CloudCore System, OMC, and BOSS parameters are documented in this guide.

The eNB GUI and the CPE GUI are used to configure and manage individual devices. The CloudCore apps can configure and organize all the operator's network devices across multiple sites through the OMC and all the subscribers and service plans through BOSS. Baicells charges a monthly CloudCore usage fee based on the number of active users.

CloudCore includes not only management apps but also provides the core LTE network functions that are shown in the figure. Private network solutions such as Local EPC and Local OMC+BOSS are also available.

Figure 1-1: Standard Baicells LTE Network



2 CloudCore

The Baicells CloudCore services include the core LTE functions mentioned in *section 1* of this document, plus the Operations Management Console (OMC) for network management and the Business and Operation Support System (BOSS) for subscriber management. This guide covers the CloudCore System, OMC, and BOSS modules.

2.1 Client Computer Requirements

Table 2-1 describes the minimum requirements for the client computer you use to access the Baicells CloudCore OMC and BOSS applications.

Table 2-1: Client Requirements

Item	Description
CPU	Higher than Intel Core 1GHz
Memory	Greater than 2G RAM
Disk	No less than 100 MB space available
Operating System	Microsoft: Windows XP, Windows Vista, or Windows 7 Mac: MacOSX 10.5 or higher
Screen Resolution	At least 1024 x 768 pixels
Browser	Google Chrome 47 or higher (recommended) Mozilla Firefox 47 or higher

2.2 Getting Started

2.2.1 Sign up for CloudCore Account

Baicells provides a CloudCore account to every operator. Each account supports multiple administrative users. For a user to access the operator's account in CloudCore, they must sign up for login credentials. Follow the steps below to sign up for access to the account.

NOTE: The first time an operator's initial administrator logs in to their CloudCore account, they are asked to enter or verify basic company information and provide a credit card number. Operators are charged monthly to use CloudCore based on the number of active users that month. Payments are administered through a secure third-party company: https://pay.stripe.com. More about the billing process is described in *section 2.3.1, Billing Menu*.

1. Open a web browser and enter the CloudCore address: *https://cloudcore.cloudapp.net/cloudcore/*
2. Click on the Sign up button (Figure 2-1).
3. Complete the mandatory fields (Figure 2-2) and click on Sign up again.
4. You will receive an email from CloudCore. In the email, click on the CloudCore link to go to the *Login* page. Enter your login user name (email address) and a password to authenticate. You are now ready to start using CloudCore!

Figure 2-1: CloudCore Web Page

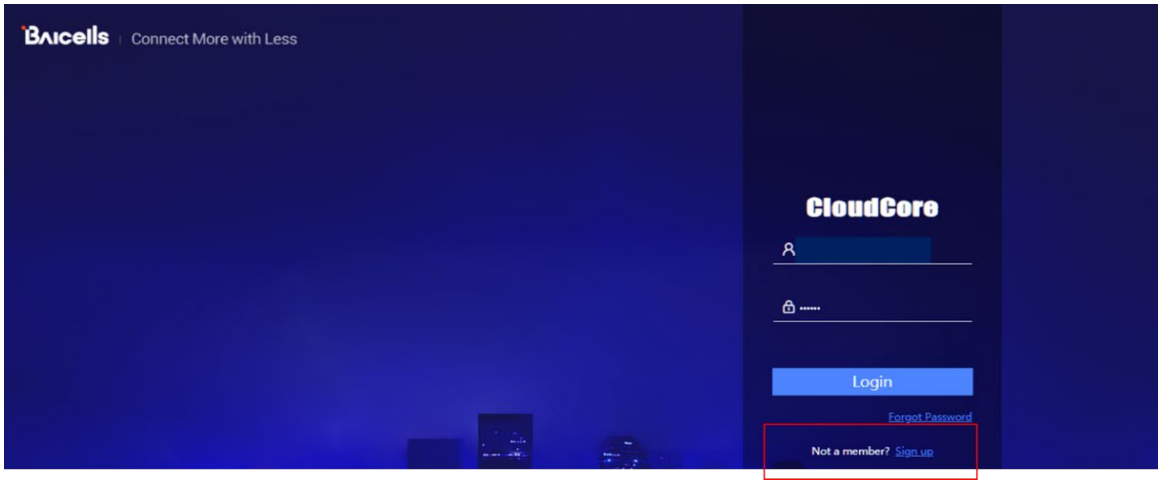
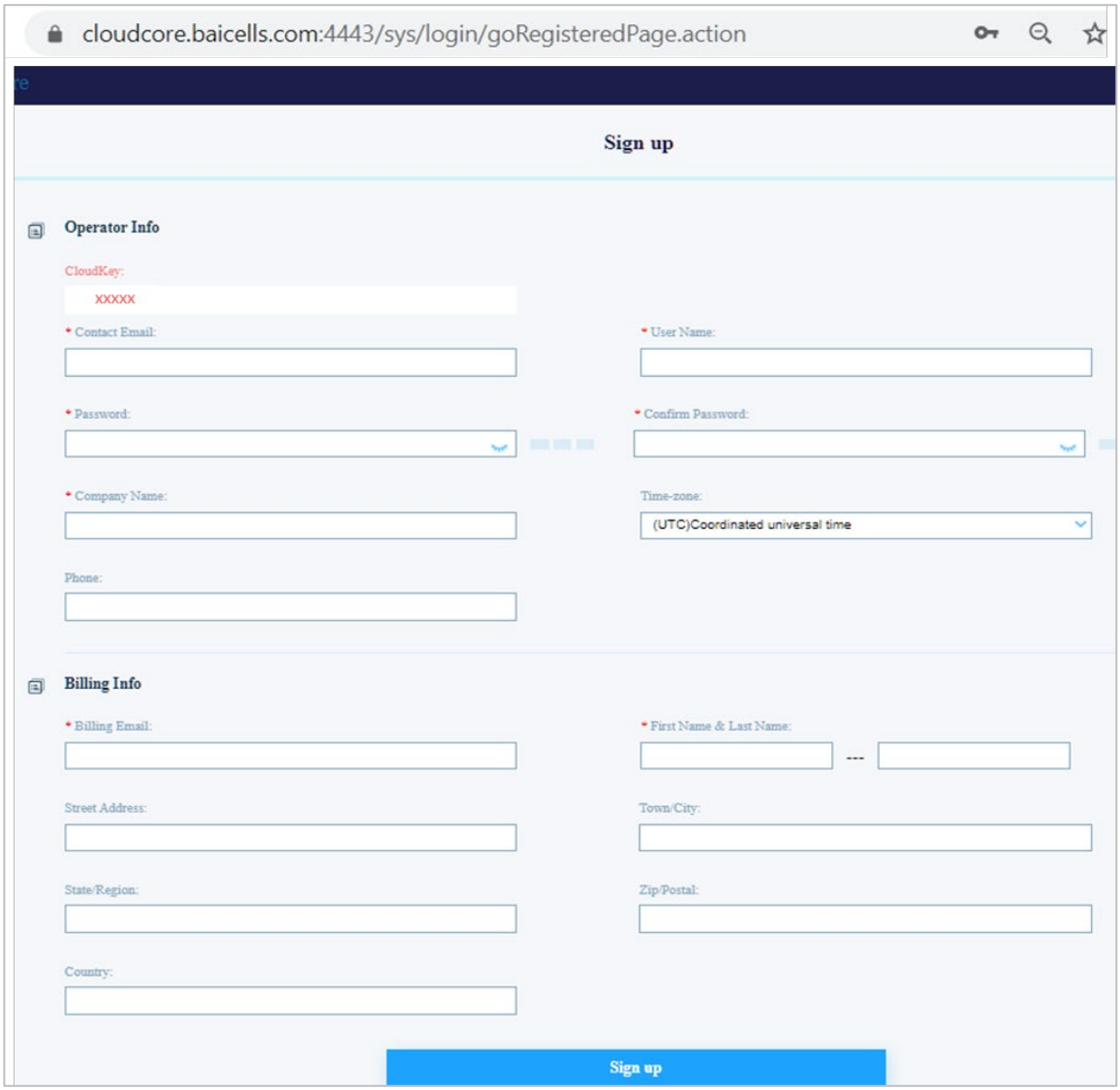


Figure 2-2: Sign up Fields



2.2.2 CloudCore Users

CloudCore users are referred to as administrators or admins. Admins added to the operator's CloudCore account must be assigned to one of two user groups, either the Cloud Default Group or Exclude Billing Group, as shown in Figure 2-3. If assigned to the Exclude Billing Group, the admin will not be prompted to enter the billing information, as discussed in the previous account, when they log in.

In this window, you can further assign an admin to one of two OMC default groups, either a Default Operator Group or a more restrictive Default User Group (Figure 2-4). BOSS has only one Default Operator Group. User group assignment determines which menus the admin can access and which actions they can take. You can create custom user groups covered in *section 2.3.3.1.2 User Group Tab*.

Figure 2-3: Default Cloud User Groups

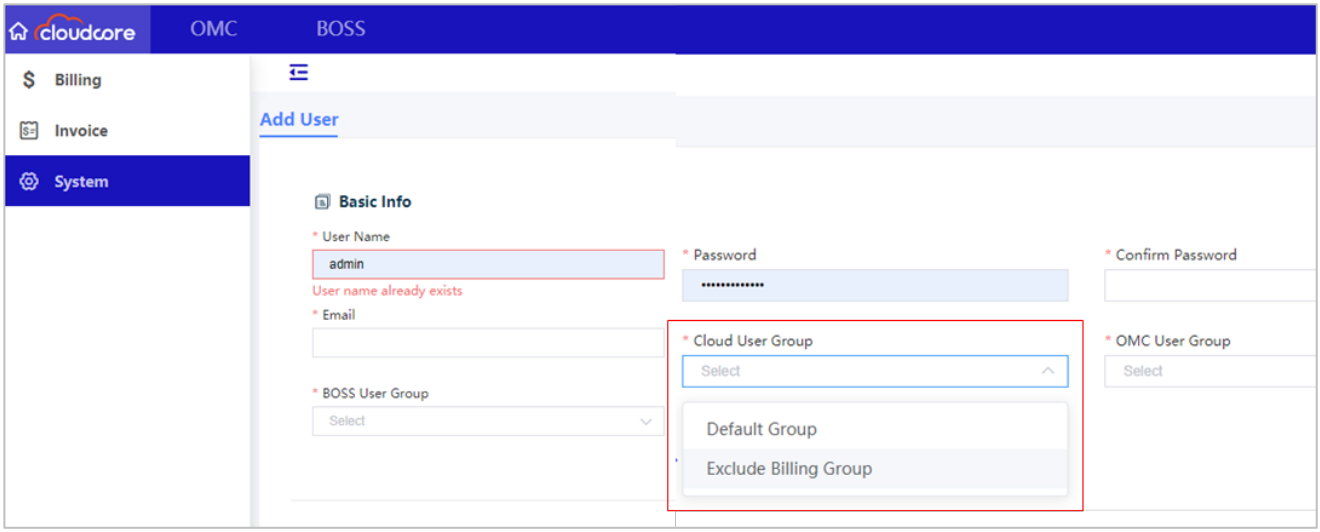
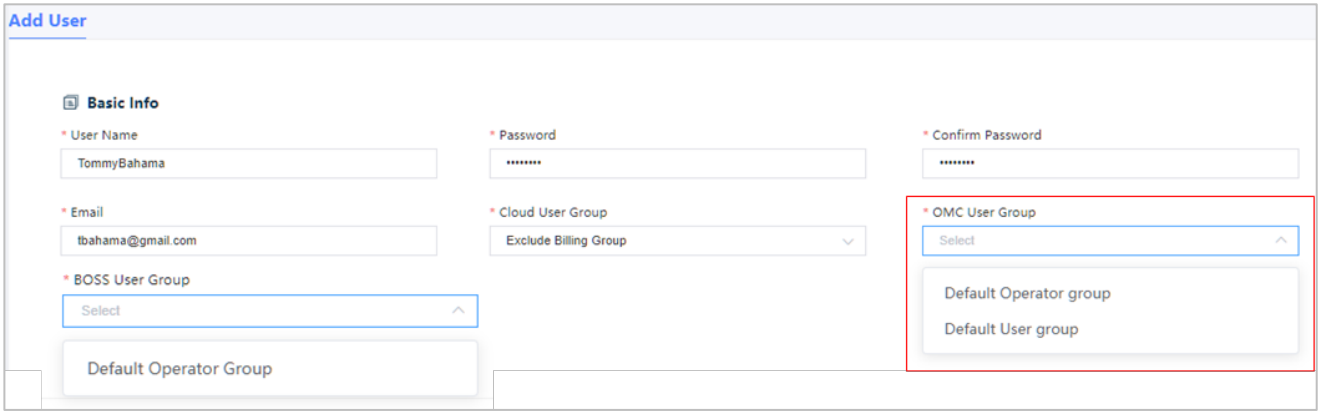


Figure 2-4: Default OMC and BOSS User Groups

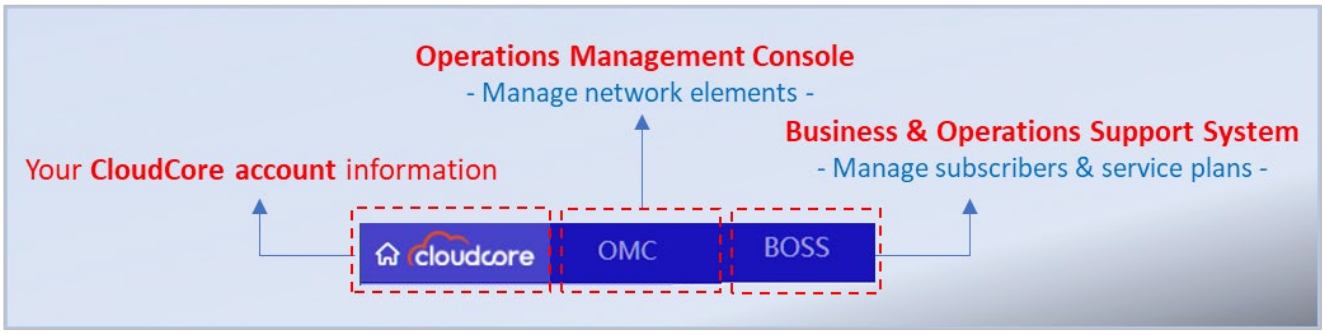


2.2.3 CloudCore GUI Layout

After logging in and assuming you have been assigned the Exclude Billing Group admin user group described in previous *section 2.2.2 CloudCore Users*, the CloudCore web page displays a horizontal blue bar at the top. The three main CloudCore modules - System (labeled "CloudCore"), OMC, and BOSS - are shown on the left.

The CloudCore System module contains the operator's account information, such as company name, contact information, etc.; invoices from Baicells for monthly use of CloudCore; and account administrator rules you define. The OMC is where you manage all of your network elements and features. The BOSS application is where you manage subscriber information, import SIM card IMSI numbers, and create service plans (Figure 2-5).

Figure 2-5: CloudCore Modules



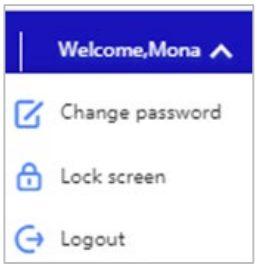
You will see the operator's unique Baicells CloudKey number on the right side of the blue bar (Figure 2-6).

Figure 2-6: CloudKey

An operator's CloudKey is used to associate eNB and CPE devices to the operator's account in the OMC. Equipment programmed with the operator's CloudKey in the device GUI during initial installation will automatically associate to the operator's OMC account when powered on. An eNB device will be listed in OMC under the *eNB > Inventory* menu. A CPE device will be listed in OMC under the *CPE > Device* menu. If you do not use the CloudKey in the device GUI, you can still add a device in either of the OMC menus mentioned.

Next to the CloudKey number is your login name and a drop-down menu that provides three essential admin user functions: Change password, Lock screen, Logout (Figure 2-7).

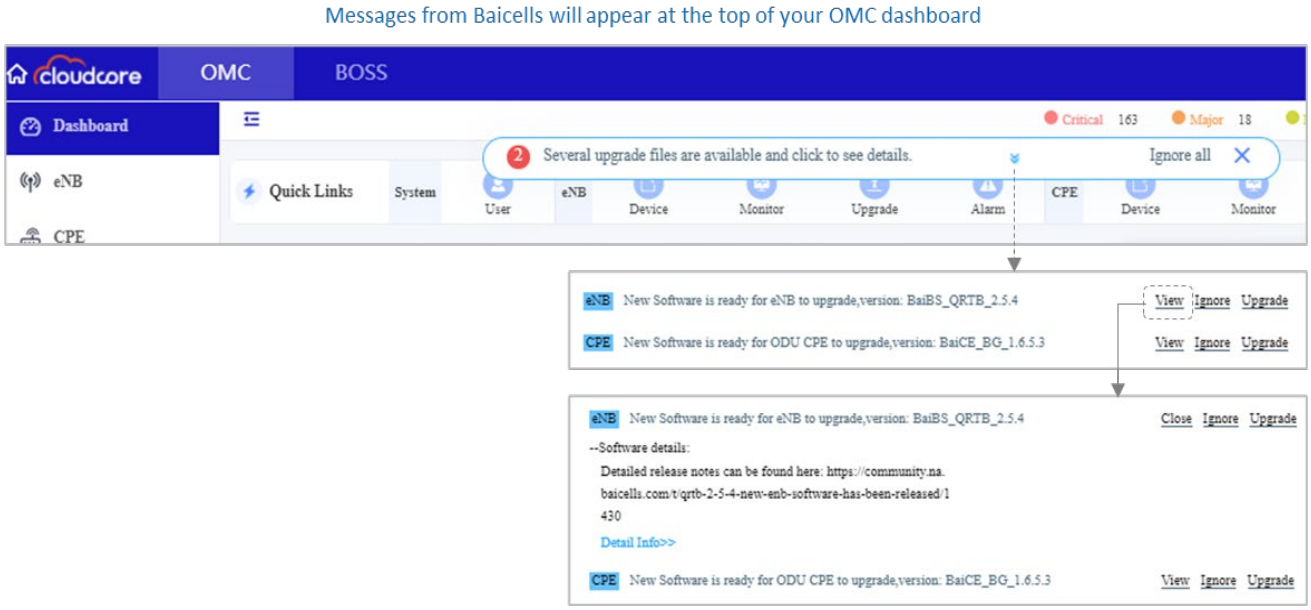
Figure 2-7: Welcome Drop-Down Menu



When you log in to CloudCore, the home page defaults to the OMC Dashboard (Figure 2-8). You can see messages from Baicells at the top, e.g., announcing the latest software available. You can either dismiss or act on these messages. Baicells recommends upgrading equipment to the latest available software code. How to upgrade eNBs is covered in *section 2.4.2.5 Upgrade*. How to upgrade CPEs is covered in *section 2.4.3.5 Upgrade*.

NOTE: The dashboard information is covered in *section 2.4.1 Dashboard Menu*.

Figure 2-8: Home Page (OMC Dashboard)



2.2.4 GUI Icons

Table 2-2 describes the icons used in the CloudCore GUI windows.

Table 2-2: Icons

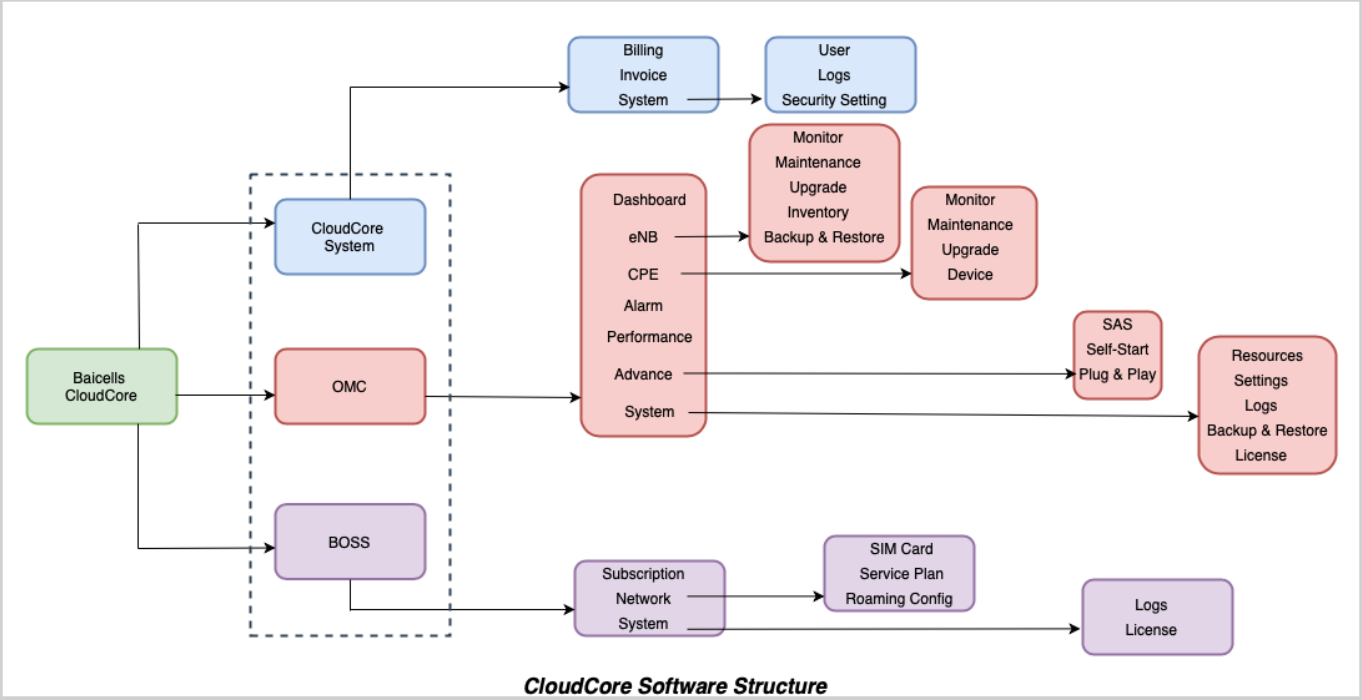
Icon	Description
	Search for a specific device or item
	Add a new device/item or a new task
	Import multiple devices at one time or upgrade file
	Export file to the local computer
	The operation menu of a device/item
	Download a file
	The device is operating normally
	The device is offline
	Setting of display or setting of tasks

Icon	Description
	Filter results according to alarm type, severity, and other status
	Create a new task
	Display the task list

2.2.5 CloudCore Software Structure

The CloudCore software enables the admin operators to configure the system, OMC, and BOSS in one place. An overview is shown in Figure 2-9. It depicts the size of the system, the readily identifiable modules, and functions; it also allows the admin to navigate through the CloudCore effortlessly.

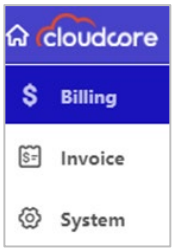
Figure 2-9: CloudCore Software Structure



2.3 System

The CloudCore System menu provides operator-specific information (Figure 2-10). The Billing, Invoice, and System menus are explained in this section.

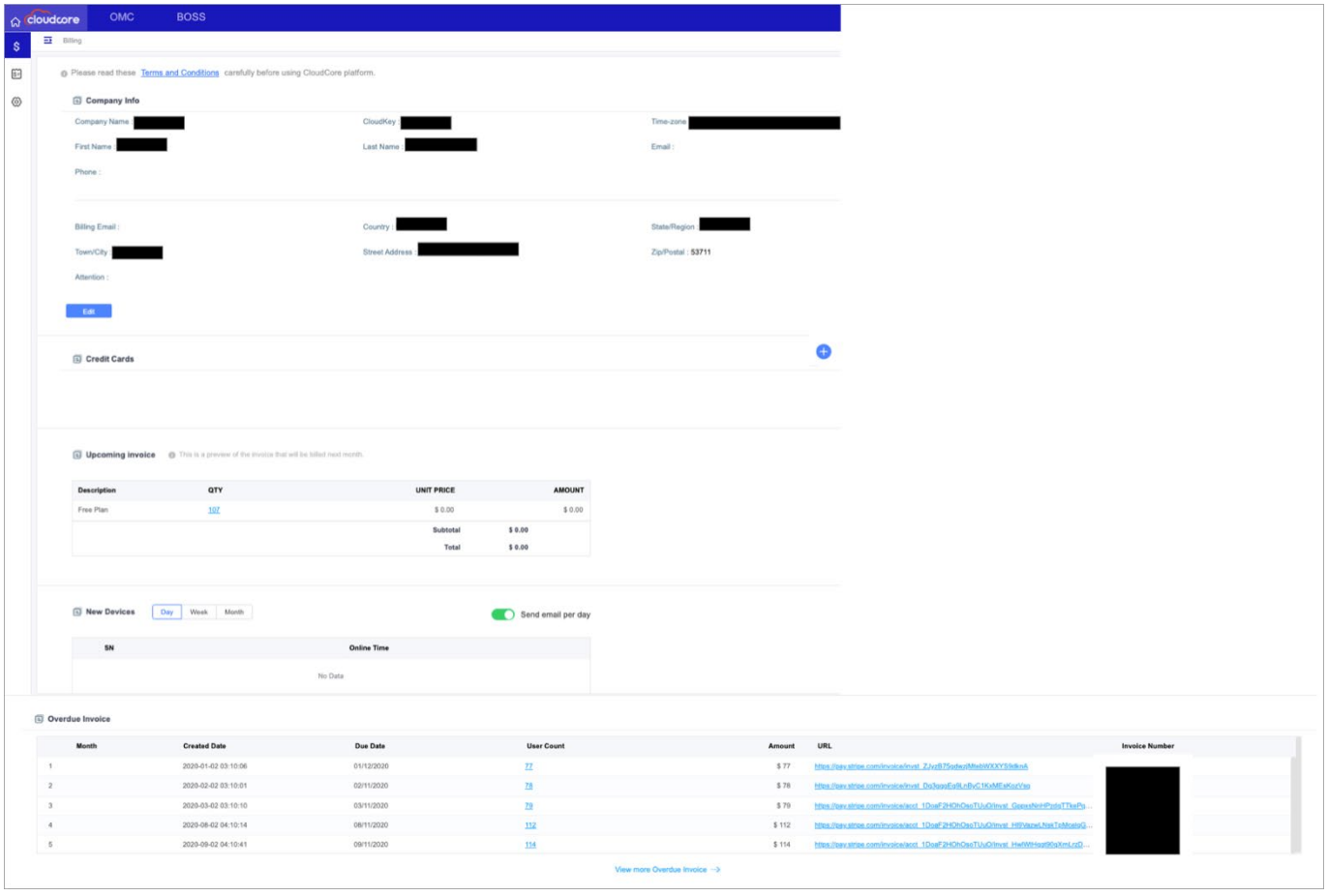
Figure 2-10: System Menu



2.3.1 Billing Menu

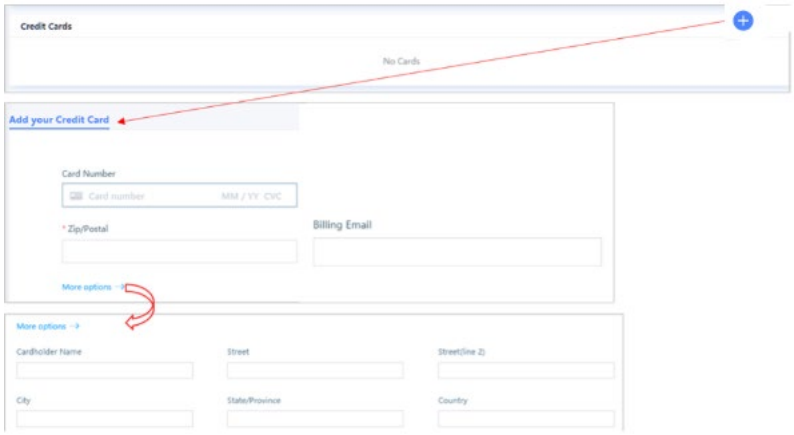
Operators are charged monthly to use CloudCore based on the number of active users that month. The Billing menu contains the operator's contact information and Baicells invoicing information for their CloudCore account (Figure 2-11).

Figure 2-11: Billing Menu



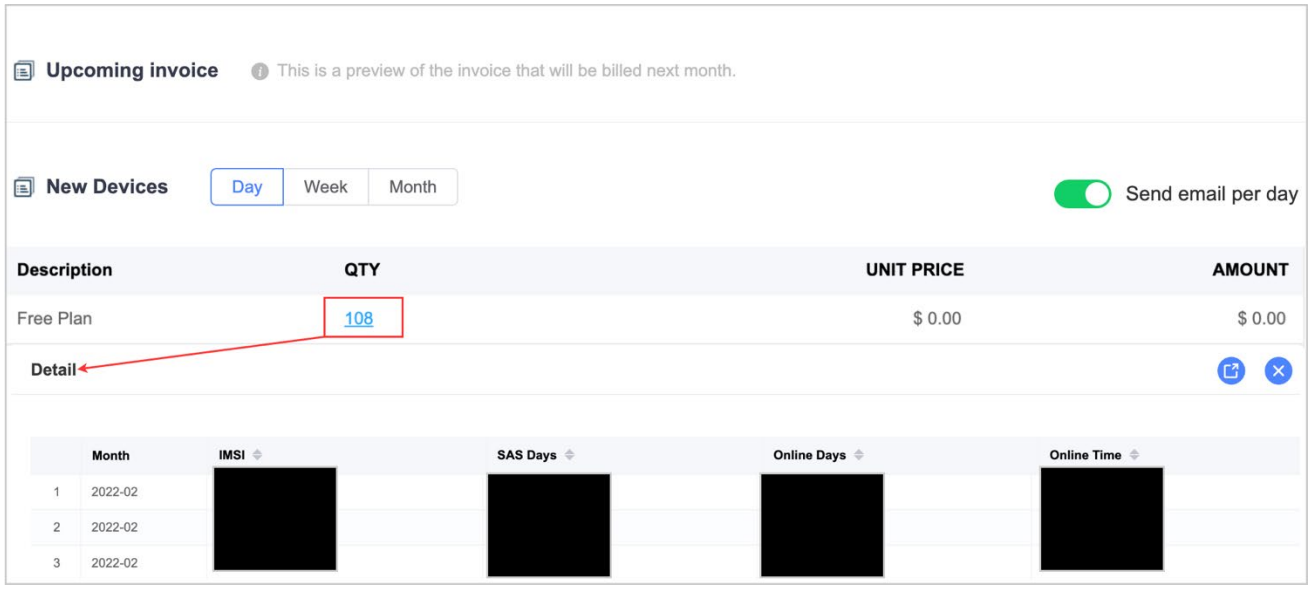
Click on + Add and enter the card number, expiration date, CVC [sic], zip code, and billing email to add credit card information. Click on More Options to add the cardholder's name, address, etc. (Figure 2-12). The credit card entry will be shown in the list. Use the *Operations* actions to View, Modify, Delete, or Set as Default.

Figure 2-12: Add Credit Card



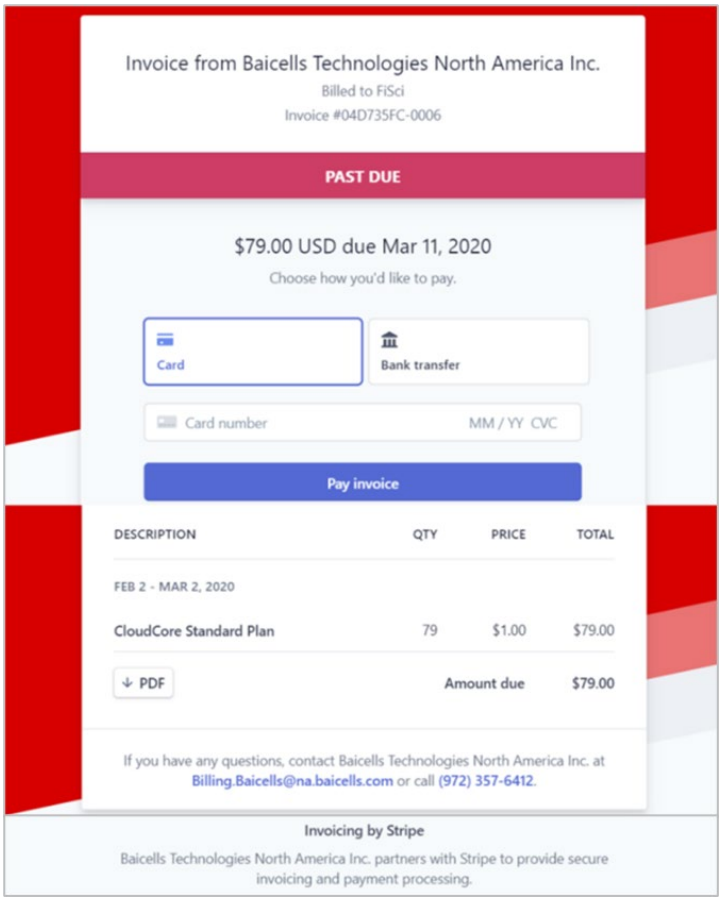
Under Upcoming Invoice, you will see the Description, QTY, unit price, and dollar amount owed. When you click on the QTY number, it takes you to the user details (Figure 2-13). In the New Devices pane, if you leave "*Send email per day*" ON (green), the system will send a reminder every day to subscribers who are behind on payments. The email will include all unpaid invoices.

Figure 2-13: Upcoming Invoice



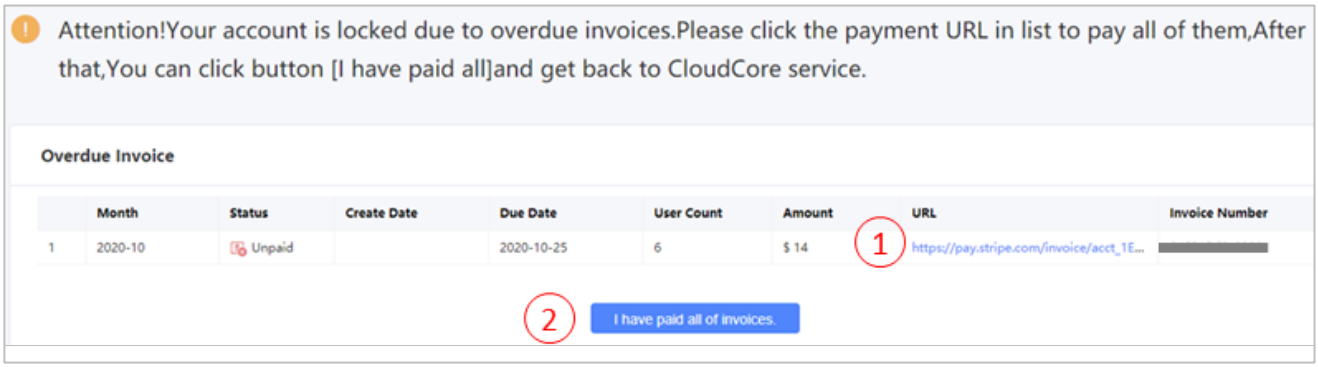
The Invoice section lists all the operator's invoices from Baicells like the billing month, status (paid/unpaid), invoice date, due date, active user count, dollar amount, date of payment, and the URL to a secure third-party e-commerce system used by Baicells: *https://pay.stripe.com*. The Figure 2-14 shows the Stripe GUI where you can pay by credit card or bank transfer, as well as download a PDF of the invoice.

Figure 2-14: Stripe Payment



If the operator fails to pay the fee in time, they cannot access CloudCore until the invoice is paid. When they try to log in, they will get a prompt window to resolve the unpaid invoice(s). The operator must click on the third-party payment service used by Baicells - currently, *https://pay.Stripe.com* - and make the payment (Figure 2-14). Once paid, the operator clicks on the *I have paid all invoices* button in the prompt window to restore their CloudCore services.

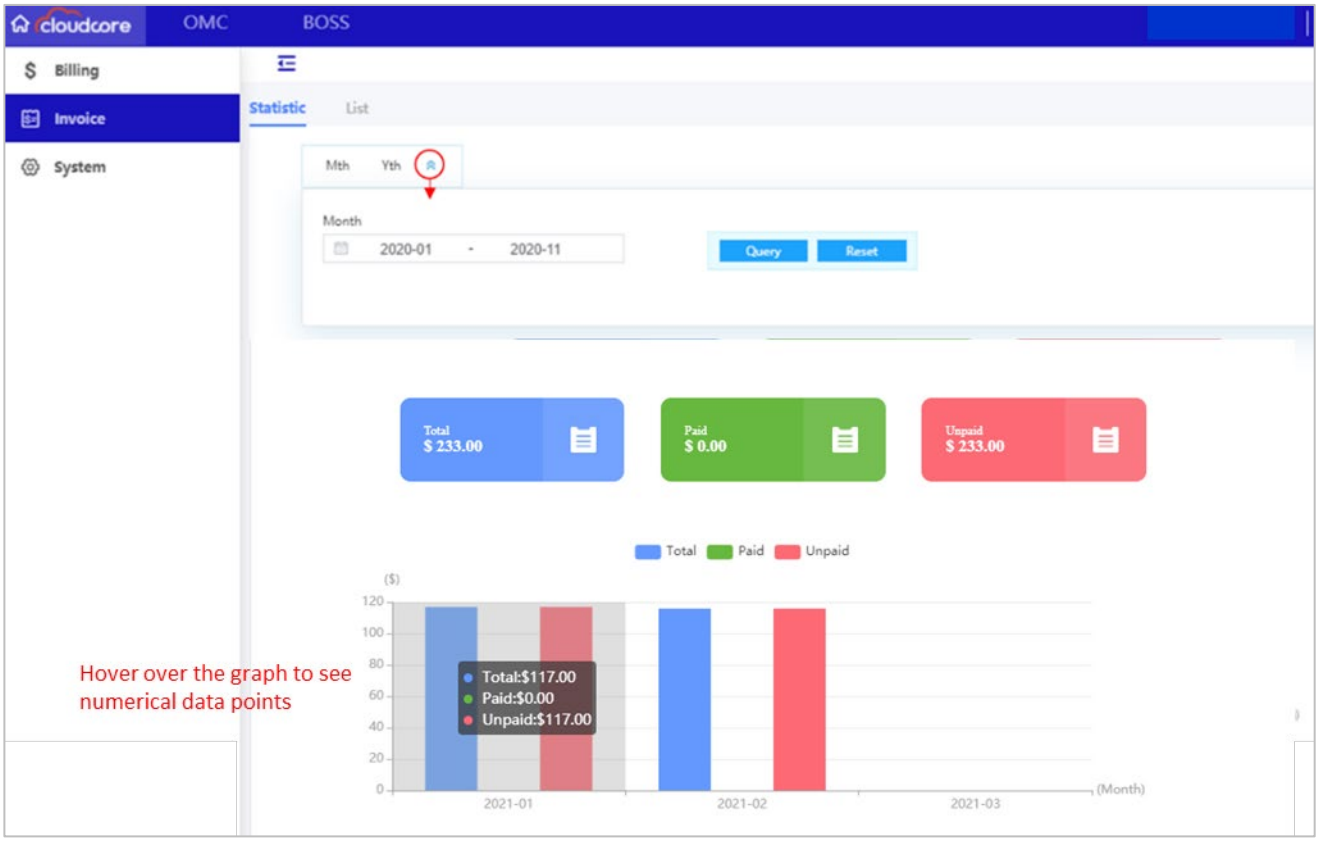
Figure 2-15: Overdue Invoice Example



2.3.2 Invoice

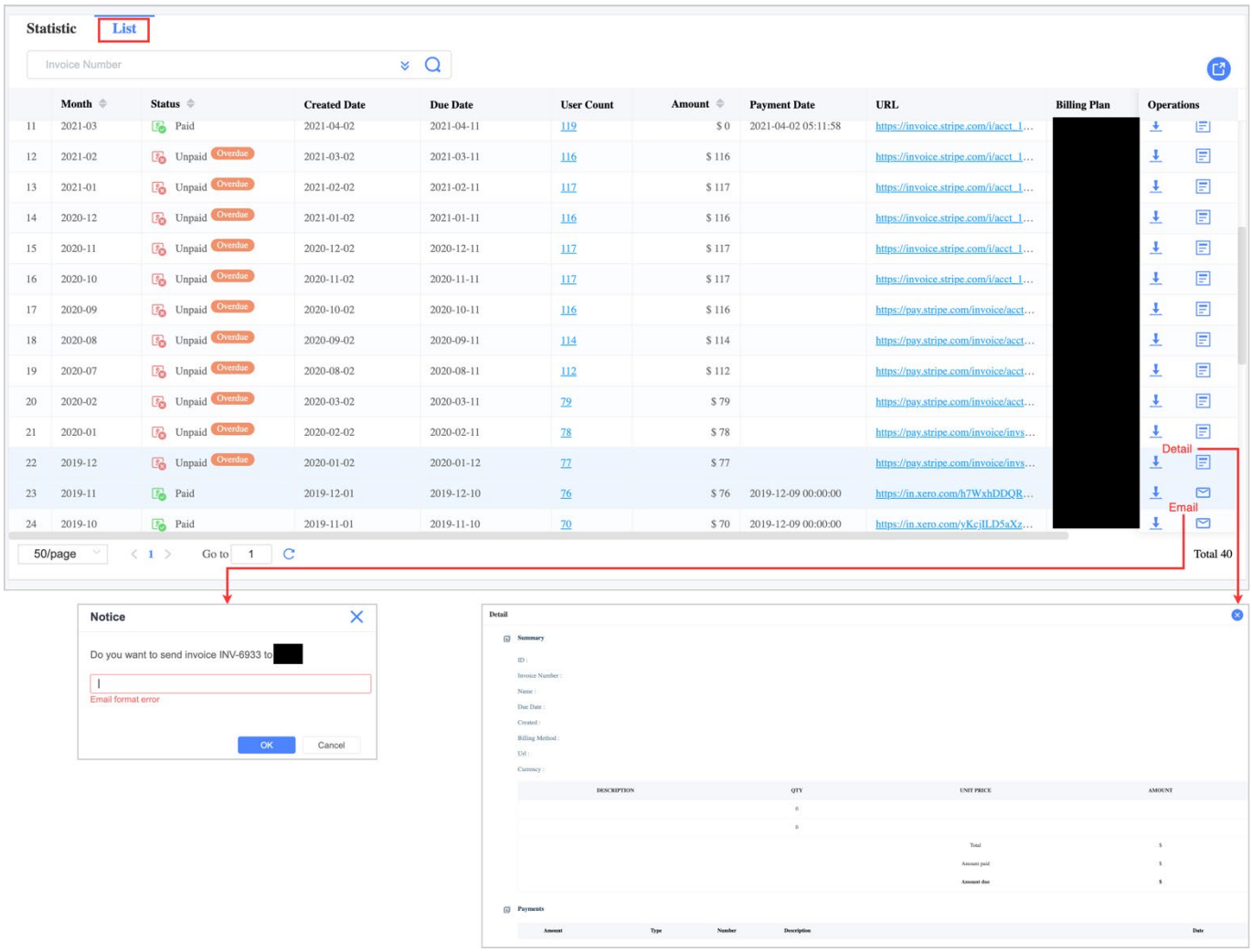
The Invoice menu has two tabs, one showing statistical data about your Baicells invoice information and one showing a detailed list of each historical invoice (Figure 2-16). The menu opens to the Statistic[s] tab, which displays the total billing amount and how much of that total has been paid or not paid during the period you select. At the top, you can set the timeframe of the statistics information you want to see. Hovering over the graph will display the numerical data for a data point.

Figure 2-16: Invoice Statistic[s] tab



The *List tab* displays all invoices received from Baicells, indicating their payment status, the number of active users, when the invoice was paid, etc. (Figure 2-17). Clicking on the User Count number will display information about each active user during the invoice period. Use *Operations* actions to download invoices, display invoice details, or send an email notification about the invoice to someone else. To Export all invoices, click on the *Export* icon, an Excel file Invoice.csv downloads to your browser.

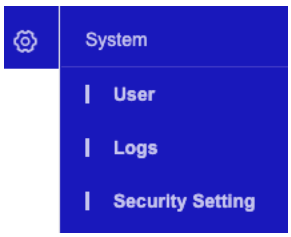
Figure 2-17: List Tab



2.3.3 System

The *CloudCore System module > System* menu is used to add CloudCore administrative users to the operator's account, view operational and security activity logs for the account, and establish security rules for the administrative users (Figure 2-18). Each of the three sub-menus - User, Logs, Security Setting- is explained in this section.

Figure 2-18: System Menu



2.3.3.1 User

In CloudCore, an administrative user (admin) is one who can access the operator's account in CloudCore to view, edit, or delete information. Depending on which role you assign to an admin, they can modify data in all CloudCore apps.

The *System module > System menu* is the only place to *add* administrative account users. However, you can assign admins to user groups, associate role sets (privilege levels), and delete user groups or role sets in any app.

There are three tabs at the top of the System window, Role Set, User Group, and User (Figure 2-19). When you add a new user's information, the user will automatically be placed in a default user group unless you assign them to a custom group you have created. Each user group can be associated with one or more role sets. For this reason, it makes sense to first create role sets and user groups before adding users.

NOTE: The default user group cannot be modified or deleted.

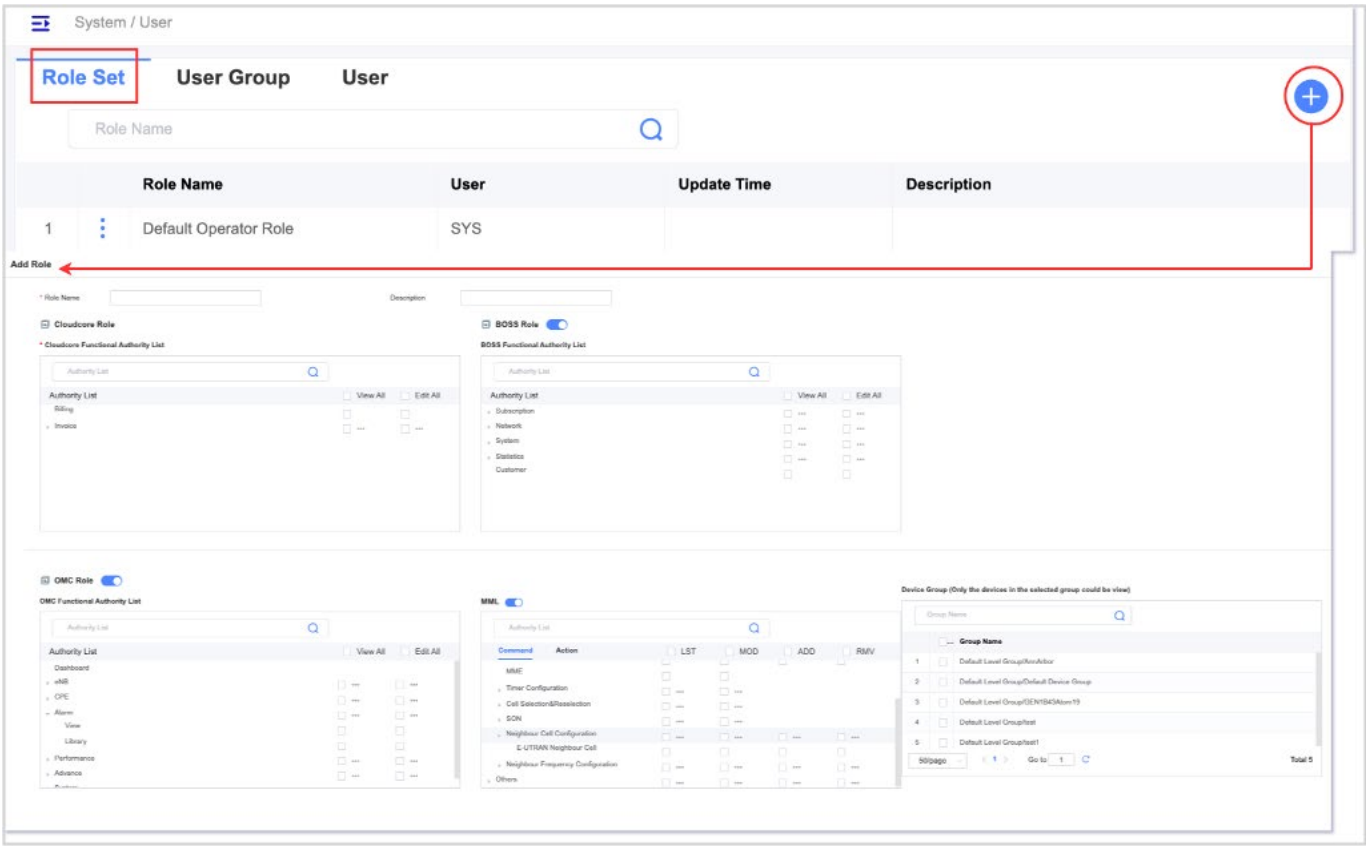
Figure 2-19: Admin User

2.3.3.1.1 Role Set Tab

A role set is a group of permissions that enables you to define various levels of CloudCore account privileges. These privileges are permissive roles given to access one or more system objects. Admin can assign roles to a user or user group, and a user or user group can have more than one role. Any existing role sets will be listed when you click on this tab. You can manage OMC/BOSS user group and role from the CloudCore. Click on the *Operations* icon to view information about a role set or to modify or delete the role set (Figure 2-20). To create a new role set:

1. Click on the **+** Add icon to open the *Add Role* window and enter a role name and description.
2. CloudCore role is a mandatory (*) authority list. Select the permissions (View, all, Edit all) that you want to designate for the role set to access the CloudCore functionalities.
3. BOSS Role, OMC Role, MML has a toggle button to create the *Functional Authority List* for each; you can select the functionalities listed under the pane and its permissions. For MML, you have additional permissions like LST (List), MOD (Modify), ADD, and RMV (Remove).
4. The device group pane allows the admins to select the device group to view the functionalities.
5. Click on *OK* to save the settings.

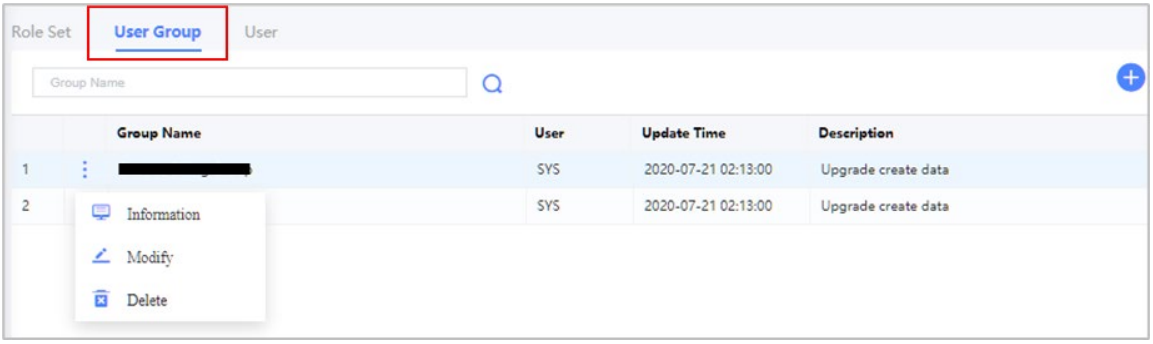
Figure 2-20: Role Set



2.3.3.1.2 User Group Tab

You can create custom admin user groups in the User Group tab. When you click on the tab, any existing user groups will be listed. Use the *Operations* actions to display group information, modify a group, or delete a group (Figure 2-21).

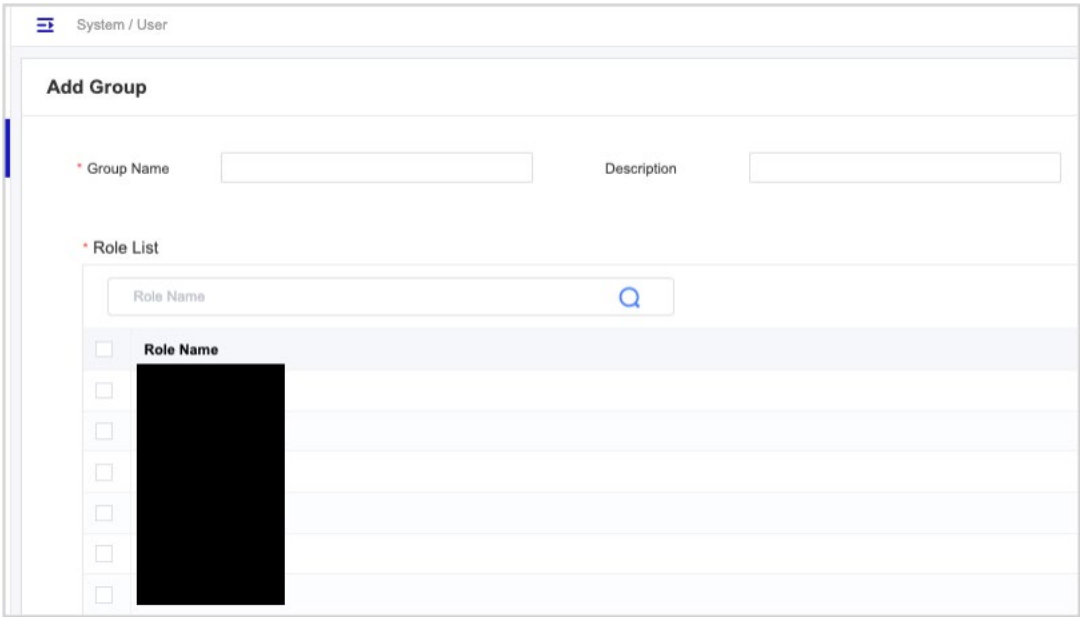
Figure 2-21: User Group



To add a new admin user group (Figure 2-22):

1. Click on the **+** Add icon to open the Add Group window.
2. Enter a Group Name and optionally a description.
3. Select the role(s) from the Role List to assign the privileges level to this group.
4. Click on *OK* to save the settings.

Figure 2-22: Add User Group



2.3.3.1.3 User Tab

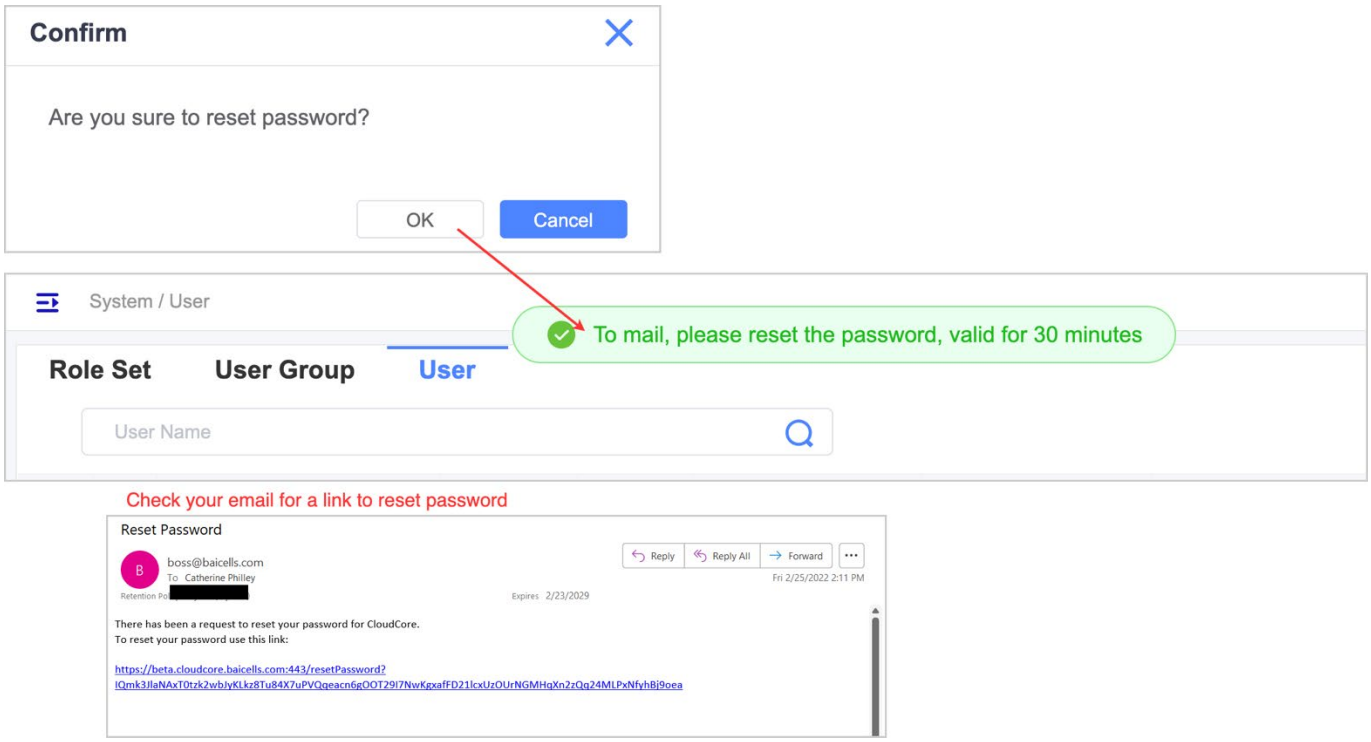
Although the *System > User* menu defaults to the User tab, setting up the role sets and user groups you intend to use is more efficient. Why? When you add a user, you must associate them to one or more user groups, and a user group has one or more associated role sets. If a user is not placed in a custom user group, the user will be placed in a default user group. The default user group cannot be modified or deleted.

Any admin users added are listed when you click on the tab (Figure 2-23). Use the *Operations* actions to view Information, Modify, Unlock, Delete, Reset Password, or Logout for an admin listed here in your account.

If you select Reset Password, the system will ask if you want to take that action. Click on *OK* if you're going to continue. The system will return a message stating "Success," You should receive an email with a link to reset the password (Figure 2-24). The user's password can include A-Z, a-z, 0-9, dash (-), and underscore (_) characters and can be 6 to 16 characters in length.

Figure 2-23: User Tab

Figure 2-24: Reset Password



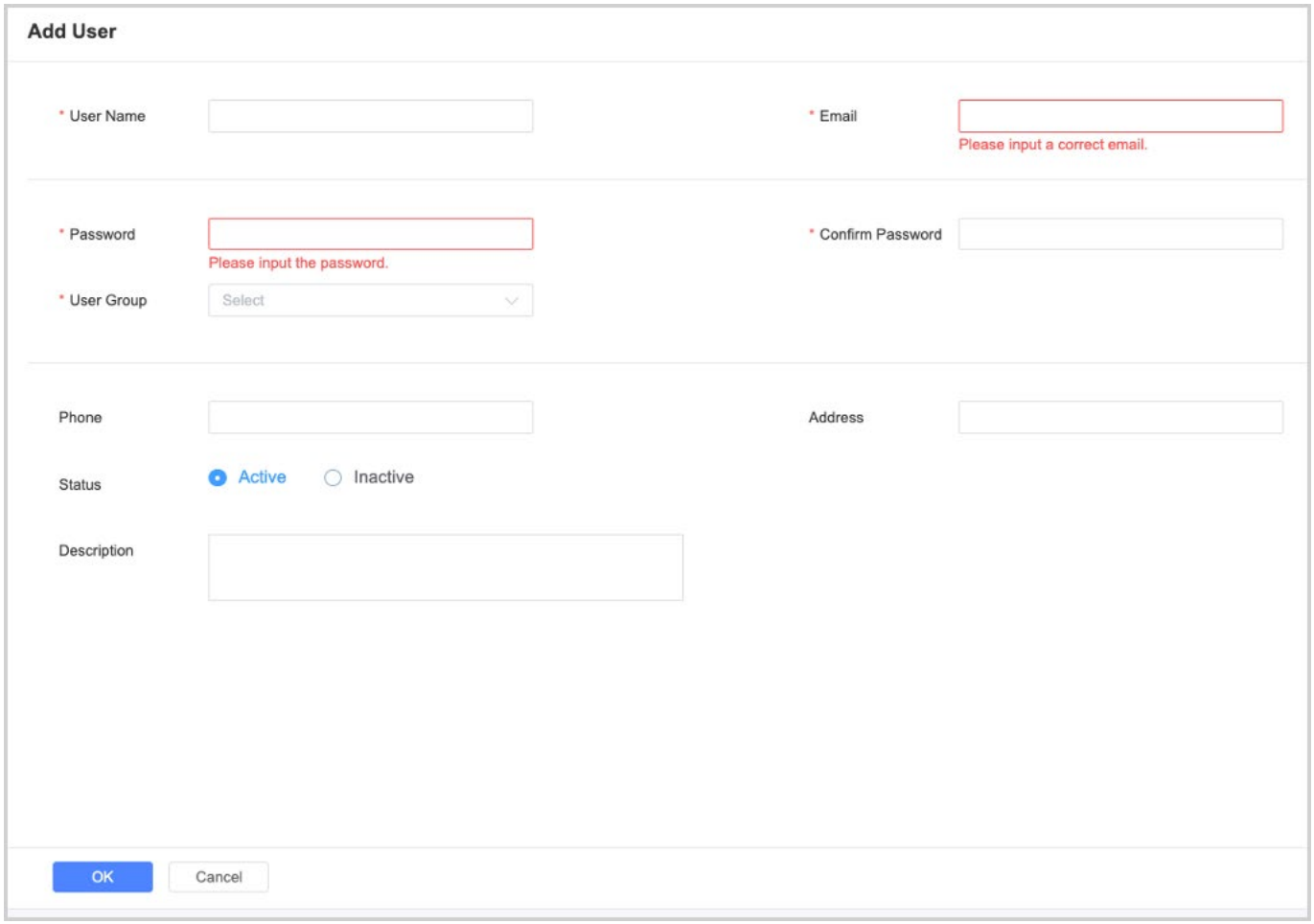
To add a new administrative user to your account (Figure 2-25):

1. Click on the **+** Add icon to open the Add User window. Fields with a star next to them are mandatory.
2. Enter a User Name and Password, and then Confirm Password.

   NOTE: The User Name and Password fields appear greyed out, but they are still editable.

3. Enter the user's Email address.
4. Select the User Group you want the new user to be added to in the following pull-down menu. The pull-down lists will include any previously configured user groups and the default user groups.
5. Optionally you can enter a Phone number, Address, change the user's status to Active or Inactive, and Description.
6. Click on *OK* to save the settings.

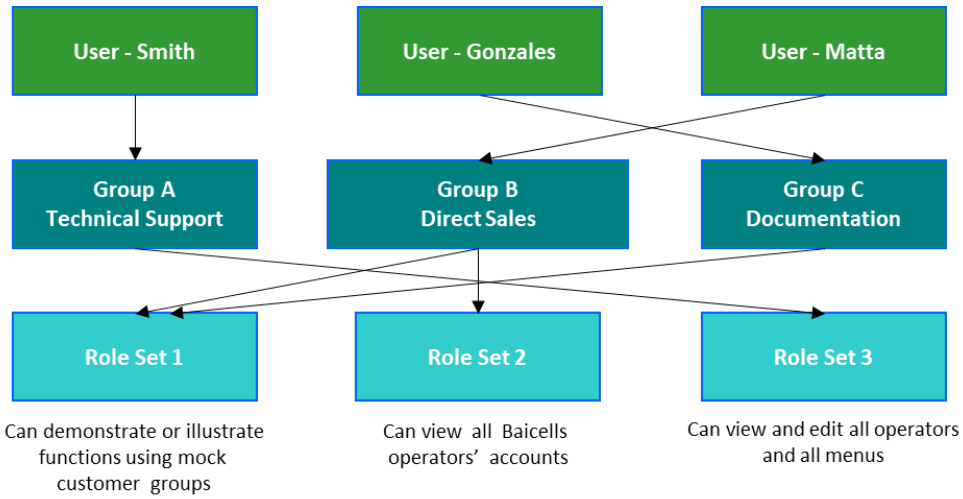
Figure 2-25: Add Administrative User



2.3.3.1.4 Summary of Admin User Setup

An example of the relationship of roles to user groups and users to user groups is illustrated in Figure 2-26.

Figure 2-26: Admin User Setup Example



2.3.3.2 Logs

The *System > Logs* menu contains operational and security event logs (Figure 2-27). The logs represent all CloudCore administrative user activity and are listed in descending order by date and time.

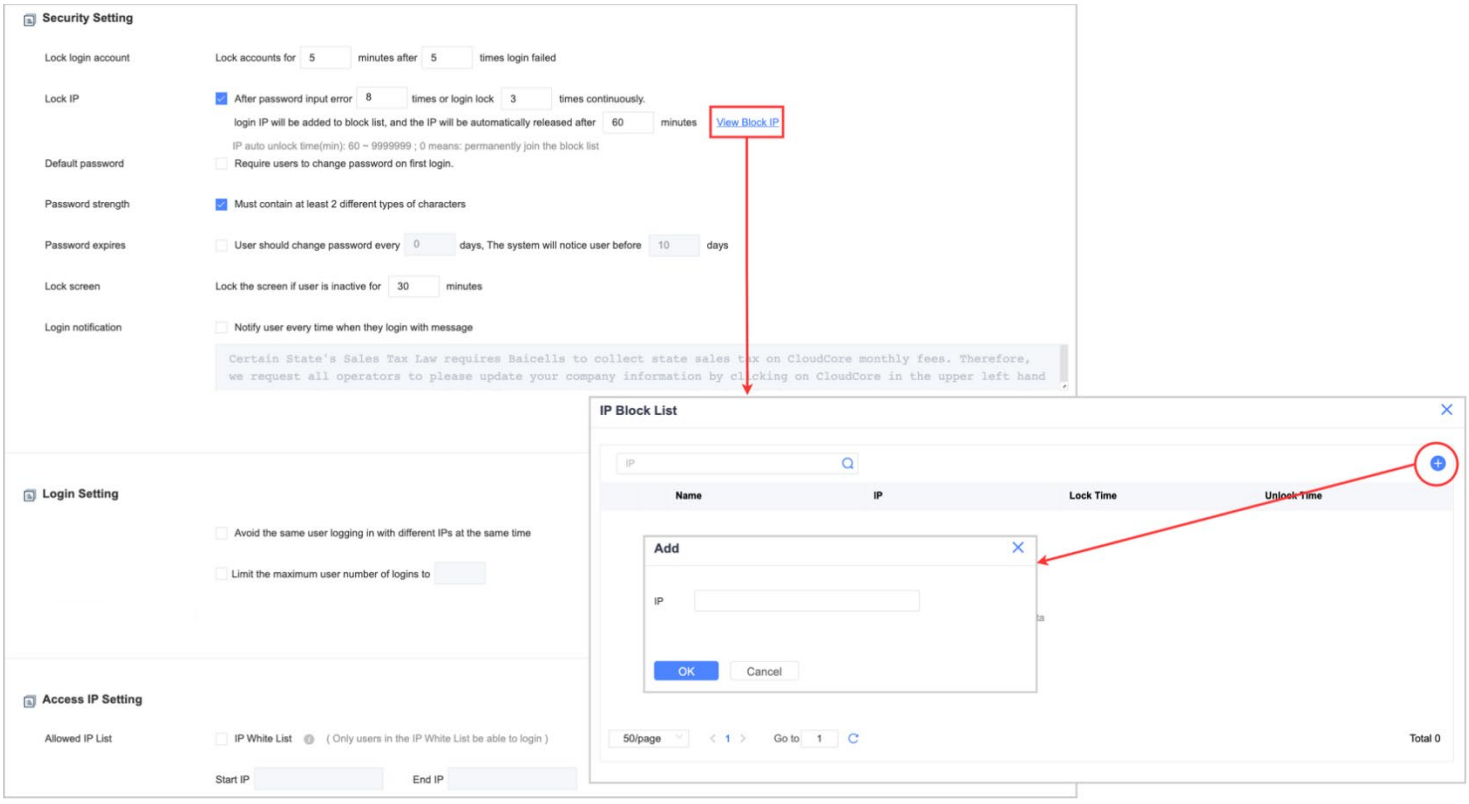
Figure 2-27: Logs

2.3.3.3 Security Setting

Selecting *System > Security Setting* allows you to set up rules concerning administrative user access to the operator's CloudCore account. Click on Security Setting to fortify the admin user access (Figure 2-28)

1. Security Setting
    a. Lock login account – Enter a number in the text boxes. You can customize the time to lock the account after frequent login failures.
    b. Lock IP – Select the check box if you want to blocklist the IP that encounters frequent login failures. To add IP manually to the blocklist, click "*View Block IP*" and click + Add icon to block IP. To remove IP from the blocklist, click "*View Block IP*" and remove the block listed IP.
    c. Default password – Select the check box if you want the users to change the password on the first login.
    d. Password strength – Select the checkbox if you want the password to contain at least two types of characters.
    e. Password expires – Select the check box if you want to determine how long a password can be used before the user is required to change it.
    f. Lock screen – Enter a number in the text box to set how long it takes to lock the screen if the user is inactive.
    g. Login notification – Select the check box if you want to display a custom message to the users when they login.
2. Login Setting
    a. Select the check box to avoid multiple logins from the same IP Address simultaneously. This setting will limit concurrent logins.
    b. Select the check box and enter a value to limit the number of active logins.
3. Access IP Setting
    a. IP Whitelist – Select the check box if you want to create IP address whitelists to limit which IP addresses can log in to the operator's CloudCore account.
    b. Start IP - when IP Whitelist is checked, enter the starting IP address
    c. End IP - when IP Whitelist is checked, enter the ending IP address

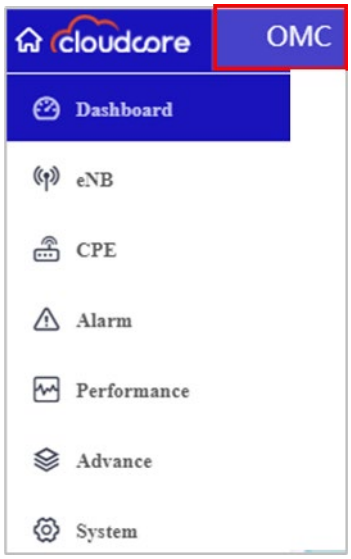
Figure 2-28: Security Setting



2.4 OMC

The CloudCore Operations Management Console (OMC) is used to manage network elements such as eNB and Customer Premise Equipment (CPE), which is also known as User Equipment (UE) (Figure 2-29).

Figure 2-29: OMC Menu



NOTE: Some menu items are available only to Beta customers trialing new features.

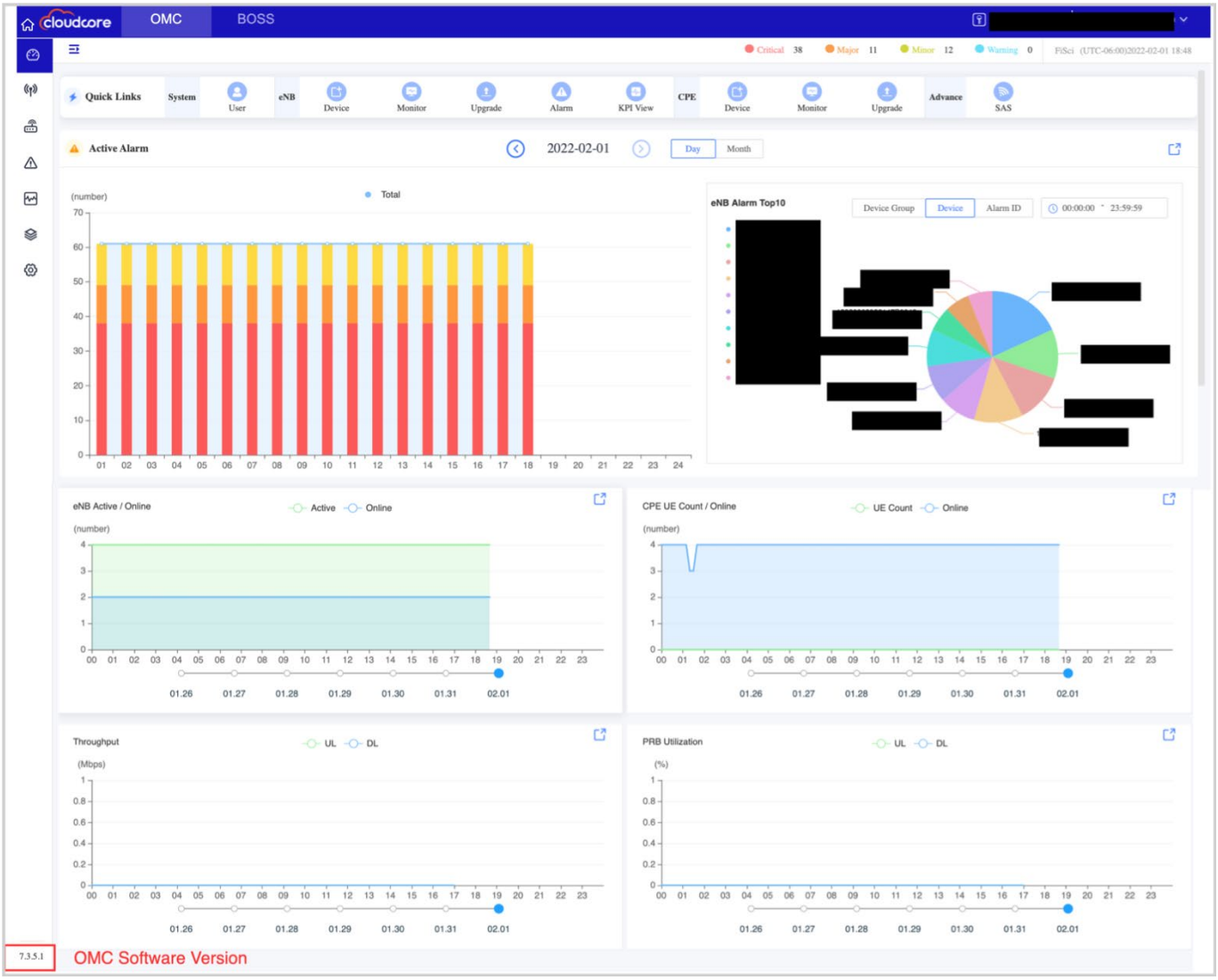
2.4.1 Dashboard Menu

When you click on the OMC module, the Dashboard's landing page. The dashboard menu provides a current, at-a-glance view of the operator's network (Figure 2-30).

- Alarm totals by severity level
- Quick Links to the other OMC menus
- Top 10 active alarms graph and pie chart
- Statistical graphs of aggregate device performance data

Each of the dashboard functions is explained in the sections below.

Figure 2-30: Dashboard



2.4.1.1 Alarm Totals by Severity Level

At the top of the dashboard, you will see the alarm totals from all eNBs in the operator's network. The system generates alarms for communications, QoS, processing, equipment, and the equipment's environment. Each type of alarm is given a severity level -- critical (red), major (orange), minor (yellow), warning (blue) -- to indicate the importance of urgency that applies to it.

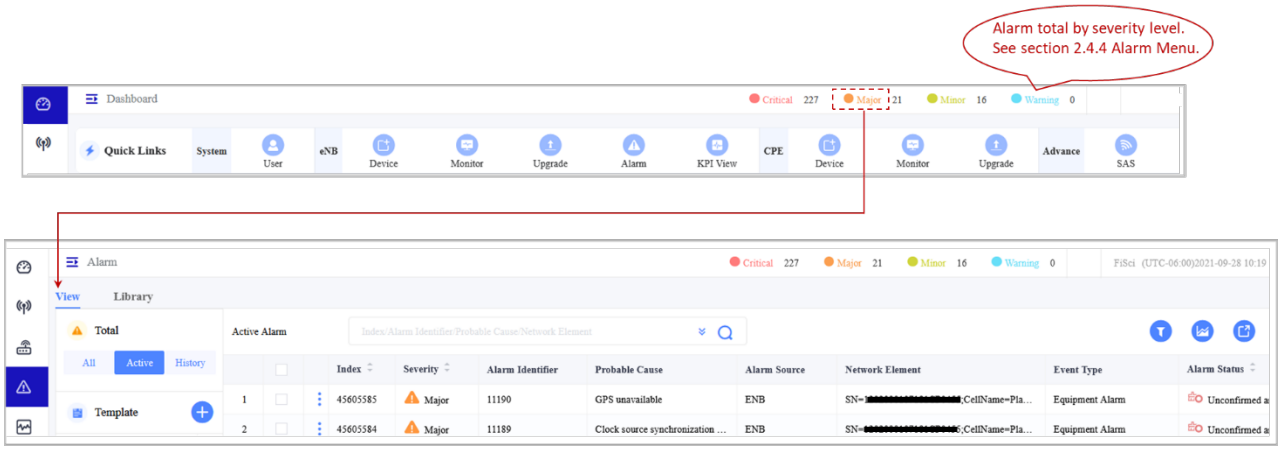
Critical alarms are incidents that can cause system outages and should be addressed immediately. Significant alarms are incidents that can cause the poor or degrading quality of service for subscribers and, therefore, should be addressed as soon as possible. Minor alarms indicate a potential issue that needs investigation but will not disrupt service. Warnings are used to indicate errors that probably need to be corrected or at least monitored but do not require any action.

If you are a beta operator, you will also see the Devices Migration icon at the top of the dashboard and to the right of the alarm severity indicators. Devices Migration allows you to move your devices from production to Beta CloudCore.

If you click on one of the alarm totals icons, the page will jump to the *Alarm > View* menu, giving details about the specific alarms at that severity level (Figure 2-31).

NOTE: The Alarm menu is documented in *section 2.4.4 Alarm Menu*.

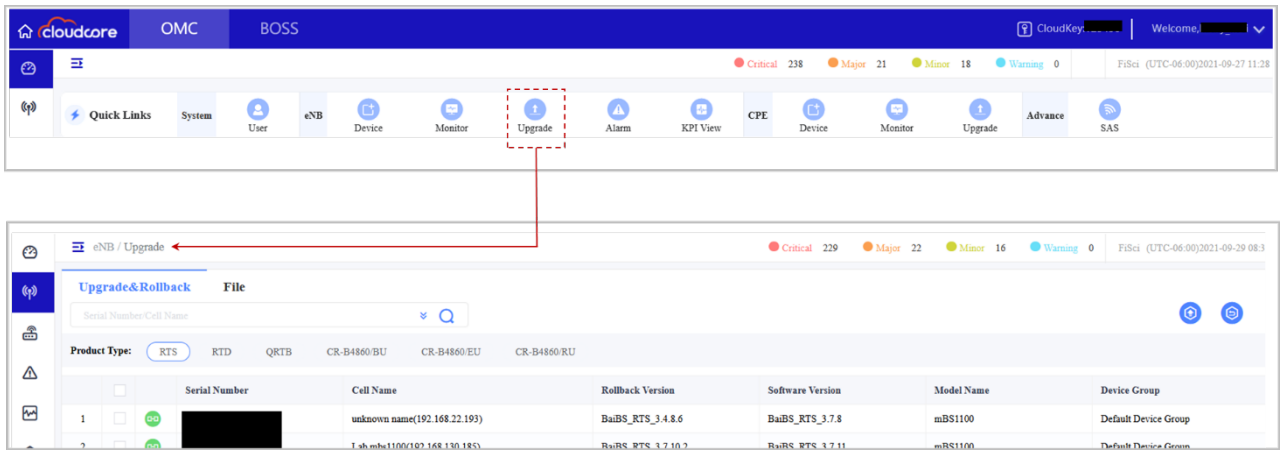
Figure 2-31: Alarm Icons



2.4.1.2 Quick Links

The Quick Links are grouped into System, eNB, CPE, and Advance, making it easy to jump into other OMC menus. For example, in the eNB section of Quick Links, if you click on Upgrade, the screen will jump to the *eNB > Upgrade* menu (Figure 2-32).

Figure 2-32: Quick Links



2.4.1.3 Top 10 Active Alarms

The Active Alarm pane contains a graph and a pie chart (Figure 2-33). The graph shows the top 10 alarms for a specified period by either day or month. The graph shows the number of alarms for each severity level for all eNBs. The pie chart shows the top 10 alarms by device group, device (serial number), or alarm ID (Figure 2-34). Hover your cursor over the graph or pie chart to see the numerical data for any given data point.

Figure 2-33: Active Alarm Pane

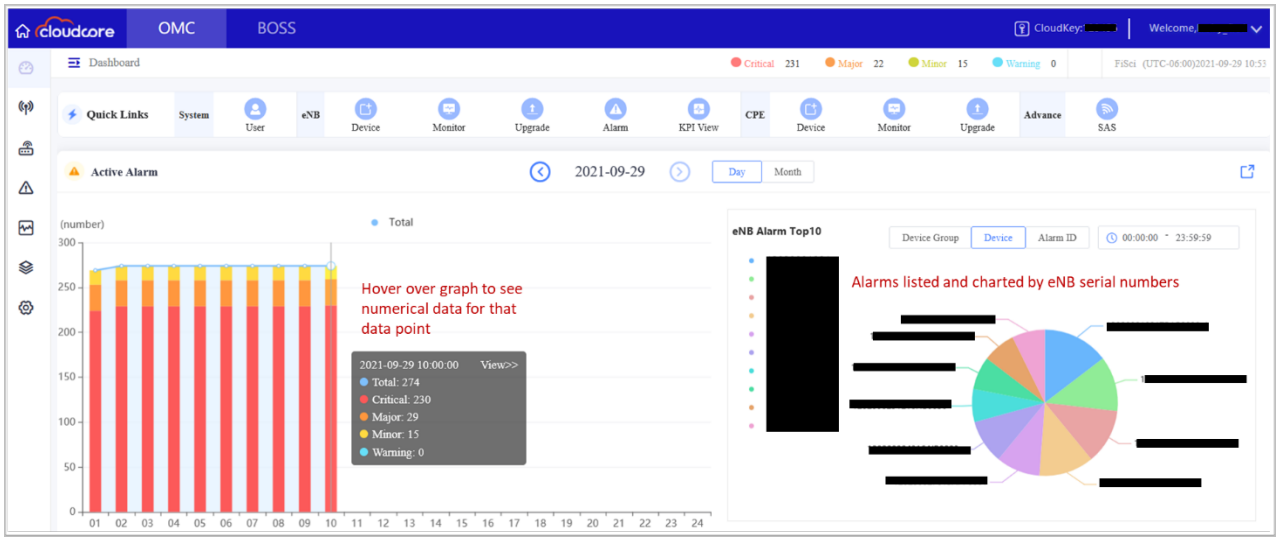
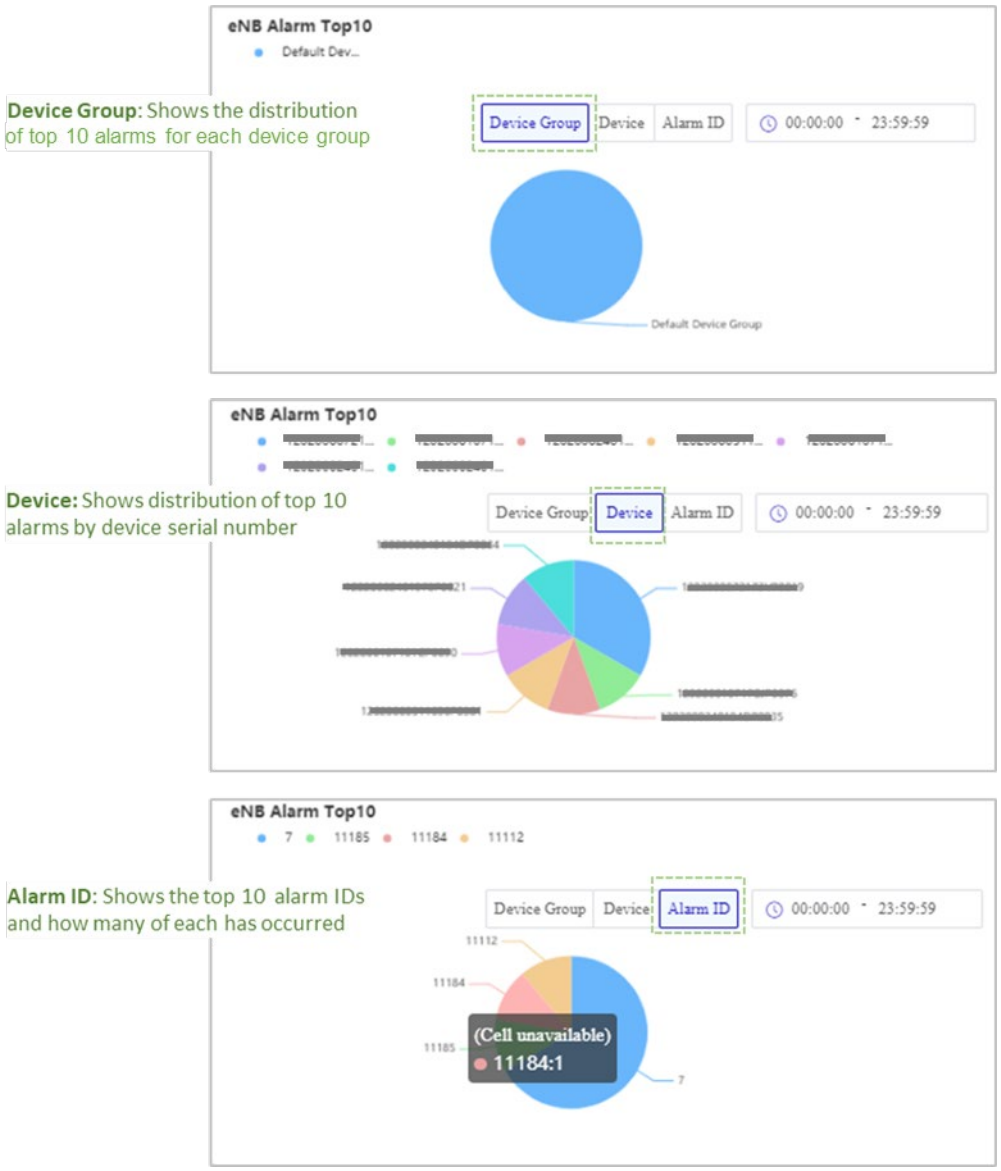


Figure 2-34: Active Alarm Pane - Pie Chart Display Options



You can change the timeframe of the graphed information to 24 hours (Figure 2-35) or an entire calendar month (Figure 2-36). To specify 24 hours, click on “Day”; next, click in the time interval field and use the time set box that displays to scroll and select a start and end time; then, click *OK*. To establish an entire calendar month, click on “Month”; next, click in the time interval field and use the calendar displayed to select a month.

NOTE: The start time and end time can also be entered in the time interval field instead of using the time set boxes if you prefer. Ensure you enter the times using the “hh:mm:ss” format with colons separating each increment.

Figure 2-35: Active Alarm Pane - 24-Hour Time Period

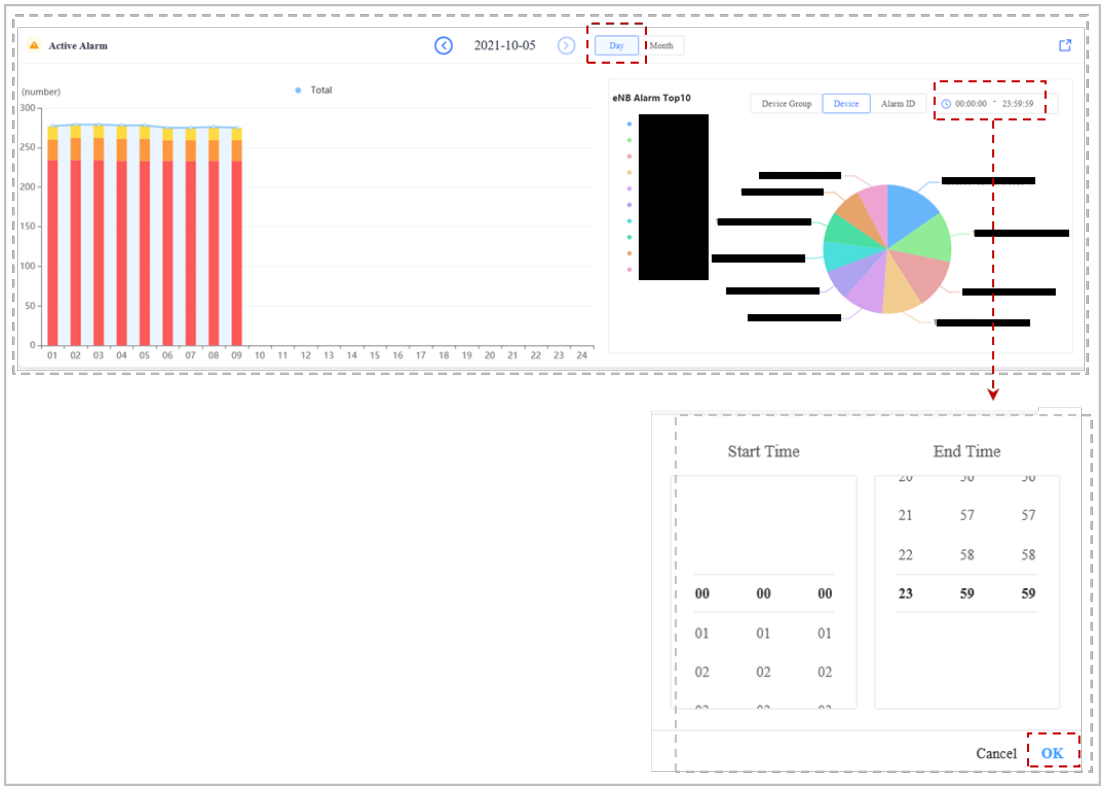
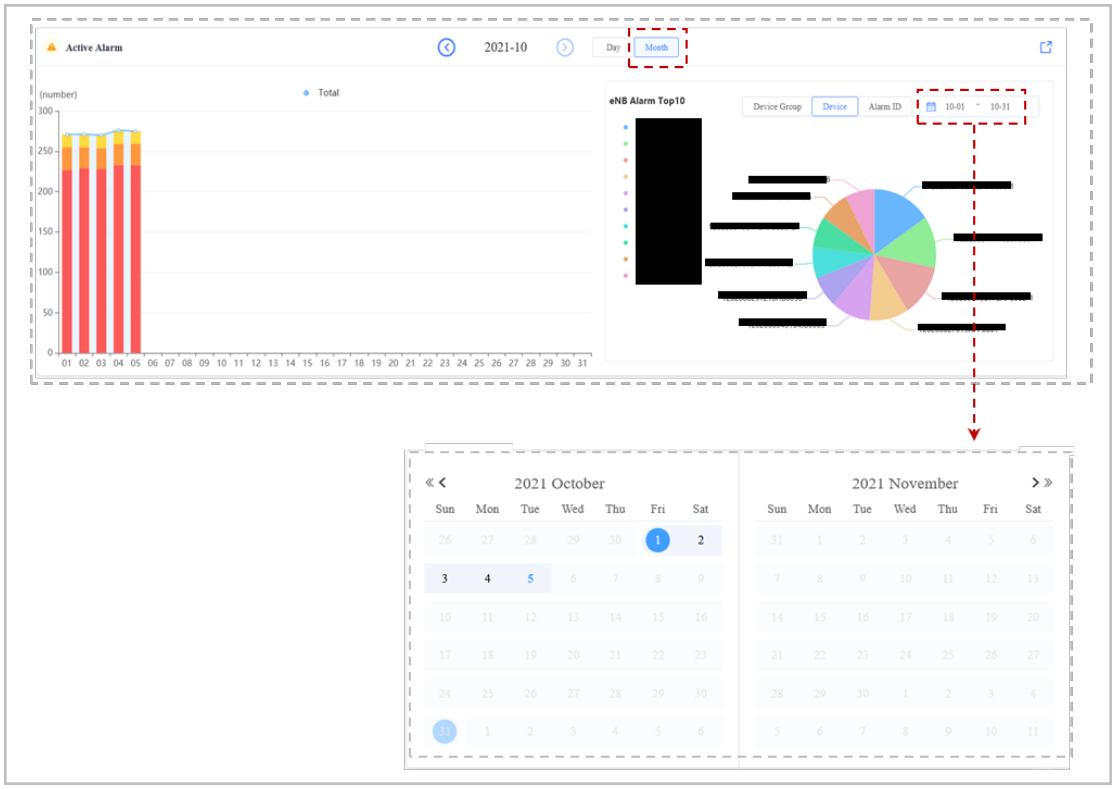


Figure 2-36: Active Alarm Pane - Full Calendar Month



2.4.1.4 Statistics

The last section of the dashboard displays aggregate eNB and CPE statistics (Figure 2-37). The graphs include the following:

- **eNB Active / Online** - number of active and online eNBs. Active refers to eNBs that are transmitting and receiving data. Online guides to eNBs that are operational but not actively transmitting or receiving data.

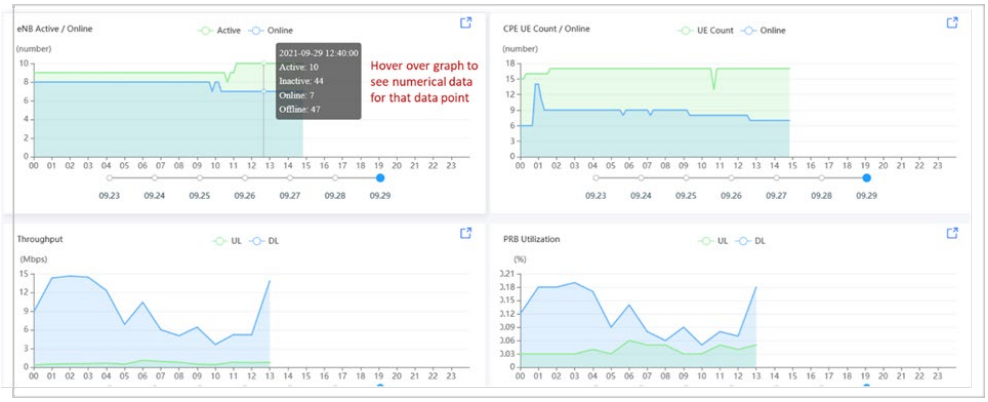
  NOTE: An offline eNB is not connected to the network or otherwise unavailable.

- **CPE UE Count / Online** - number of CPEs in the network and of those, the number of online CPEs
- **Throughput** - uplink (UL) and downlink (DL) throughput, in Mbps
- **PRB Utilization** - UL and DL Physical Resource Block (PRB) utilization. PRB is the smallest element of physical layer resource allocation assigned to each user by the LTE eNB scheduler.

The network elements sync with the OMC to refresh the data every 5 minutes.

The data displayed via the graphs cover a period of one week, the current day, and the previous 6six days. You can select which days to view using the timeline underneath each graph. To see the numerical data for any point on a graph, simply hover your cursor over the graph, and the information will pop up.

Figure 2-37: Dashboard Statistics



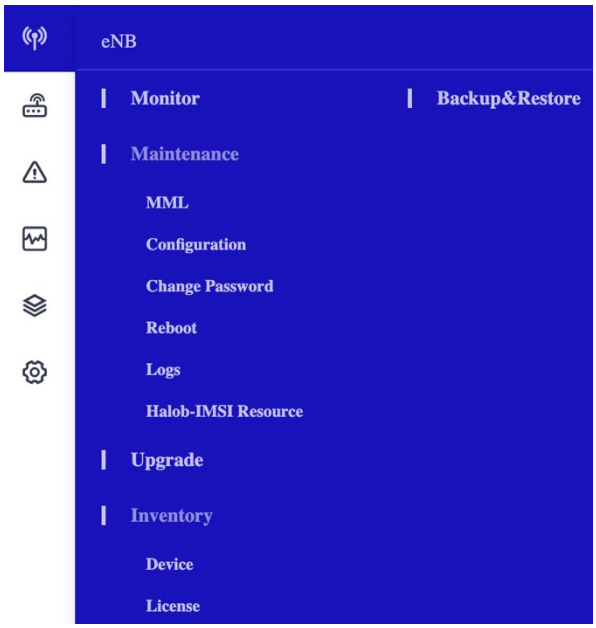
2.4.2 eNB Menu

2.4.2.1 Overview of Sub-Menus

The eNB menu provides essential functions for managing, monitoring, and maintaining eNBs in the operator's network (Figure 2-38).

NOTE: Some menu items are available only to Beta customers trailing new features.

Figure 2-38: eNB Menu



- **Monitor** - View all of the operator's eNBs that have connected with the OMC (*aka*, online), including their specifications, status, and operational measurements; perform quick operational actions and view aggregate eNB product and status graphs.
- **Maintenance** - Use MML commands or scripts to batch-configure eNBs, configure eNBs, change the password, create reboot and recurring reboot tasks, and collect logs.
- **Upgrade** – Upgrade or rollback the software image or download patch or FPGA files to multiple eNBs.
- **Inventory** – Add or delete eNB devices in OMC, manage HaloB eNBs, and manage feature licenses.
- **Backup&Restore** – Backup or restore eNB configuration.

2.4.2.2 Monitor

2.4.2.2.1 Landing Page Description

The *eNB > Monitor* window contains two tabs, Table (Figure 2-39) and Map (Figure 2-40), and the window opens first to the Table tab view. The table tab is described in more detail in *section 2.4.2.2.2 Table Tab*, and the map tab is described in *section 2.4.2.2.7 Map Tab*. See Table 2-3 for a description of the *eNB > Monitor* fields and Table 2-4 for *eNB > Monitor* graphs.

Figure 2-39: eNB > Monitor - Table Tab General Layout

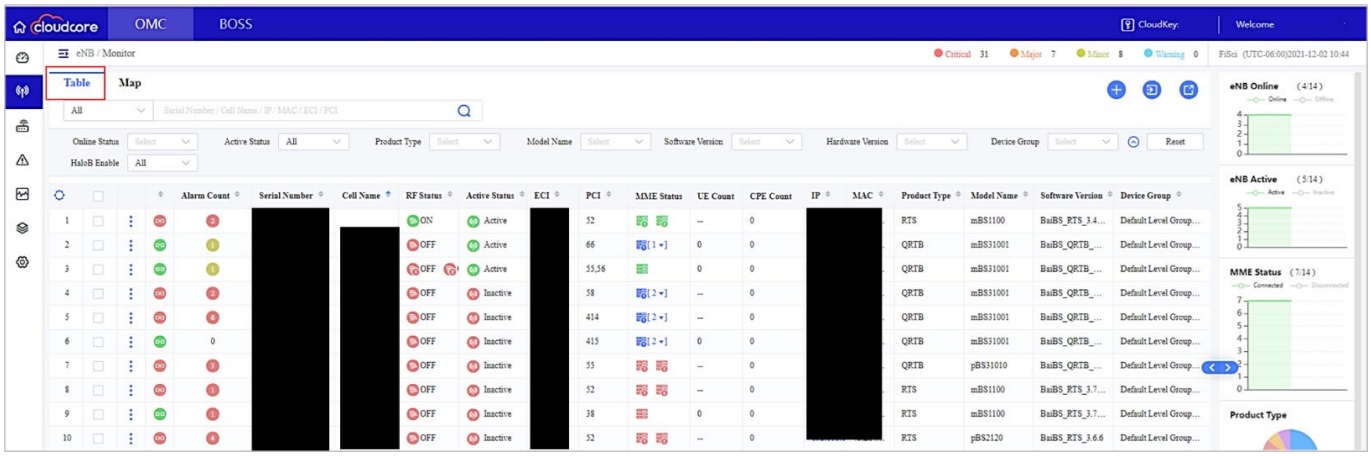
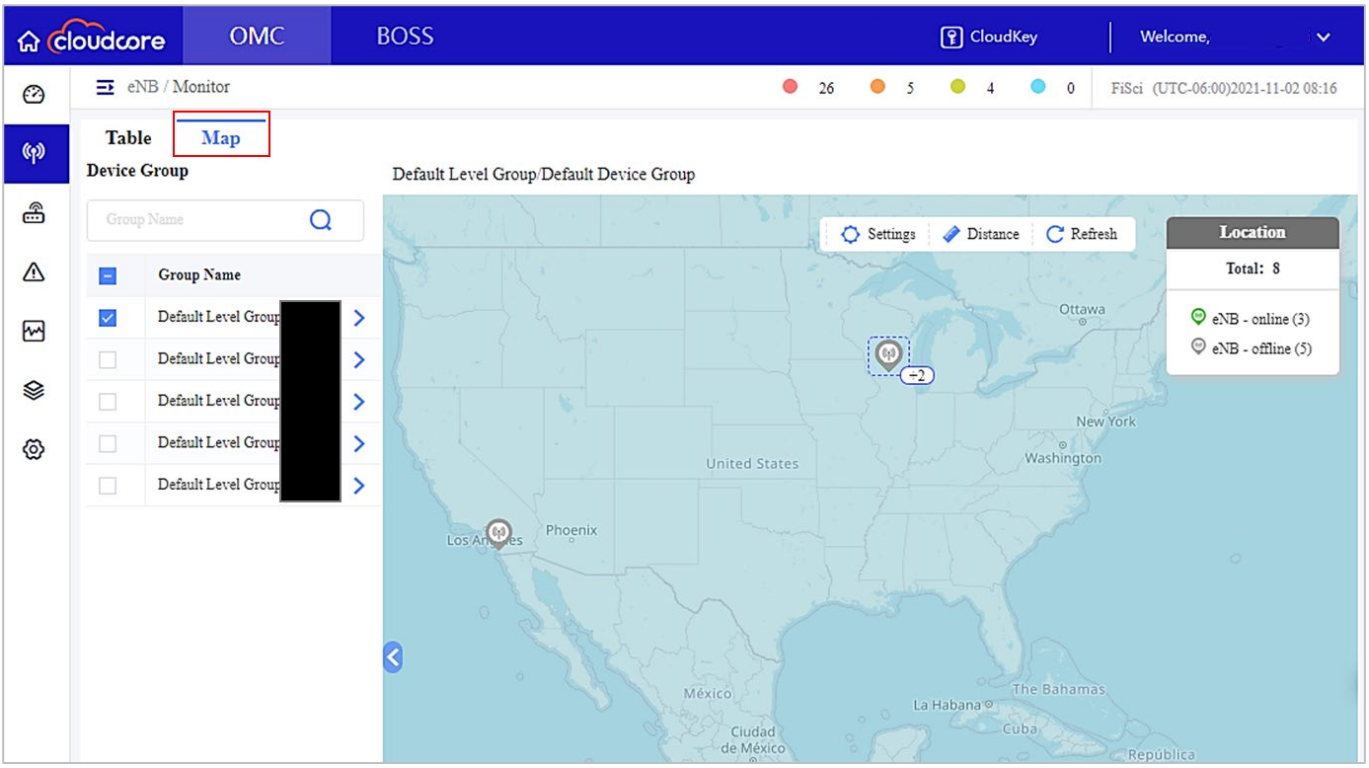


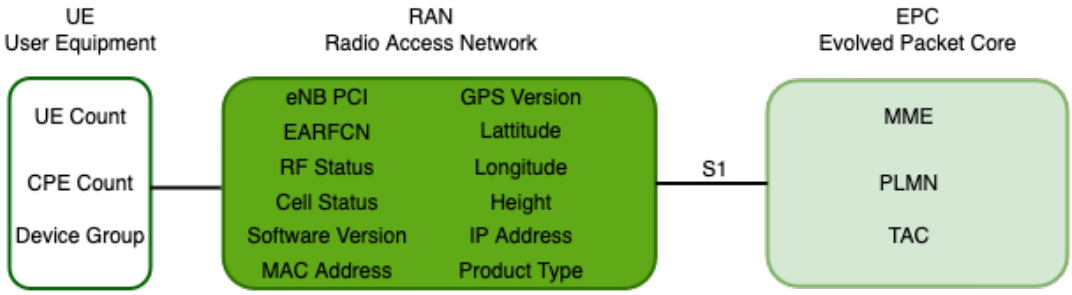
Figure 2-40: eNB > Monitor - Map Tab General Layout



2.4.2.2.2 Table Tab

The Table tab view displays a list of the operators' eNB devices. In the Table tab view, you can sort the eNB device list using the filtering fields across the top of the page; the pull-down options for each field are shown in Figure 2-42. The Table Tab shows various fields. Each field shown on the Table tab is associated with different functions in the LTE architecture. Refer to Figure 2-41 to identify each field to its function.

Figure 2-41: Table Tab Fields



The Table tab view has two main sections – the list of eNBs registered with the OMC, their individual stats on the left, and the graphs of aggregate eNB data on the right.

Figure 2-42: eNB > Monitor Table Tab

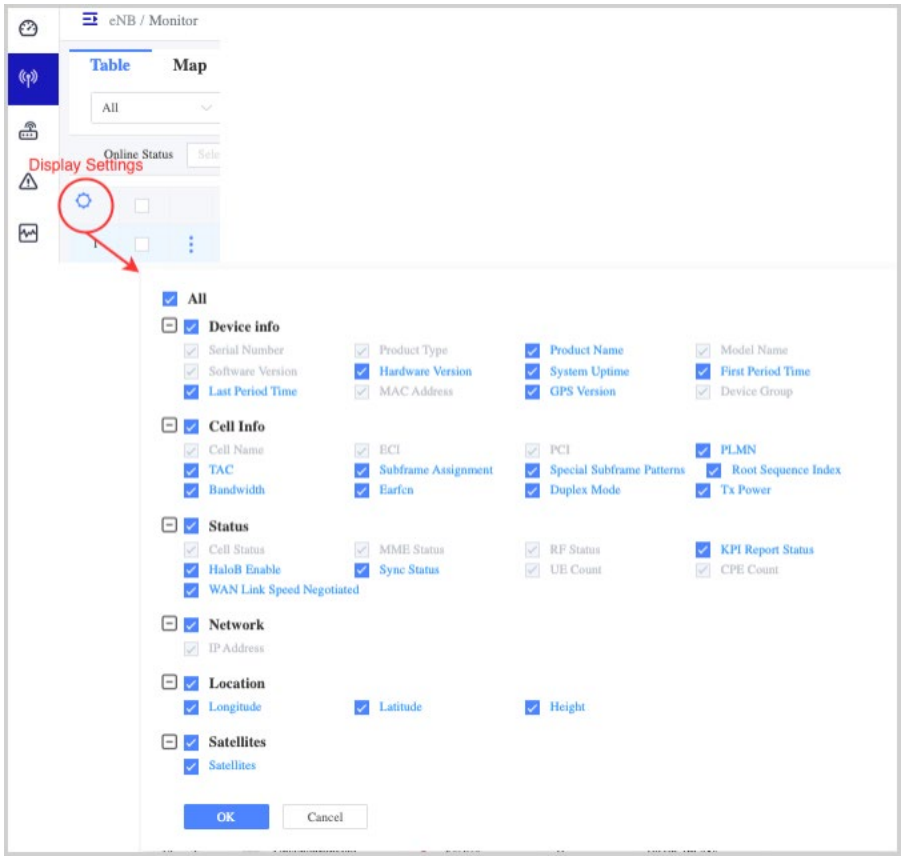
2.4.2.2.3 Display Settings

To manage which columns of information are displayed on the Monitor page, click on the Settings icon in the upper left of the window (Figure 2-43)

Select All to see all columns of information, or select specific column names, and click on *OK*. Refer to Table 2-3 *eNB > Monitor fields*, which follows, for a description of each column.

NOTE: Select All to view all the information of eNB and newly added features.

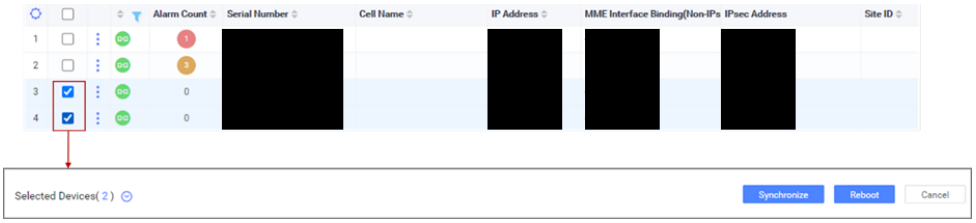
Figure 2-43: Display Settings

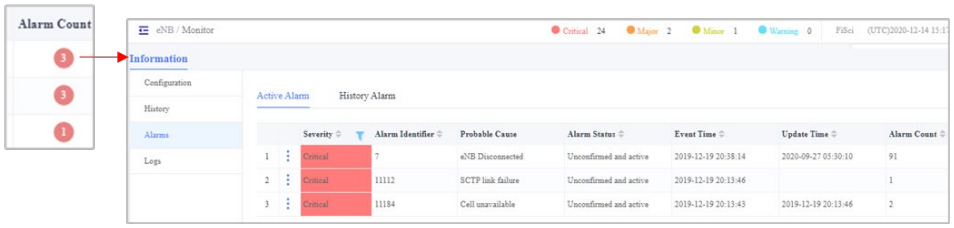
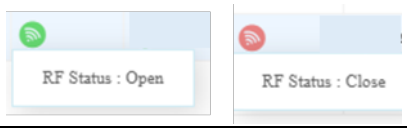


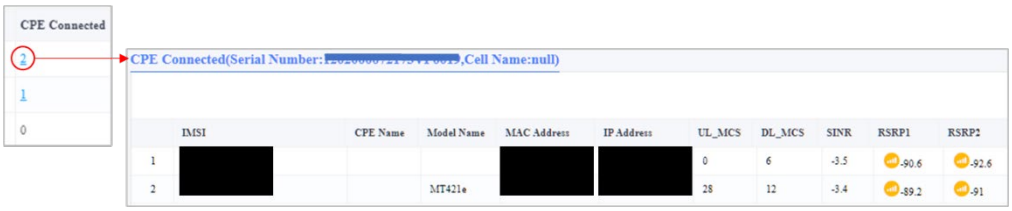
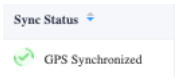
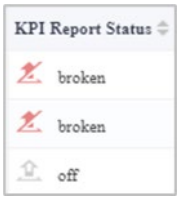
2.4.2.2.4 Field Descriptions

Table 2-3 describes each information column on the left side of the *eNB > Monitor* window.

Table 2-3: eNB > Monitor Fields

Field	Description
Checkbox	Select the checkbox for one or multiple eNBs to perform either a Synchronize action (eNB data to OMC display) or Reboot action from the Monitor page: 
Operations	Each row of eNBs has an Operations drop-down menu: Information, Settings, Actions. Each of these functions is described in *section 2.4.2.3.5 Operations.*
	Icons indicating an eNB's present status: The eNB is operating normally The eNB is offline Use the arrow at the top of the column to toggle the list by status.

Field	Description
Alarm Count	The number of alarms at each severity level. Click on the icon to open the *Operations > Information* tab for the selected eNB. eNB > Monitor ----------► eNB > Monitor > Operations > Information 
Serial Number	eNB serial number
Cell Name	Operator-configured eNB name
RF Status	Shows if the eNB's radio is on or off 
Cell Status	The eNB is active (operating - green icon) or inactive (not operating - red icon). 
ECI	E-UTRAN Cell Identifier - LTE standard network identifier is a number given to a unique cell site within the operator's network. One ECI represent multiple eNBs/PCIs on the same tower or other structure.
PCI	Physical Cell Identifier (PCI), or Layer 1 identity, is an essential configuration parameter of a radio cell that uniquely identifies each cell site in the wireless network. PCI planning is crucial for quality of service (QoS). The value can be only between (0-503) to avoid PCI confusion.
MME Status	The Mobility Management Entity (MME) plays a key role in CPEs mobility and access network. It verifies the authentication of UE to camp on operator's PLMN and initiates UE roaming restrictions. You can find the information on MME status and PLMN by clicking [2 ▾] or hovering. 
PLMN	Public Land Mobile Network ID which identifies the service provider for this eNB
Bandwidth	According to 3GPP specification, LTE supports four different bandwidth configurations such as 5 MHz, 10 MHz, 15 MHz, and 20 MHz

Field	Description
UE Count	Number of User Equipment (UEs/CPEs) actively connected to this eNB. Click on the number to display a list of the UEs and their information. 
CPE Count	Number of CPEs currently connected to the network. Click on the number to display the list of CPEs and their information. 
WAN Link Speed Negotiated	Negotiated speed between Ethernet ports (WAN and LAN ports). This field helps the operator locate speed issues on the networks.
IP	The eNB's current IP address. A clickable IP address feature is introduced to easily locate the IP.
MAC	The eNB's MAC address
Product Type	Auto populated eNB description used in OMC, e.g., RTS, RTD, QRTB, etc. The descriptions refer to the software stream name used on this product. For a description of all product types, refer to *Table 2-5 Product Types / Software Streams*.
Product Name	The name of the Baicells eNB
Model Name	The name of the eNB equipment model, which functions like a part number
Software Version	Software version currently running on the device
Device Group	The device group the eNB is assigned to by the operator. If no custom device groups have been created, the eNB will be assigned automatically to the default device group.
Earfcn	EARFCN frequency the eNB is currently using
Sync Status	The eNB is either synchronized or unsynchronized with other eNBs in the same cell 
KPI Report Status	The Key Performance Indicators (KPI) report status is normal, broken, or off. 
Satellites	The number of GPS satellites found and reported by the eNB. Note that some eNB models do not support this reporting function.
System Uptime	Length of time this eNB has been operational - dd:hh:mm:ss

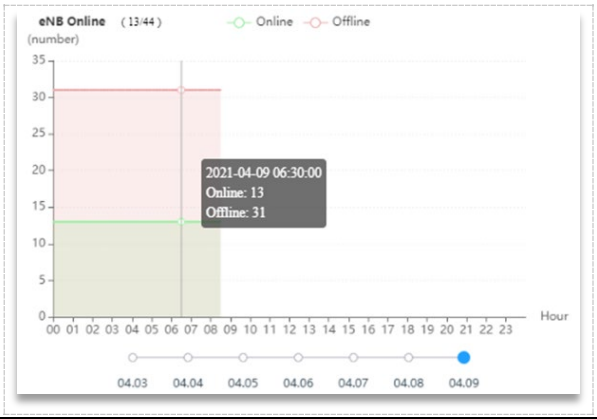
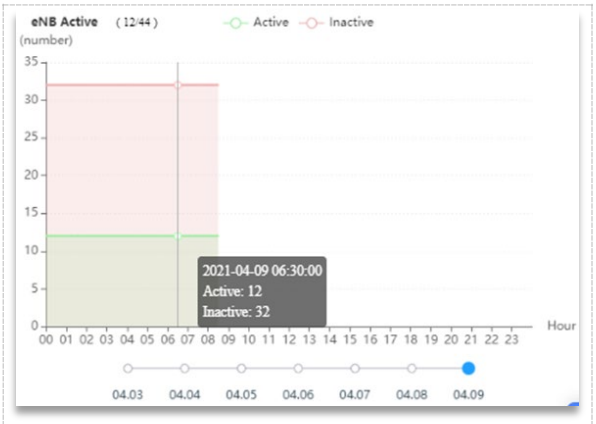
Field	Description
First Period Time	The first day and time the OMC got an inform message from the eNB, i.e., that it is online
Last Period Time	The last updated day and time the OMC got an inform message from the eNB, e.g., is offline
Duplex Mode	LTE duplexing scheme used on this eNB, either TDD or FDD
Hardware Version	The version of hardware in this device
GPS Version	GPS software version currently being used
HaloB Enable	The HaloB feature is either on or off. For more information about HaloB, refer to the *HaloB User Guide*.
TAC	Tracking Area Code ID used to identify a geographical area within the operator's network coverage area
Subframe	In TDD, DL and UL are organized into radio frames of 10 ms each. Each frame duration contains 10 equal sub-frames the duration of each is 1 ms
Special Subframe	TDD mode must switch transmission from DL to UL and UL to DL, therefore a special subframe is required between transmissions.
Root Sequence Index	This allows UE to calculate which PRACH preamble it can use to attach to the eNB.
Longitude	The eNB's longitude coordinate
Latitude	The eNB's latitude coordinate
Height	The eNB's antenna height, in meters
Tx Power	The transmission power is set at the eNB when the RF transmission is active. Depending on the mode of operation indoor or outdoor, the transmission power varies from 24 dBm to 30 dBm (100 mw). If the eNB is not in active transmission (i.e., RF status is inactive), then the transmission power is set to 0 dBm.

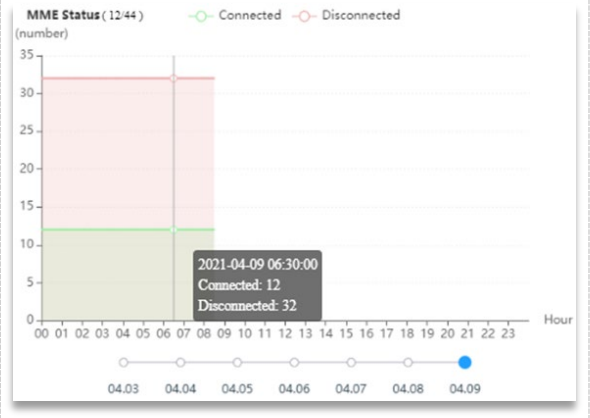
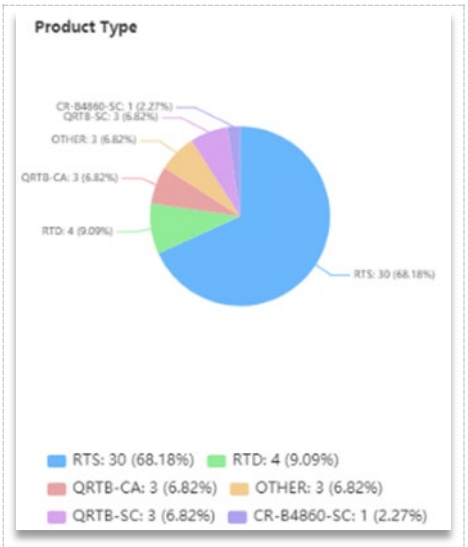
2.4.2.2.5 Graph Descriptions

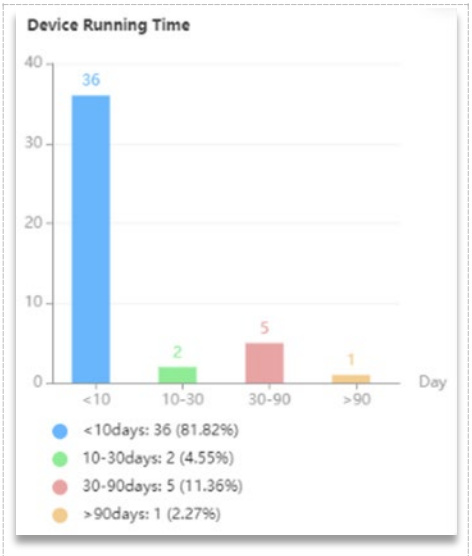
When you expand the right side of the *eNB > Monitor* window, you will see five graphs showing aggregate eNB data for all eNBs in the operator's network. The time window for the three main x-y graphs is one week, from the current date and back six days.

When you select a specific day in the timeline under the eNB Online, eNB Active, or MME Status graphs, all three graphs simultaneously update. Likewise, hovering over one of these three graphs will display the numerical data for that hour on all three. Refer to Table 2-4 for a description of each graph.

Table 2-4: eNB > Monitor Graphs

Graph	Description
eNB Online/Offline	Shows how many of the operator's eNBs are online, that is, operational but not currently transmitting or receiving data; and/or how many are offline, that is, not connected to the network or otherwise unavailable to provide service. Hover your cursor over the graph to see numerical data for that data point. In the lab example below, the graph indicates that there are 44 eNBs in the network, with 13 of those online and 31 offline on April 9. 
eNB Active/Inactive	Indicates how many eNBs are actively transmitting or receiving data and/or how many eNBs are inactive. Any eNBs that are reported as inactive means they are online but not currently active. Hover your cursor over the graph to display the numerical data for that data point. 

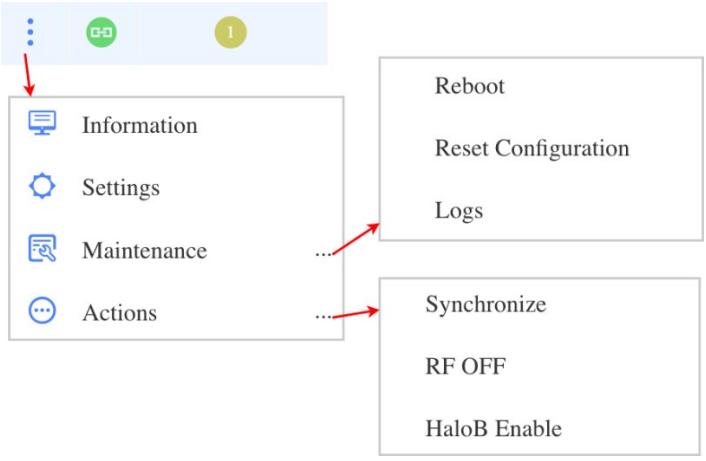
Graph	Description
MME Status	The Mobility Management Entity (MME) is one of the core LTE network components with which the eNBs interface for user management. This graph pertains to the number of eNBs that were successfully connected to, and/or were disonnected from, the MME. Hover your cursor over the graph to display the numerical data for that data point. NOTE: An eNB operating in HaloB mode has embedded MME functionality and does not use the S1 signaling interface to the core network. 
Product Type	The pie chart shows the distribution of the operator's eNBs based on which software stream they use, e.g., RTS, RTD, QRTB-CA (Carrier Aggregation), QRTB-DC (Dual Carrier), etc. 

Graph	Description
Device Running Time	Summarizes how long eNBs in the network have been online 

2.4.2.2.6 Operations

Use the Operations menu to configure each eNB to the operator's preferred settings. The menu opens are Settings, Maintenance, and Actions (Figure 2-44). Each menu item is explained below.

Figure 2-44: Operations



2.4.2.2.6.1 Information

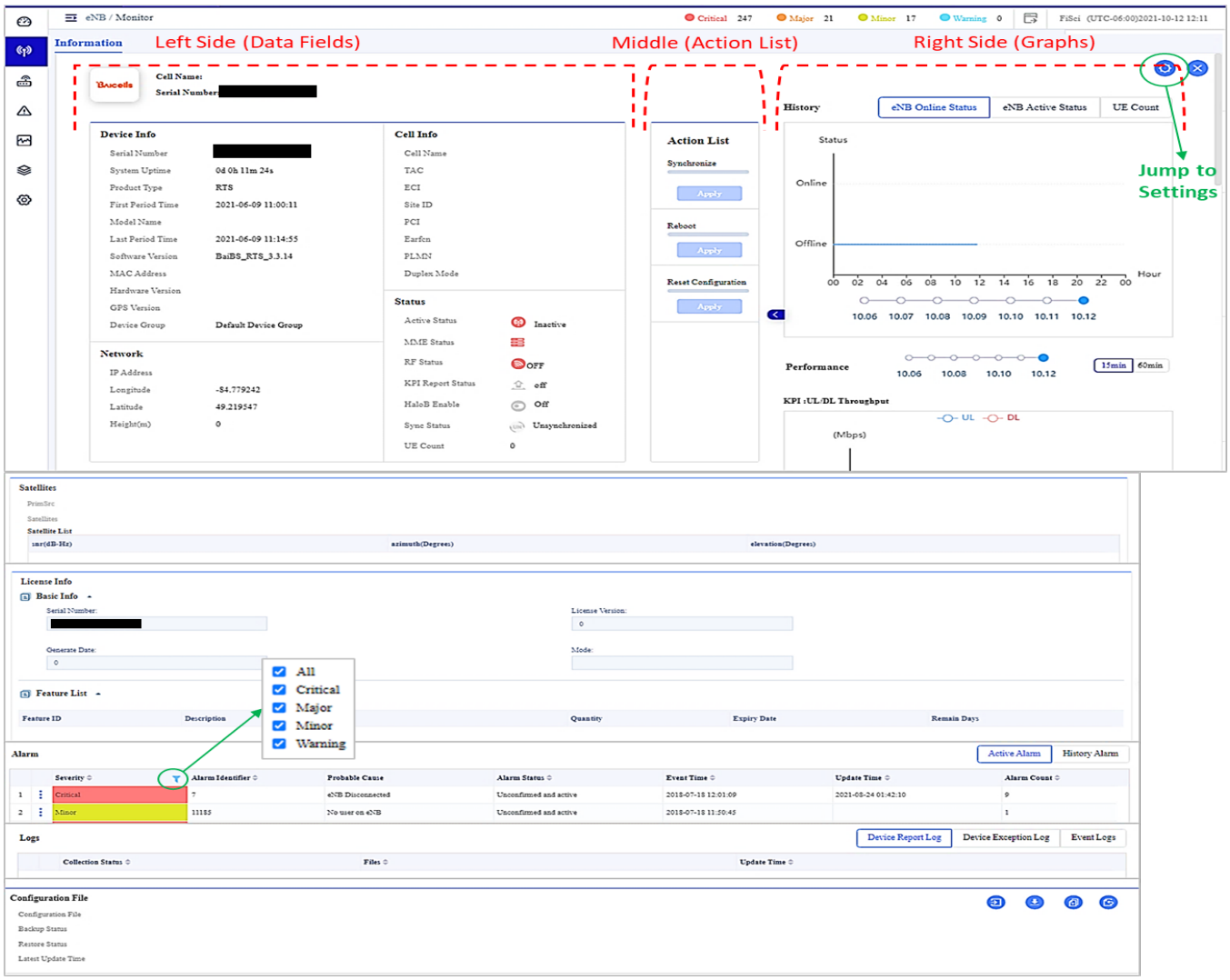
An overview of all the eNB information is shown here. A quick view of this will outline the status of the eNB. As shown in the *Operations > Information* window's left side displays data about the eNB - its cell name and serial number, device information, cell information, network information, status, satellite information, licenses, features, alarms logs, and configuration file. In the middle of the window is the Action List. The action allows you to synchronize, reboot, and reset the configuration of the eNB. The right side contains information about the eNB in the graphs described below. The data is the same information you see on the main *Monitor* page, as described in Table 2-3 *eNB > Monitor Fields* in *Field Descriptions,* but it is visually organized in categories.

As with information on the Monitor page, the eNB's data is synced with the OMC every 5 minutes. To check when the OMC last received an eNB's information, refer to the Last Period Time field under the Device Info pane. The First Period Time is when the eNB first sent an Informed message to the OMC to let them know it was online.

NOTE 1: Not all licensed features are available on all eNB models.

NOTE 2: Some licenses are issued by quantity, and some have expiration dates. The OMC will generate an alarm (ID 13) 30 days before the license expiration.

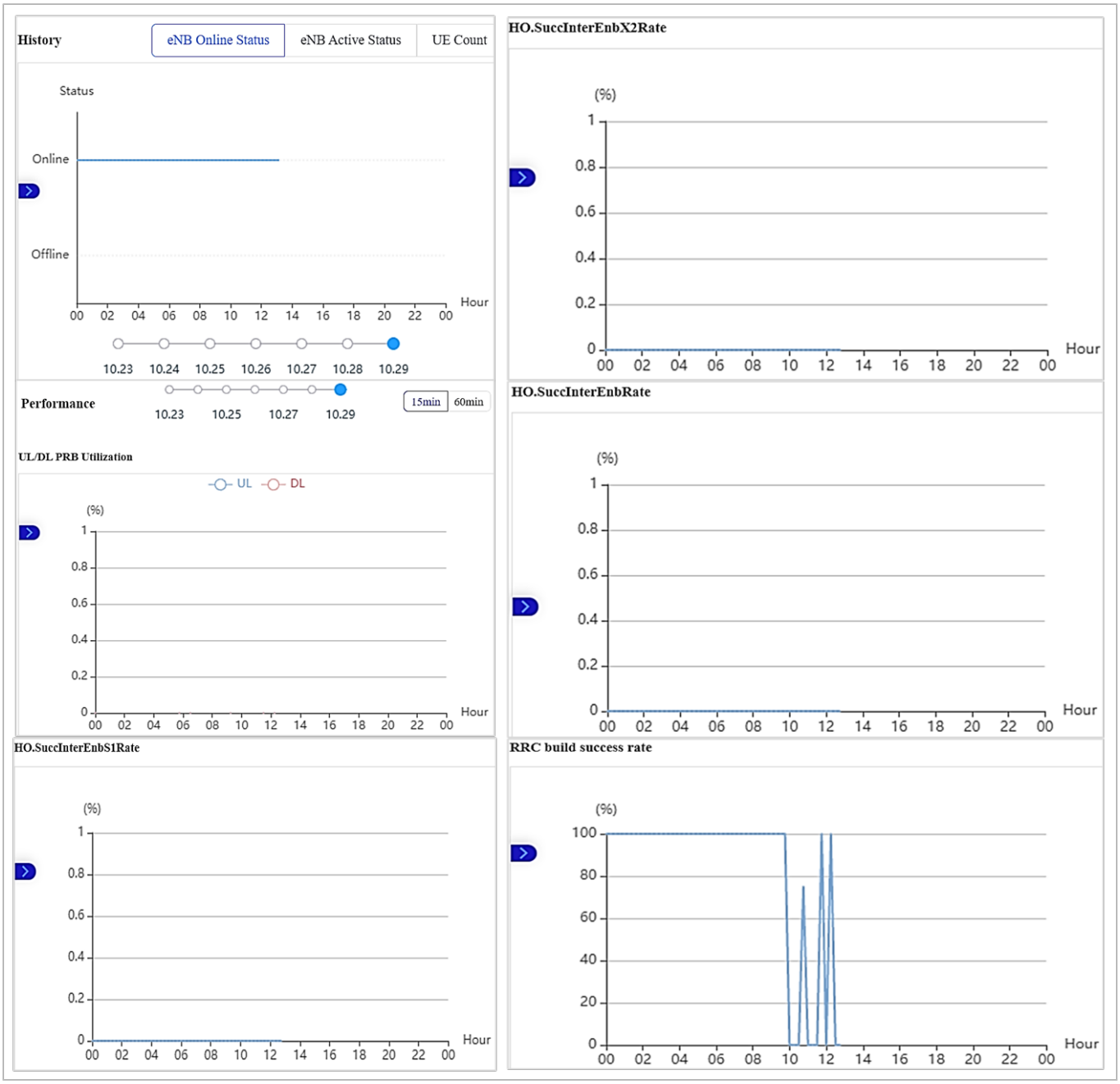
Figure 2-45: Information (Left Side and Middle)



Clicking on the blue arrow  between the left and right side of the Information window opens the graphs section (Figure 2-46). The History graph reports online status, active status, and UE count for the selected eNB. Beneath the History graph is the Performance graphs. The LTE Key Performance Indicators (KPI) comprise several measurements that indicate an eNB's operational performance. Which graphs are presented depends on the KPI template(s) assigned to the eNB in the Performance menu. See *section 2.4.5 Performance Menu* for more information about the Performance menu.

*NOTE: The Performance menu is typically used by customers trialing OMC features and by operators using a private network version of OMC, referred to as "Local OMC."

Figure 2-46: Graphs (Right Side)



2.4.2.2.6.2 Settings

Reference: *eNodeB Configuration Guide*

The *Operations > Settings* function is how you configure or change an eNB's settings through CloudCore. You can configure the eNB through the eNB GUI and CloudCore GUI. Refer to the eNodeB Configuration Guide above to get a detailed description of the parameters in the settings to configure each eNB.

Caution: In the Network settings window, it is highly recommended to leave the Advance Setting fields with their default values. Improper changes will lead to system exceptions.

Note: A few features in the settings will be displayed only when the eNB status is active, and RF is ON.

- *RTS Product Type Settings*

  Click on the *Operations* > *Settings* to view the Settings tab for the RTS product type. There are four main settings: Basic (Figure 2-47), Network (Figure 2-48), LTE (Figure 2-49), and eNB (Figure 2-50).

Figure 2-47: Basic Tab

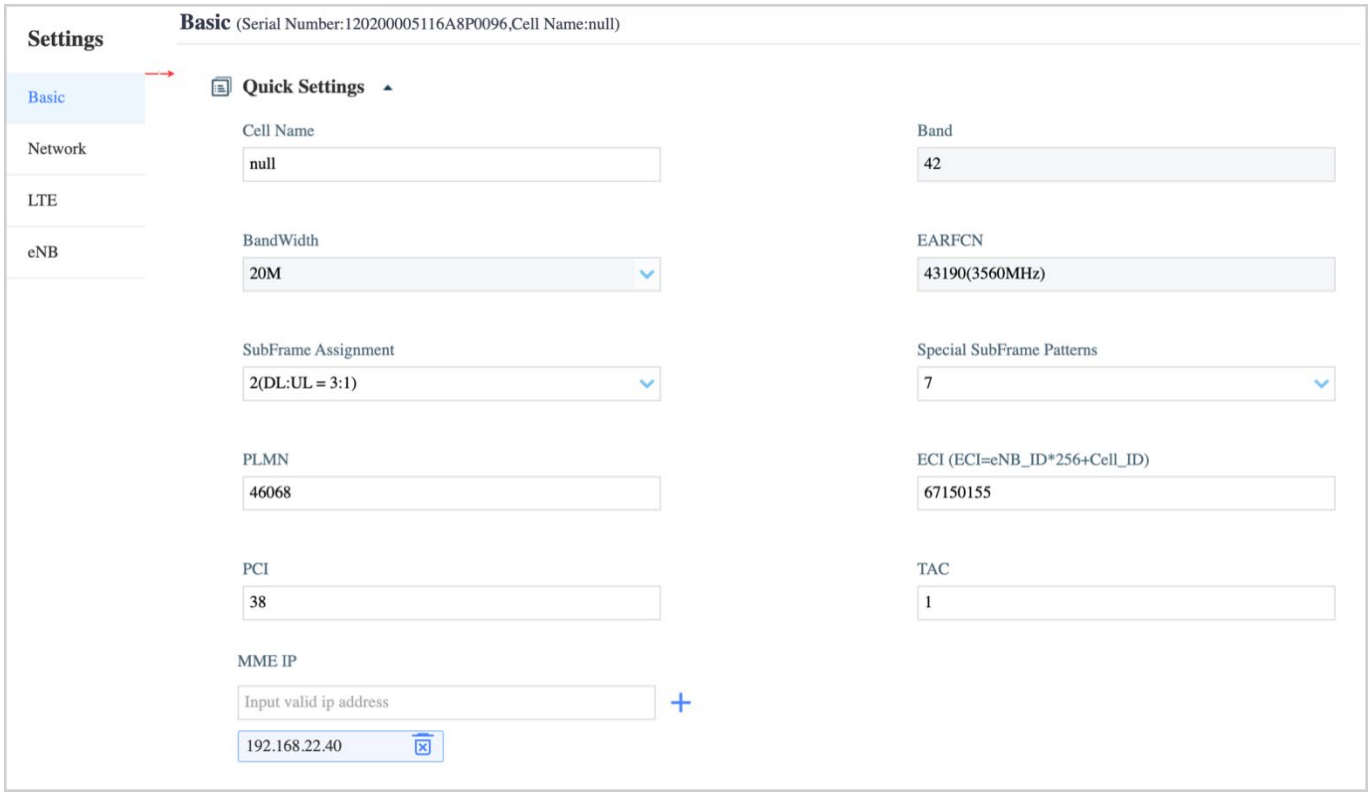


Figure 2-48: Network Tab

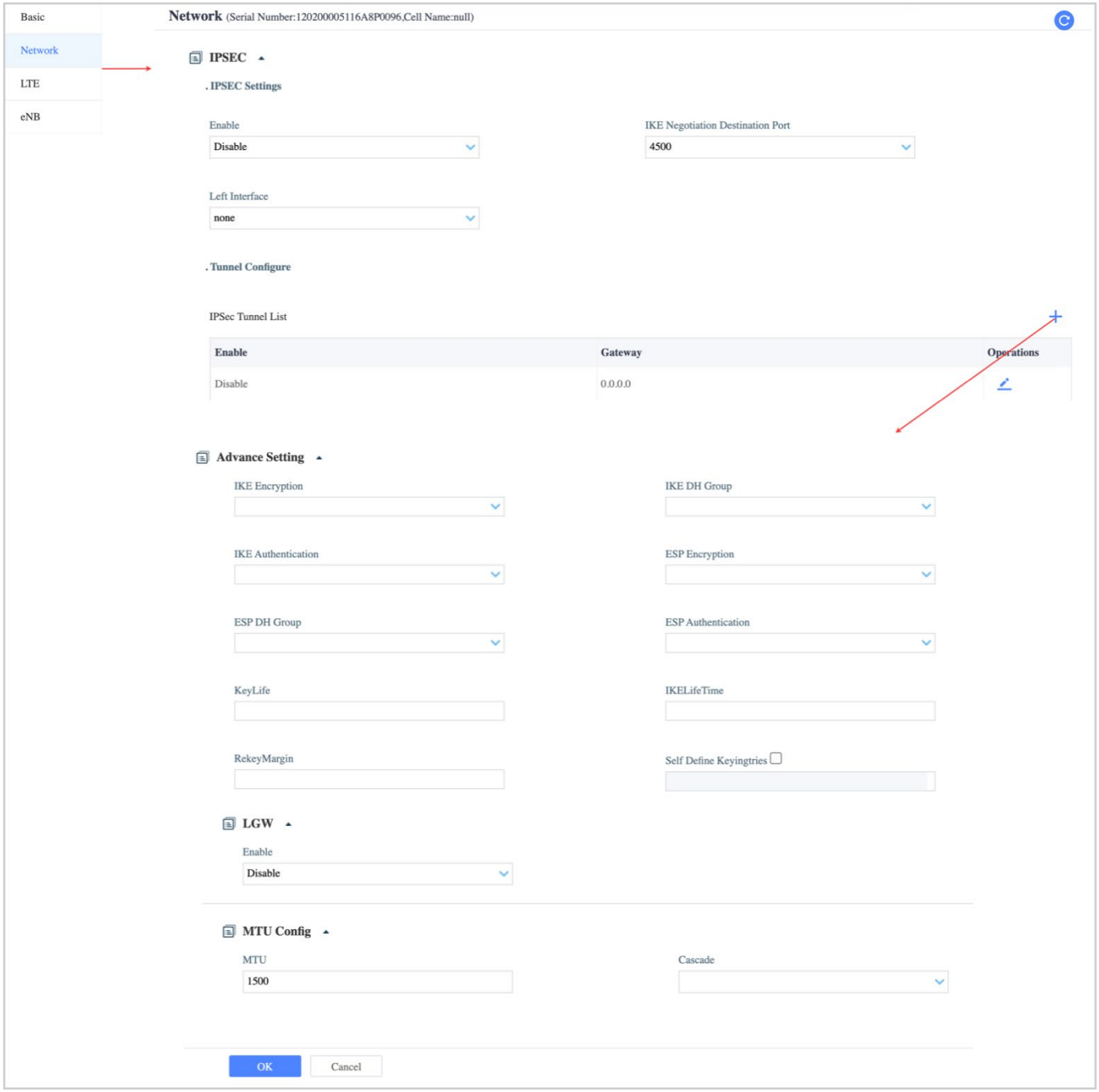


Figure 2-49: LTE Tab

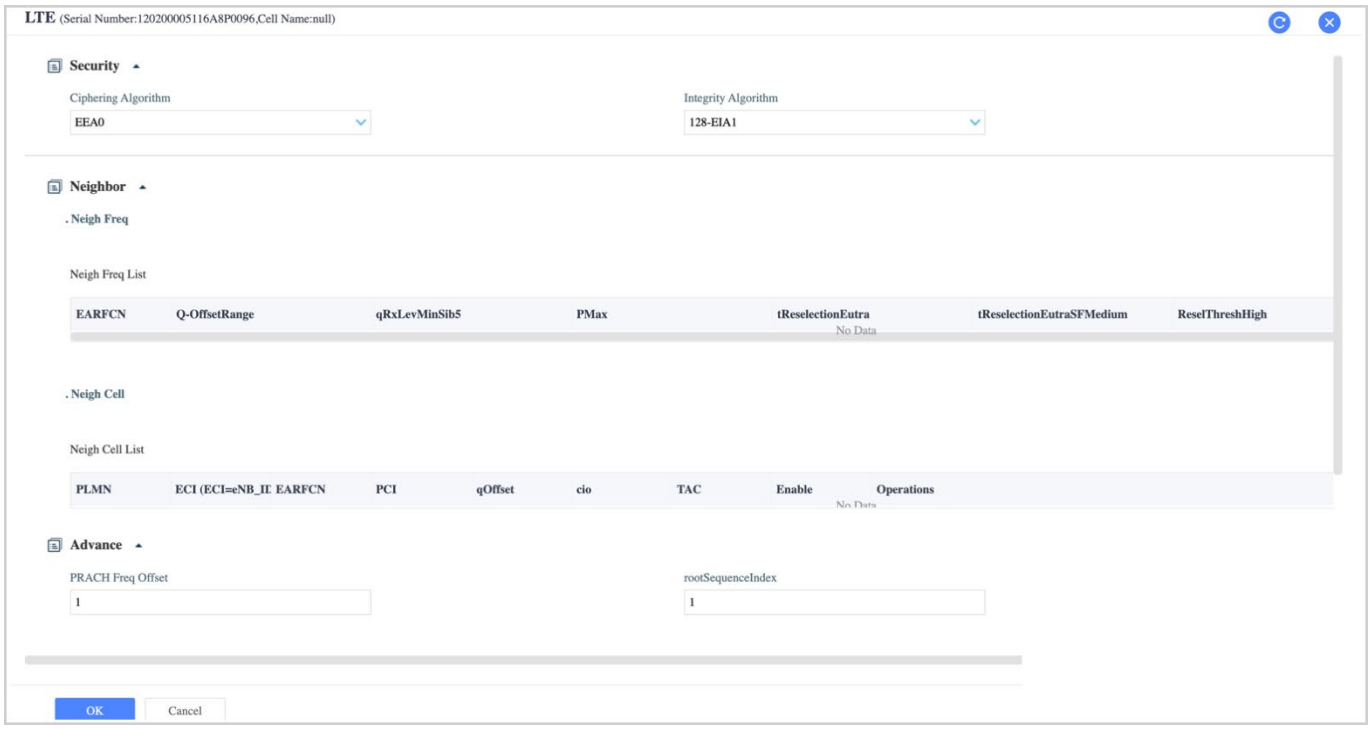
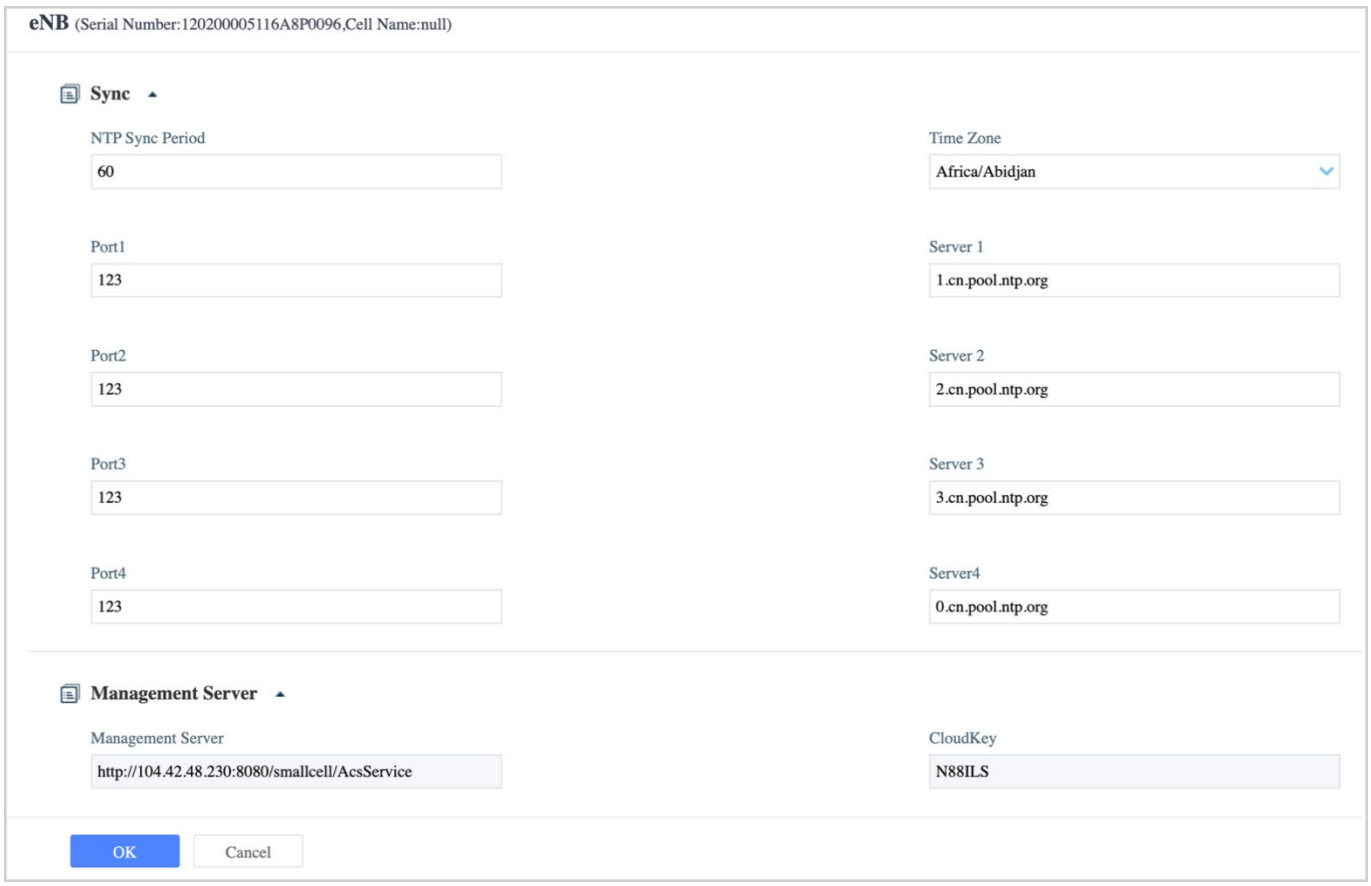


Figure 2-50: eNB Tab



- *QRTB Product Type Settings*

  Click on the *Operations > Settings* to view the Settings tab for the QRTB product type. There are four main settings: Quick Settings (Figure 2-51), Network (Figure 2-52), LTE (Figure 2-53, Figure 2-54, Figure 2-55, and Figure 2-56), and BTS (Figure 2-57, Figure 2-58, and Figure 2-59).

Figure 2-51: Quick Settings Tab

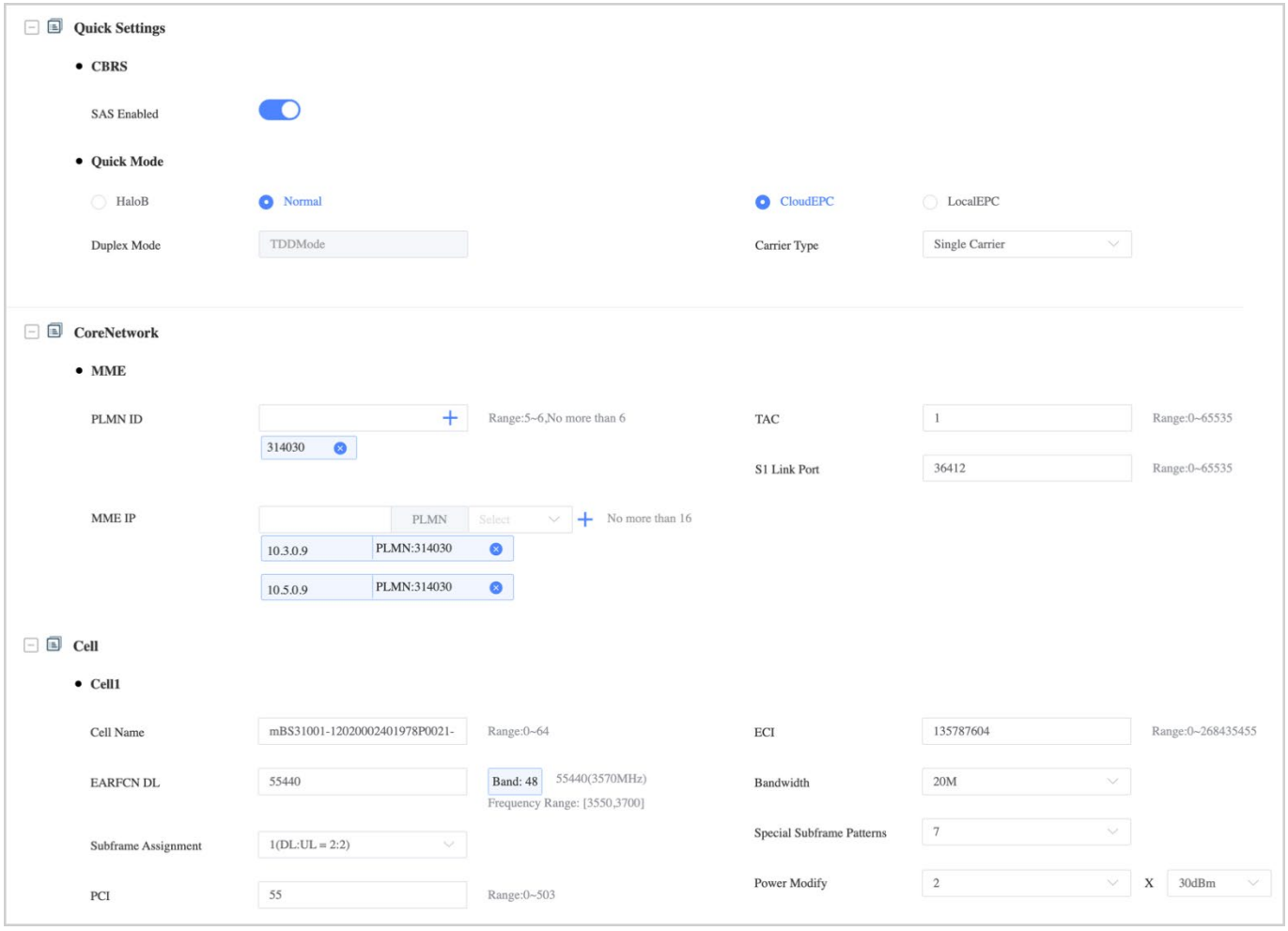


Figure 2-52: Network Tab

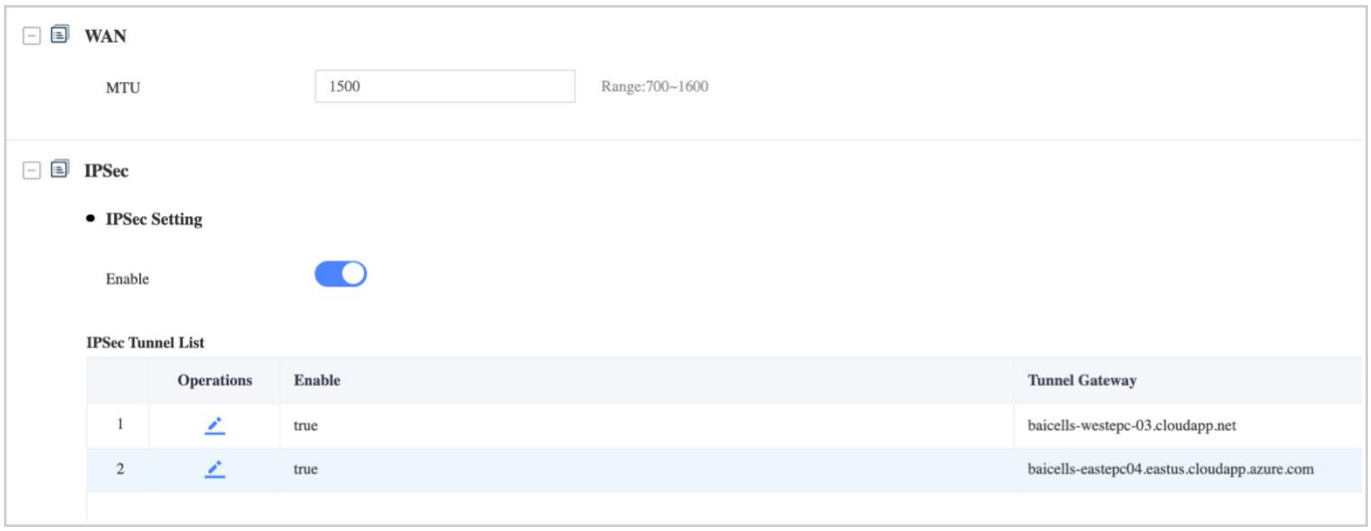


Figure 2-53 LTE Tab (1 of 4)

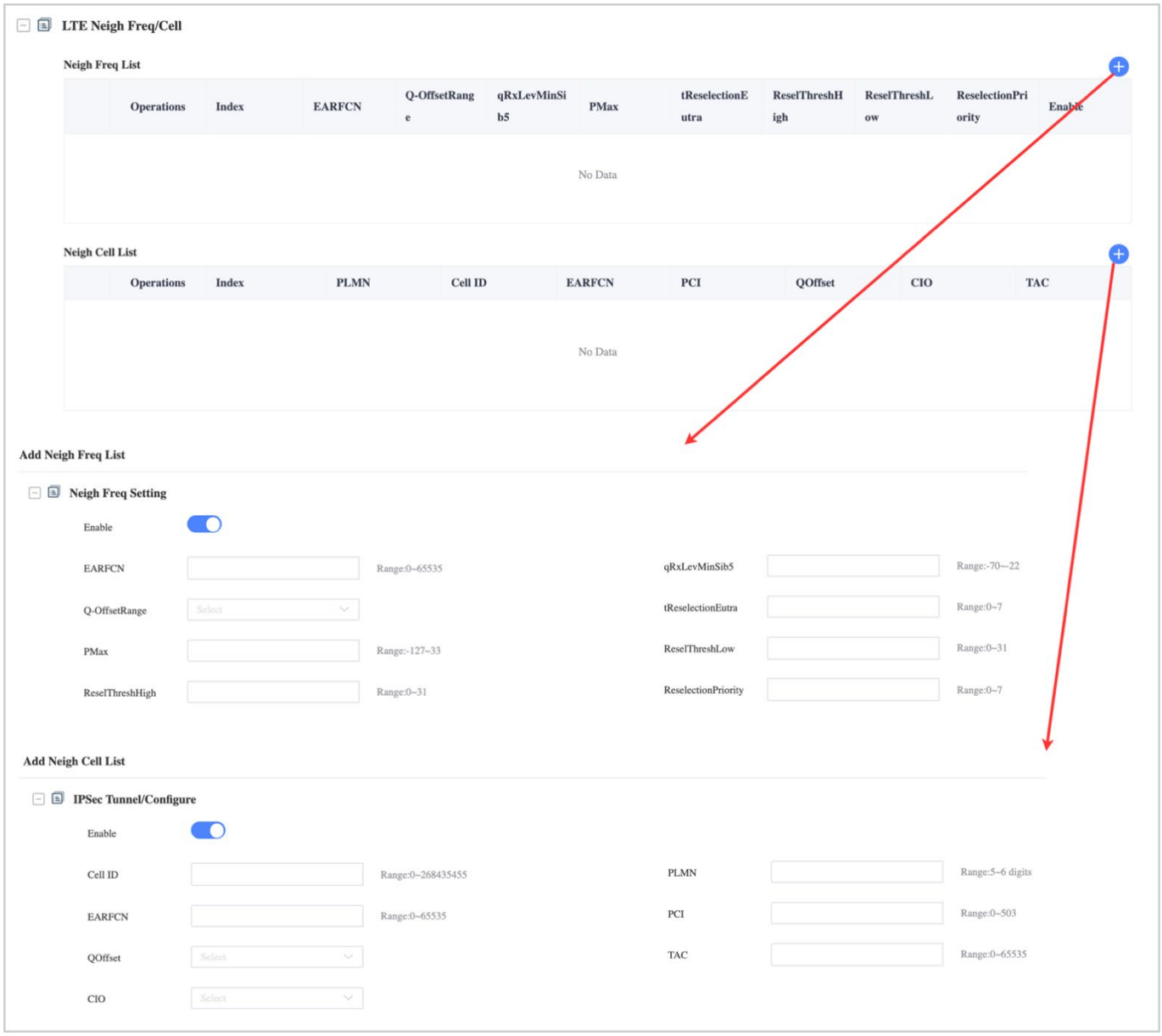


Figure 2-54: LTE Tab (2 of 4)

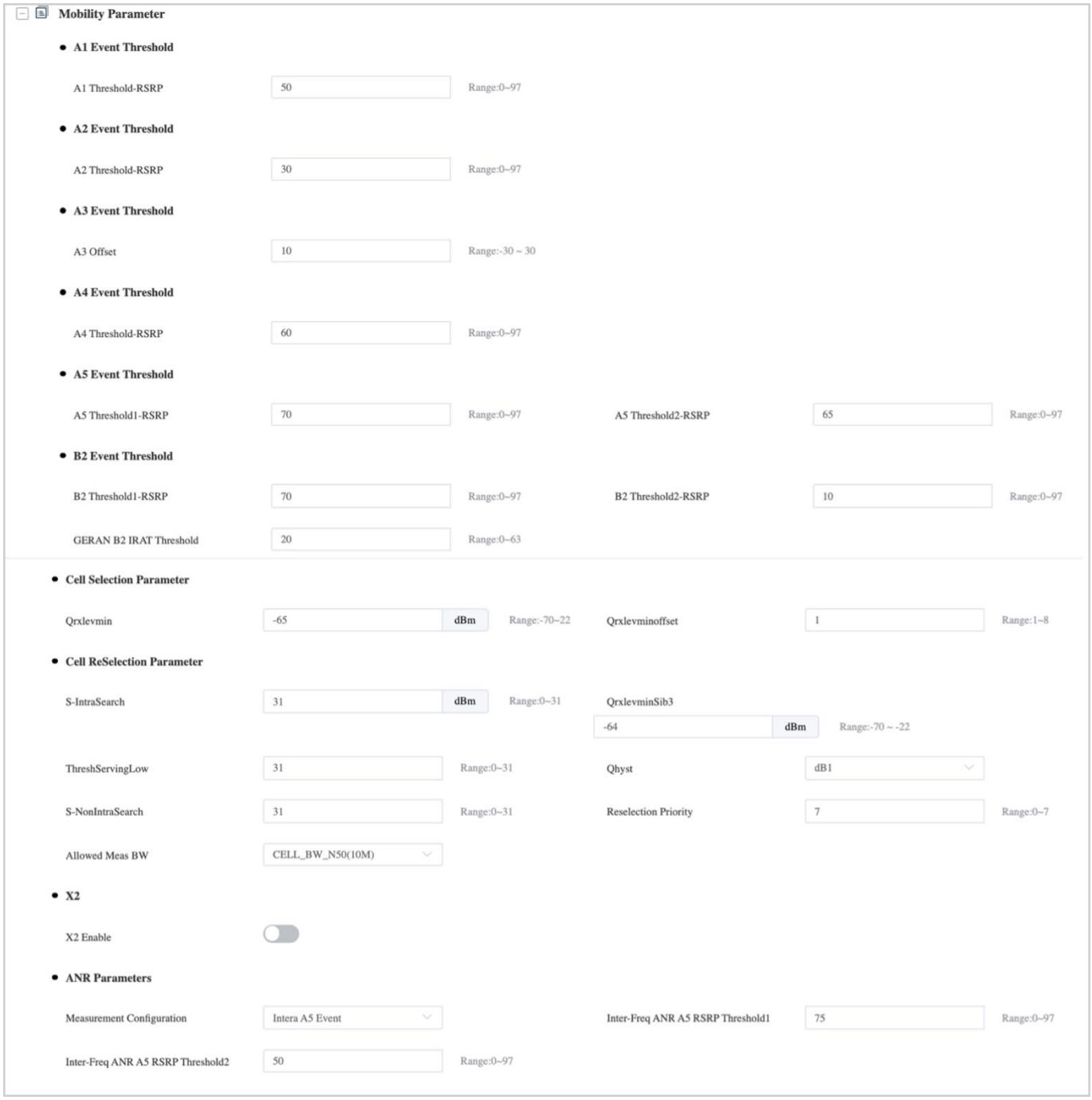


Figure 2-55: LTE Tab (3 of 4)

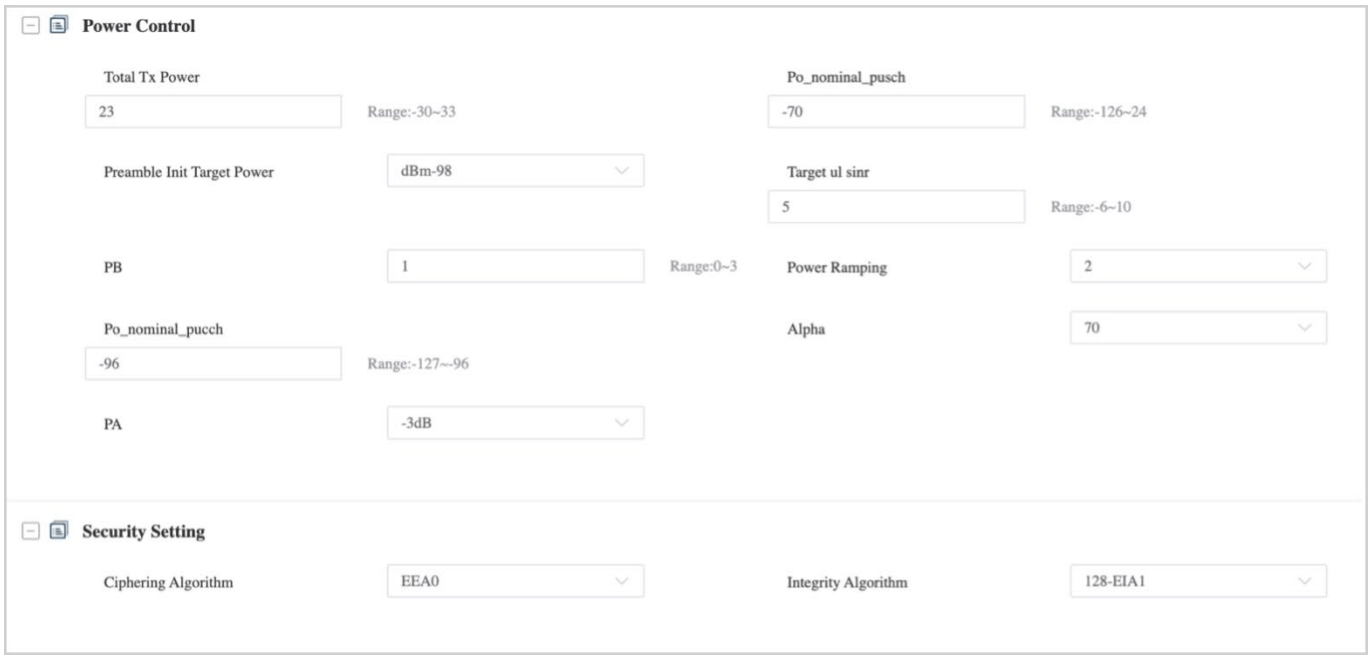


Figure 2-56: LTE Tab (4 of 4)

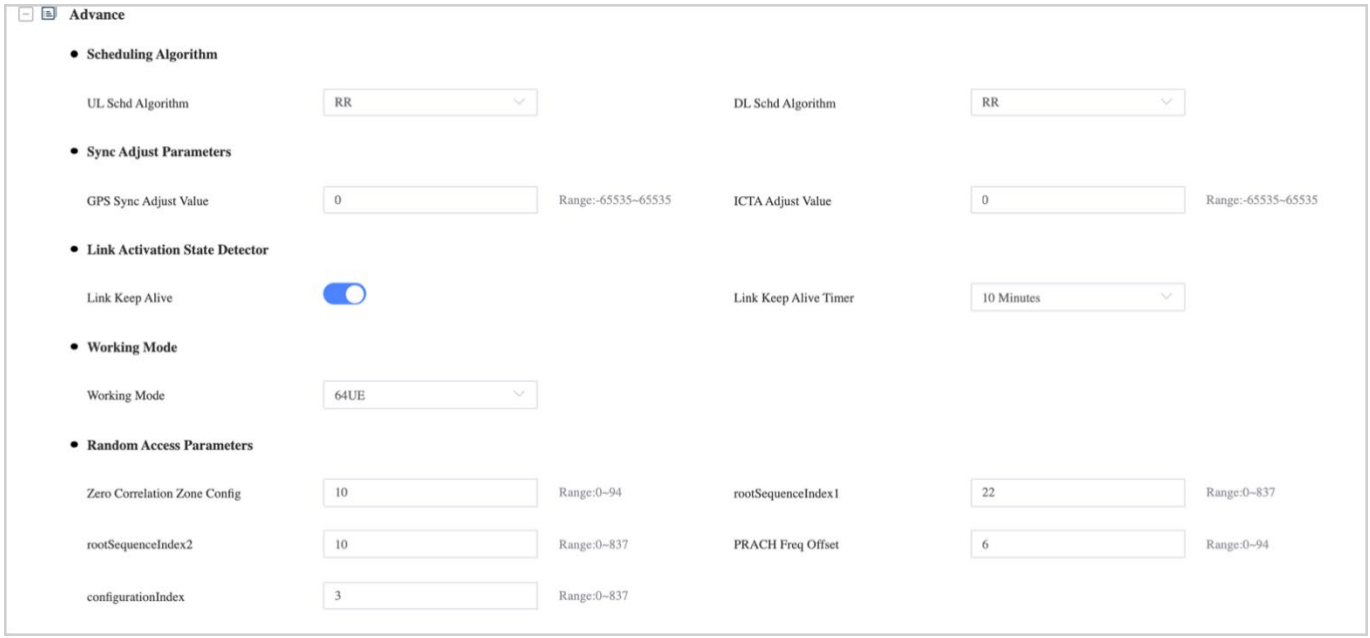


Figure 2-57: BTS Tab (1 of 3)

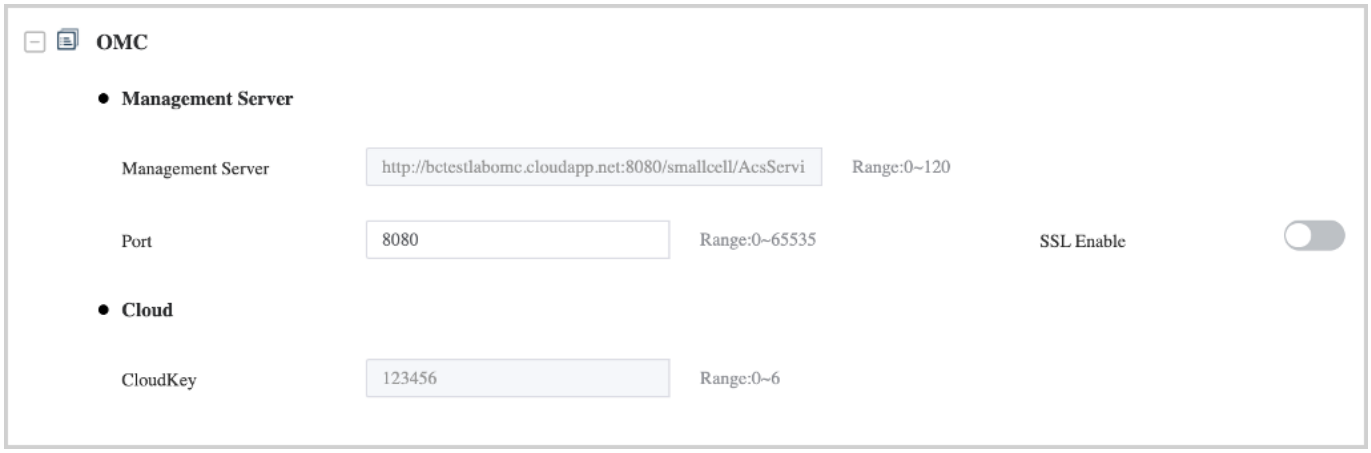


Figure 2-58: BTS Tab (2 of 3)

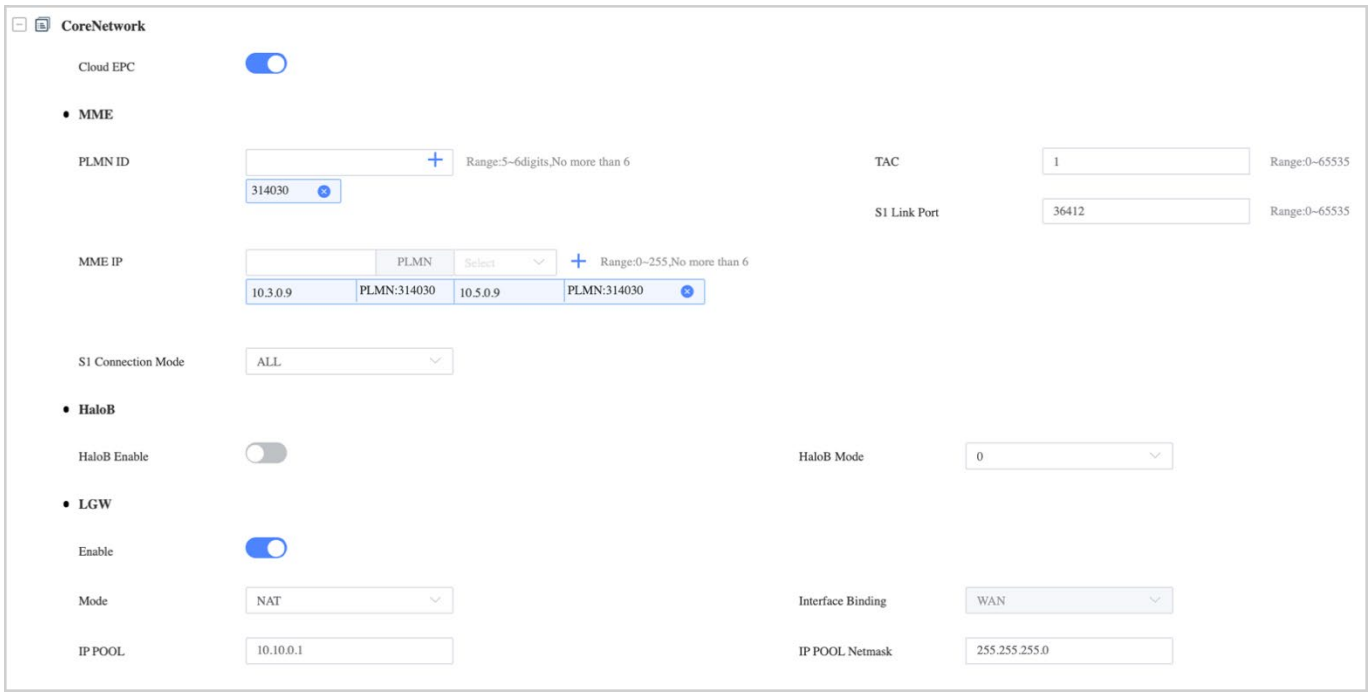
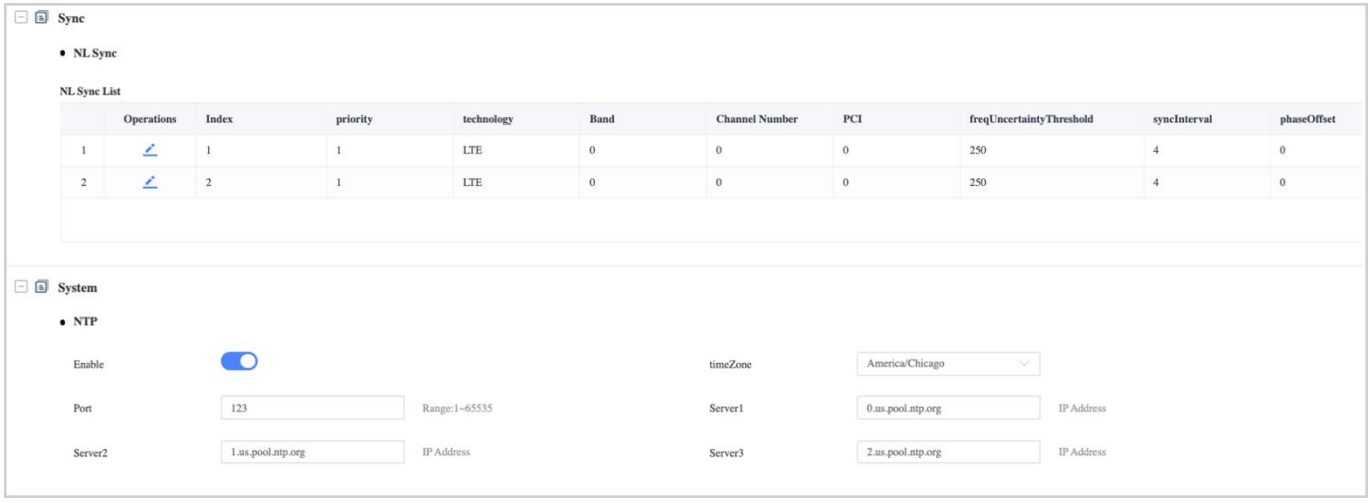


Figure 2-59: BTS Tab (3 of 3)



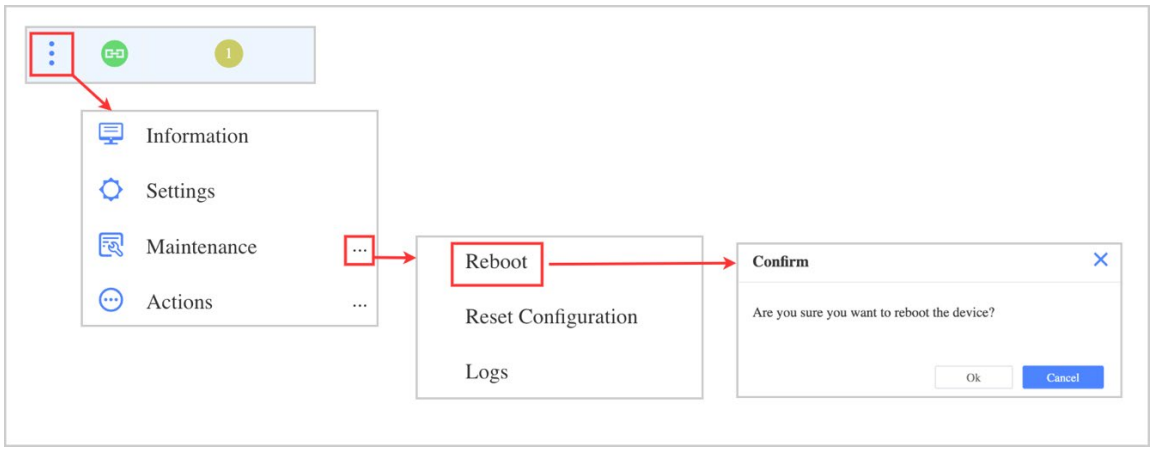
2.4.2.2.6.3 Maintenance

The *Operations* > *Maintenance* function perform quick maintenance actions for a selected eNB. Maintenance actions include *Reboot*, *Reset Configuration,* and *Logs*.

- Reboot

  To reboot an eNB, select *Operations* > *Maintenance* > *Reboot.* When the confirmation dialogue box opens, click *Ok (*Figure 2-60).

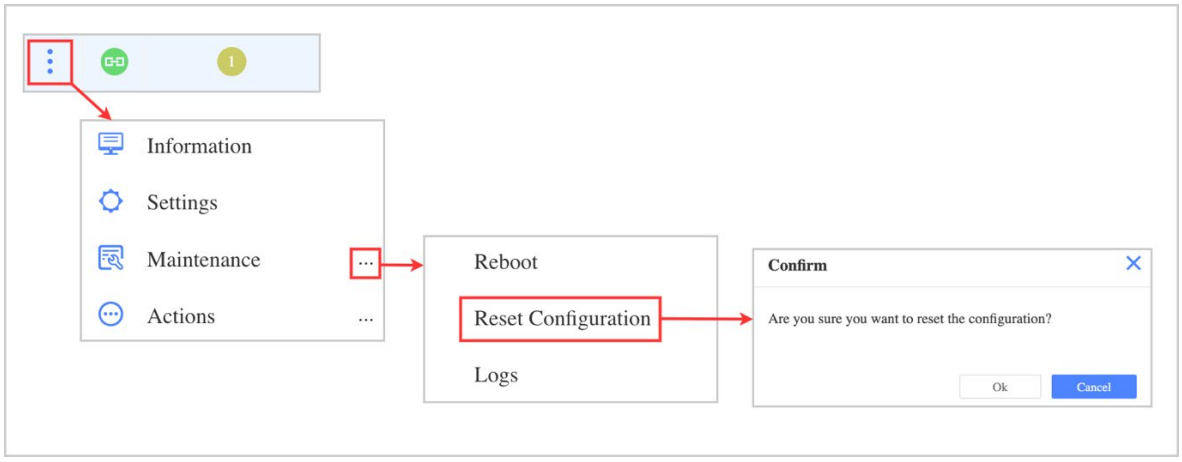
Figure 2-60: Reboot



- Reset Configuration

  You can reset an eNB to its default settings by selecting *Operations* > *Maintenance* > *Reset Configuration*. When the confirmation dialogue box opens, click *Ok (*Figure 2-61).

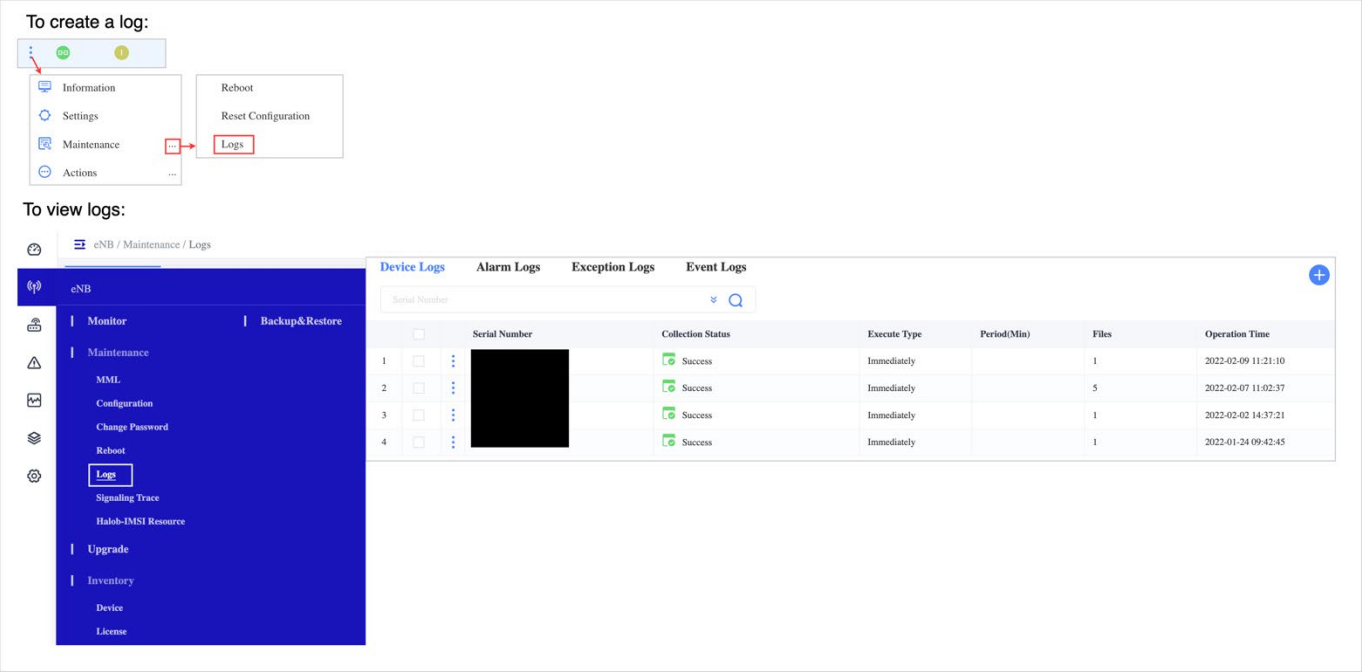
Figure 2-61: Reset Configuration



- Logs

  To create a device log for an eNB, select *Operations* > *Maintenance* > *Logs,* and a message will inform you that the log collection task has been created. Go to the main eNB GUI and click Logs under the Maintenance tab to view the log. Under *Device Logs,* click the checkbox next to the log record you want to view and select *Download (*Figure 2-62).

Figure 2-62: Logs



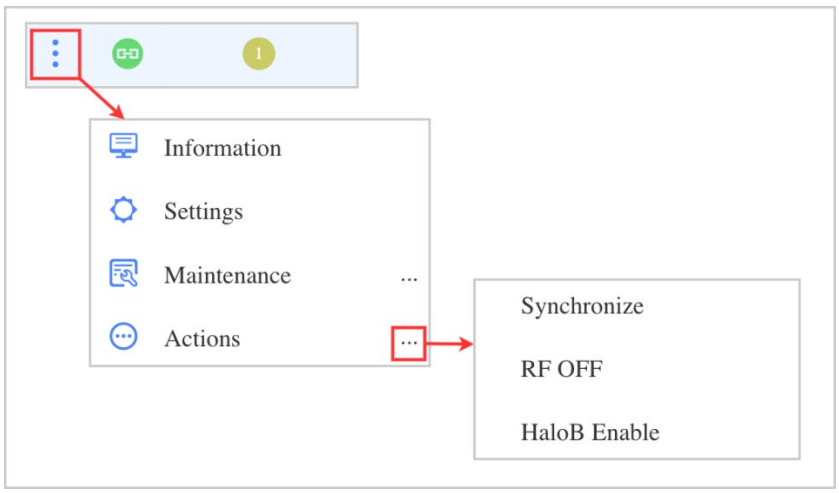
2.4.2.2.6.4 Actions

Additional operations can be performed when you highlight an eNB in the Monitor window, select *Operations*, and then select Actions (Figure 2-63):

- **Synchronize** - updates the OMC with the latest information from the eNB
- **HaloB Enable/Disable** - Enable or disable HaloB mode on the eNB (if the eNB has the HaloB software license); the actions will include any software license option to enable/disable operation
- **RF ON/OFF** - Toggle to turn the RF transmissions for this eNB ON or OFF
- **Force RF Disable** - When SAS is enabled on the eNB, operators can disable RF transmissions even if the grant request is in an Authorized state

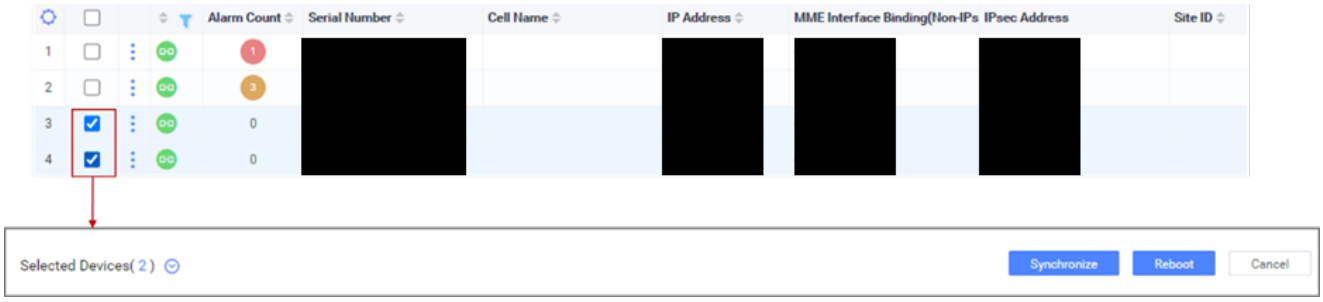
NOTE: The available *Operations > Actions* will vary by eNB type and operating mode.

Figure 2-63: Actions



If you select the checkbox for more than one eNB listed in the Monitor window, a dialogue box will open at the bottom of the screen where you can simultaneously synchronize those eNBs to the OMC or reboot them at the same time (Figure 2-64). To synchronize an eNB means to refresh the OMC display with the eNB's local data.

Figure 2-64: Multi-Device Operations

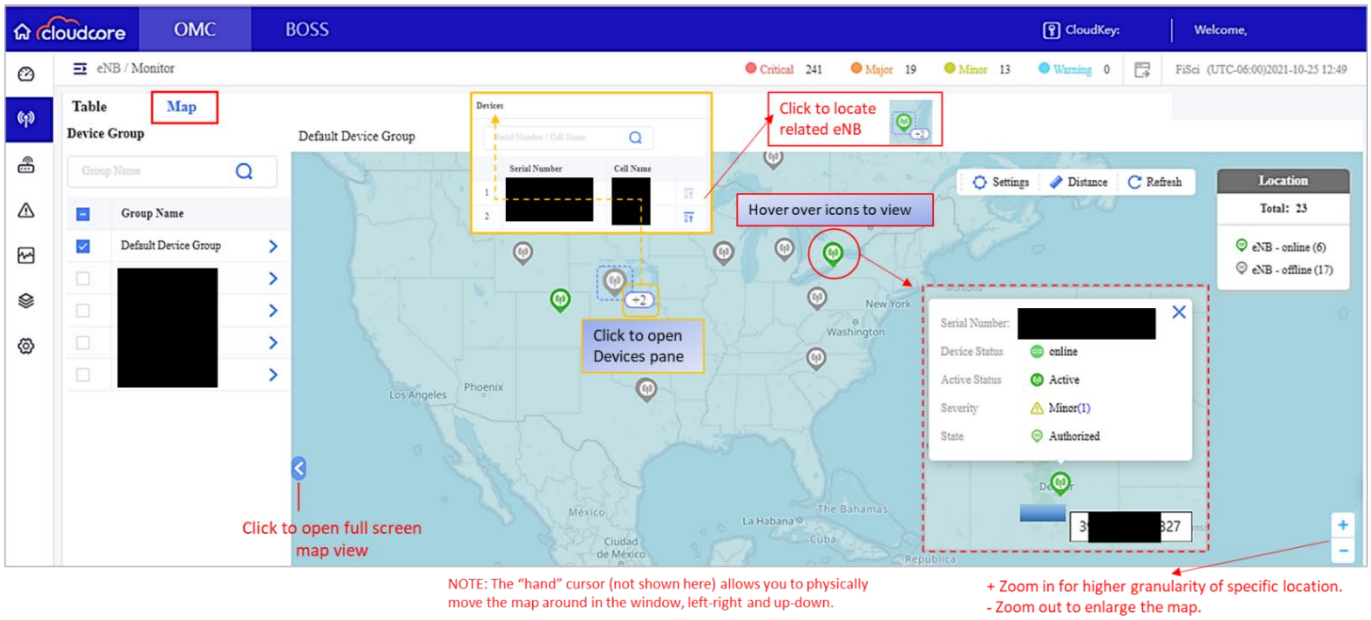


2.4.2.2.7 Map Tab

The *eNB > Monitor > Map* tab view displays a topographical map that shows which eNB devices are online and offline and identifies each location (Figure 2-65). The *Location* legend in the upper right indicates the number of eNBs online and offline compared to the total number of eNBs in the network. If you hover over one of these symbols on the map, it will display the *Serial Number, the Device Status, Active Status, Severity*, and *State* of an eNB.

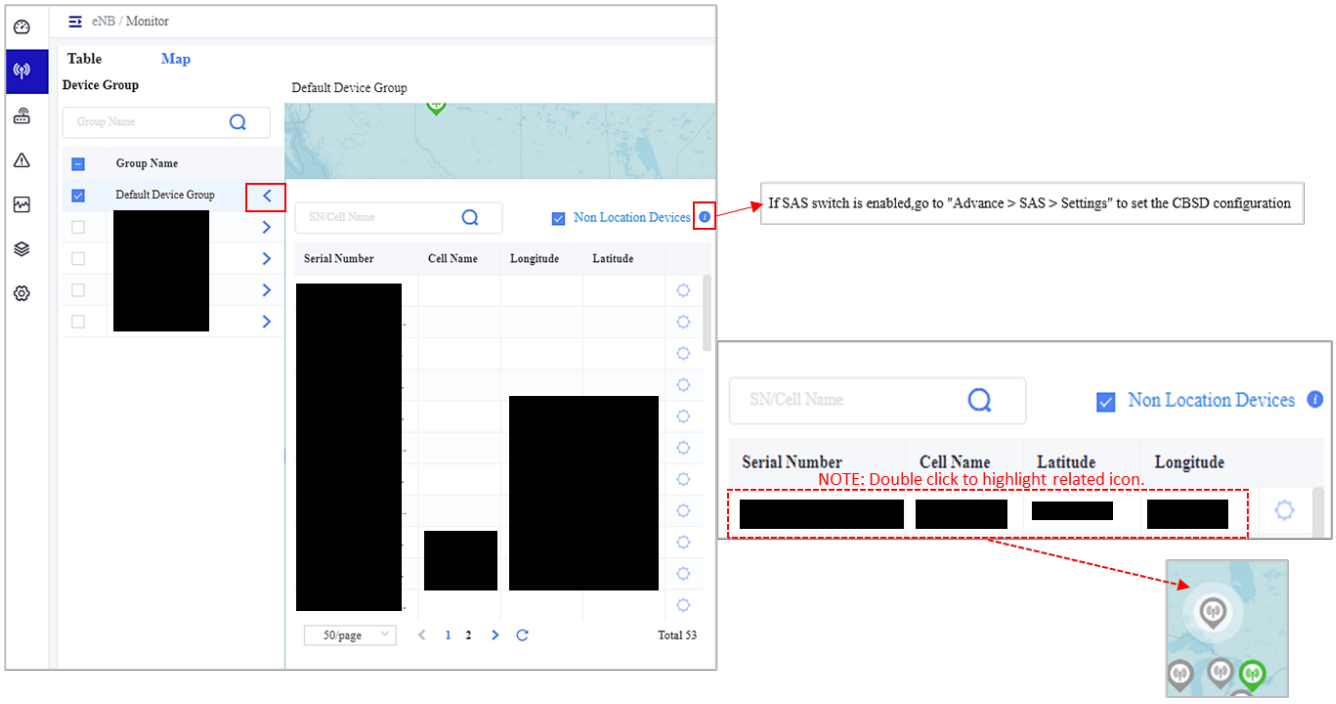
Additionally, hovering over a map icon displays the device's latitude and longitude location. You can click on a legend icon with a plus (**+**) and number to open the *Devices* pane, which indicates the serial number and cell name of additional eNBs. Click the icon next to the eNBs cell name to locate the eNB on the map. The legend icon associated with that eNB will become green. The hand cursor enables you to move the map around, while the **+** and **-** functions provide a way to zoom in for greater granularity or out to enlarge the map.

Figure 2-65: Map Tab View



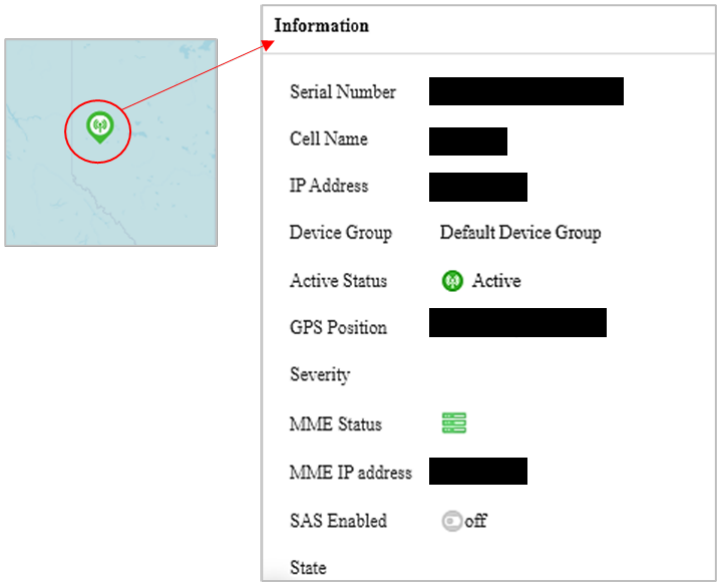
As shown in Figure 2-66, to view an eNBs serial number, cell name, longitude, and latitude, click on the right blue arrow. You can search for a cell by its serial number or cell name by typing either into the search box. Once the eNB information is displayed, you can double click on any of the eNBs information to highlight that eNBs location on the map. The *Non-Location Devices* checkbox views the eNBs configured without the Latitude and Longitude. If you click the information icon next to *Non-Location Devices,* you will see a dialogue box with instructions and disabling SAS settings.

Figure 2-66: Optional Information View



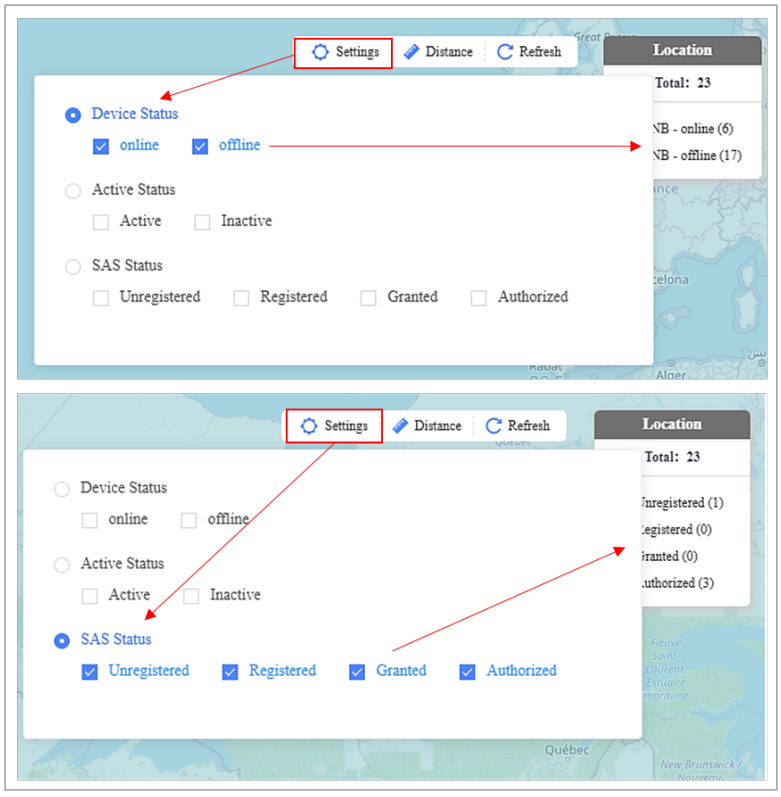
Clicking on a map icon opens an *Information* pane, providing more information about the eNB (Figure 2-67). The *Information* pane provides the eNBs serial number, cell name, IP address, device group, active status, GPS position, severity, MME status, MME IP address, SAS enabled or not, and state (authorized or not).

Figure 2-67: Information Pane



You can use the tabs in the top right corner to filter which eNBs show on the map. The *Settings* tab allows you to filter by *Device Status, Active Status*, and *SAS Status*. The *Location* pane will reflect your choice (Figure 2-68).

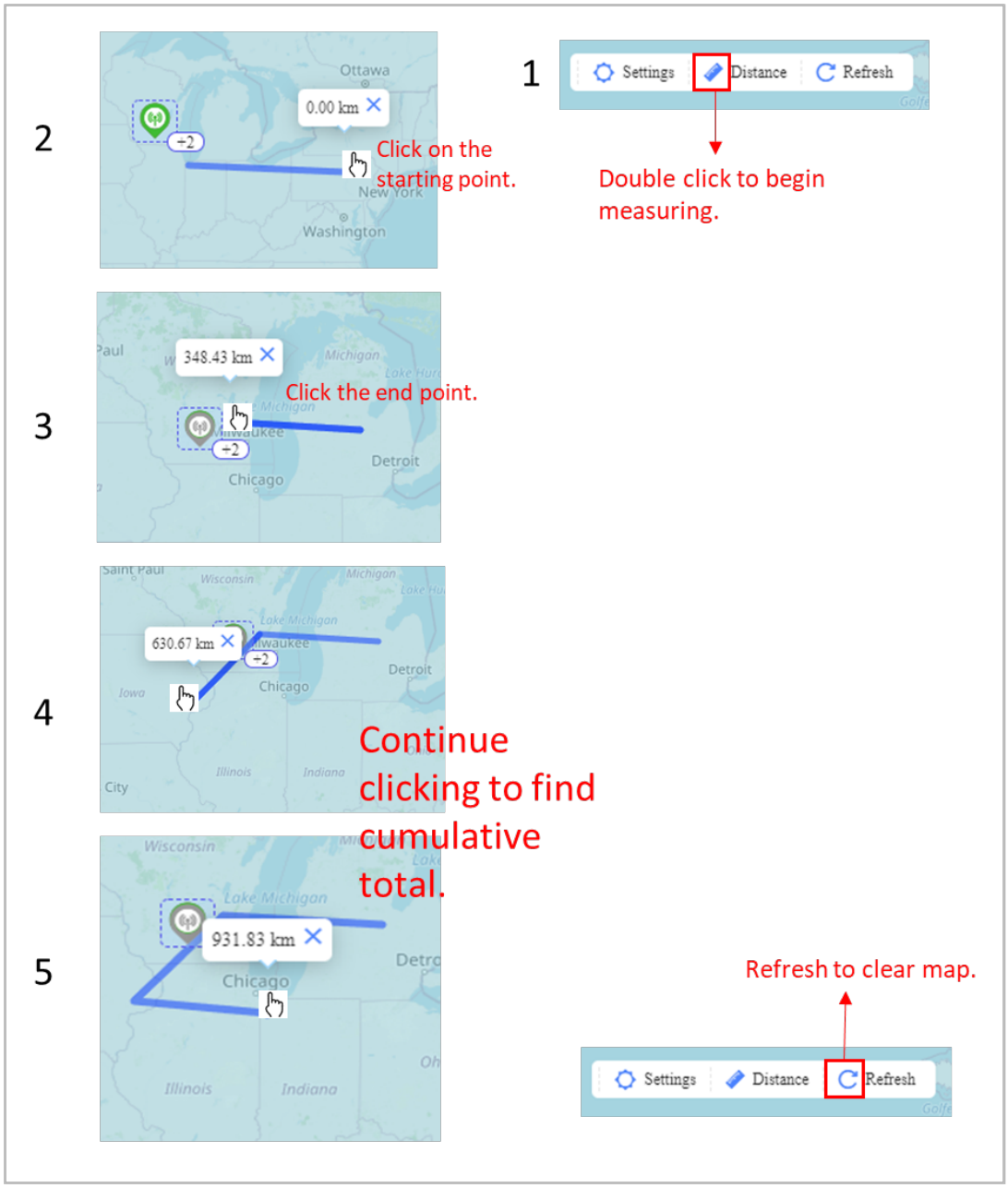
Figure 2-68: Map Display Filters



2.4.2.2.8 Distance Tab

The Distance tab calculates the inter-distance between two eNBs and between the CPEs and the corresponding eNB. As shown in Figure 2-69, you can view the distance between one or more selected points on the map. To begin, double-click the ruler icon next to *Distance.* Then use the hand tool icon to click on the desired starting point you want to measure. A distance box will appear displaying 0.00 km (your starting point). A blue line will follow as you move the hand tool icon on the map, measuring the distance between your starting point and the endpoint. Once you have chosen the endpoint, click again, and the distance between the points will appear. You can move the hand tool to several issues. Each time you click again, distance is cumulatively added. At any point, click refresh to end measuring and clear the map.

Figure 2-69: Display Tab



2.4.2.3 Maintenance

The *eNB > Maintenance* menu covers Man-Machine Language (MML) batch configuration, Configuration, Change Password, Reboot, and Logs eNB functions (Figure 2-70). For each part, you can define and schedule tasks that will apply to one or more eNBs.

Figure 2-70: Maintenance

2.4.2.3.1 MML

After eNBs are registered in OMC, you can configure them in batches using MML commands. You can modify eNB and core network configuration information by MML commands. The *eNB > Maintenance > MML* menu contains two tabs: MML and MML Script

Figure 2-71: MML Menu

2.4.2.3.1.1 MML Tab

To use MML configuration, follow the steps below while referring to Figure 2-72.

1. In the MML window, select the software stream from the drop-down list to identify the type of eNB(s) you want to display. See *Table 2-5 Product Types / Software Streams* concerning Baicells products and software. You can also search by eNB serial number or name.

Figure 2-72: MML Tab

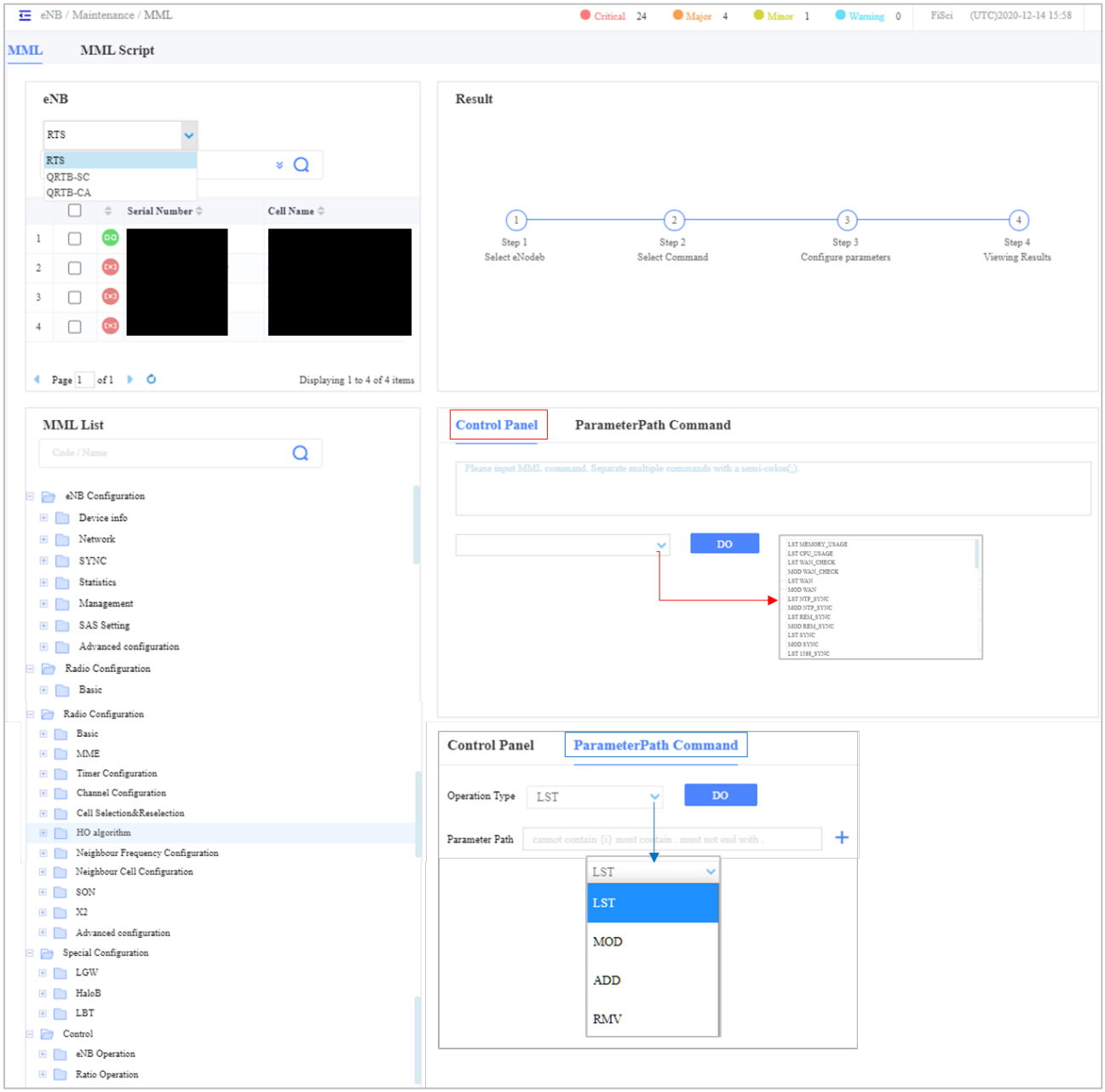


Table 2-5: Product Types / Software Streams

Software Stream	Description	Example(s)
CR-B4860	Future 5G product with NXP processors	Nova846, Pulsar4G
Neutrino430	Two-carrier indoor eNBs with Qualcomm processors and running in LTE TDD duplexing mode	Neutrino430
QAFA	Single-carrier eNBs with Qualcomm processors	Neutrino224
QAFB	Two-carrier eNBs with Qualcomm processors and running in LTE FDD duplexing mode	Nova246 FDD mode
QRTB-DC	Two-carrier eNBs with Qualcomm processors running in Dual Carrier (DC) / split mode	Nova436Q in DC/split mode, Neutrino430 in DC/split mode
QRTB-CA	Two-carrier eNBs with Qualcomm processors running in Carrier Aggregation (CA) mode	Nova436Q CA mode, Neutrino430 CA mode
RTS	Single-carrier eNBs with Intel processors	Nova227, Nova233, Nova243
RTD	Two-carrier eNBs with Intel processors	Nova246 TDD mode

2. In the list of eNBs that appears, select the checkbox next to the ones you want to batch configure.
3. To identify the MML commands you want to execute:
    a. MML List: In the MML List pane, select the MML command to execute. The Control Panel pane will display the MML command and its parameters. You can choose more MML commands if each is separated by a semi-colon (;).
    b. Control Panel: In the Control Panel pane, fill in the MML parameters, separating multiple commands with a semi-colon (;), and click on DO. Or use the pull-down menu to select each command.
    c. ParameterPath Command: In the Control Panel pane, click on the ParameterPath Command tab and use the Operation Type pull-down menu to select the type of action to be performed:
        i. LST - List
        ii. MOD - Modify
        iii. ADD - Add
        iv. RMV - Remove

        You can also type the command directly into the field.
    d. Then, type the MML command(s) directly into the MML command window. The path cannot contain brackets, e.g., [1], and must include a period (.) but not end with a period (.).
    e. Click on DO to execute the command. The results will display in the Results pane.

2.4.2.3.1.2 MML Script Tab

The batch configuration of eNB devices is done by creating an MML script task. You can generate MML scripts by importing and executing MML script files. Select the MML Script tab in the *eNB > Maintenance > MML* menu and follow the steps below (Figure 2-73).

1. Click on the **+** Add icon to open the New Task window.
2. Export the MML template and enter the MML script. Save; do not change the file name.
3. Accept the auto-generated Task Name or enter a new one.
4. Select MML Script, click on the import icon, and navigate the completed script file.
5. Select an Execute Type, per *Table 2-6 Execute Modes*, determining when the task executes.
6. Click on *OK* to save the settings. The new task will be added to the MML Script list.

Figure 2-73: MML Script

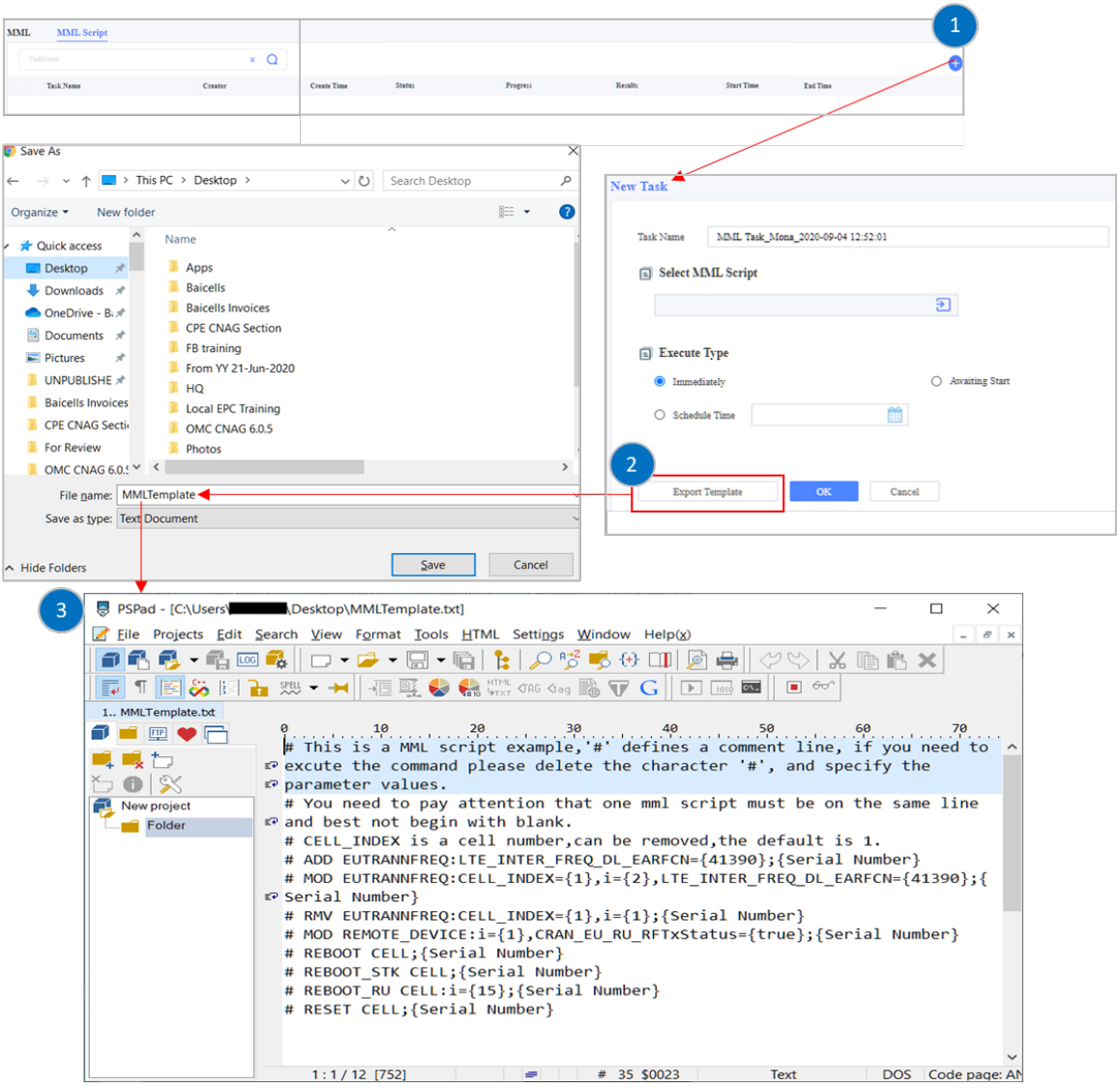


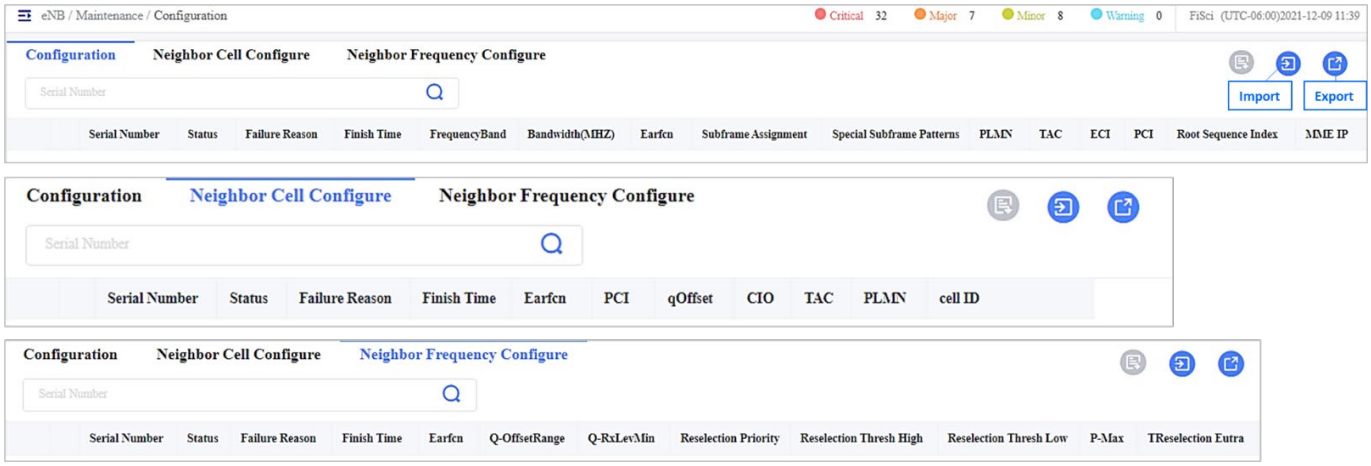
Table 2-6: Execute Modes

Mode	Description
Immediately	The task will execute as soon as you click on *OK*.
Awaiting Start	Suspends the execution until you are ready to choose one of the other two options - to run it immediately or schedule a day and time for the task to execute
Schedule Time	Identify a day and time for the task to take place.

2.4.2.3.2 Configuration

The *eNB > Maintenance > Configuration* page is where you configure an eNB. The configuration menu contains three tabs: *Configuration, Neighbor Cell Configure,* and *Neighbor Frequency Configure* (Figure 2-74). Refer to the *eNB Configuration Guide* for a description of each parameter.

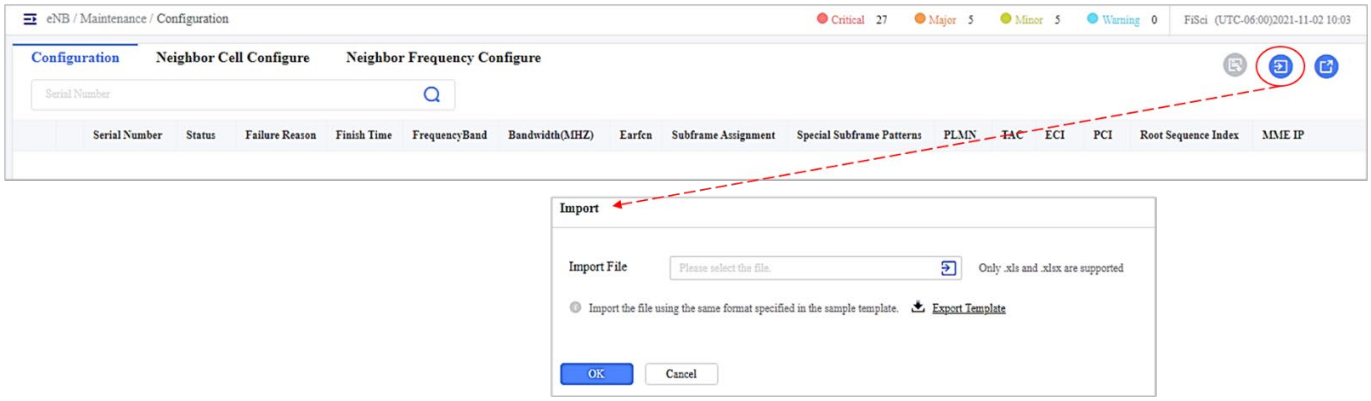
Figure 2-74: eNB Configuration



2.4.2.3.2.1 Import/Export

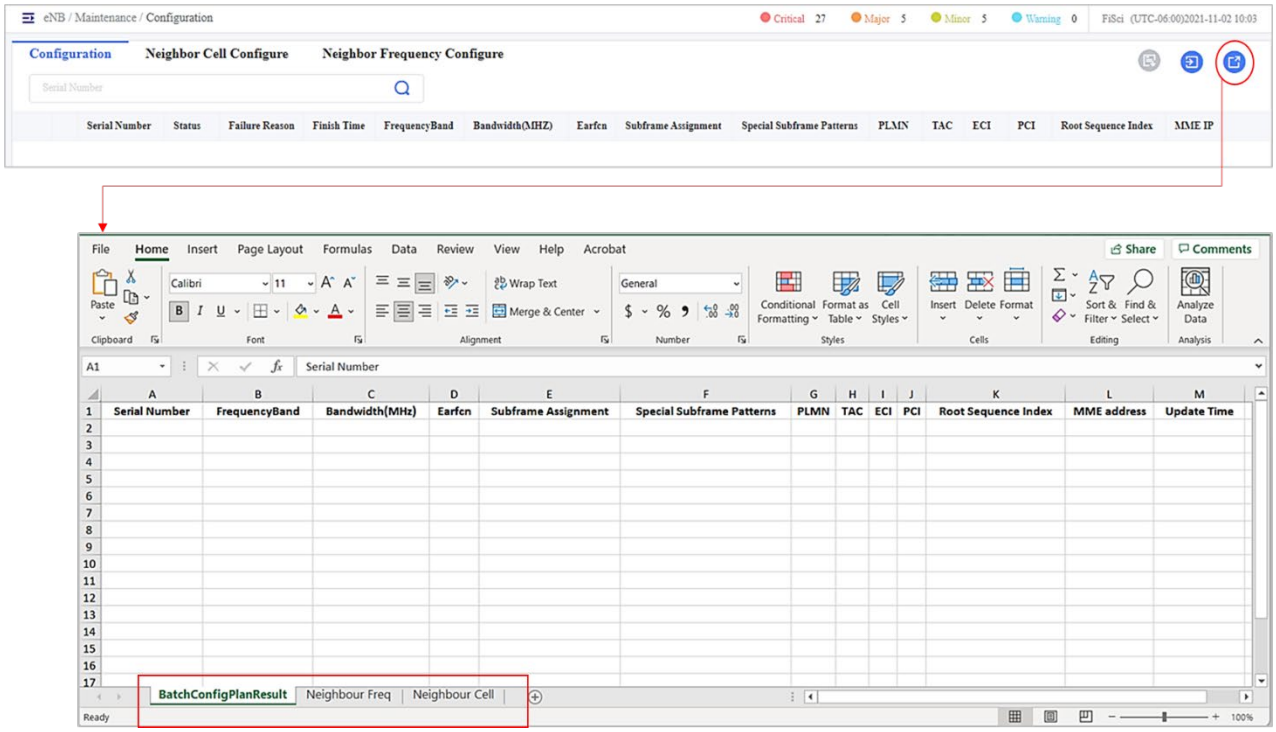
To know the information of the neighboring cells and their frequency, the eNB needs information about the cells. You can import a spreadsheet (Figure 2-75) to quickly configure one or more eNBs and give information about neighbor cells and neighbor frequency. This can lead to smooth handover and overcome interference issues. It must be in the .xlx or .xlxs extension to import a file. To download a sample template for the file format, click on an *Export template* as shown in (Figure 2-75). Click the *Import* icon and select the file from your computer. Then click *OK*.

Figure 2-75: Import



To export a .xlsx spreadsheet and view *Batch Config Plan Results, Neighbor Frequency,* and *Neighbor Cell* information of each eNB, click the *export* icon, and the file will begin to download automatically (Figure 2-76). This file will contain all the configuration parameters of the eNB.

Figure 2-76: Export



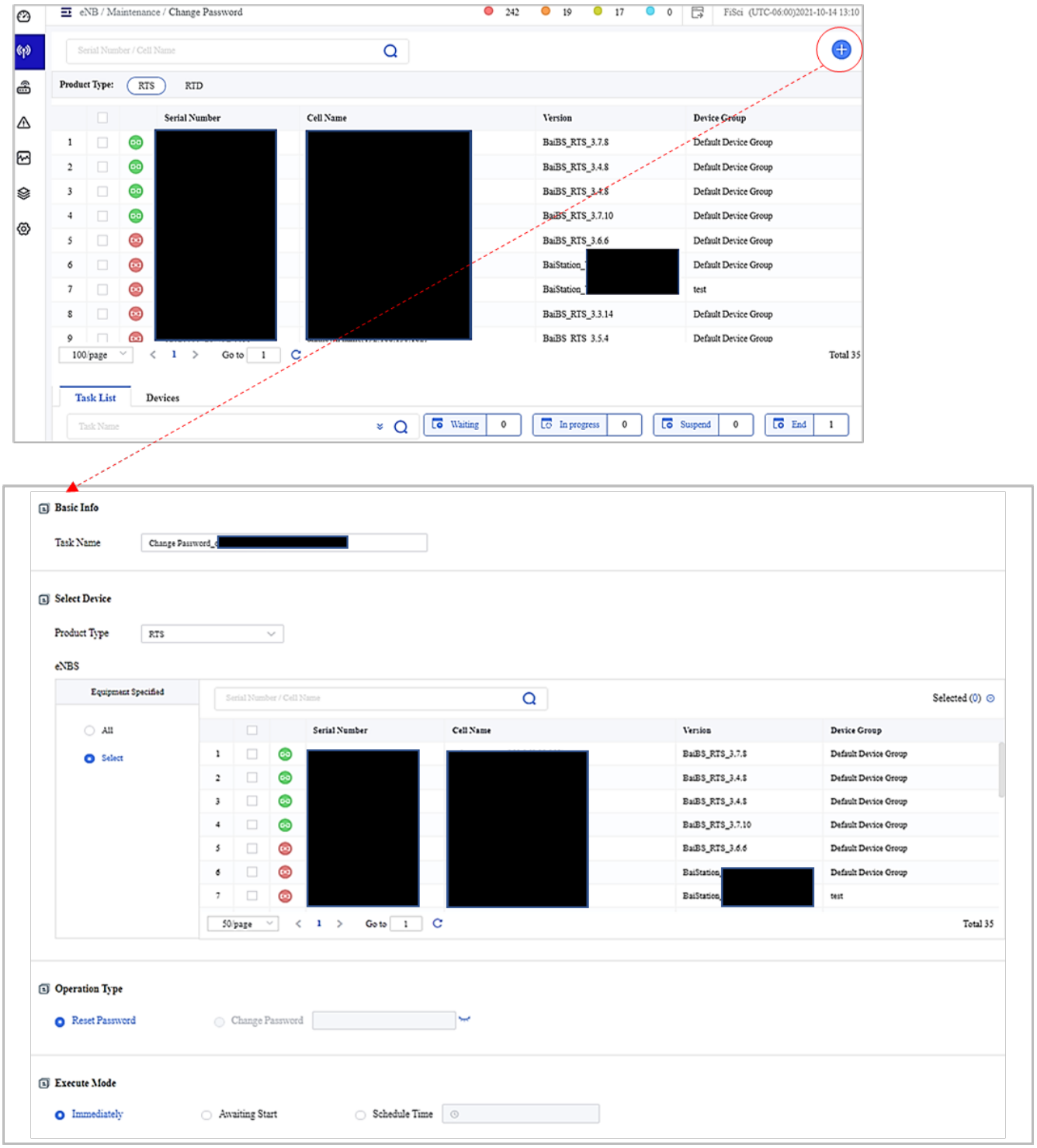
2.4.2.3.3 Change Password

This *eNB > Maintenance > Change Password* menu is used to create tasks pertaining to eNB passwords. You can reset the password on one or more eNBs to the default password (typically, admin) or change the password to a new character string. When you open the Change Password window, any existing tasks will be listed along with information about the execution of that task.

To create a Change Password task:

1. Click on the **+** Add icon to open the New Change Password Task window (Figure 2-77).
2. Accept the auto-generated task name or enter a new name.
3. Under *Select Device*, search for the eNB by product type or click the checkbox next to the target eNB devices for this task. You can select the radio button next to *All* to choose all eNBs.
4. For Operation Type, choose the radio button for either Reset Password or Change Password.
5. Choose an Execute Type, per *Table 2-6 Execute Modes*, determining when the task executes.
6. Click on *OK* to save the settings. The new task will be added to the Change Password list.

Figure 2-77: Change eNB Password



Use the *Operations* functions to view the task results, to start or terminate the task, modify, or delete the task (Figure 2-78). Task results will appear at the bottom of the window. You can view additional information about a task by selecting *Operations* > *Information*.

Figure 2-78: Task List Operations

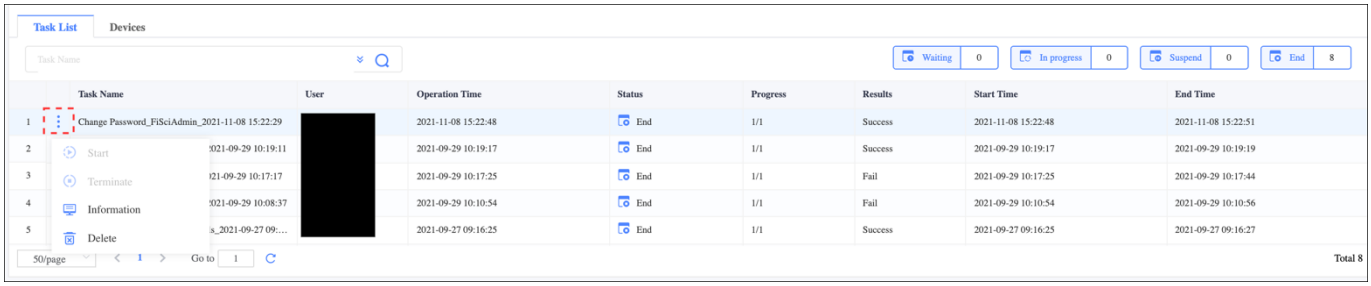
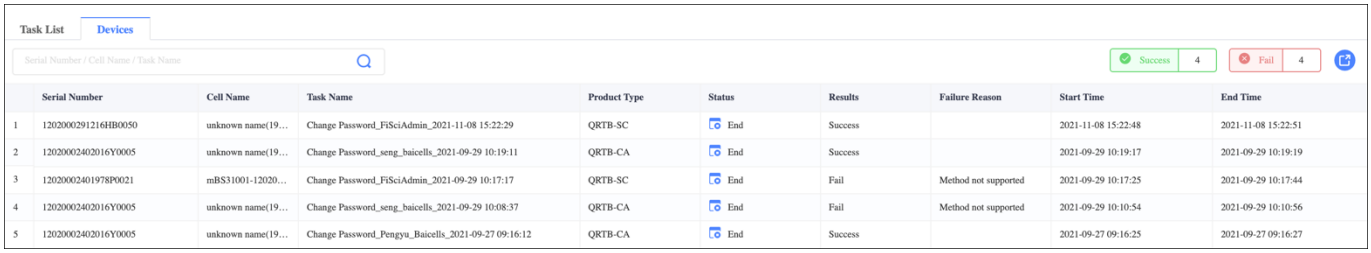


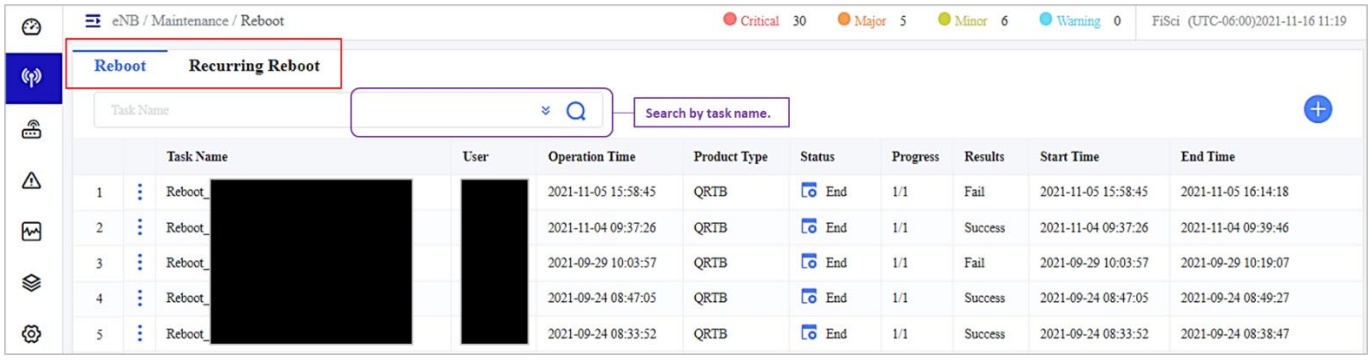
Figure 2-79: Devices Tab



2.4.2.3.4 Reboot

The *eNB* > *Maintenance* > *Reboot* page allows you to view existing and completed reboot tasks or create a reboot or recurring reboot task for one or more eNBs. The *eNB* > *Maintenance* > *Reboot* window has two tabs, Reboot and Recurring Reboot (Figure 2-80). You can search for a task by entering the task name in the search box.

Figure 2-80: Reboot



2.4.2.3.4.1 Reboot Tab

Any existing and completed reboot tasks are listed in the reboot tab window. Task list information includes the task name, user, operation time, product type, status, progress, results, and start and end time (Figure 2-80).

2.4.2.3.4.2 Create a Reboot Task

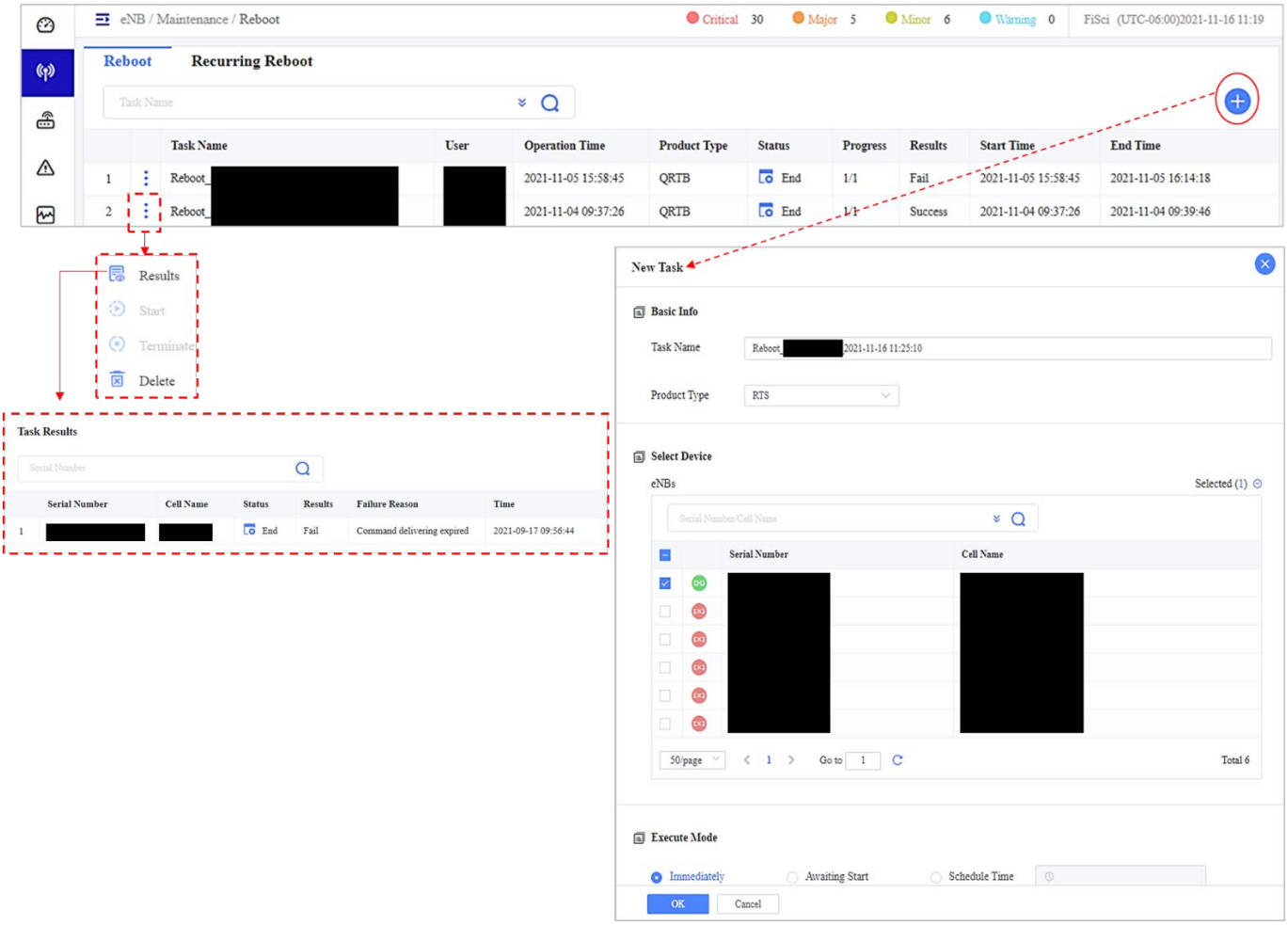
Caution: A reboot will take the device(s) out of service for a few minutes.

To create a new reboot task (Figure 2-81):

1. Click on the **+** *Add* icon to open the *New Task* window.
2. Accept the auto-generated task name or enter a different task name.
3. Select the *Product Type*, per *Table 2-5 Product Types / Software Streams,* and choose the target eNB devices.
4. Choose an *Execute Type*, per *Table 2-6 Execute Modes* which will determine when the task executes.
5. Click on *OK* to save the settings. The new task will be added to the *Reboot* list.

In the *Reboot* window task list, the *Operations* functions include *Results* (view the task execution results), *Start* (begin the task), *Terminate* (end the task), and *Delete* (remove the task). Clicking *Operations* > *Results* opens the *Task Results* window where the eNB's serial number, cell name, status, results, failure reason, and time are displayed, as shown in Figure 2-81.

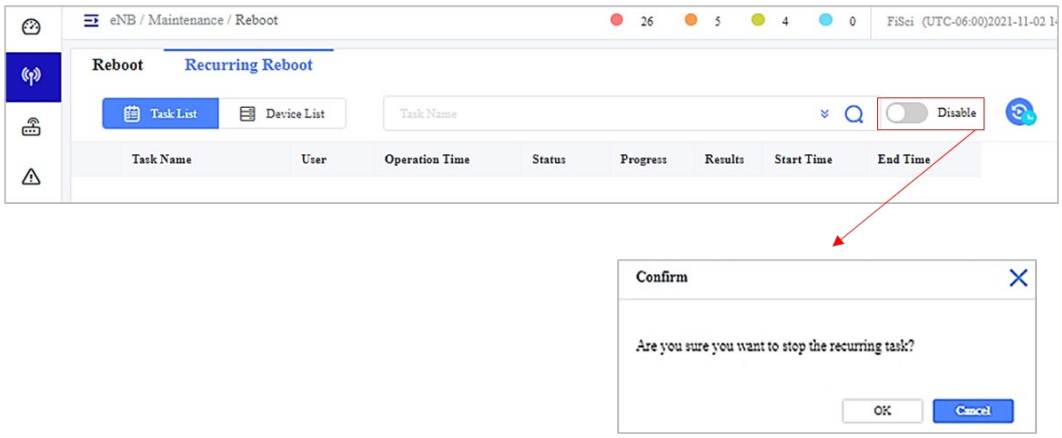
Figure 2-81: Create a Reboot Task



2.4.2.4.4.3 *Recurring Reboot Tab*

Any existing and completed reboot tasks are listed under Task List in the Recurring Reboot tab window. Tasklist information includes the task name, user, operation time, status, progress, results, and start and end time. You can start or stop a recurring reboot task by clicking the checkbox next to the task and clicking the *Enable/Disable* radio button (Figure 2-82). Click *OK* to confirm your selection or *Cancel* in the dialogue box.

Figure 2-82: Recurring Reboot



You can search for a task by entering the task name in the search box or using the *Advance Query* and entering the task name and start and end time (Figure 2-83).

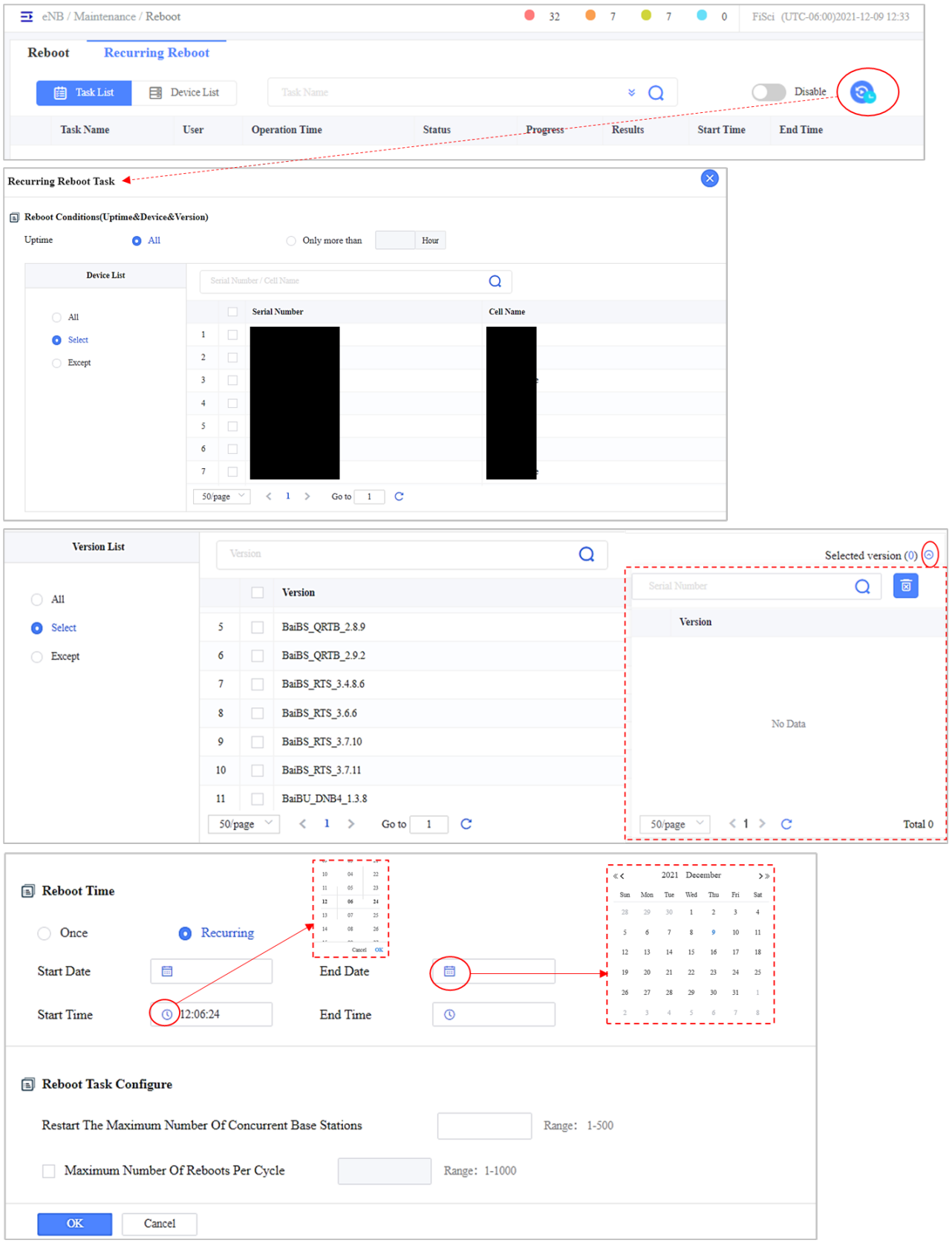
Figure 2-83: Advanced Query Search

2.4.2.3.4.3 Create a Recurring Reboot Task

To create a recurring reboot task (Figure 2-84):

1. In either the *Task List* or the *Devices List* tab window, click the blue *Settings* button in the right corner to open the *Recurring Reboot Task* window.
2. From the *Device List*, choose *All* for all devices, *Select* and choose individual devices, or *Except* to choose all devices except specific devices.
3. Select the radio button next to Once or Recurring in the Reboot Time window and enter the start and end time and date. Click the calendar icon to open a window and select the date. Use the arrows to move quickly through the calendar. Click the clock icon to choose to open a window and select the time.
4. In the *Reboot Task Configure* window, enter the base stations to reboot concurrently. The maximum number of base stations that can reboot concurrently is 500.
5. You can choose the number of reboots in a reboot cycle by clicking the checkbox next to *Maximum Number of Reboots Per Cycle*. Enter the number of reboots between 1-1000.
6. Click *OK*.

Figure 2-84: Creating Recurring Reboot Task



2.4.2.3.4.4 Export a Recurring Reboot Task

The *Device List* tab displays a device's serial number, cell name, task name (tasks associated with that device), status, results, failure reason, and start and end time. You can search for a device by entering the device's serial number or task name in the search box (Figure 2-85). The device tab also shows the number of recurring reboot successes and fails in the right corner.

To export the recurring reboot task (Figure 2-85):

1. In the *Devices List* tab window, click the blue *export* button to download the recurring reboot tasks in the right corner.
2. A .csv file will be downloaded

Figure 2-85: Recurring Reboot Devices List

2.4.2.3.5 Logs

The *eNB > Maintenance > Logs* menu offers four categories of eNB log reports (Figure 2-86):

- Device Logs - select one or more eNBs to collect and download the eNB log reports, or create a logging task
- Alarm Logs - select one or more eNBs to download just the alarm logs, or create a log task
- Exception Logs - select one or more eNBs to download only the exception (error) logs, e.g., when an eNB crashes
- Event Logs - view a list or chart of all (aggregate) eNB log events, reboots, or both

Figure 2-86: Logs

You can create tasks to generate the log files for the device and alarm logs for up to 5 eNBs. The *Operations* functions for all, but the Exception Logs are Results, Terminate, Download, and Delete.

2.4.2.3.5.1 Device Logs

To report the operation log information of the eNB regularly or immediately create a new Device log task.

To add a new Device Logs task (Figure 2-87):

1. Select the Device Logs task and click on the **+** Add icon to open the New Device Report Log Task window.
2. Select up to 5 eNBs from the list.
3. Select an Execute Type, per *Table 2-6 Execute Modes*, which will determine when the task executes.

4. If you select Immediately, the new task will run as soon as you click *OK*. Click within the Start Time and End Time rectangular fields to schedule a day and time. A calendar for each will pop up. You can also select a Period(min) to specify how long the log collection should occur, either 15, 30, or 60 minutes. Click on *OK* to save the settings.

5. The new log task will appear in the main Device Logs window, showing status and, when completed, providing results. In the *Operations* > *Results* window, you can view, download, or delete the log files.

Figure 2-87: New Device Log Task

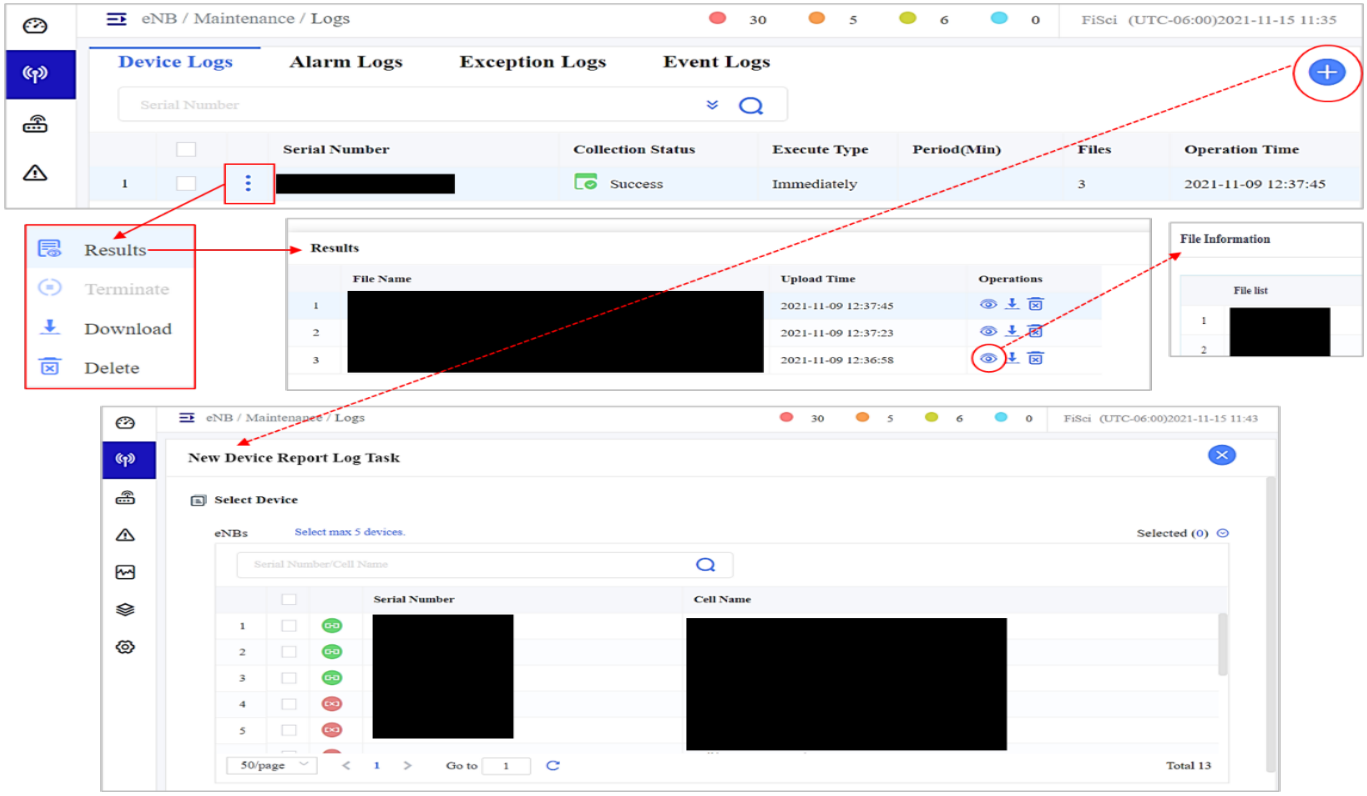
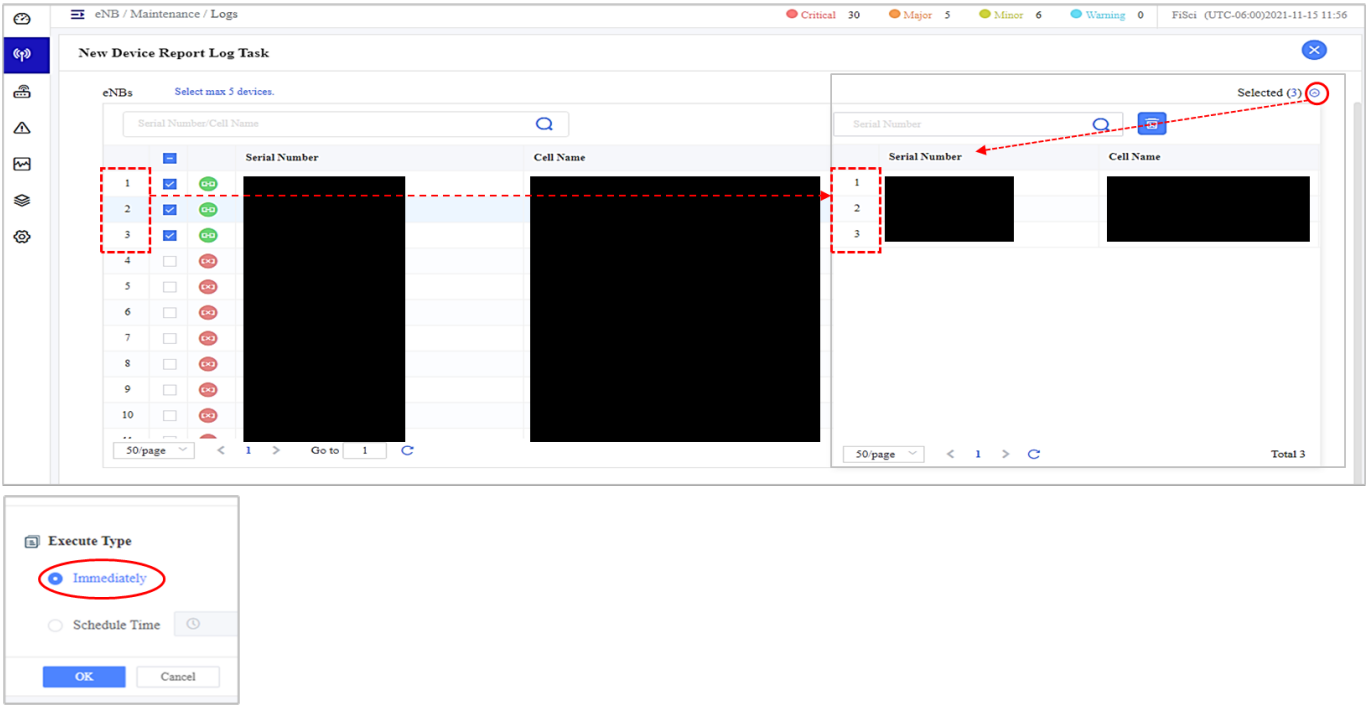
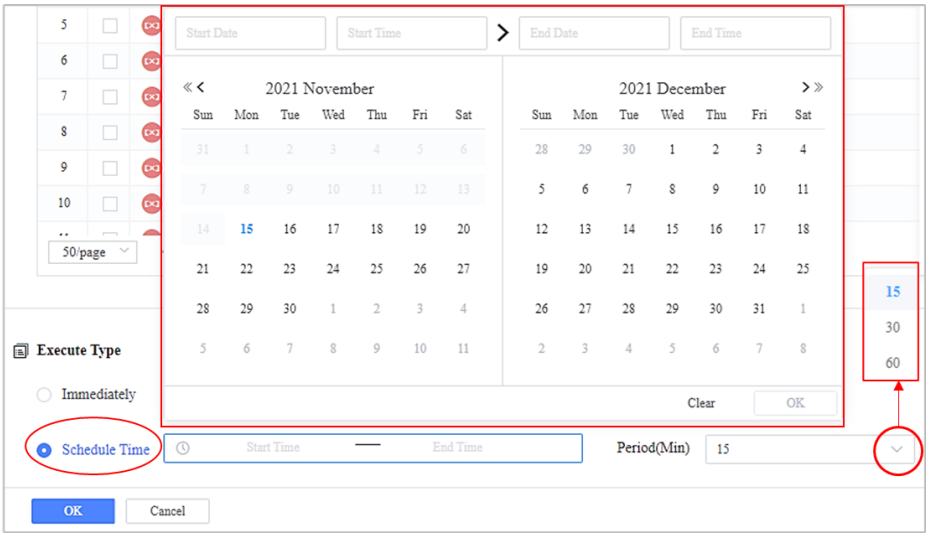


Figure 2-88: Execute Type

Execute Type: Immediately



Execute Type: Schedule Time



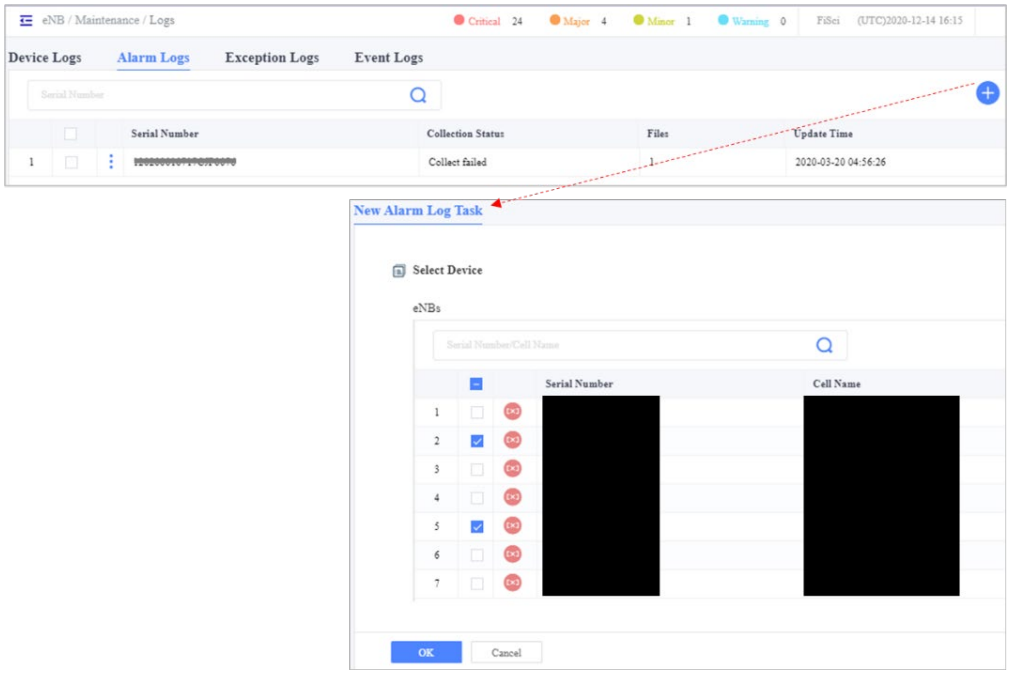
2.4.2.3.5.2 Alarm Logs

By creating an Alarm log task, the alarm information of the eNB is collected. It supports the operation of viewing, terminating, downloading, and deleting the results of the alarm log task.

To create an Alarm Logs task (Figure 2-89)

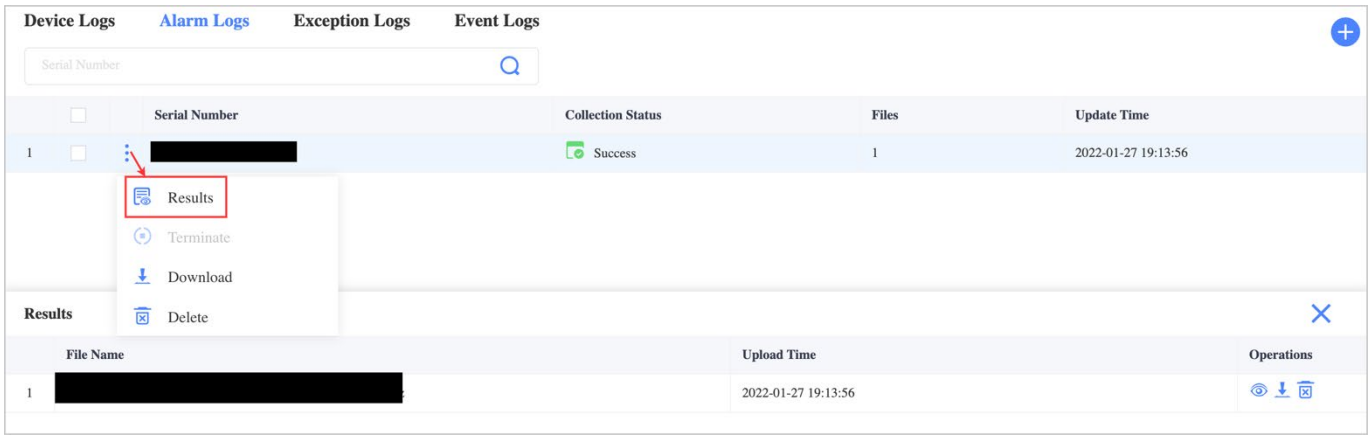
1. Select the Alarm Logs tab and click on **+** ADD to open the New Alarm Log Task window.
2. Select the eNBs from the list and click on *OK*. The new task will appear in the main Alarm Logs window, and the alarm logs will start collecting immediately.

Figure 2-89: New Alarm Log Task



After the Alarm logs are collected, the *Collection status* will show the *Success* or *Failure* for a given eNB. You can view, terminate, download, or delete the Alarm log task by clicking the *operations* (Figure 2-90).

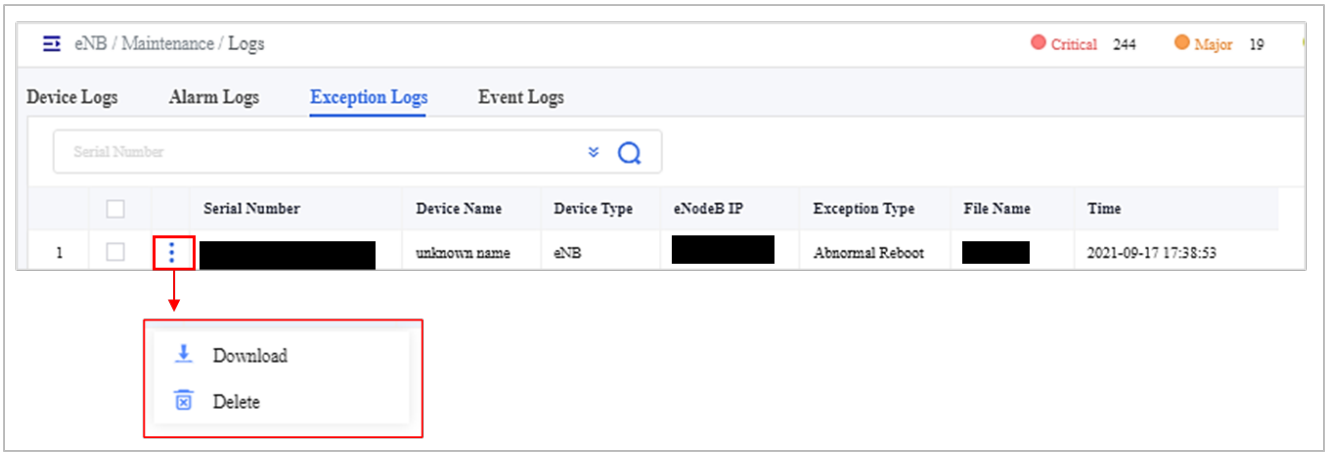
Figure 2-90: Results of The Alarm Log



2.4.2.3.5.3 Exception Logs

The OMC automatically collects and records abnormal conditions of the eNB. In the Exception Logs tab, select one or more eNBs and use the *Operations* actions to download or delete the exception (error) logs (Figure 2-91). An example of when you might want to download exception logs would be when an eNB crashes or when the eNB is experiencing an abnormal start. When you open a support ticket, the support team will ask you to send the log files.

Figure 2-91: Exception Logs



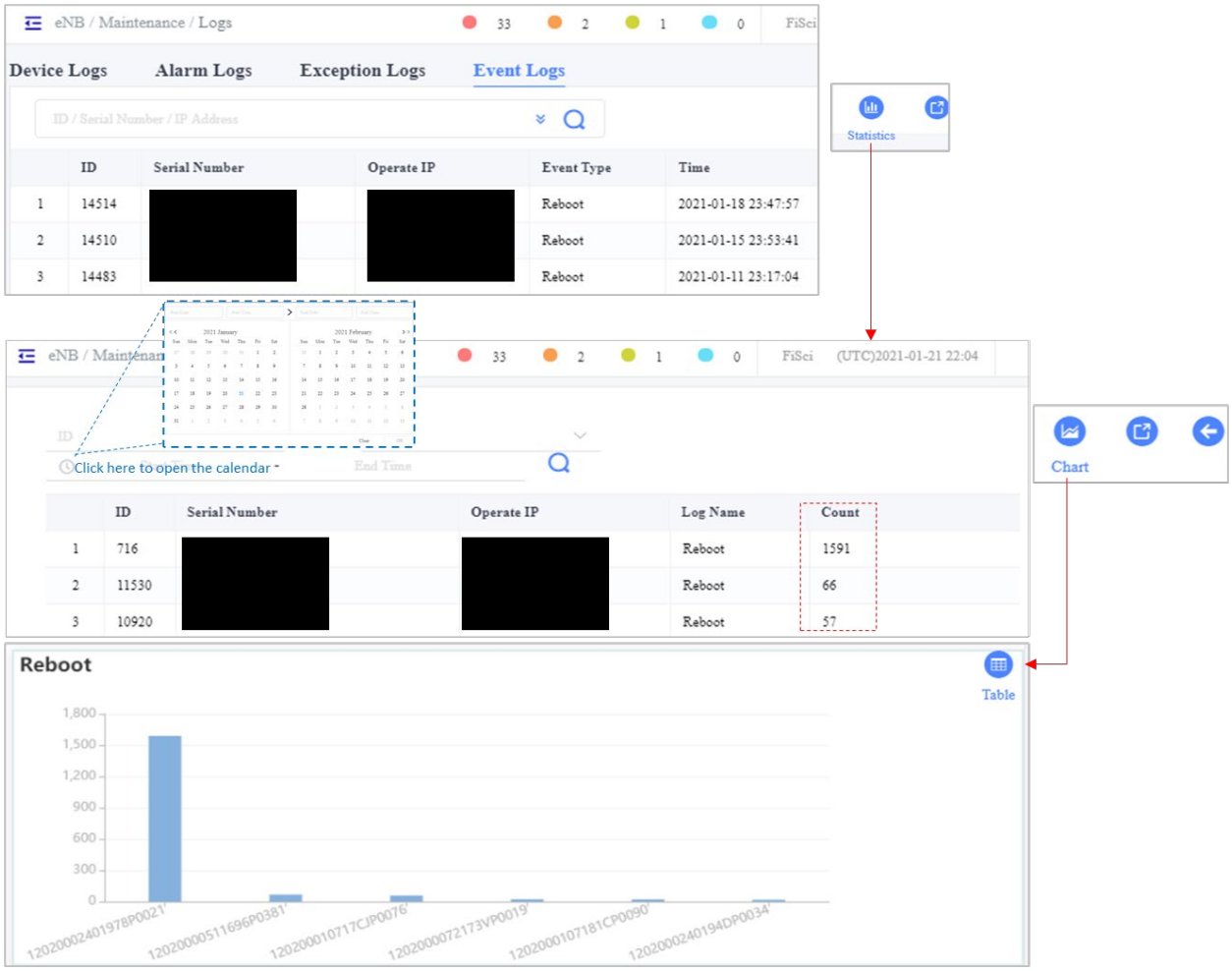
2.4.2.3.5.4 Event Logs

The OMC automatically collects and records events and information of the eNB. For example, it records events like a reboot of the eNB. The Event Logs tab lists all eNB devices' event logs in descending order by date and time (Figure 2-92). Use the Export icon in the upper right to export the data to a .csv file on your computer for further analysis.

Clicking on the Statistics icon will summarize the total count of each event ID for the period you specify in the Start Time and End Time fields. The list will show the highest to the least number of logs per ID.

The Chart icon will display the statistics data in a chart format, one graph per event ID. Select the Table icon to return to the Statistics list, and from there, click on the back arrow to return to the main Event Logs list.

Figure 2-92: Event Logs



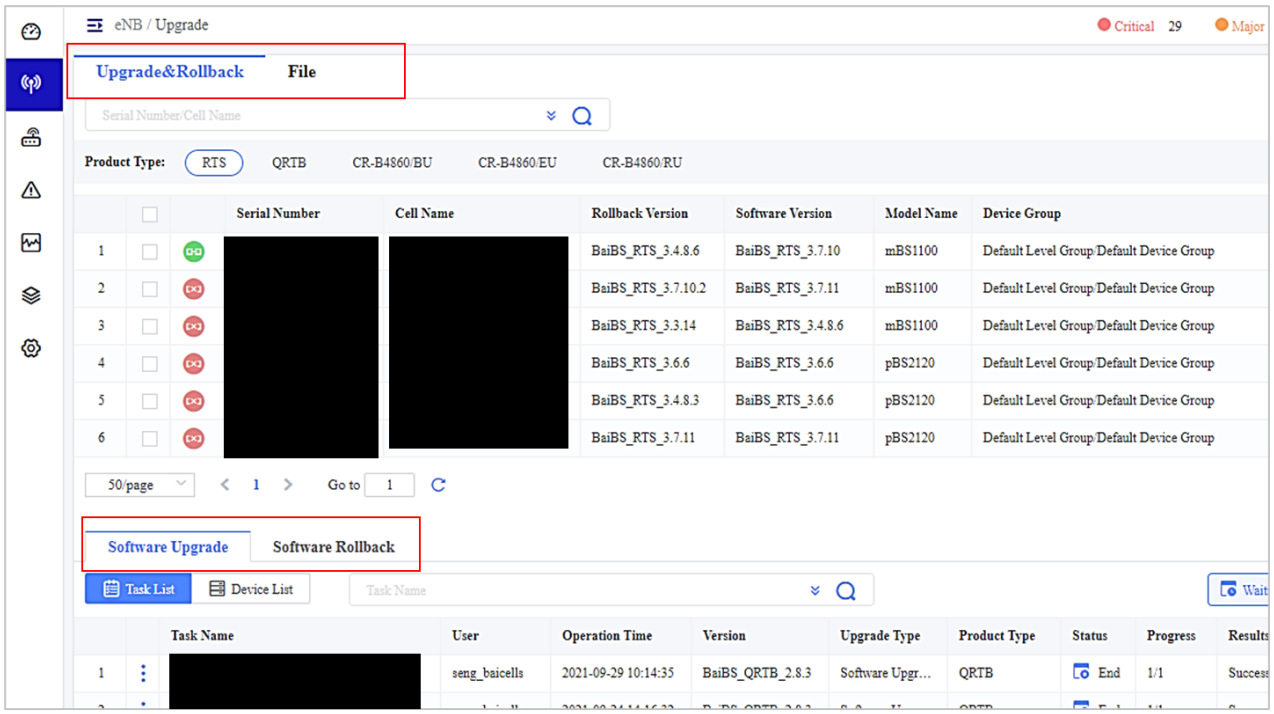
2.4.2.4 Upgrade

New software typically contains the latest features and bug fixes, and it is generally recommended to implement the newest version in the field. You can also return (rollback) one or more eNBs to their previous software version.

Caution: A software rollback requires a reboot of the eNB, which will take the device out of service for a few minutes.

Baicells notifies operators of newly available software by including a message at the top of the OMC window. You can select the link in the message to go straight to the upgrade menu as explained in *section* 2.4.1.2 *Quick Links* or use the *eNB* > *Upgrade* menu. The top of the *eNB* > *Upgrade* landing page has two main sections, *Upgrade&Rollback* and *File* (Figure 2-93). The bottom of the landing page contains software upgrade and rollback tasks, viewable by task list or device list.

Figure 2-93: eNB > Upgrade Landing Page



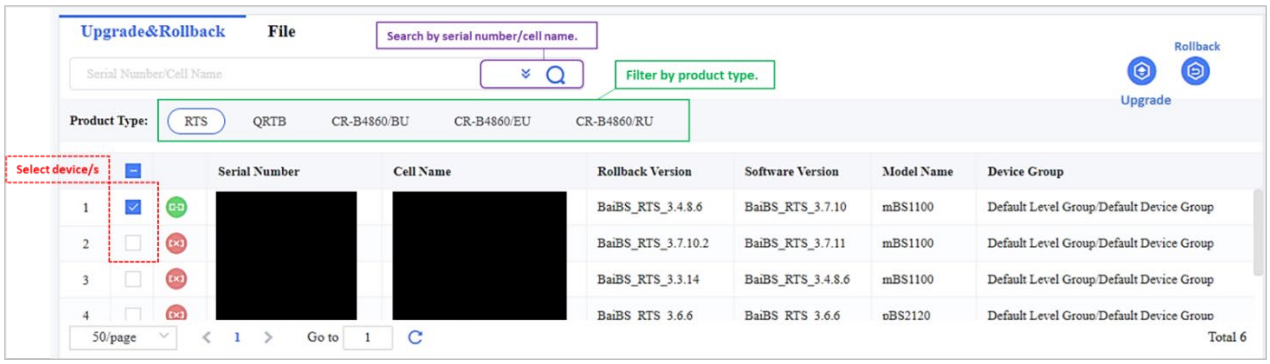
2.4.2.4.1 Upgrade & Rollback

The *Upgrade & Rollback* tab displays a list of available software. Clicking on a software version filters the list of devices below by product type to which the software applies. Device information includes serial number, cell name, rollback version (the software version to which the device would revert), software version (current software version), model name, and device group.

NOTE: After you execute a rollback, you cannot roll the software back again unless you have subsequently upgraded the eNB software at least once.

As shown in Figure 2-94 to upgrade or rollback, use the checkbox to choose a device/s, or search for a device by entering the eNBs serial number or cell name. Then select the upgrade or rollback button to perform the selected desired action.

Figure 2-94: eNB > Upgrade > Upgrade & Rollback



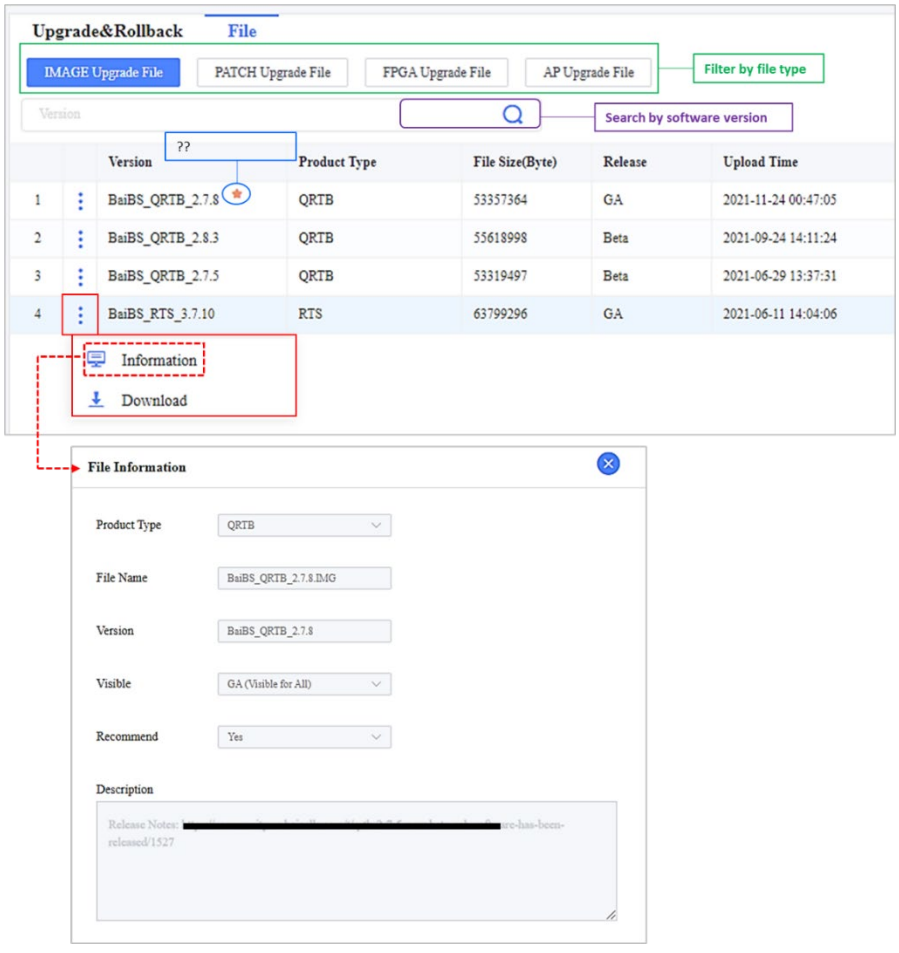
2.4.2.4.2 File

The *eNB > Upgrade > File* tab provides additional information about available software and contains four-choice types: *IMAGE Upgrade File, PATCH Upgrade File, FPGA Upgrade File,* and *AP Upgrade File* (Figure 2-95). An image file is an operating software on the eNB. A patch file is a software patch to an existing software version, typically for bug fixes. An FPGA file pertains to semiconductor hardware within the eNB. An AP file upgrades the eNBs access point.

The window displays the available software list, the version name, product type to which it applies, file size, release status* and upload time (date and time the file was uploaded). The *Operations* actions are *Information*, which displays additional information about the software file, and *Download*, an option to download the software file.

*NOTE: "GA" means General Availability to customers. BETA release status means the software is being trialed by a few customers and is not yet generally available.

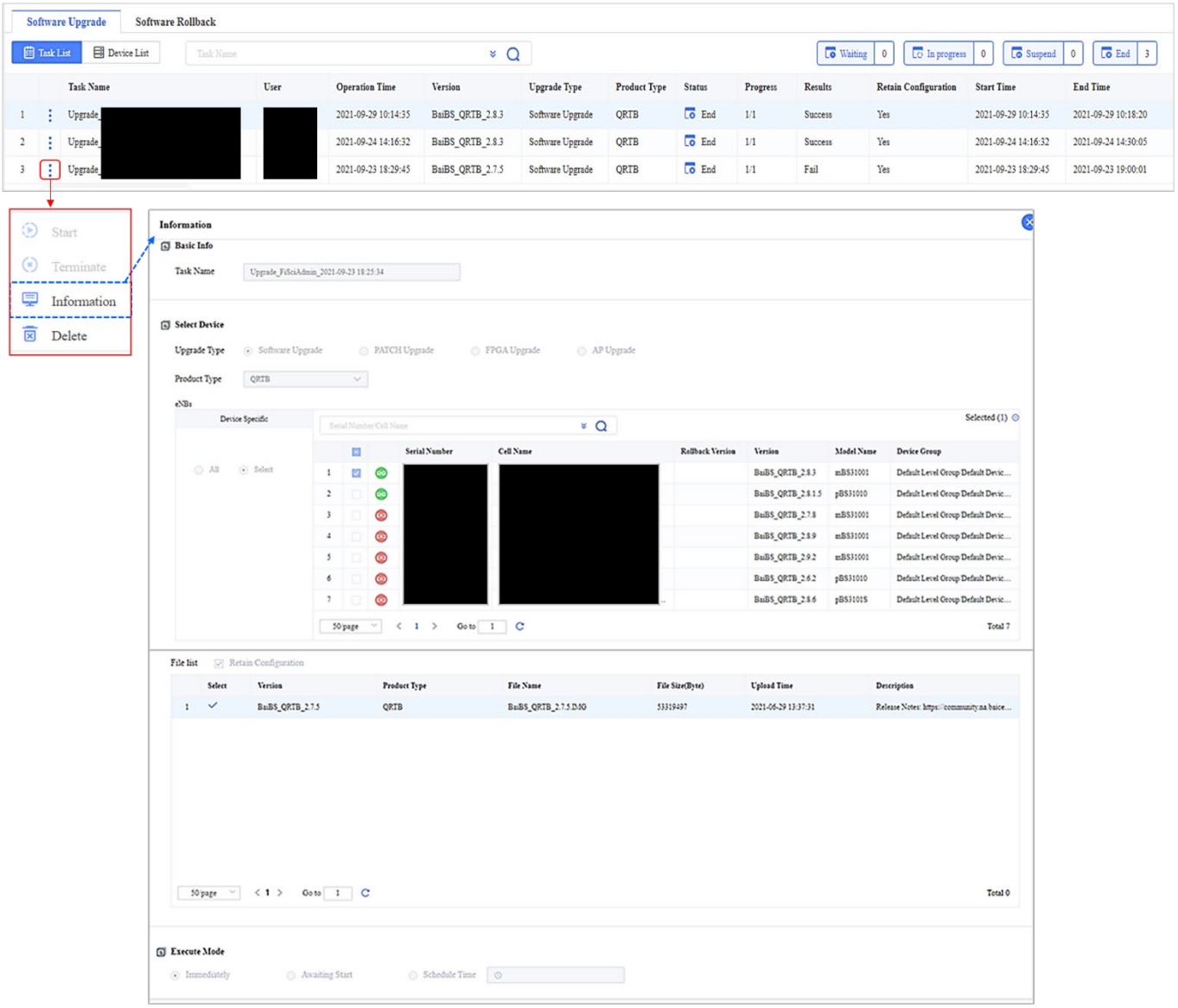
Figure 2-95: eNB > Upgrade > File



2.4.2.4.3 Software Upgrade and Software Rollback

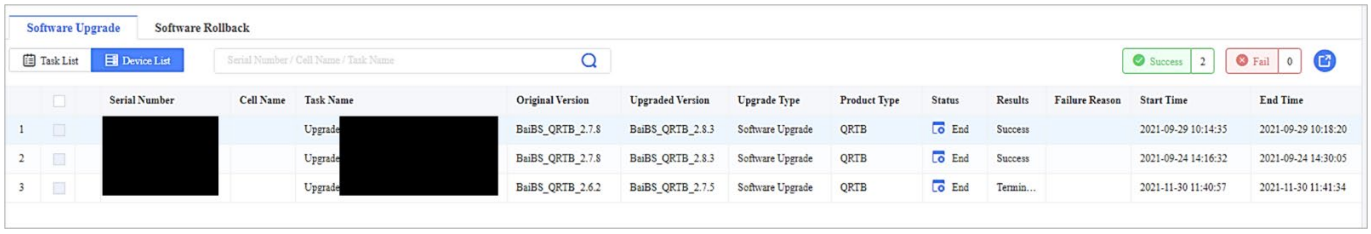
As shown in (Figure 2-96), The *Software Upgrade* and *Software Rollback* window allow you to view any upgrade and rollback tasks in waiting by task or device. In the *Task List,* you will see the task name, the user who created the task, operation time, version, upgrade type, product type, status, progress, results, retain configuration, and the start and end time of the task. The *Operations* actions are *Start, Terminate, Information, and Delete*.

Figure 2-96: Task List



In the Device List (Figure 2-97), you will see the serial number, cell name, task name, original version, upgraded version, upgrade type, product type, status, results, failure reason, and the start and end time.

Figure 2-97: Device List



2.4.2.4.4 Upgrade From the OMC Upgrade Messages

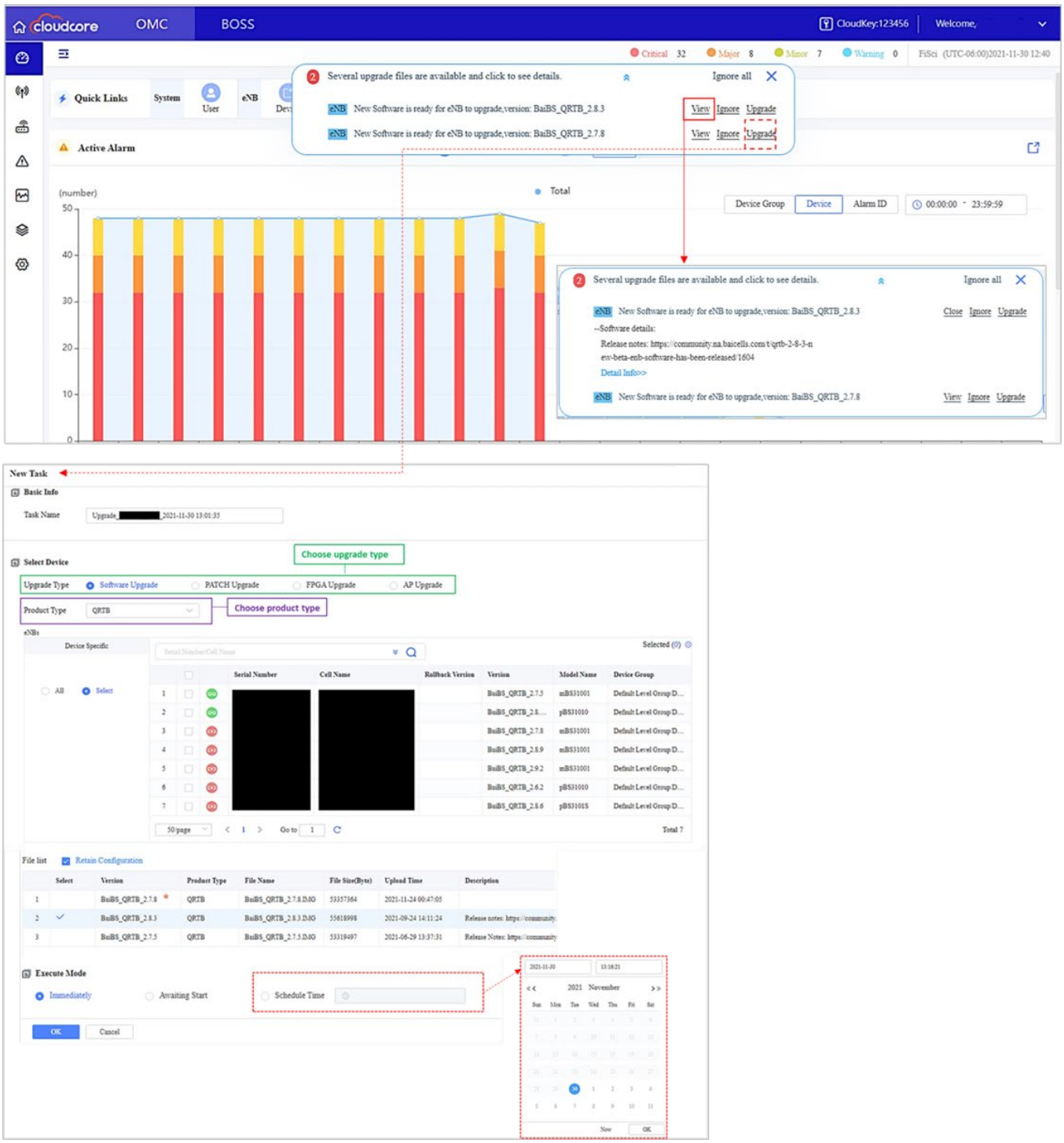
Baicells notifies operators of available new software/firmware versions using a message format at the top of the OMC window explained in (Figure 2-98). If you click on the down arrow, the message window displays each available software version. It gives you the ability to view information about that version, ignore the message, or upgrade to the new software. If you select Upgrade, it opens the Upgrade Task window.

You can configure an upgrade task for one or more eNBs of the same product type (refer to *Table 2-5 Product Types / Software Streams*). Product types are grouped according to their common chipset and software. If you are unsure of an eNB's product type, check the *eNB > Monitor* window Product Type column.

To configure an upgrade task in the Upgrade Task window:

1. Accept the Task Name or enter a new name for this upgrade task.
2. In the eNBs list, you can leave the default list of All the device groups [sic], or you can select a specific device group to filter the list of eligible eNBs for this software version.
3. Select the specific eNBs that you want to include in this task. The eNB will appear in the Selected pane as you click on a checkbox.
4. Select an Execute Type, per *Table 2-6 Execute Modes*, determining when the task executes.
5. Click on *OK* to save the settings. The new task will be added to the eNB Upgrade list. Use the *Operations* function to view results, view eNB information, or delete the task.

Figure 2-98: Upgrade from the OMC Upgrade Messages



2.4.2.5 Inventory

Equipment configured with the operator's CloudKey in the device GUI during initial installation will automatically associate to the operator's OMC account when powered on. Therefore, it will appear in the *eNB > Inventory > Device* list (Figure 2-99). Otherwise, use the *Inventory* menu to add, delete and modify devices and device groups, register devices by adding their serial number, view a list of all CPE's associated with an eNB that is operating in HaloB mode, import and export one or more eNB, and register software licenses.

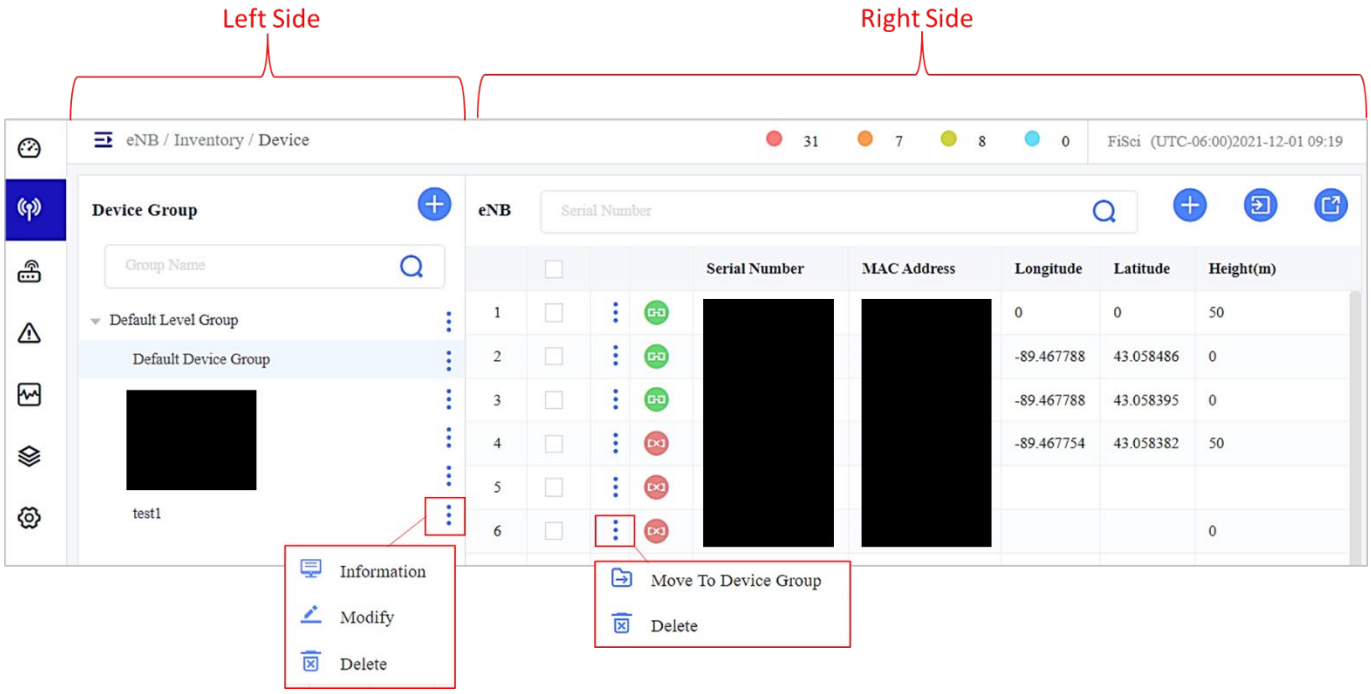
Figure 2-99: Inventory

2.4.2.5.1 Device

The Device menu is where you can create custom eNB device groups; add eNBs to device groups; delete device groups or delete eNBs (Figure 2-100). If not assigned to a custom group, an eNB will be added to the default device group. Using device groups, grouping eNBs with the same parameters or characteristics is valuable in executing configuration changes, reboots, upgrades, and other tasks affecting multiple devices.

NOTE: Default groups cannot be modified or deleted.

Figure 2-100: Device



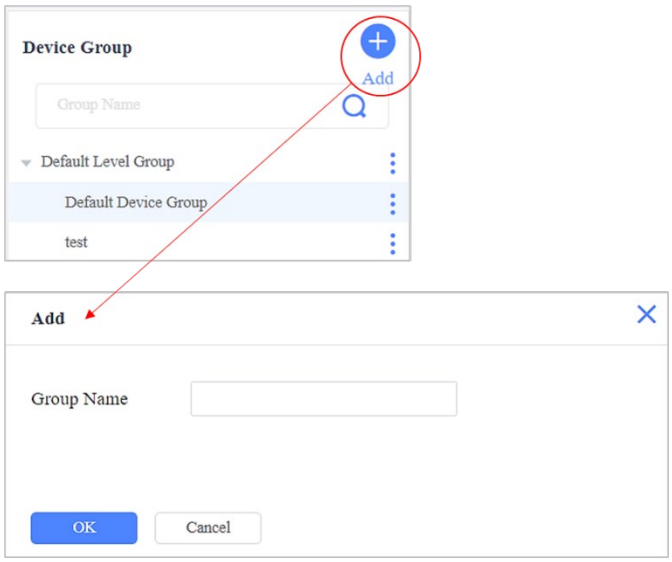
The Device Group pane (left side) lists the default device group and previously defined custom groups. The *Operations* functions allow you to view the group information, and in the case of custom groups, also modify or delete the group.

The right side of the *Inventory > Device* window is a list of the operator's eNBs, showing each one's serial number, MAC address, longitude, latitude, and height. Use the *Operations* functions to move an eNB into a device group or delete an eNB.

To create a new device group (Figure 2-101):

1. Click on the **+** Add icon in the Device Group pane to open the Add Group window.
2. Enter a group name and description.
3. Select the eNBs you want to include in the list.
4. Click on *OK* to save the settings. The new group will appear in the list of device groups.

Figure 2-101: Add Group



2.4.2.5.1.1 Adding an eNB in OMC

The easiest way to add an eNB in the OMC is to configure the operator's CloudKey in the device GUI. When the eNB comes online, it will automatically register in the operator's OMC account. The CloudKey is described in *section 2.2.3, CloudCore GUI Layout*.

You can add an eNB in the OMC either before or after the eNB is online – *online,* meaning connected to the OMC and LTE network. However, it must be online to configure an eNB in the OMC.

You will need the eNB serial number to add it to the OMC. To add an eNB to the OMC:

1. Go to *eNB > Inventory > Device.*
2. Click on the **+** *Add* icon to open the Add eNB window in the upper right.
3. In the empty field, enter the serial number. You can add multiple eNBs by adding a semi-colon (;) at the end and hit *Enter*. Put each serial number in this way on a separate line.
4. Select a device *Group Name* (or let the eNB automatically be placed in the default group).
5. Click on *OK*.

Referring to section 2.4.2.2.6.2 Settings, you can configure an eNB once it is online or change an eNB's settings:

1. Go to *eNB > Monitor*.
2. Find the device in the list, click on the *Operations* icon, and select *Settings > eNB*.
3. Refer to the *eNodeB Configuration Guide* for a description of all the parameters. Once you complete the configuration, click on *OK* to save it.

Or, as described in *section 2.4.2.3.2 Configuration* in the OMC, go to *eNB > Maintenance > Configuration*.

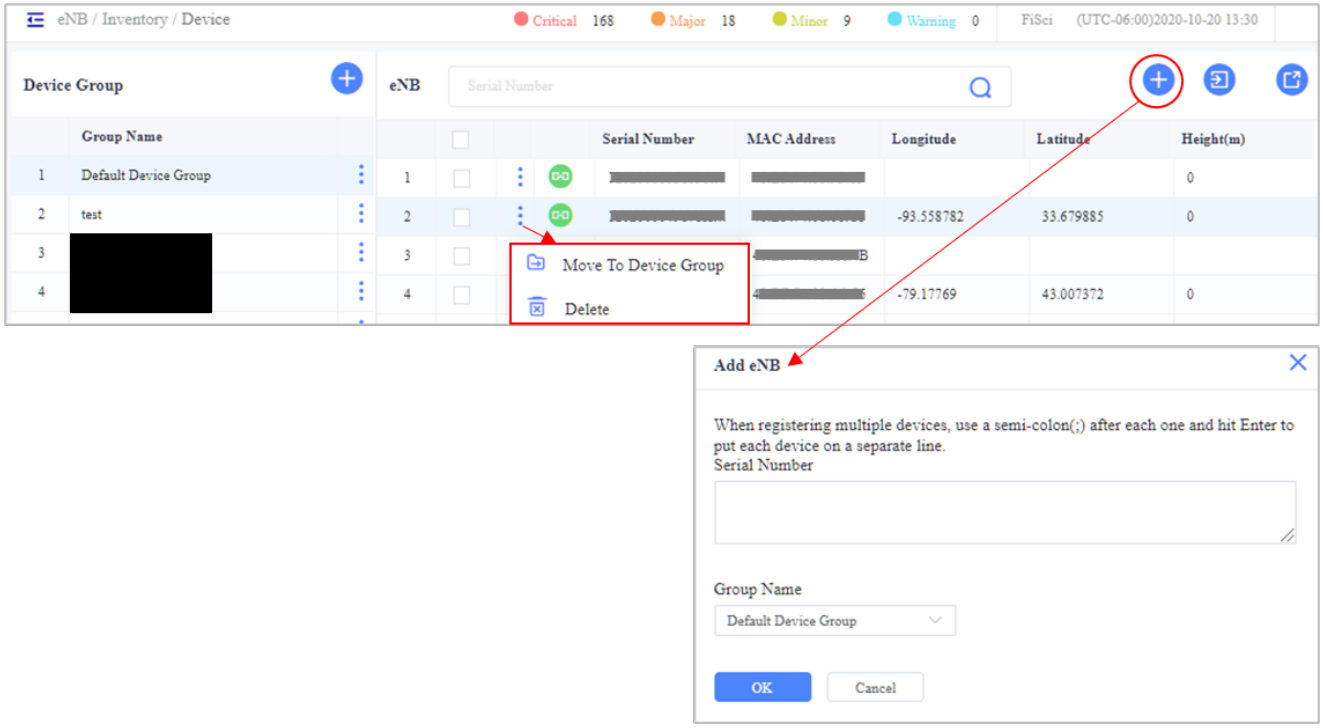
NOTE: Alternatively, in the *eNB > Monitor* window, you can click on the device's IP address to open a new browser tab to the eNB's GUI.

2.4.2.5.1.2 Register an eNB in OMC

To register an eNB in OMC (Figure 2-102):

1. Click on the **+** Add icon to open the Add eNB window.
2. Enter the eNB serial number for each eNB. You can add more than one eNB simultaneously by entering each serial number on a separate line, using a semi-colon (;) at the end of each entry, and hitting Enter.
3. If you want to add the eNBs to a device group, use the pull-down Group Name field to select the group.
4. Click on *OK* to save the settings. The new eNB will be added to the eNB list.

Figure 2-102: Register eNB in OMC

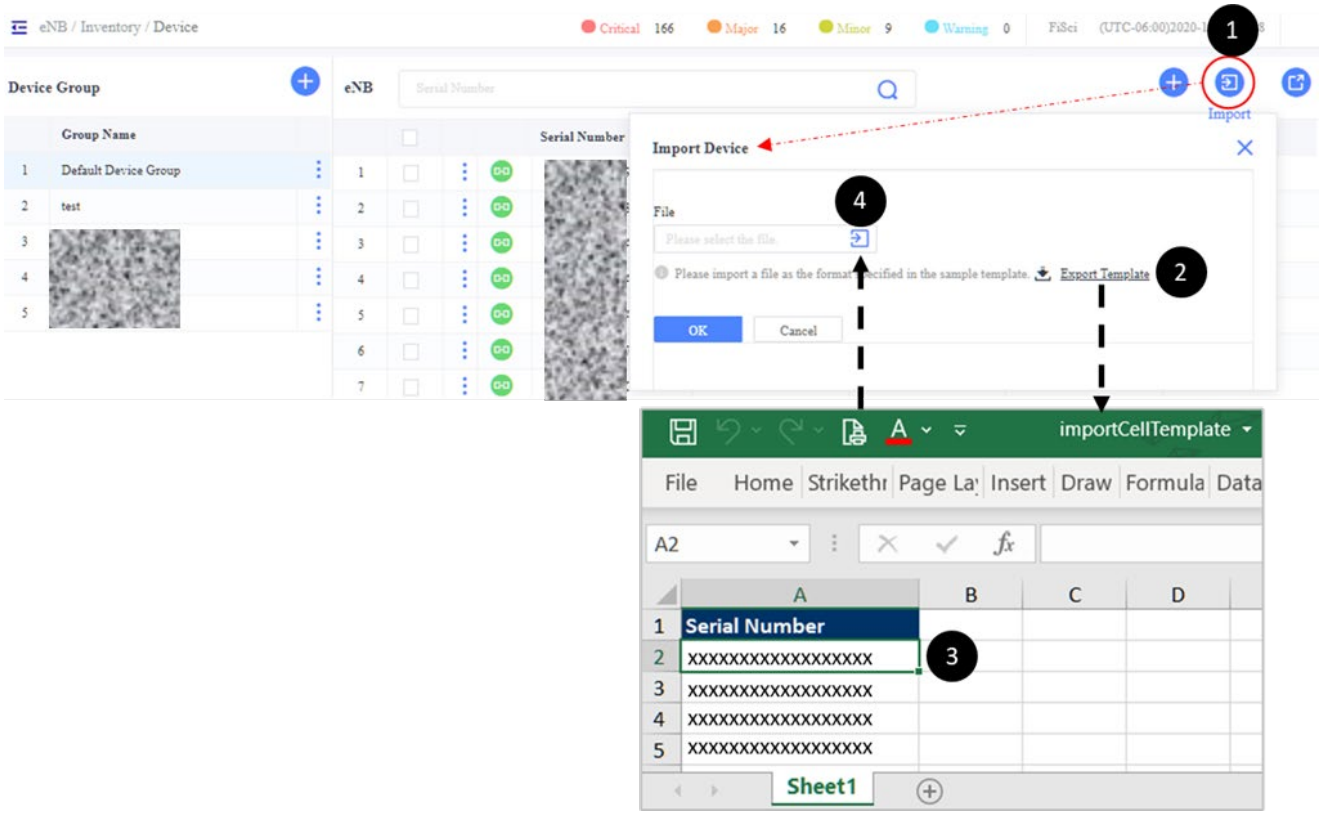


2.4.2.5.1.3 Import Multiple eNBs

Another way to add multiple eNB devices is by importing the information using a template. To use this method (Figure 2-103):

1. Click on the Import icon to open the Import Device window.
2. Select Export Template and save the file to your computer (do not change the file name).
3. Enter the eNB serial numbers on each row of column A in the template and save the file.
4. Click on the File field icon to navigate the completed template and import it.
5. Click on *OK* to save the settings. The new eNBs will be added to the eNB list.

Figure 2-103: Import eNB information



2.4.2.5.2 License

Licenses are required for specific software options and are issued on a per-eNB basis based on the serial number. Examples of software licenses are HaloB, Carrier Aggregation (CA), and Dual Carrier (Split Mode).

NOTE 1: Not all licensed features are available on all eNB models.

NOTE 2: Some licenses are issued by quantity, and some have expiration dates. The OMC will generate an alarm (ID 13) 30 days before the license expiration.

2.4.2.5.2.1 Basic License

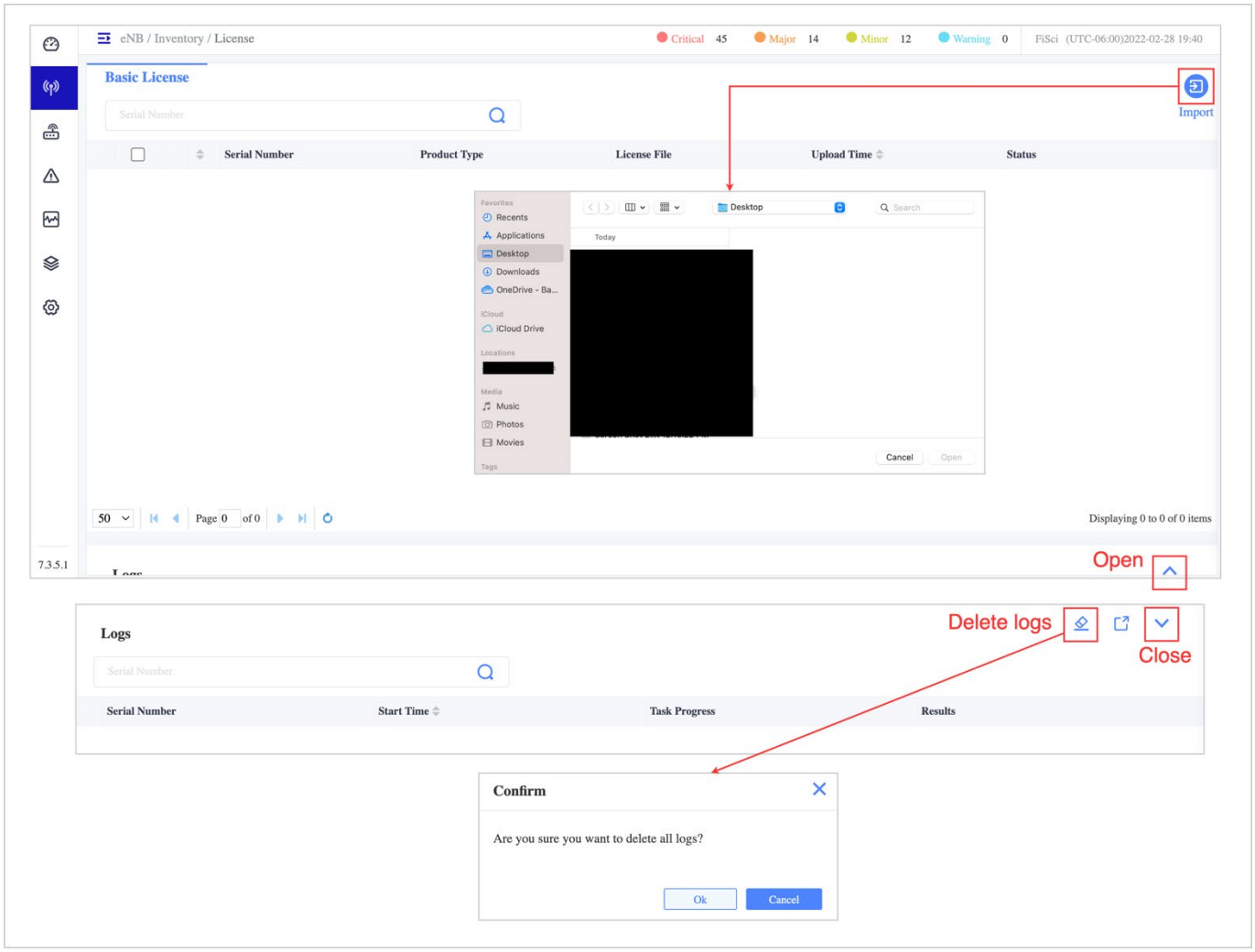
In the *Inventory > License* window (Figure 2-104), the *Basic License* tab will display the list of license files by serial number. At the bottom of the window, you can view or delete the log of imported licenses. The log task list includes the serial number, start time, task progress, and result. Both windows have the option to search for an eNB's license by serial number.

2.4.2.5.2.2 Import Basic License

To import a basic license file:

1. Go to *eNB > Inventory > License*.
2. Click on the import icon, and navigate to the license file.
3. The file will be imported into OMC and included in the Basic License list when you select the file.
4. Find the serial number in the main Basic License tab list and select *Operations > Execute*.

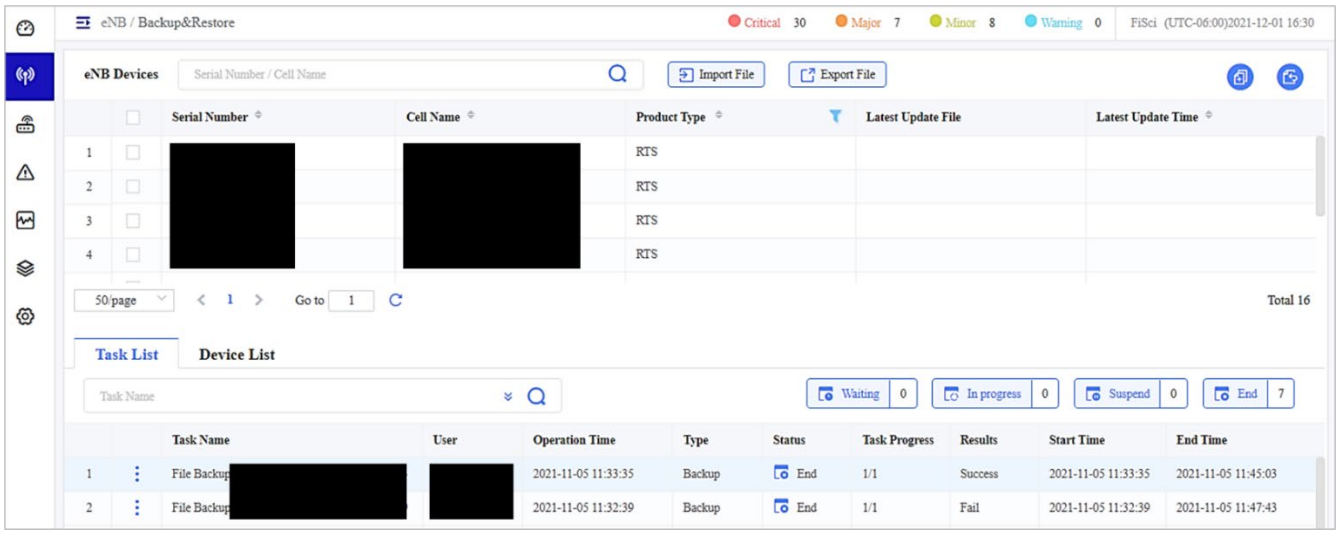
Figure 2-104: Basic License



2.4.2.6 Backup & Restore

Backup & restore is where you can backup and restore one or more eNBs configurations. The *eNB > Backup&Restore* landing page displays eNB devices, a *Task List,* and a *Device List* (Figure 2-105)

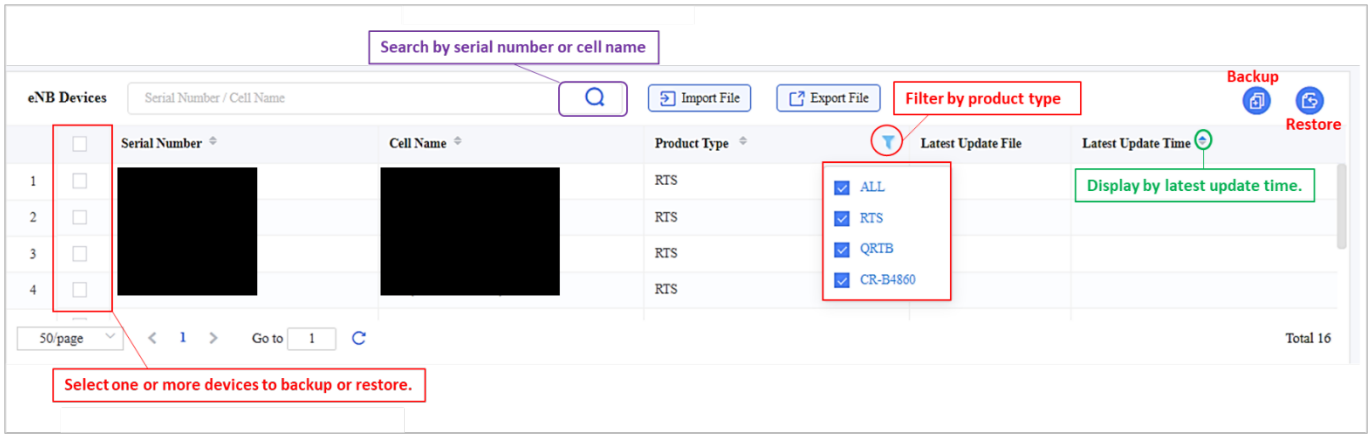
Figure 2-105: Backup & Restore Landing Page



2.4.2.6.1 eNB Devices

The eNB Devices pane (Figure 2-106) displays a device's serial number, cell name, product type, latest update file, and latest update time. To backup or restore one or more device/s, you can search for a device by its serial number or cell name and filter devices by product type. Then select the operation you want to execute (backup or restore).

Figure 2-106: eNB Devices



2.4.2.6.2 Import File/Export File

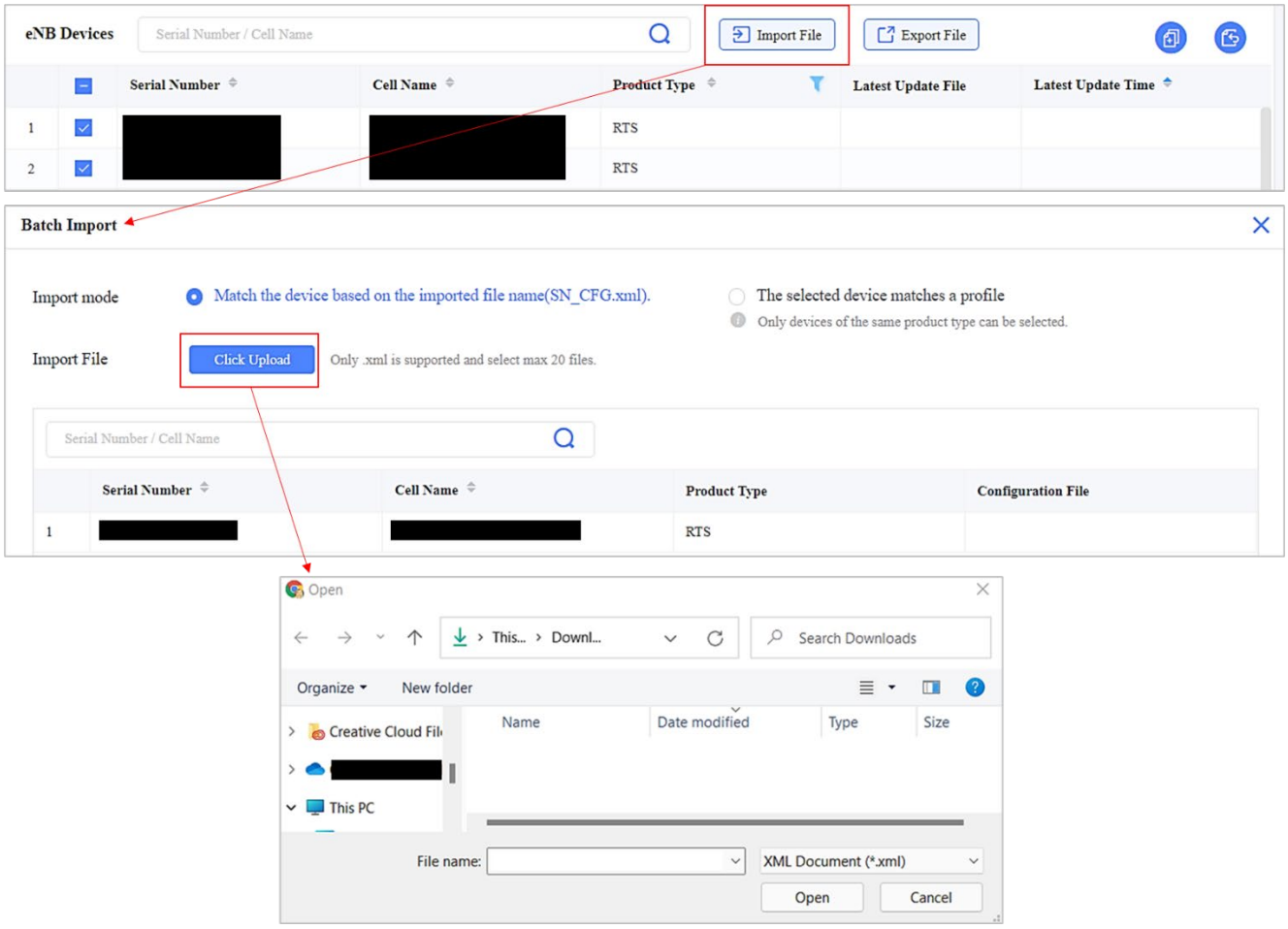
From the *eNB > Backup & Restore > eNB Devices* window, you can import and export configuration files for one or more devices.

To batch import a .xml file (Figure 2-107):

1. Select one or more devices.
2. Click *Import File*.
3. In the *Batch Import* window, select *Click Upload*.
4. Navigate to the file/s you wish to upload and select *Open*.

Note: The maximum number of files that can be imported is 20.

Figure 2-107: Import File



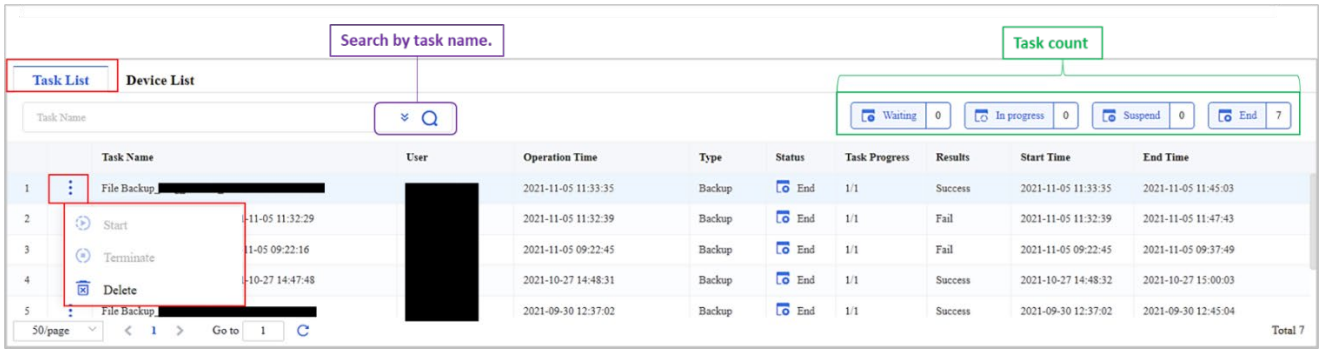
To export a .xml file:

1. Select one or more devices using the checkbox/es.
2. Select *Export File*.
3. Open, unzip, and save the file to your computer.

2.4.2.6.3 Task List

The *Task List* (Figure 2-108) contains a count of tasks in waiting, in progress, tasks suspended, and tasks that have ended. The task list includes the task name, the user who performed the task, the operation time, type, status, progress, results, and the start and end time. You can start, terminate, and delete tasks by selecting the *Operations* function next to the task name.

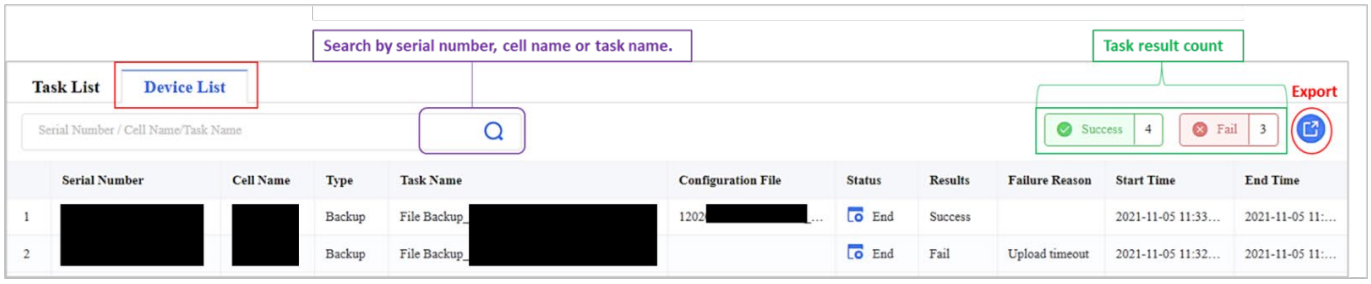
Figure 2-108: Task List



2.4.2.6.4 Device List

The *Device List* (Figure 2-109) contains a count of tasks assigned to a device and the success or failure status. The Device List includes the serial number, cell name, type (of task), task name, configuration file name, status, results, failure reason, and start and end time. You can search for a task by serial number, cell name, or task name. There is an option to download the *Backup&Restore* task device list.

Figure 2-109: Device List



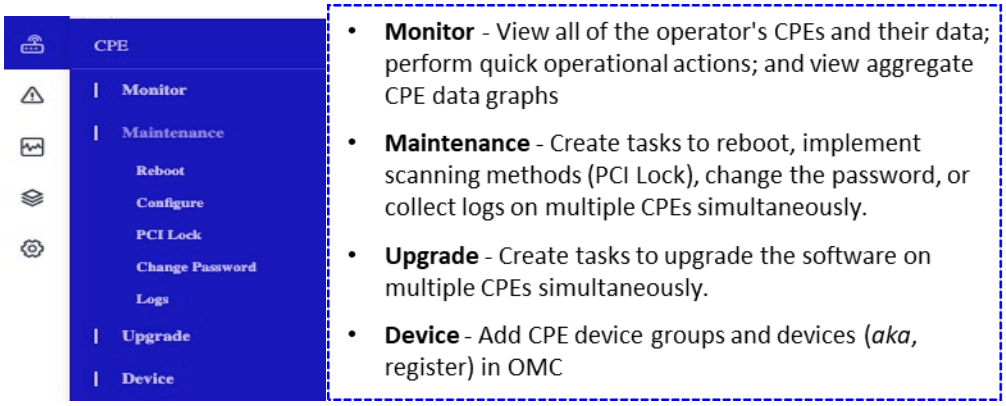
2.4.3 CPE Menu

2.4.3.1 Description of Sub-Menus

The CPE menu provides essential functions for managing, monitoring, and maintaining CPEs in the operator's network (Figure 2-110). Each sub-menu is described below the figure.

NOTE: Some menu items are available only to Beta customers trialing new features.

Figure 2-110: CPE Menu



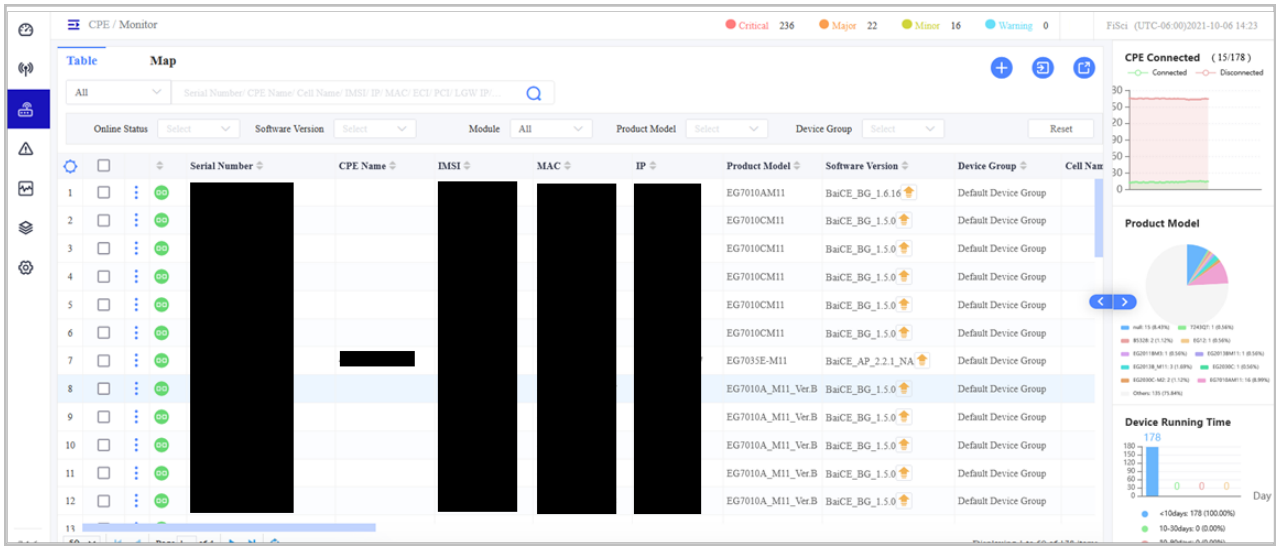
- **Monitor** - View all of the operator's CPEs and their data; perform quick operational actions; and view aggregate CPE data graphs
- **Maintenance** - Create tasks to reboot, implement scanning methods (PCI Lock), change the password, or collect logs on multiple CPEs simultaneously.
- **Upgrade** - Create tasks to upgrade the software on multiple CPEs simultaneously.
- **Device** - Add CPE device groups and devices (*aka*, register) in OMC

2.4.3.2 Monitor

2.4.3.2.1 Landing Page Description

The *CPE > Monitor* window contains two tabs (Table and Map), and the window opens first to the Table tab view (Figure 2-111). Each tab is described in more detail in the following sections. See Table 2-7 for a description of the *CPE > Monitor* fields and graphs.

Figure 2-111: CPE > Monitor General Layout



2.4.3.2.2 Table Tab Description

The Table tab view displays a list of the operator's CPE devices. In the Table tab view, you can sort the CPE devices list using the filtering fields across the top of the page; the pull-down options for each field are shown in Figure 2-112. The Table tab view has two main sections - the list of CPEs with their stats on the left (Figure 2-113) and the graphs of aggregate CPE data on the right (Figure 2-114).

Figure 2-112: CPE Monitor – Table Tab (1 of 3)

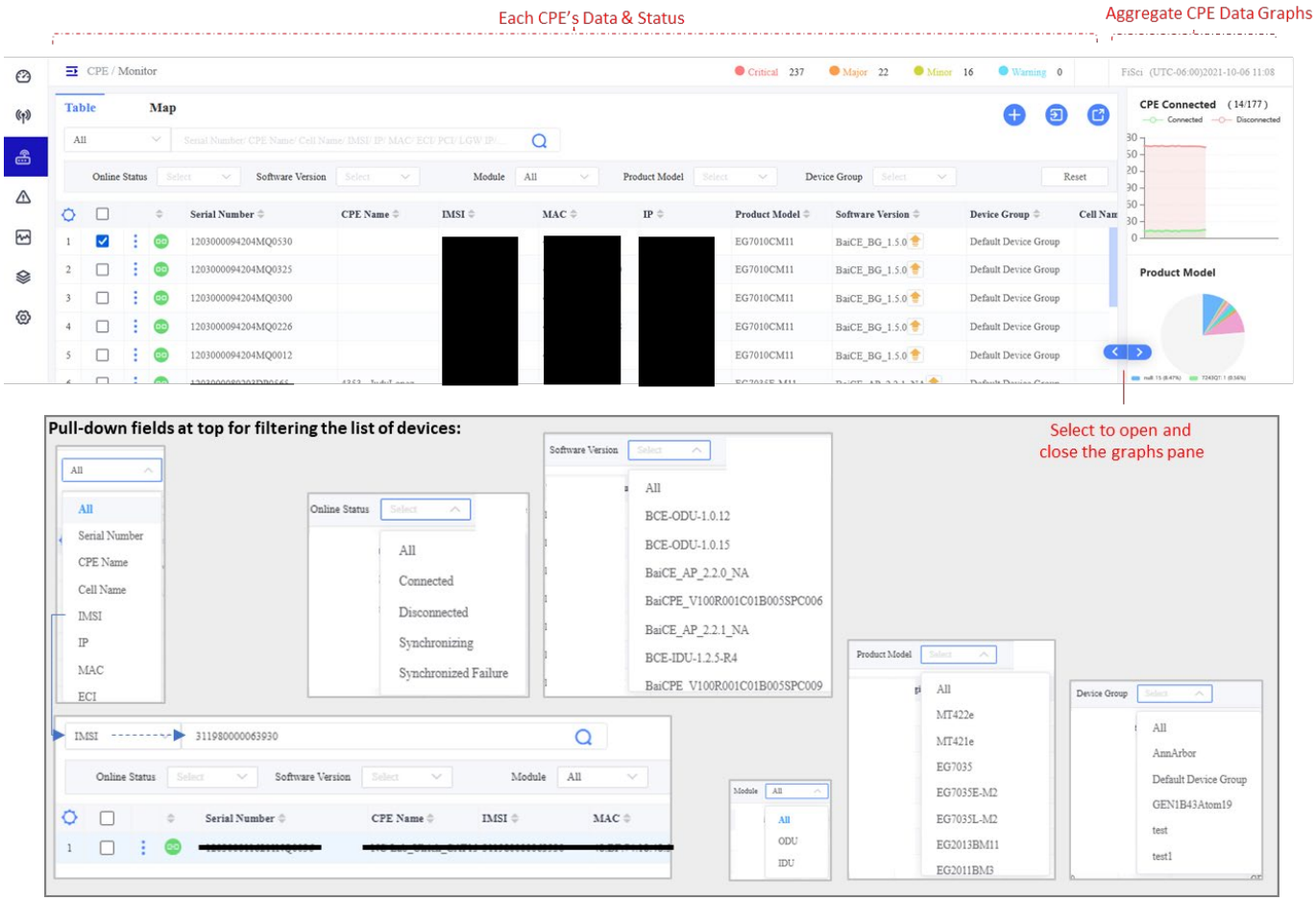
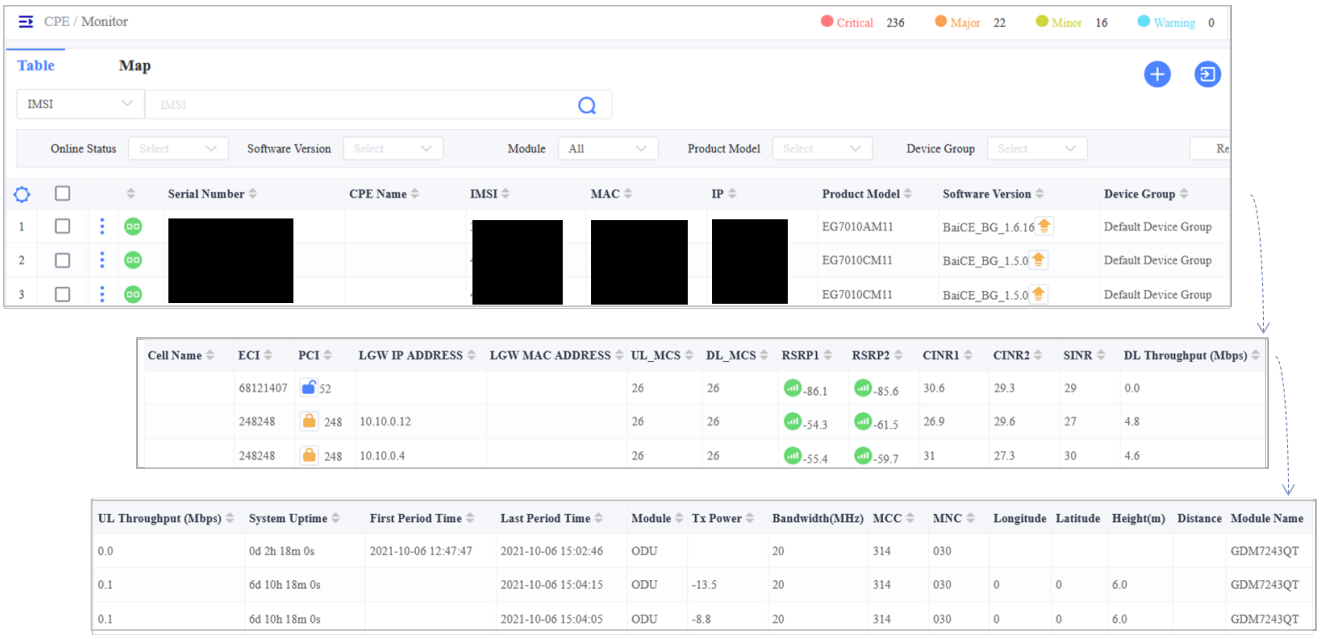


Figure 2-113: CPE Monitor – Table Tab (2 of 3)



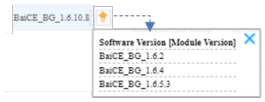
Icons:

Status column:
- Online
- Offline

PCI column:
- One-click to lock the PCI
- One-click to unlock the PCI

Software Version column:
- More up-to-date software is available

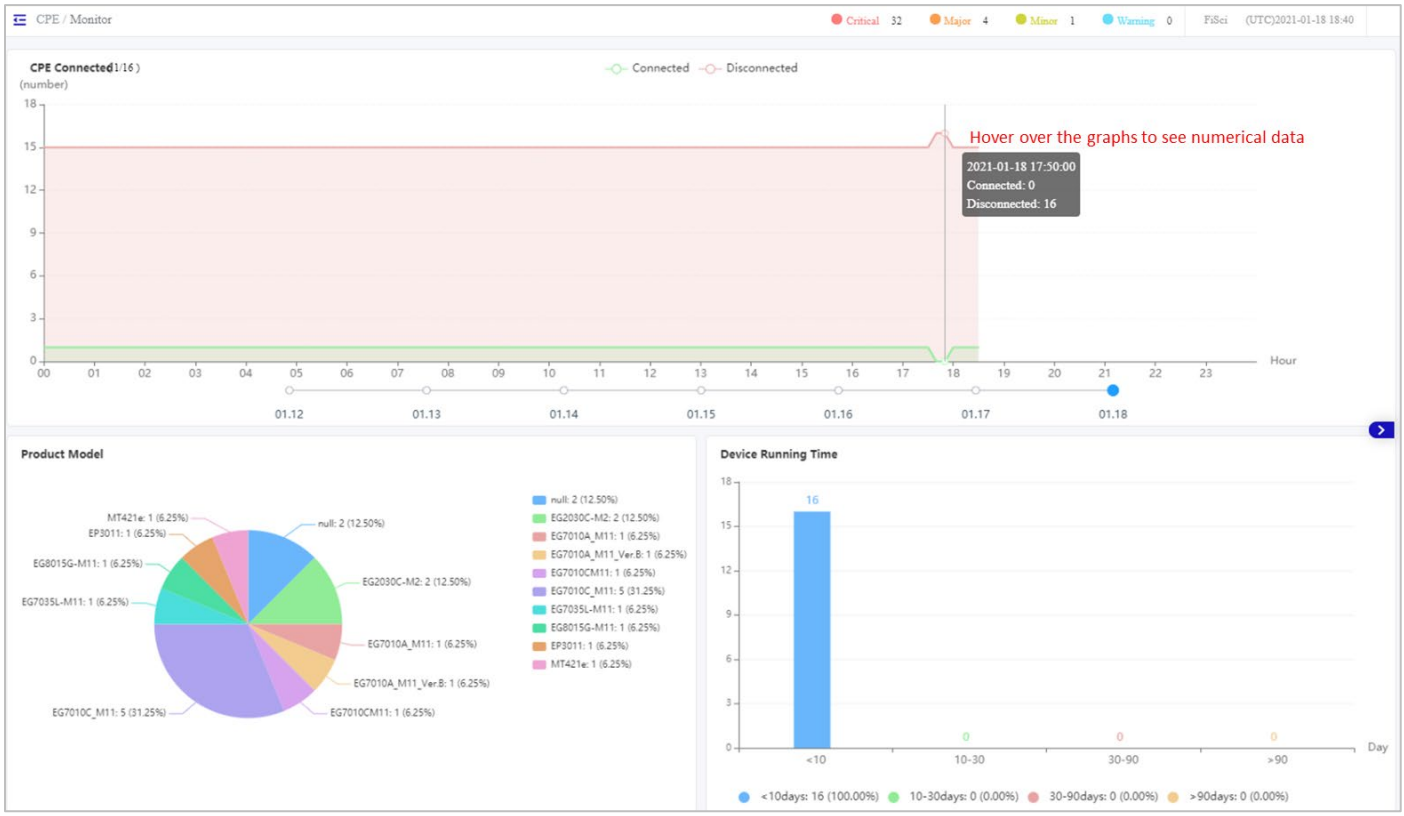
Example:



RSRP columns:

Green: In the normal range
Gold: Almost outside of the normal range
Red: Outside of the normal range

Figure 2-114: CPE Monitor – Table Tab (3 of 3)



2.4.3.2.3 Map Tab Description

The Map tab view shows a topographical map of the CPE devices and their status (Figure 2-115).

Figure 2-115: CPE Monitor Map Tab

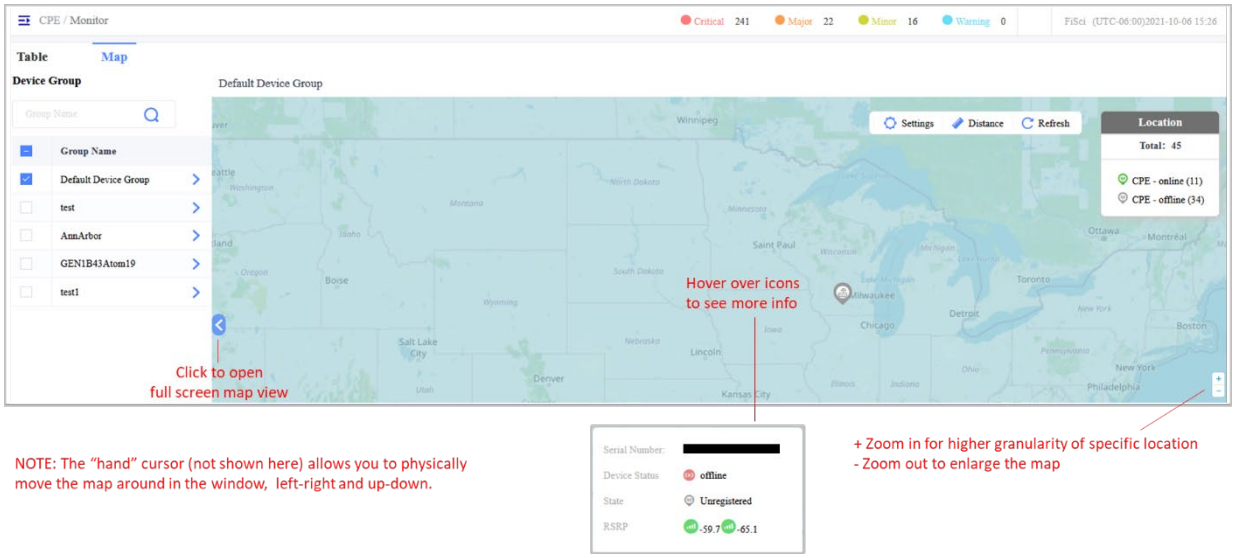
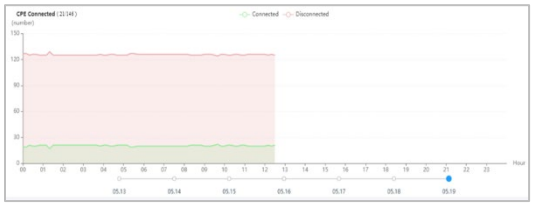
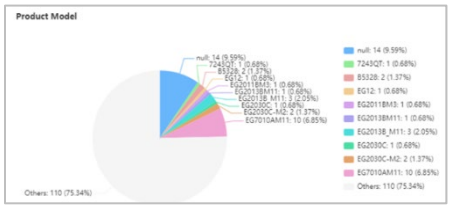
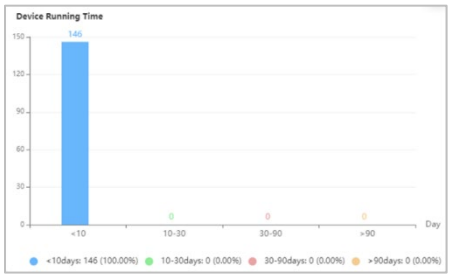


Table 2-7: CPE > Monitor Fields

Field Name	Description
Left Side Data (Per CPE)	
<Untitled>	When you select the row of a CPE and click on the Operations icon a list of actions you can take on that CPE is displayed: Information, Settings, and Reboot. Refer to *section 2.4.3.2.4 Operations*.
<Untitled>	The column with only a filter icon at the top can be used to change the CPE list based on sync status. Green means the CPE device data is synchronized with the OMC, and red means the CPE is offline. Hover over the icon to see the status description. Use the filter icon to toggle the list by sync status, i.e., to see all "green" CPEs first or vice-versa. 
Serial Number	The CPE unit's serial number
CPE Name	Name given to the CPE by the operator
IMSI	The CPE's unique International Mobile Subscriber Identity (IMSI) number
MAC	The CPE unit's MAC address
IP	The CPE's current IP address
Product Model	The specific CPE hardware model

Field Name	Description
Software Version	The current version of software loaded on this CPE. A yellow arrow  next to the version means there is a later version of software available for this CPE product type. Click on the arrow to display the software version(s) that are available. Baicells recommends running the latest version available to address any known bugs that have been fixed as well as to provide the latest features.
Device Group	The configured CPE device group to which this CPE belongs
Cell Name	The name of the cell in which the CPE's currently serving eNB is identified
ECI	E-UTRAN Cell Identifier -- LTE identifier for an operator's cell site; each ECI/site have multiple eNBs, each with a unique Physical Cell Identifier (PCI)
Scan Mode	Refer to *Table 2-8 Scan Modes* for a description of each option
PCI	Currently serving eNB's Physical Cell Identifier, or Layer 1 identity, which uniquely identifies each cell site in the wireless network. The blue lock icon means the CPE is not locked to an eNB; the gold icon indicates it is locked to an eNB's PCI(s) and/or EARFCN(s) (frequency).
LGW IP Address	The IP address of the eNB to which the CPE is currently attached. A clickable IP address feature is added.
LGW MAC Address	The MAC address of the eNB to which the CPE is currently attached
UL_MCS	The currently serving eNB's Modulation and Coding Scheme (MCS) index value on the uplink. The value is based on channel quality. If the value reaches single digits, you likely have channel quality problems.
DL_MCS	The currently serving eNB's Modulation and Coding Scheme (MCS) index value on the downlink. The value is based on channel quality. If the value reaches single digits, you likely have channel quality problems.
LTE Uptime	The LTE Uptime represents the RF active duration in-terms of days hours minutes seconds
DL BLER	This indicates the block error rate and is used to determine the in-sync or out-sync indication during radio link monitoring.
RSRP1 and RSRP2	Reference Symbol Received Power (RSRP) is an LTE power metric, in dB, which indicates signal strength. RSRP uses an average of the RF power in each subcarrier. If there are 2 antenna cables from the eNB to the RF antenna, or dual polarity, RSRP is reported on each. Weak signal strength can cause connectivity issues and dropped sessions.
CINR1 and CINR2	Carrier-to-Interference-plus-Noise Ratio (CINR) is a measurement (dB) of multiple subcarriers, which reflects the signal quality of the LTE carrier system. (For most eNBs there are 2 antenna cables from the eNB to the RF antenna, with dual polarity. The system measures the CINR on each.)
SINR	Signal-to-Interference-plus-Noise-Ratio (SINR), also known as the carrier-to-interference ratio (CIR or C/I), is a quantity (dB) used to give theoretical upper bounds on channel capacity. SINR is calculated based on the power of a certain signal of interest divided by the sum of interference power from all the other interfering signals and background noise.
DL Throughput (Mbps)	The current downlink data rate from eNB to CPE - in Megabits per second (Mbps)
UL Throughput (Mbps)	The current uplink data rate from CPE to eNB - in Megabits per second (Mbps)

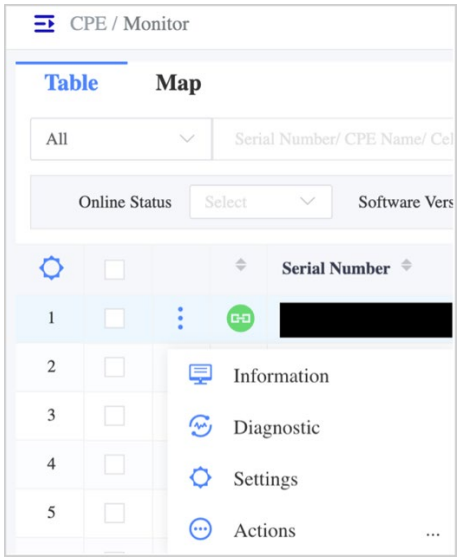
Field Name	Description
System Uptime	Number of hours the CPE has been powered on
First Period Time	The first day and time the OMC got an inform message from the CPE, e.g., is online
Last Period Time	The last updated day and time the OMC got an inform message from the CPE, e.g., is offline
Module	Indoor Unit (IDU) or Outdoor Unit (ODU)
Tx Power	Current CPE transmit power, in dBm
EARFCN	The CPE needs to operate on the same EarFcn of eNB
Bandwidth	Channel bandwidth used by the eNB and CPE, e.g., 20 MHz or 10 MHz Depending on the CPE model and software version, the field display as 20000 or 20 for 20 MHz, or 10000 or 10 for 10 MHz
MCC	Mobile Country Code - used to uniquely identify the operator of a telecommunications network. MCC + MNC = PLMN.
MNC	Mobile Network Code - uniquely identifies a mobile network operator (carrier) using the GSM (including GSM-R), UMTS, and LTE public land mobile networks. MCC + MNC = PLMN.
Longitude	CPE antenna longitude
Latitude	CPE antenna latitude
Height(m)	CPE antenna height, in meters
Distance	The operator can enter the distance between the CPE and the serving eNB for reference
Link Condition	This shows the condition or reliability of the radio link between the CPE and eNB
Module Name	Name of the CPE hardware module, e.g., MT422e
Module Version	The CPE software module version
Right Side (Aggregate Data Graphs)	
CPE[s] Connected / Disconnected	Displays the number of CPEs connected (green) and disconnected (red) to/from the network out of the total number of CPEs. Hover over the graph to see the numerical data for a given data point. Example: 
Product Model	Pie chart indicates the number and percentage of CPEs per model name Example: 

Field Name	Description
Device Running Time	Graph of the number and percentage of CPEs running < 10 days, 10-30 days, 30-90 days, and > 90 days Example: 

2.4.3.2.4 Operations

The *CPE > Monitor Operations* on each row of CPEs includes information about the CPE, the available CPE settings, and actions such as rebooting the CPE (Figure 2-116).

Figure 2-116: CPE Operations



2.4.3.2.4.1 Information

The *Operations > Information* window has two sections. On the left are data fields; on the right are graphs. The left side includes the CPE's identity details, serial number, model, current software version, etc., and its wireless and LAN connection status (Figure 2-117).

If a CPE has a CBRS SAS* license, the window will include a CBSD Status pane at the bottom. The pane provides the only action you can take from the Information window to enable/disable SAS operation on the CPE. This pane also shows the CPE's connection status with the SAS provider. You can jump from the Information window into the Settings window by clicking on the Settings icon in the upper right.

*NOTE: Please refer to the *SAS Deployment Guide* for information about this feature.

To expand the right side of the window, click on the blue arrow pointing left . The graphs render cumulative, historical LTE measurements for the CPE (Figure 2-118 and Figure 2-119). These measurements are essential to understanding the CPE's wireless communications with the serving eNB(s) and the backhaul network. Information about performance metrics can be found in *section 2.4.5 Performance Menu*.

If you hover your cursor over any point on a graph, it will display the numerical data for that data point. You can change the time reported in the History graphs by selecting either Day or Month in the top right of the window. Selecting Day will report the last seven days of KPIs, beginning with today's date. Selecting Month will report the current month and then the previous 4-month, 8-month, and 12-month periods so you can compare the CPE's performance over time.

Figure 2-117: CPE Monitor Information (Left Side)

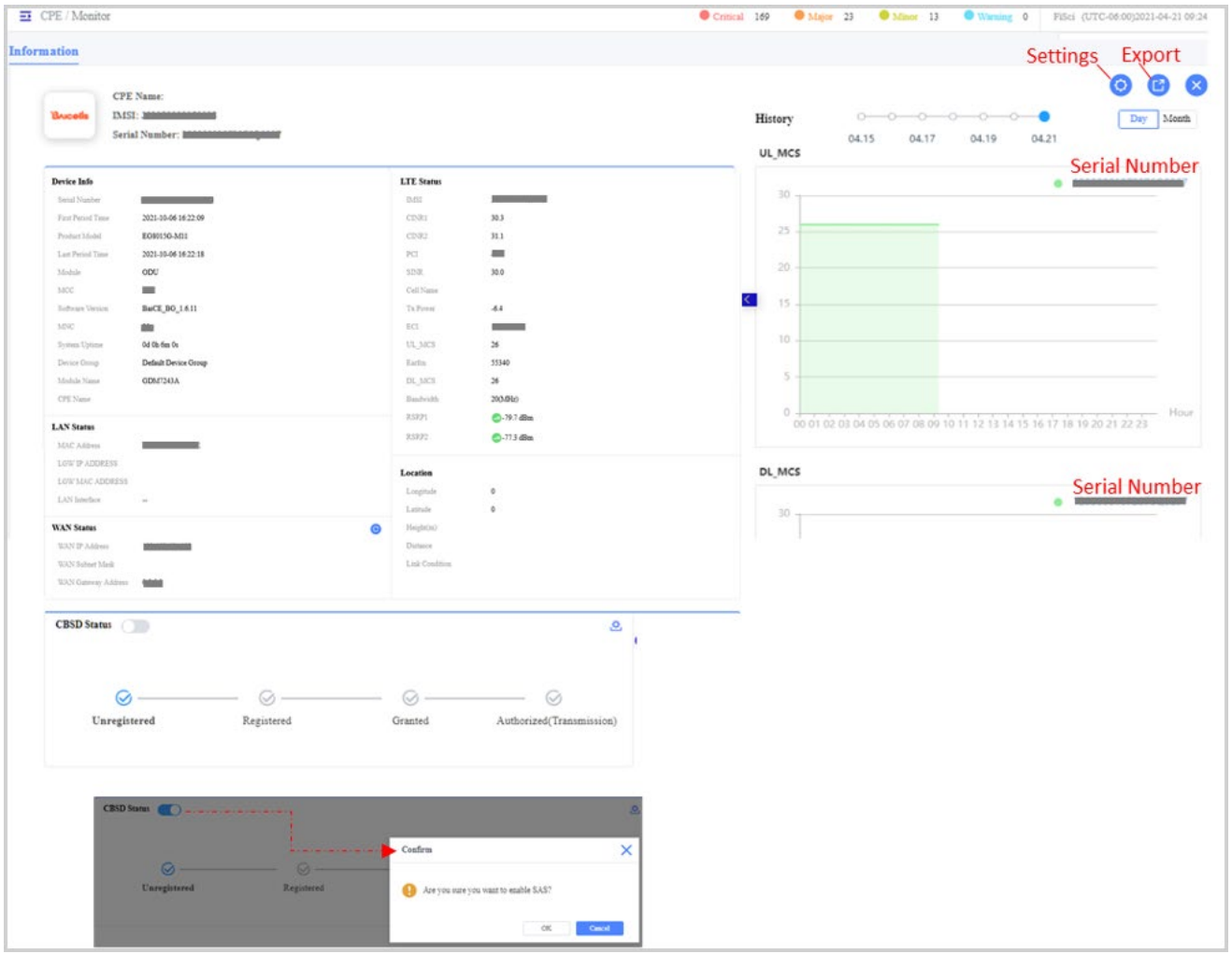


Figure 2-118: CPE Monitor Information – Graphs (Right Side, 1 of 2)

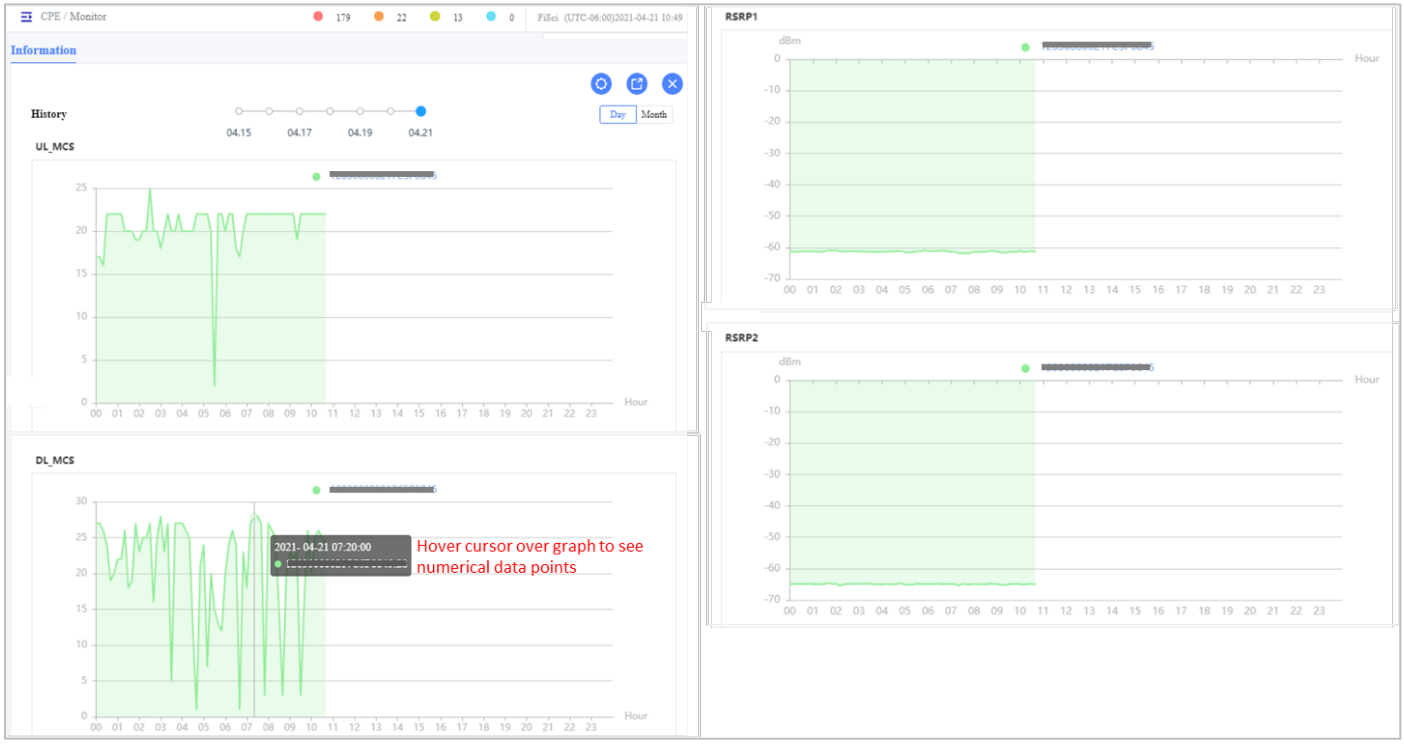
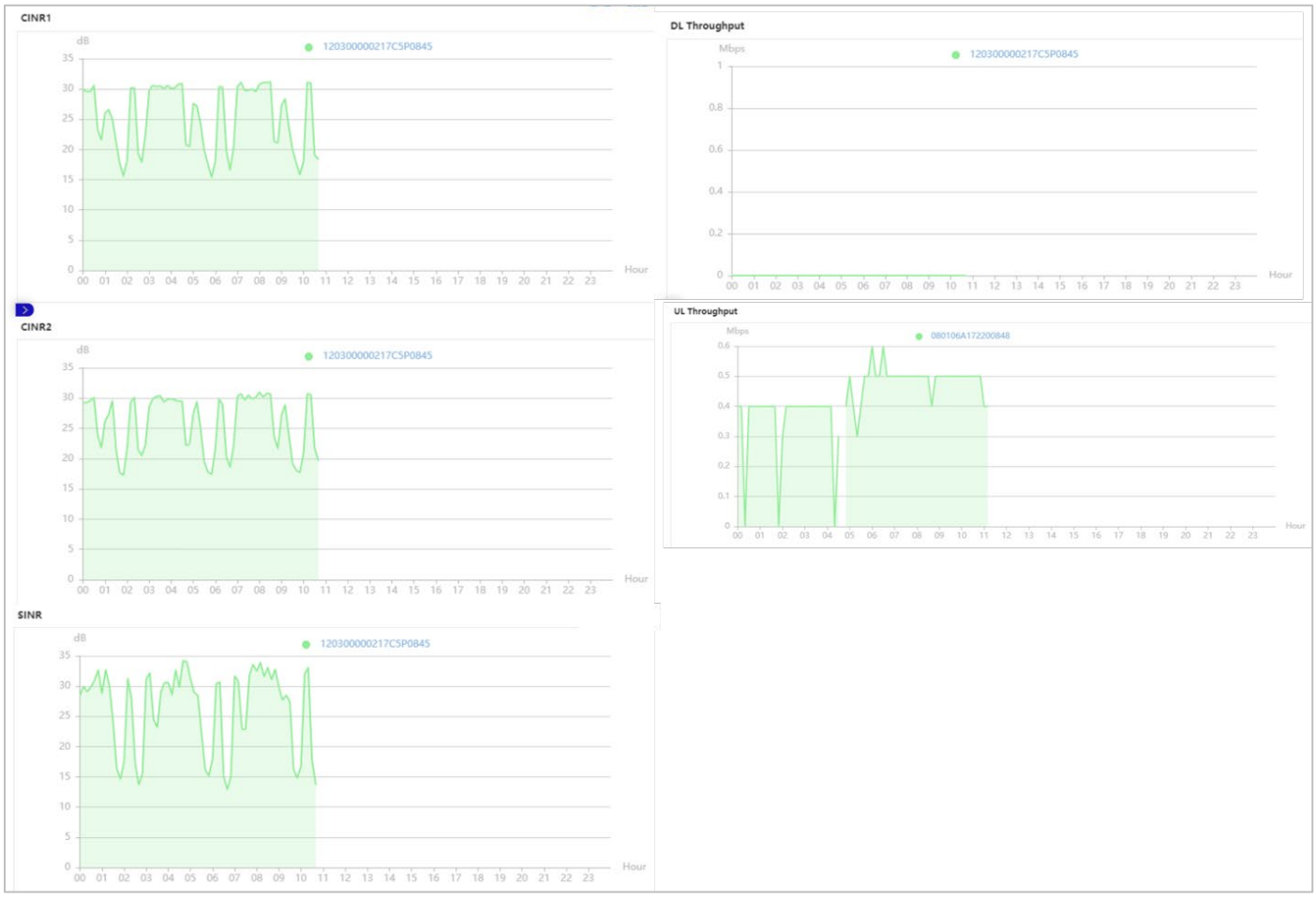


Figure 2-119: CPE Monitor Information – Graphs (Right Side, 2 of 2)

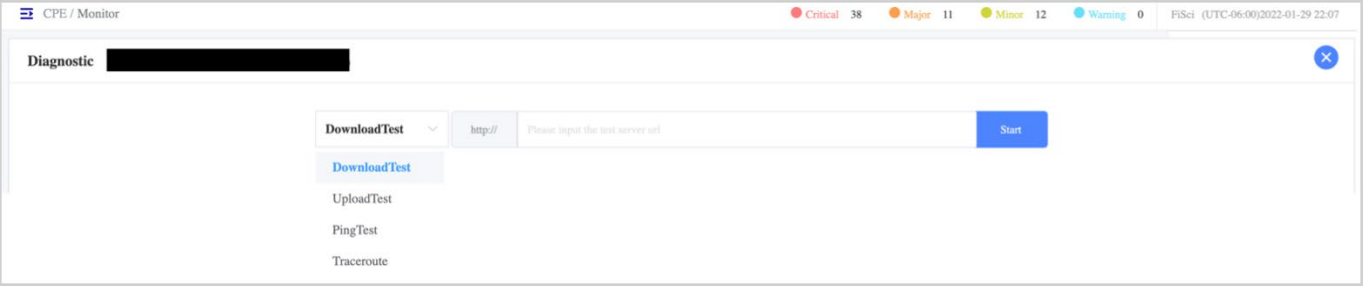


2.4.3.2.4.2 Diagnostic

To monitor and diagnose the state of the network path serving numerous subscribers who use the CPE, the operators can leverage this generic diagnostic tool to provide a platform for validating QoS objectives. A vital benefit of this tool is that the operators can procure CPE performance data and identify the fault point that seems weak and likely to cause problems. You can perform DownloadTest, UploadTest, PingTest, and Traceroute functions through this Diagnostic feature. The diagnostic tab will open by clicking the *Operation > Diagnostics* (Figure 2-120).

NOTE: To get help to configure the Diagnostic settings, contact the support team.

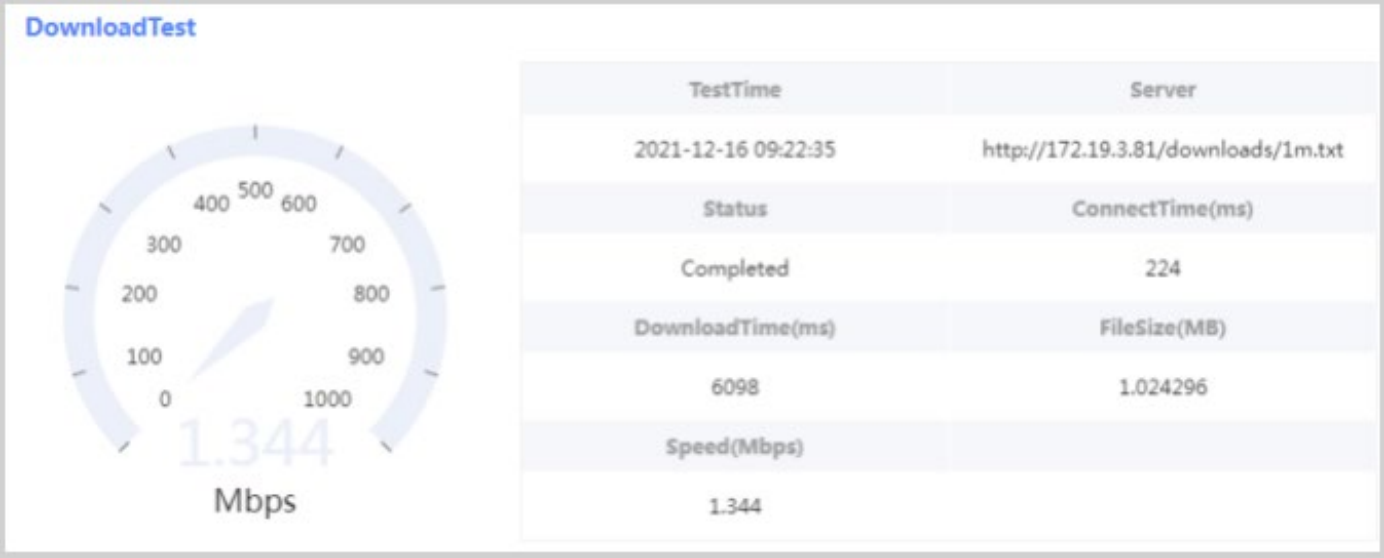
Figure 2-120: Diagnostic



- **DownloadTest**

  This feature can test the download speed of CPE files and display parameters such as TestTime, Time server address, Status, ConnectedTime (ms), DownloadTime (ms), FileSize (MB), and Speed (Mbps) refer (Figure 2-121).

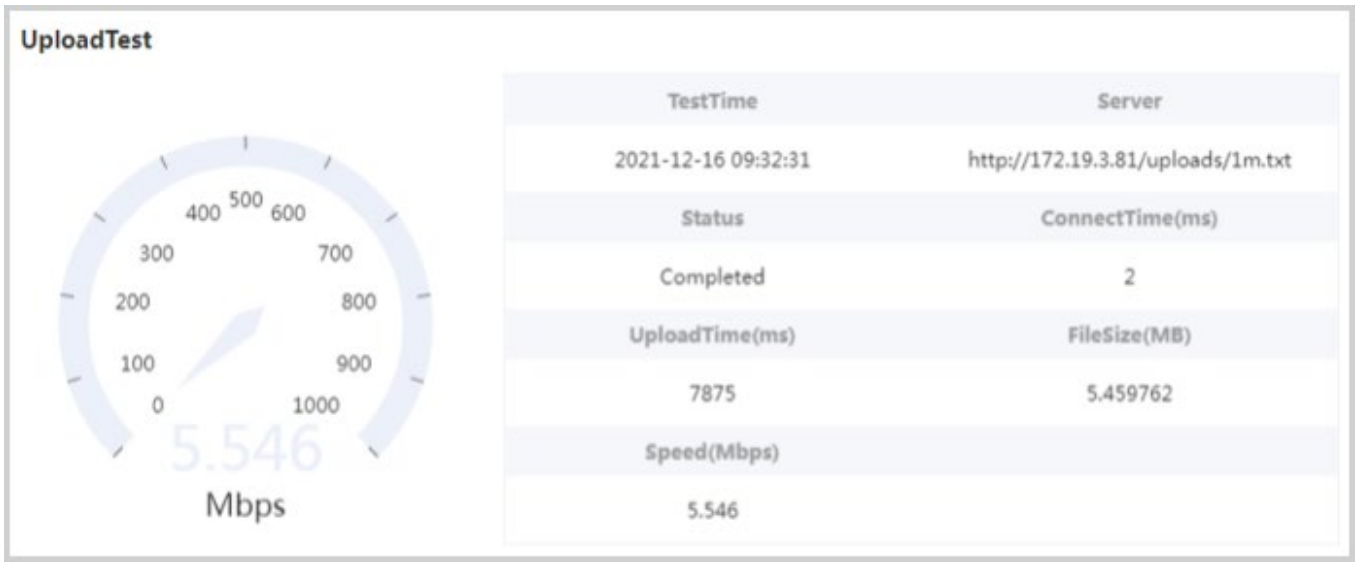
Figure 2-121: DownloadTest



- **UploadTest**

  To test the upload speed of CPE files and display parameters such as TestTime, Test server address, Status, ConnectedTime (ms), UploadTime (ms), FileSize (MB), and Speed (Mbps), refer to (Figure 2-122).

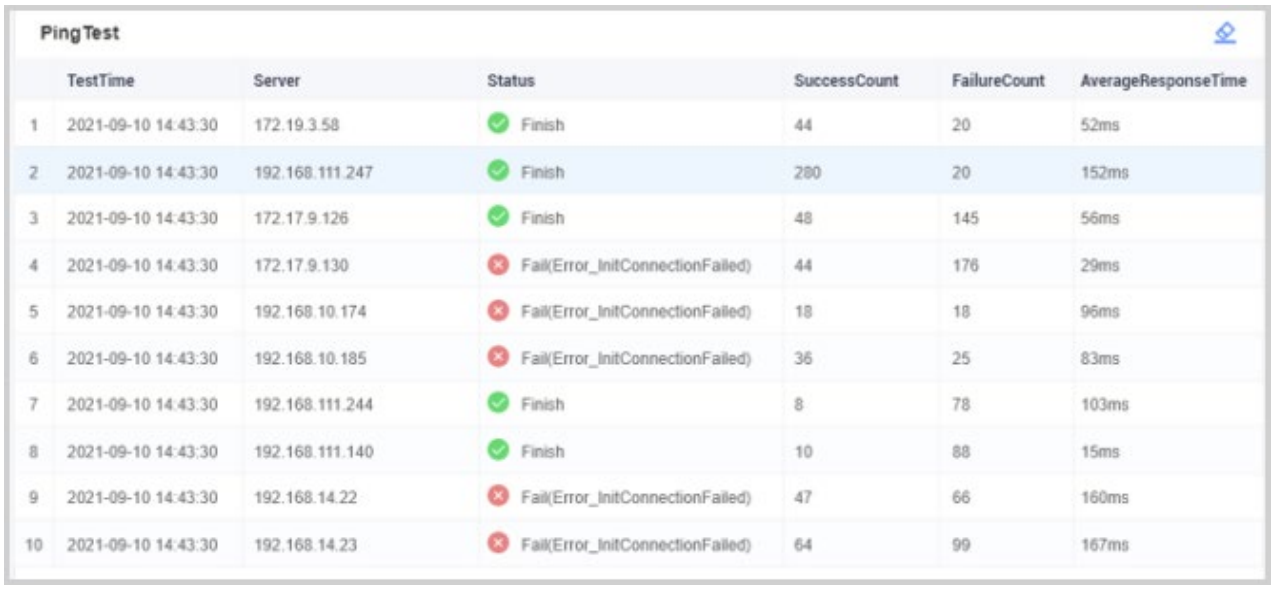
Figure 2-122: UploadTest



- **PingTest**

  Ping is a network utility that helps in sending signals out across the network to the CPE, which then sends its signal back. This signal is the Average Response Time in milliseconds (ms), which helps the operator know how long it takes for a packet of data to travel from the CPE to a server on the internet and back. PingTest helps identify the latency and connection between CPE and the server. The ping test displays parameters such as TestTime, URL of Test Server, Status, Success Count, Failure Count, and Average Response Time as shown in (Figure 2-123).

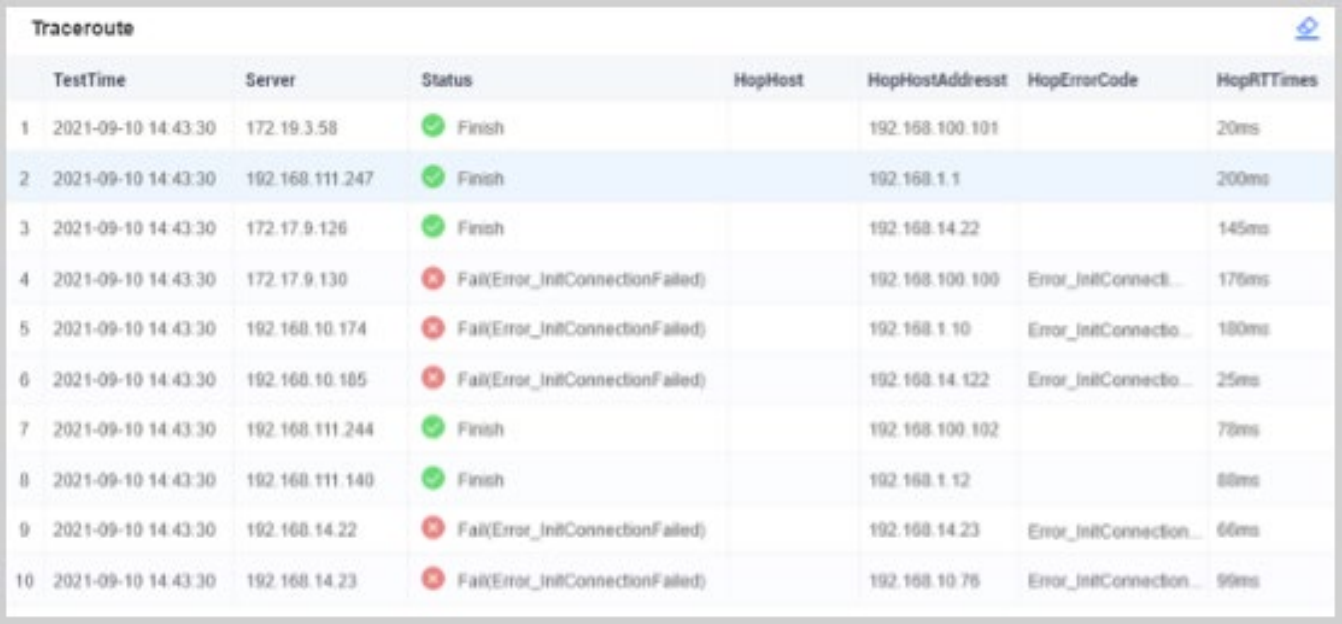
Figure 2-123: PingTest



	TestTime	Server	Status	SuccessCount	FailureCount	AverageResponseTime
1	2021-09-10 14:43:30	172.19.3.58	Finish	44	20	52ms
2	2021-09-10 14:43:30	192.168.111.247	Finish	280	20	152ms
3	2021-09-10 14:43:30	172.17.9.126	Finish	48	145	56ms
4	2021-09-10 14:43:30	172.17.9.130	Fail(Error_InitConnectionFailed)	44	176	29ms
5	2021-09-10 14:43:30	192.168.10.174	Fail(Error_InitConnectionFailed)	18	18	96ms
6	2021-09-10 14:43:30	192.168.10.185	Fail(Error_InitConnectionFailed)	36	25	83ms
7	2021-09-10 14:43:30	192.168.111.244	Finish	8	78	103ms
8	2021-09-10 14:43:30	192.168.111.140	Finish	10	88	15ms
9	2021-09-10 14:43:30	192.168.14.22	Fail(Error_InitConnectionFailed)	47	66	160ms
10	2021-09-10 14:43:30	192.168.14.23	Fail(Error_InitConnectionFailed)	64	99	167ms

- **Traceroute**
  Traceroute examines the direction of how data travels on the internet from source to destination. Traceroute report lists data pertaining to every router the packets pass through as they move towards their destination. Running the traceroute helps identify routing hops data must go through and response delays across the eNBs. It also helps in conveniently locating the point of failure for operators. The HopRTTtime in milliseconds denotes the time to send data from CPE to the router and back. Traceroute diagnostic displays, TestTime, Server, Status, HopHost, HopHostAddress, HopErrorCode, and HopRTTtimes (Figure 2-124).

Figure 2-124: Traceroute



2.4.3.2.4.3 Settings

Reference: *CPE Configuration Guide*

Most operators use the CPE GUI to configure the end-user devices. The CPE GUI menus and fields are described in the above-referenced document. Based on operator feedback concerning which CPE settings operators change most often from the OMC, only a limited number of settings are offered through the OMC: CPE Name, Remote Web Login, and Frequency Lock (*aka*, Scan Mode or PCI Lock) (Figure 2-125). When you click on *Operations > Settings,* the page opens to show more tabs. Depending on which version of the CPE is running, you can see Basic Settings, Network, LTE, and System tabs. Examples are shown in the figure.

The Settings page defaults to the Basic Settings tab to enter or change the CPE Name. The Network tab is where you enable/disable remote login to the CPE in the Network. Use the LTE tab if you want to lock the CPE to one or more specific PCIs and frequencies via the Scan Mode field.

Scan Mode refers to how the CPE performs its routine scan of available eNBs and frequencies to select the best available one for attaching to the network. Sometimes, an operator requires the CPE to use a specific eNB PCI and a specific frequency, e.g., to avoid ping-ponging between two adjacent eNBs, where the cell coverage areas overlap. The Scan Mode fields will display differently based on which option you select. Refer to *Table 2-8 Scan Modes* for a description of each option. More information about this feature can be found in *section 2.4.3.3.2 PCI Lock*.

Figure 2-125: Settings

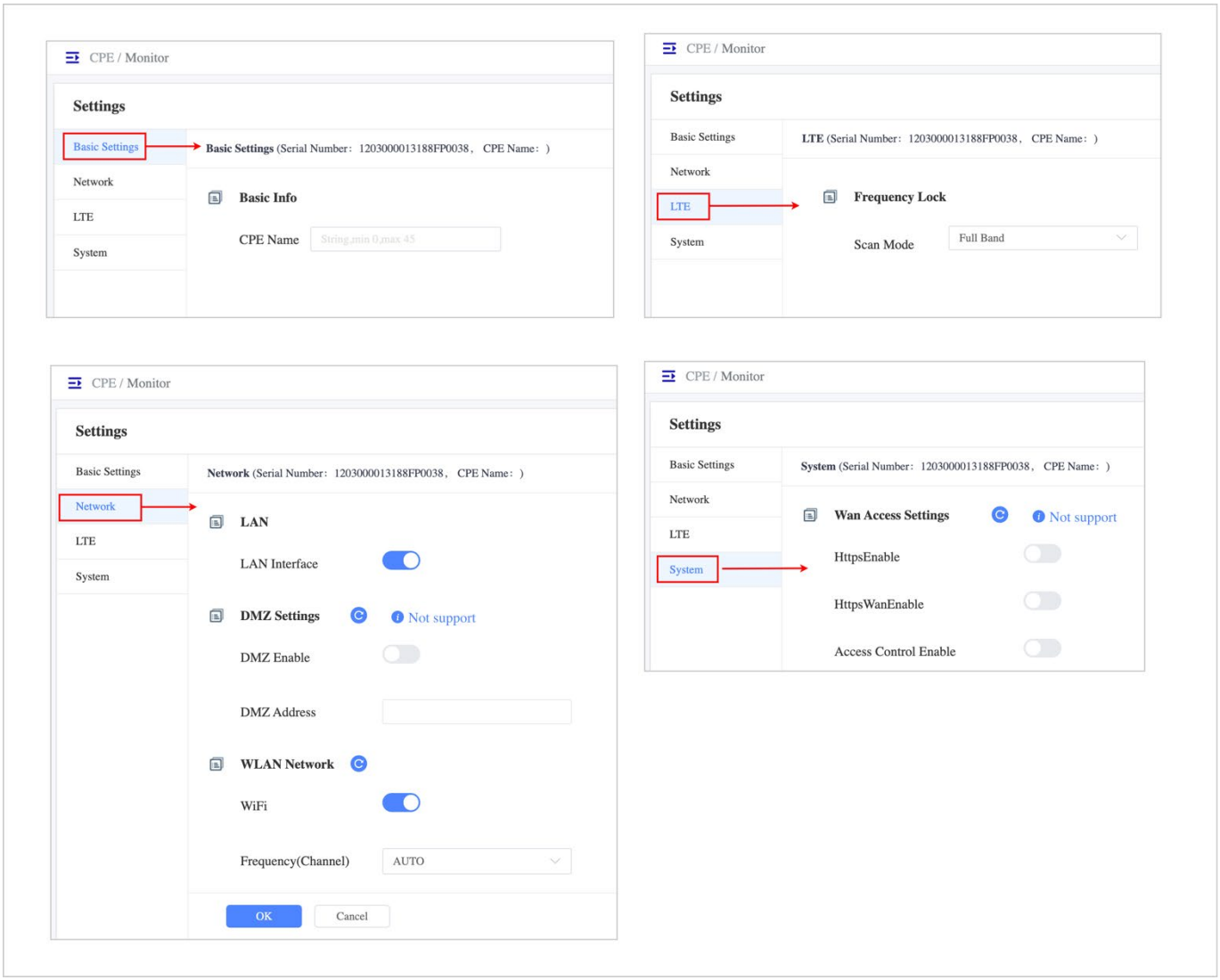


Table 2-8: Scan Modes

Field Name	Description
Full Band	The CPE will scan all available frequencies within the band and select the one with the best signal quality
Band/Frequency Preferred	You can identify specific frequencies you want the CPE to use for network connection.
PCI Lock	Enter one or more frequency + PCI combinations to limit the network connection options
PCI Only Lock	Specify one or more PCIs to which the CPE can connect

2.4.3.2.4.4 Actions

The only *CPE Operations > Action* available is Reboot, as shown in Figure 2-126. To reboot more than one device simultaneously, select the checkbox next to the CPEs in the list to pop up a dialogue box at the bottom of the window. Select *Reboot* and all the selected CPEs will immediately reboot.

You can use this same method to simultaneously change the password on multiple devices to reset them to the same password (Figure 2-127).

Figure 2-126: Reboot

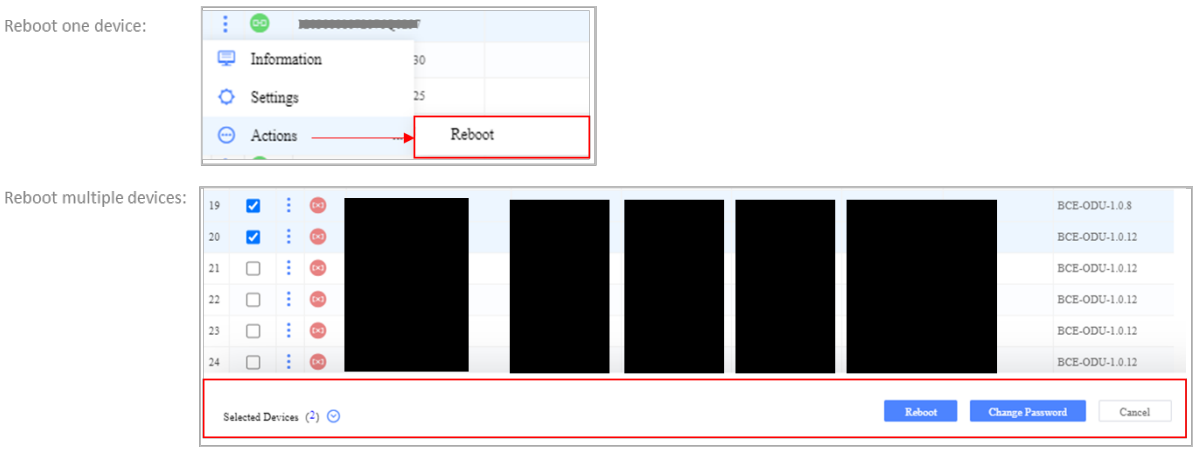
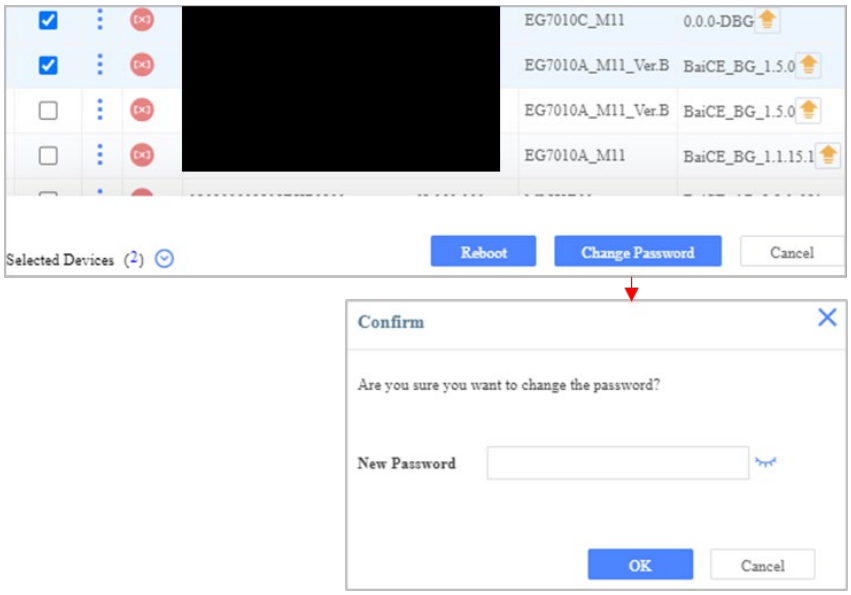


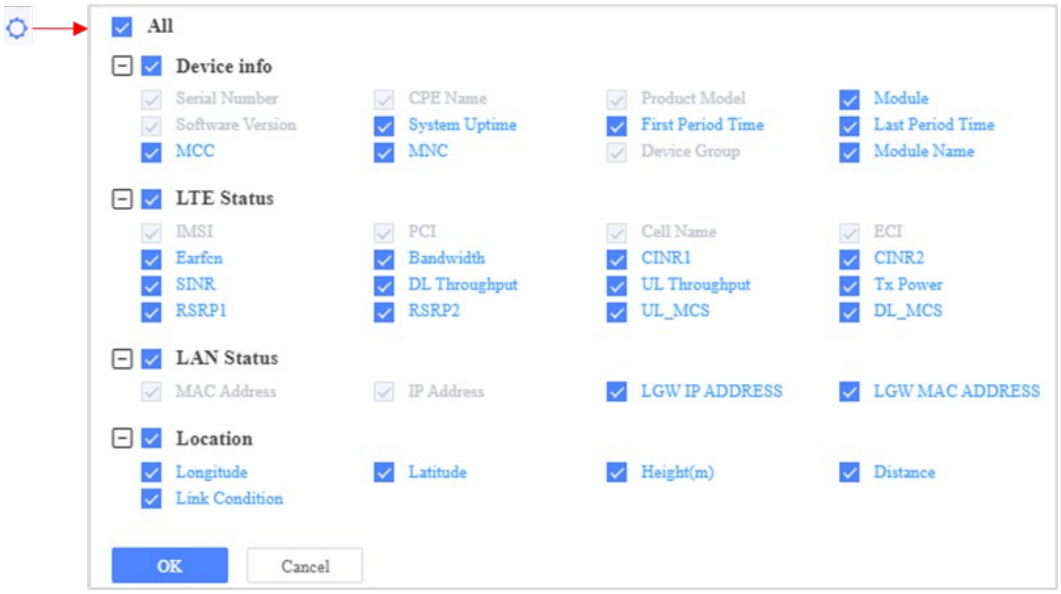
Figure 2-127: Change Password



2.4.3.2.5 Display Options

You can customize the columns displayed in the *CPE > Monitor* window. To do so, click on the gear icon in the upper left of the window (Figure 2-128). Select the checkbox for All if you want all columns of information displayed or choose the specific column headers to view.

Figure 2-128: Display



2.4.3.2.6 Adding a CPE in OMC

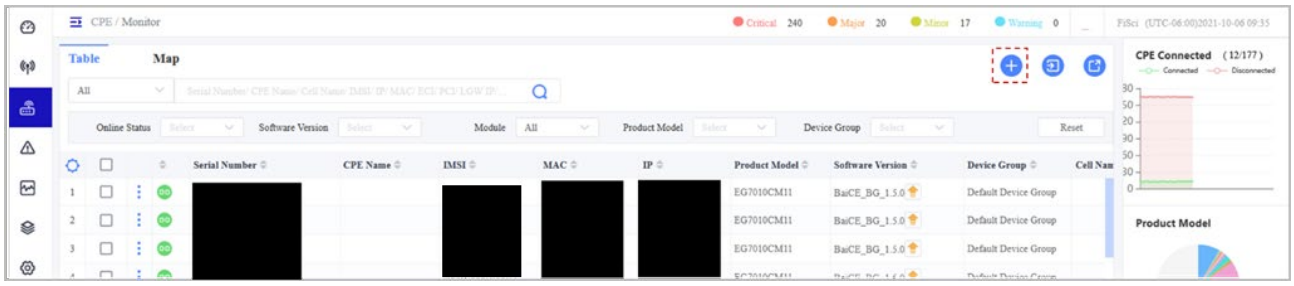
The easiest way to register (add) a CPE in the OMC is to configure the operator's CloudKey in the device GUI. When the CPE comes online, it will automatically register in the operator's OMC account. The CloudKey is described in *section 2.2.3, CloudCore GUI Layout*.

You can add a CPE in the OMC either before or after the CPE is online - in other words, connected to the LTE network. However, the CPE must be online before you can configure or change its configuration settings in OMC. You will need the device's MAC address to add it to OMC. There are two ways you can add a CPE in the OMC: from *CPE > Device* menu (see *section 2.4.3.5 Device*) or from *CPE > Monitor* menu and performing the steps below:

To add the device (Figure 2-138):

1. Go to *CPE > Monitor* and click on the **+** Add icon in the upper right to open the Add CPE dialogue window.
2. Enter the device's MAC address.
3. Select a device group (or let the CPE automatically be placed in the default group).
4. Optional: In the Link Condition pull-down menu, select NLOS, pLOS, or LOS if you want to identify the RF propagation conditions between the CPE and the nearest eNB:
    - NLOS – Non-Line-of-Sight: Problematic physical signal obstructions such as trees, buildings, terrain
    - pLOS - Partial Line-of-Sight: Some physical signal obstructions
    - LOS - Line-of-Sight: No physical signal obstructions
5. Click on *OK*.

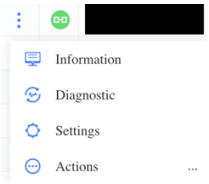
Figure 2-129: CPE Monitor Add a Device



Most operators use the CPE GUI to configure the end-user devices. Based on operator feedback concerning which CPE configuration fields they most often use the OMC to change, only a few key fields are available: CPE Name, Remote Web Login, and Scan Mode.

Referring to *section 2.4.3.2.4.2 Settings*, to configure any of the three types of settings in OMC once the CPE is online, or to change these settings:

1. Go to *CPE > Monitor*.
2. Find the device in the list, click on the Operations icon, and select Settings.

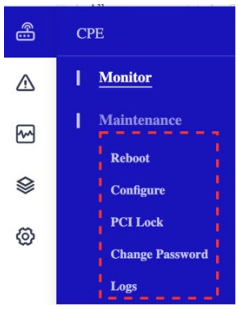


3. Enter the parameters, referring to the *CPE Configuration Guide* to describe all CPE settings.
4. Once you complete the configuration, click on *OK* to save it.

2.4.3.3 Maintenance

The *CPE > Maintenance* menu is used to create Reboot, Configure, PCI Lock, Change Password, and Logs tasks for one or more CPEs (Figure 2-130). Creating a task enables you to achieve the same action on multiple devices simultaneously and schedule when the task will occur. This is called Batch Config. For example, you can create a task to upgrade several CPEs to the latest software version but make the event happen later.

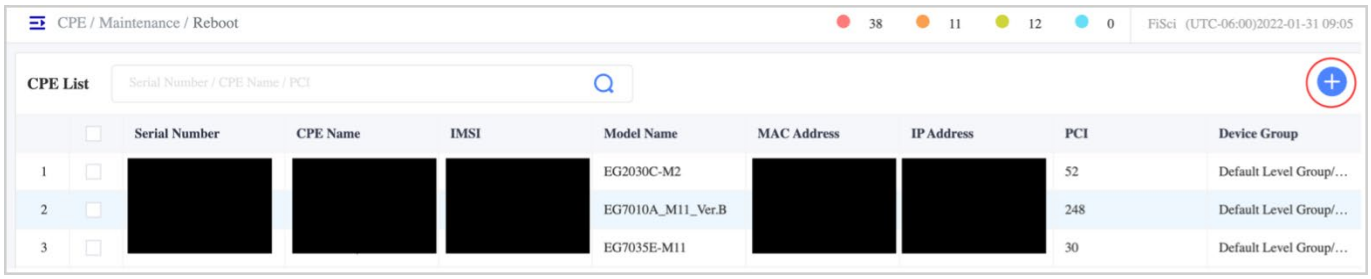
Figure 2-130: Maintenance



2.4.3.3.1 Reboot

Any CPE reboot tasks that have been created will be listed in the *Maintenance > Reboot* window (Figure 2-131).

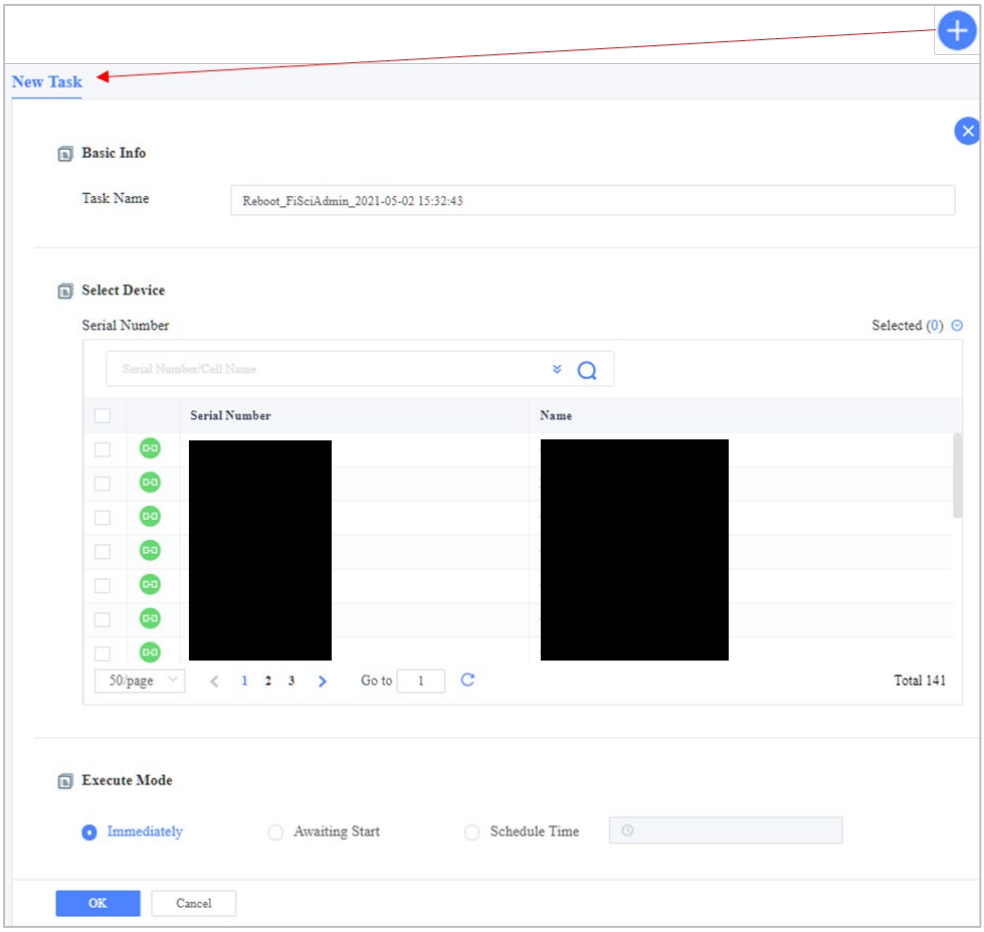
Figure 2-131: Reboot



To create a new reboot task for one or more CPEs (Figure 2-132):

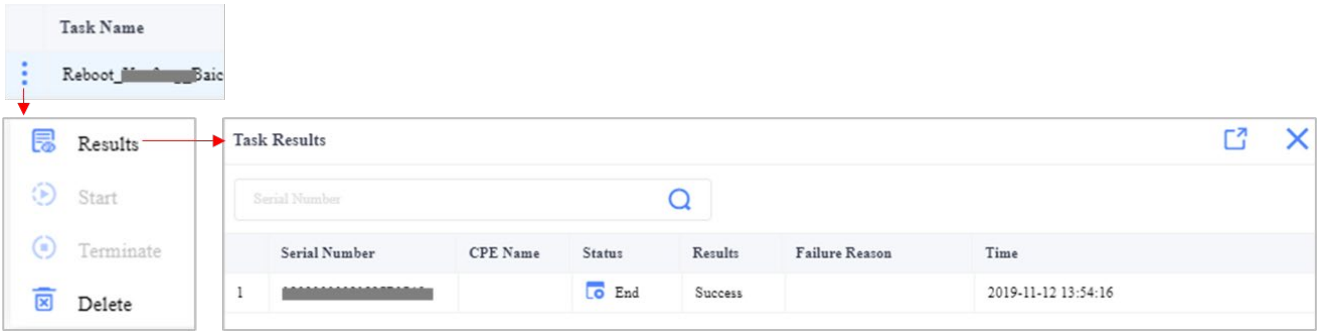
1. Click on the + Add icon to open the New Task window in the Reboot window.
2. Accept the default task name or enter a new name.
3. Select the CPEs you want to include in this task.
4. Choose an Execute Mode, per *Table 2-6 Execute Modes*, determining when the task executes.
5. Click on *OK* to save the settings. The new task will appear in the Reboot window.

Figure 2-132: New Task



Using the *Operations* actions next to a task in the main window, you can view the results of an executed task, or start, terminate, or delete a task (Figure 2-133). Terminating a task stops the task while it is running. Deleting the task completely removes the task from the list.

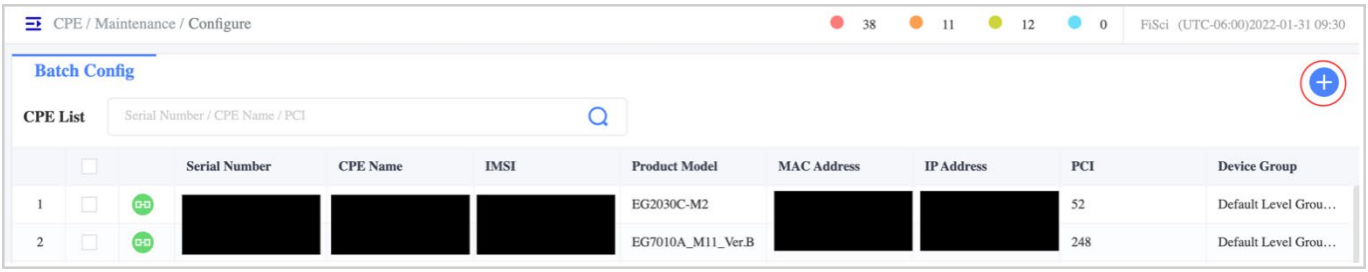
Figure 2-133: Operations



2.4.3.3.2 Configure

To configure the parameters of many CPEs, go to *Maintenance* > *Configure* (Figure 2-134)

Figure 2-134: Configure



To create a new Configure task for one or more CPEs (Figure 2-135):

1. In the *Configure* window, click on the **+** Add icon to open the New Task window.
2. Accept the default task name or enter a new name.
3. Select the CPEs you want to include in this task.
4. Enter the parameters, referring to the *CPE Configuration Guide* to describe all CPE settings.
5. Once you complete the configuration, click on *OK* to save it.
6. The Task will run in the Task List tab. To see the results of successfully configured devices, click on the Device List Tab. You can Export the Batch Configure CPEs and their information by clicking the Export icon.

Figure 2-135: Task and Device List

2.4.3.3.3 PCI Lock

2.4.3.3.3.1 Overview

In an LTE network, each eNB is identified by a Physical Cell Identifier (PCI) number. The PCI Lock function (also referred to as Frequency Lock in some menus and fields) enables you to select how the CPE's routine scan of available eNBs and frequencies is determined. If left in default mode, the scan method will be Full Band, meaning the CPE will scan all frequencies within the band - giving it more selections and taking longer to complete the scan, select the best option, and connect to the network.

Configuring a scan method other than Full Band can be instrumental. For example, suppose a CPE is ping-ponging between two adjacent eNBs where the cell coverage overlaps, thereby disrupting user service. In that case, the operator can bind the CPE to a specific eNB or configure one or more particular eNBs and frequencies to limit those that the CPE scans and chooses for its network connection.

The scan options are Full Band, Band/Frequency Preferred, PCI lock, and PCI Only Lock. Refer to *Table 2-8 Scan Modes* for a description of each. The fields will vary depending on which option you select.

The *CPE > Maintenance > PCI Lock* menu presents two tabs: eNB and CPE (Figure 2-136). The eNB tab can bind one or more CPEs to selected eNBs. The CPE tab can be used to specify the scan mode for one or more CPEs.

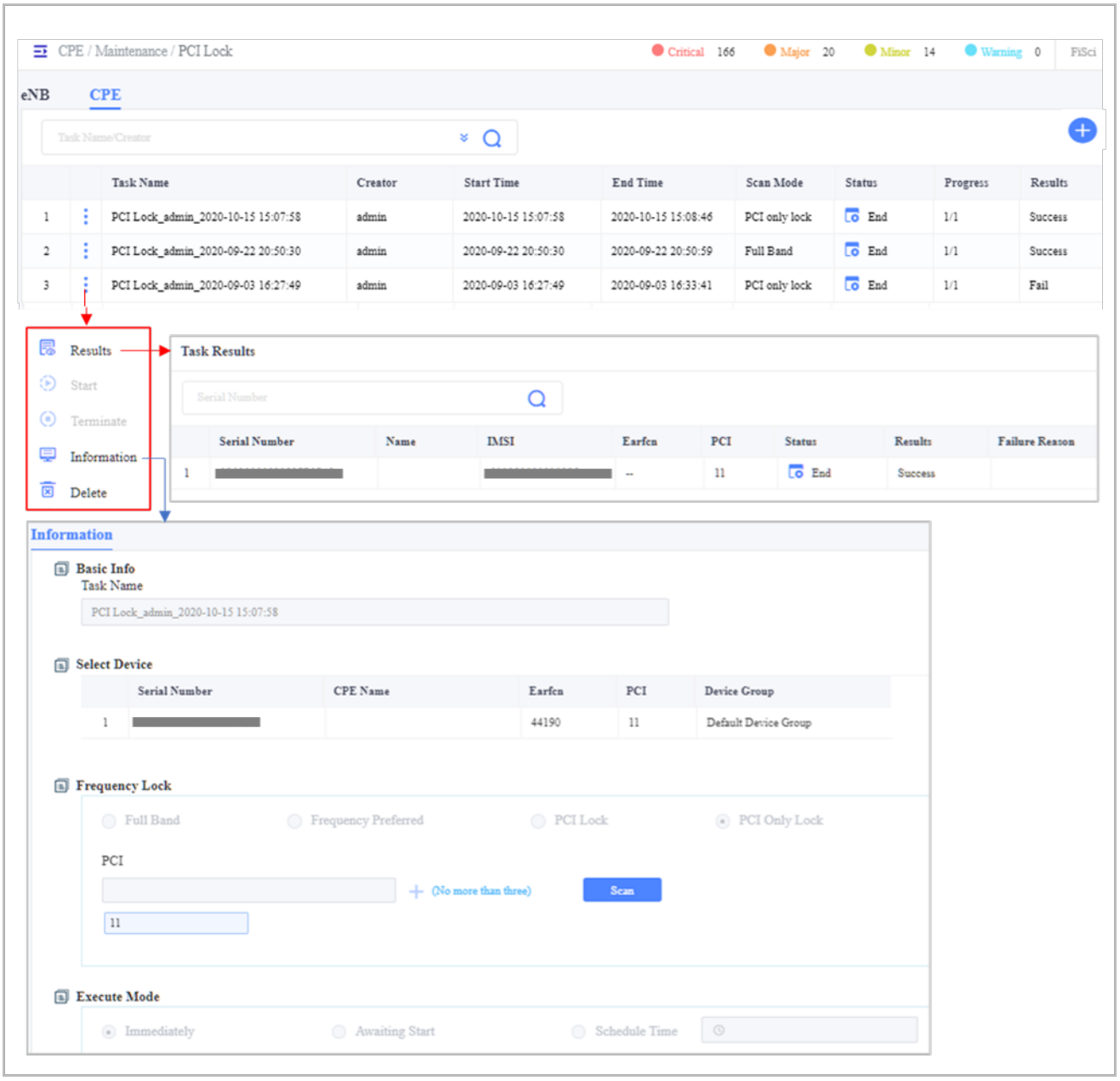
The figure also shows the *Operations* actions: View the Results of an executed task, Start the task, Terminate the task, view the task Information, or Delete the task.

Caution: When a task is run, it performs a warm reboot of the affected devices, momentarily interrupting service.

Important: During the execution of a task, any offline CPEs will not receive the change. You need to check the status of each one and possibly reinitiate the task to ensure all CPEs are updated.

Refer to *section 2.4.3.4.2.2 eNB Tab* and *section 2.4.3.4.2.3 CPE Tab* on creating a new task.

Figure 2-136: PCI Lock

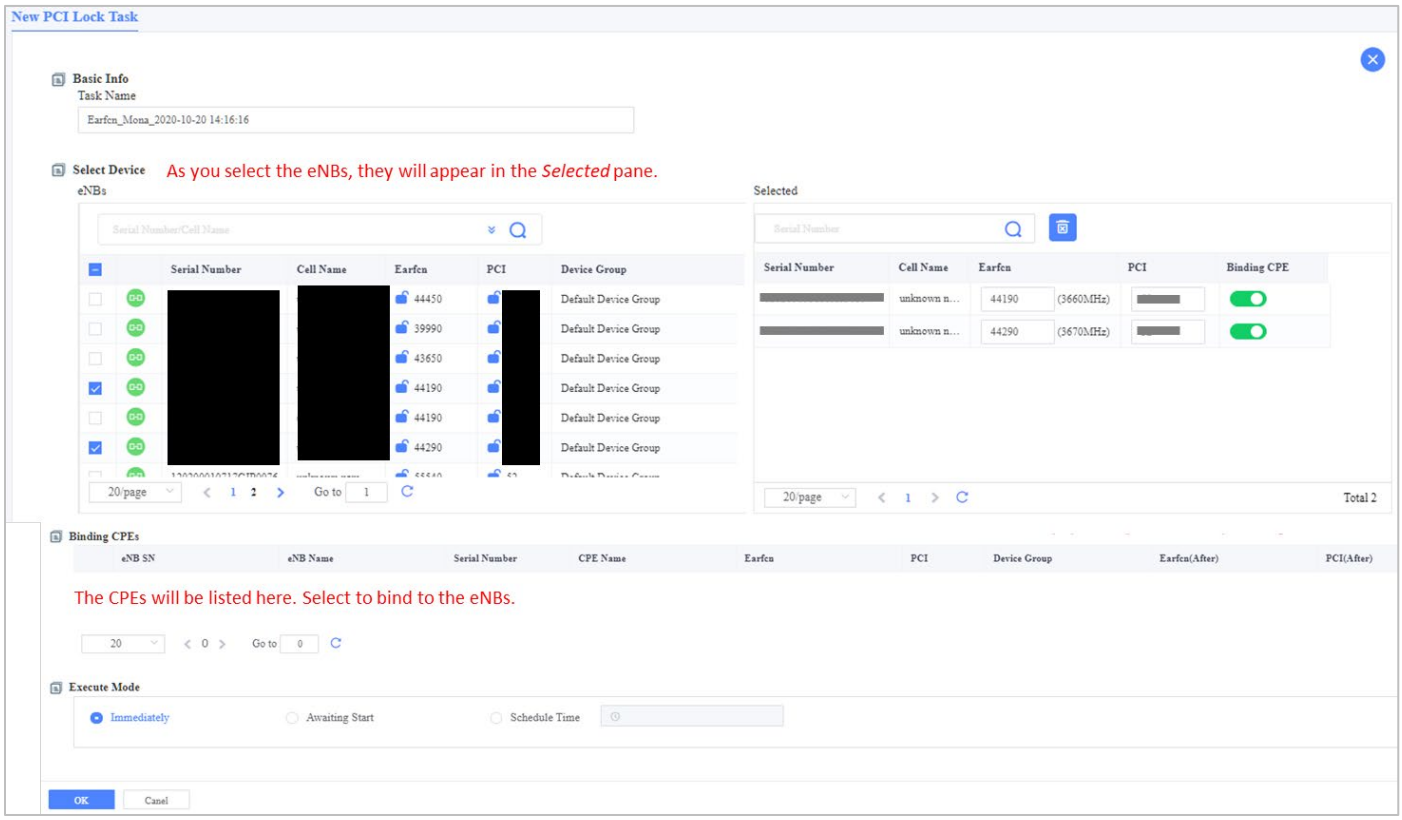


2.4.3.3.3.2 eNB Tab

Select the *eNB* tab to bind CPEs to specific eNBs. To create a new PCI Lock task (Figure 2-137):

1. Click on the **+** Add icon and accept the auto-generated task name or create a new name.
2. Select the eNBs to which you want to bind CPEs. Refer to *section 2.4.3.4.2.4 Advanced Query Fields* for ways to limit the list of devices.
3. In the list of CPEs, select the ones you want to bind to the chosen eNBs.
4. Choose an Execute Mode, per *Table 2-6 Execute Modes*, determining when the task executes.
5. Click on *OK* to save the settings. The new task will appear in the eNB PCI Lock window.

Figure 2-137: New PCI Lock Task (eNB Tab)



2.4.3.3.3.3 CPE Tab

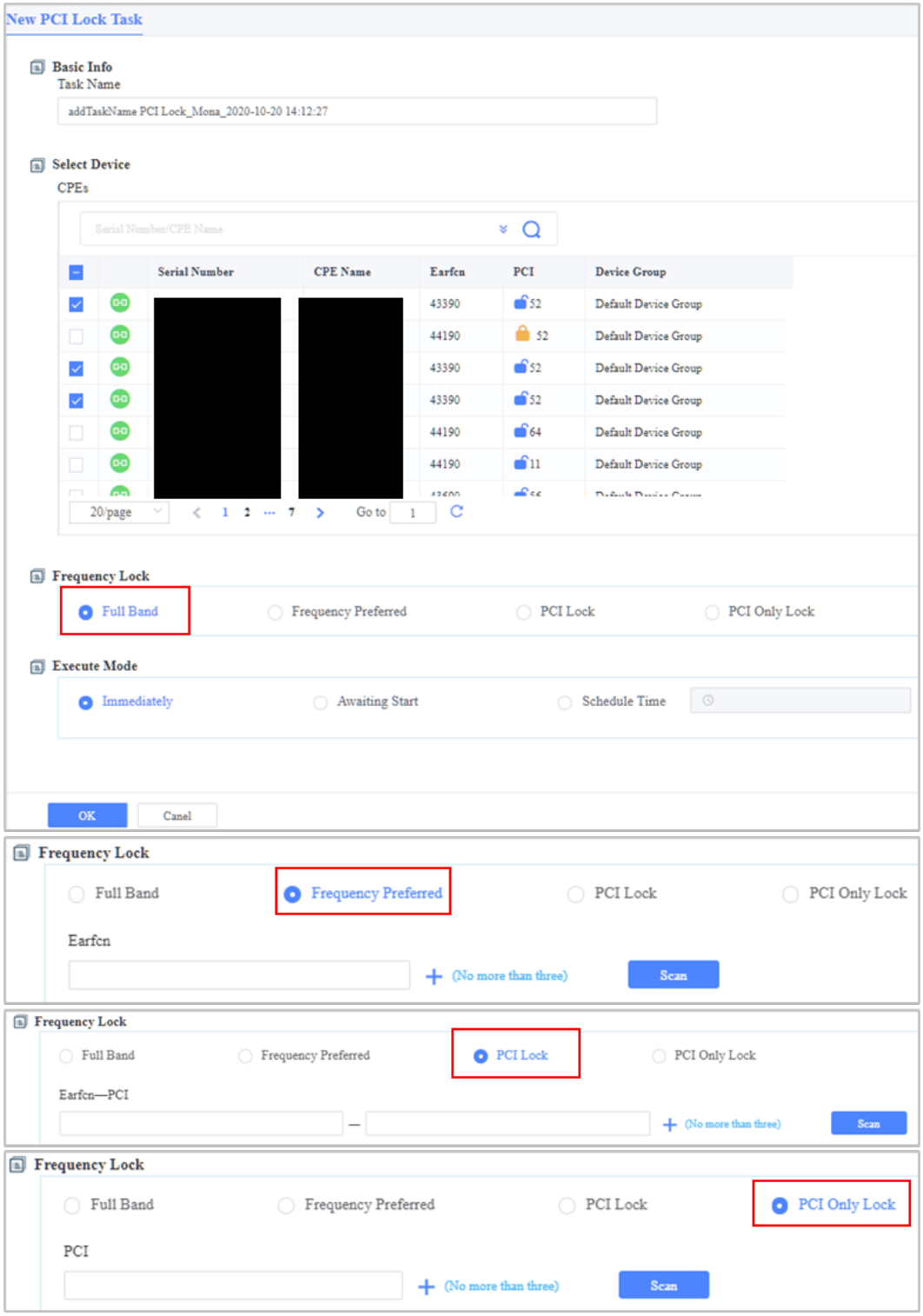
Select the *CPE* tab to configure specific PCIs, EARFCNs/frequencies, or a combination of PCI+EARFCN/frequency for one or more CPEs. To create a *New PCI Lock Task* (Figure 2-138):

1. Click on the **+** Add icon and accept the auto-generated task name or create a new name.
2. Select the CPEs you want to lock using the same scan method (see *Table 2-8 Scan Modes*). Refer to *section 2.4.3.4.2.4 Advanced Query Fields* for ways to limit the list of devices.

   NOTE 1: You can configure up to 3 EARFCNs/frequencies, EARFCN+PCI combinations, or PCIs.
   NOTE 2: The resulting fields will vary based on which scan option you choose.

3. Select the Frequency Lock: Full Band, Frequency Preferred, PCI Lock, or PCI Only Lock
4. Choose an Execute Mode, per *Table 2-6 Execute Modes*, determining when the task executes.
5. Click on *OK* to save the settings. The new task will appear in the CPE PCI Lock window.

Figure 2-138: New PCI Lock Task (CPE Tab)

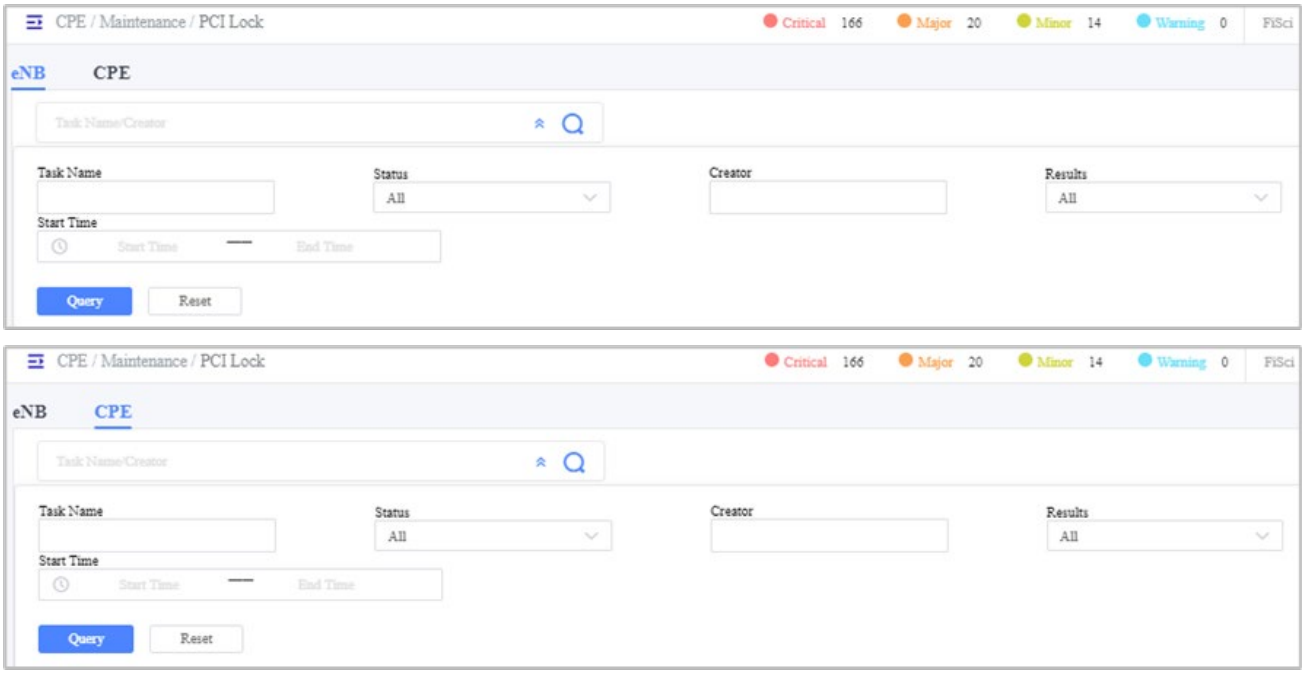


2.4.3.3.3.4 Advanced Query Fields

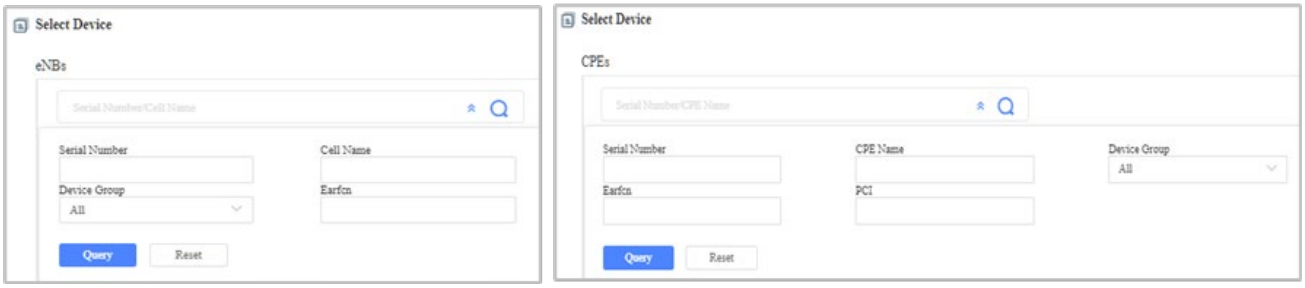
To search for a specific device or to limit the list of devices shown in either tab, use the Advanced Query pull-down fields as shown in (Figure 2-139). When creating a new PCI Lock task, you can also use Advanced Query for the same purpose.

Figure 2-139: Advanced Query Fields

eNB & CPE Advanced Query Fields:



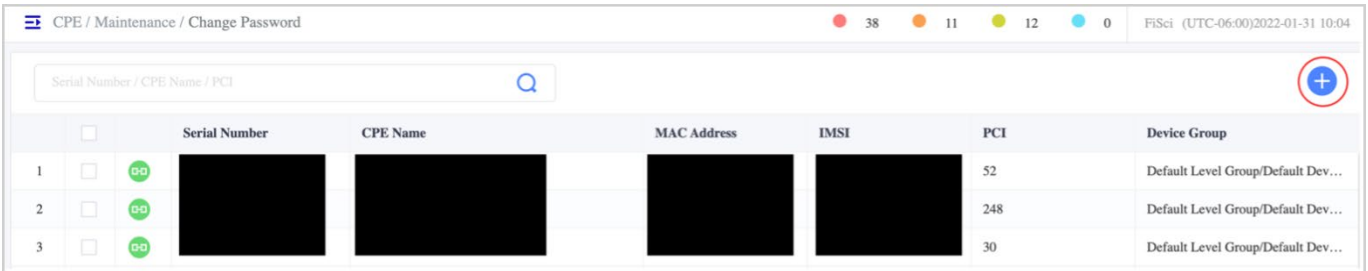
eNB & CPE New PCI Lock Task Advanced Query Fields:



2.4.3.3.4 Change Password

To change the password on one device or set the same password for multiple CPE devices, you can create a task using the Change Password task (Figure 2-140).

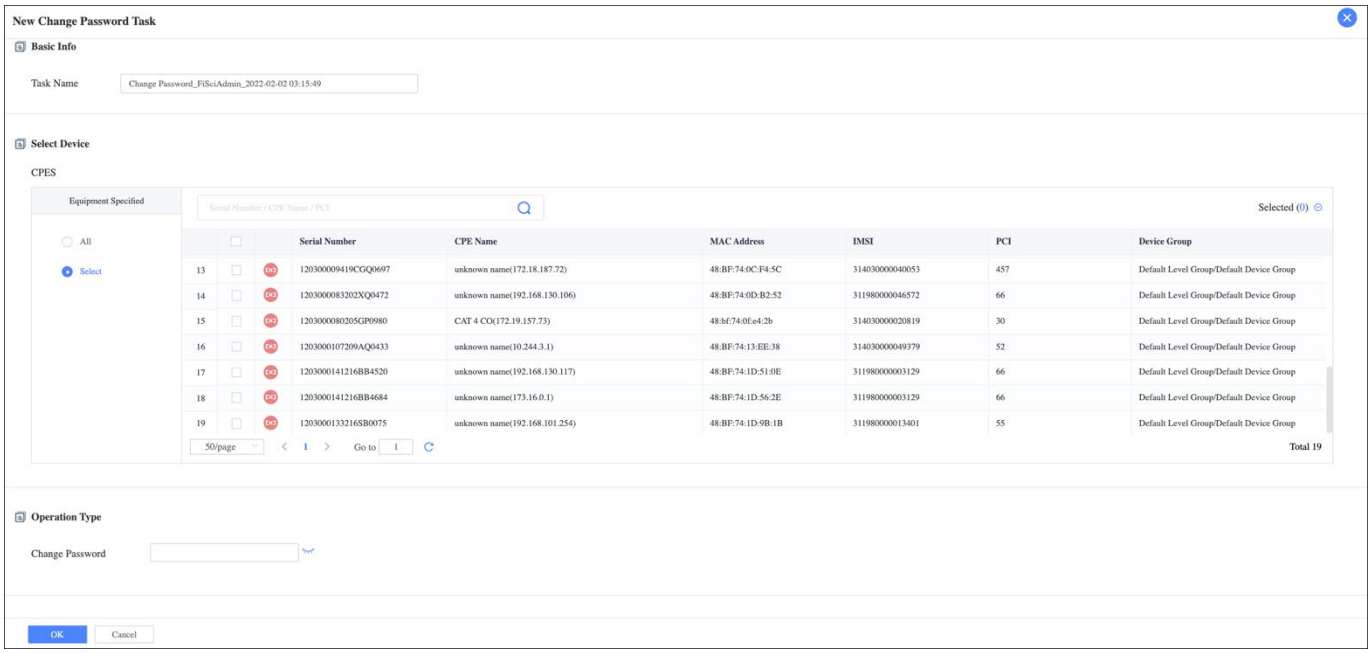
Figure 2-140: Change Password



To create a new Change Password task for one or more CPEs (Figure 2-141):

1. Click on the + Add icon to open the New Task window in the Change Password window.
2. Accept the default task name or enter a new name.
3. Select all or the CPEs you want to include in this task.
4. Under Operation type, give the new password.
5. Choose an Execute Mode, per *Table 2-6 Execute Modes*, determining when the task executes.
6. Once you complete the change password task, click *OK* to save it.

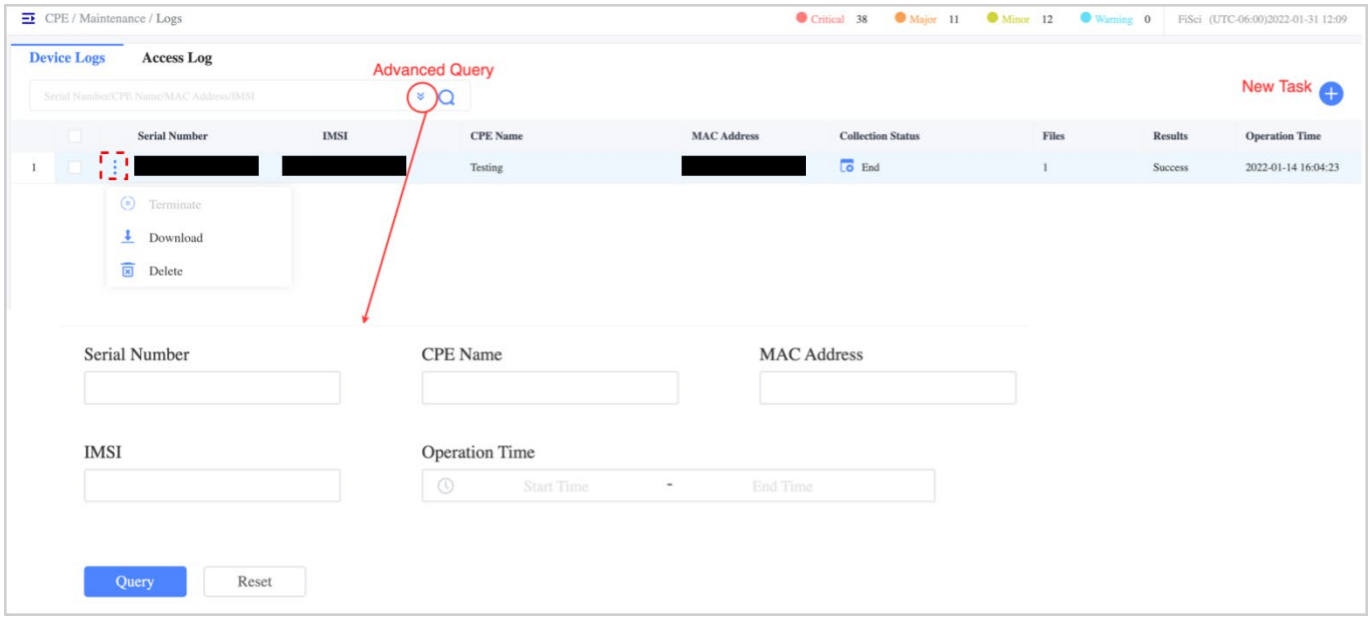
Figure 2-141: New Change Password Task



2.4.3.3.5 Logs

Logs are highly valuable when it comes to gaining insight into security and system performance. You can create a device log task to report the operation log information of CPE regularly or immediately. There are two tabs, Device Logs, and Access Logs. To automatically export all the log information, go to the Access Log tab and click on the Export icon (Figure 2-144).

Figure 2-142: Device Log



To create a new Device Log Task for one or more CPEs (Figure 2-143):

1. Click on the + Add icon to open the New Task window in the Device Log task.
2. Select the CPEs you want to include in this task; only a max of 20 devices can be included for one task.
3. Choose an Execute Mode, per *Table 2-6 Execute Modes*, determining when the task executes.
4. Once you complete the change password task, click *OK* to save it.
5. The new task will appear at the Device Log tab. By clicking the operation, you can Terminate, Download or Delete the Task.

Figure 2-143: New Device Log Task

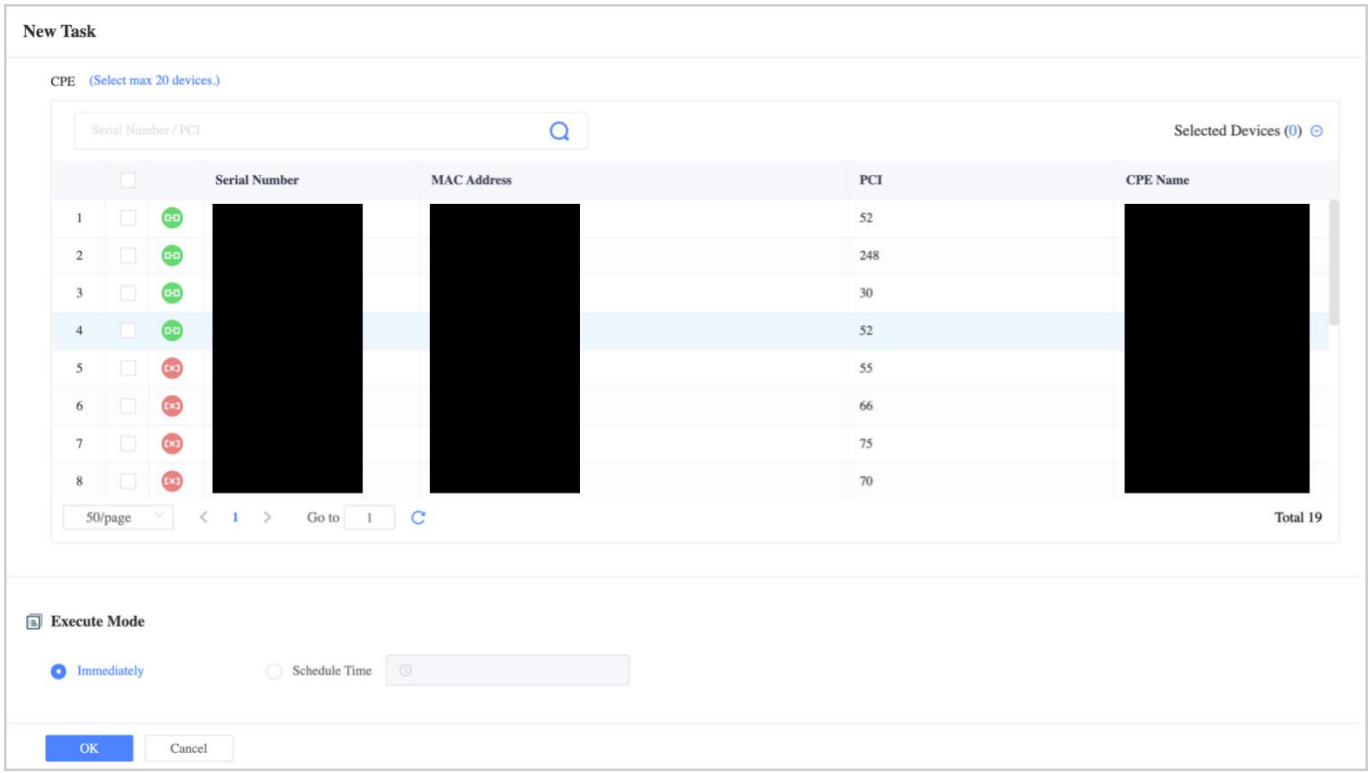
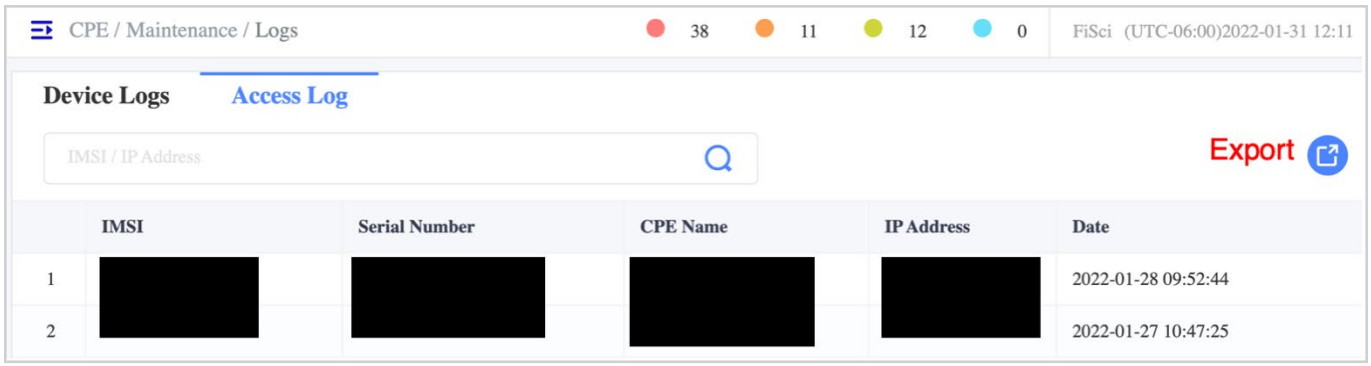


Figure 2-144: Access Log



2.4.3.4 Upgrade

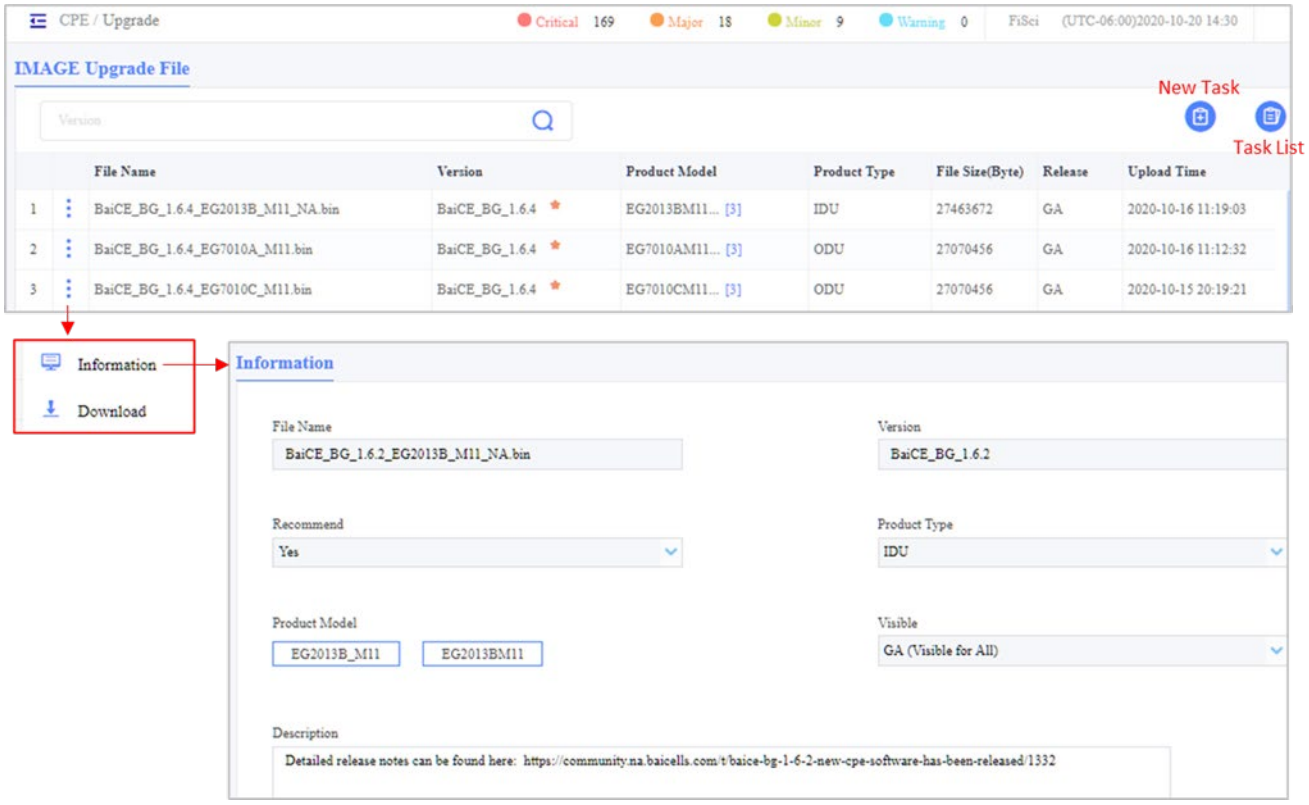
Caution: A software upgrade requires a reboot of the CPEs; the reboot action will temporarily take the CPEs out of service.

New software typically contains new features and bug fixes, and it is generally recommended to implement the latest version in the field. Baicells notifies operators of newly available software by including a message at the top of the OMC window. You can select the link in the message to go straight to the upgrade menu, in this case, the *CPE > Upgrade* menu, as explained in *section 2.4.2.5.1 Upgrade From the OMC Upgrade Messages*.

The Upgrade window will display a list of available software files for the outdoor unit (ODU) and the indoor unit (IDU), as well as CAT4 and CAT6/7 CPE models. Use the *Operations* functions to view the software version or download the .bin file. Refer to Figure 2-145.

NOTE: A CPE's current software version is displayed under *CPE > Monitor* in OMC and the *CPE GUI Status > Overview* window. The CPE GUI is documented in the *CPE Configuration Guide*.

Figure 2-145: CPE > Upgrade



To create a new upgrade task for one or more CPEs of the same product type (Figure 2-146):

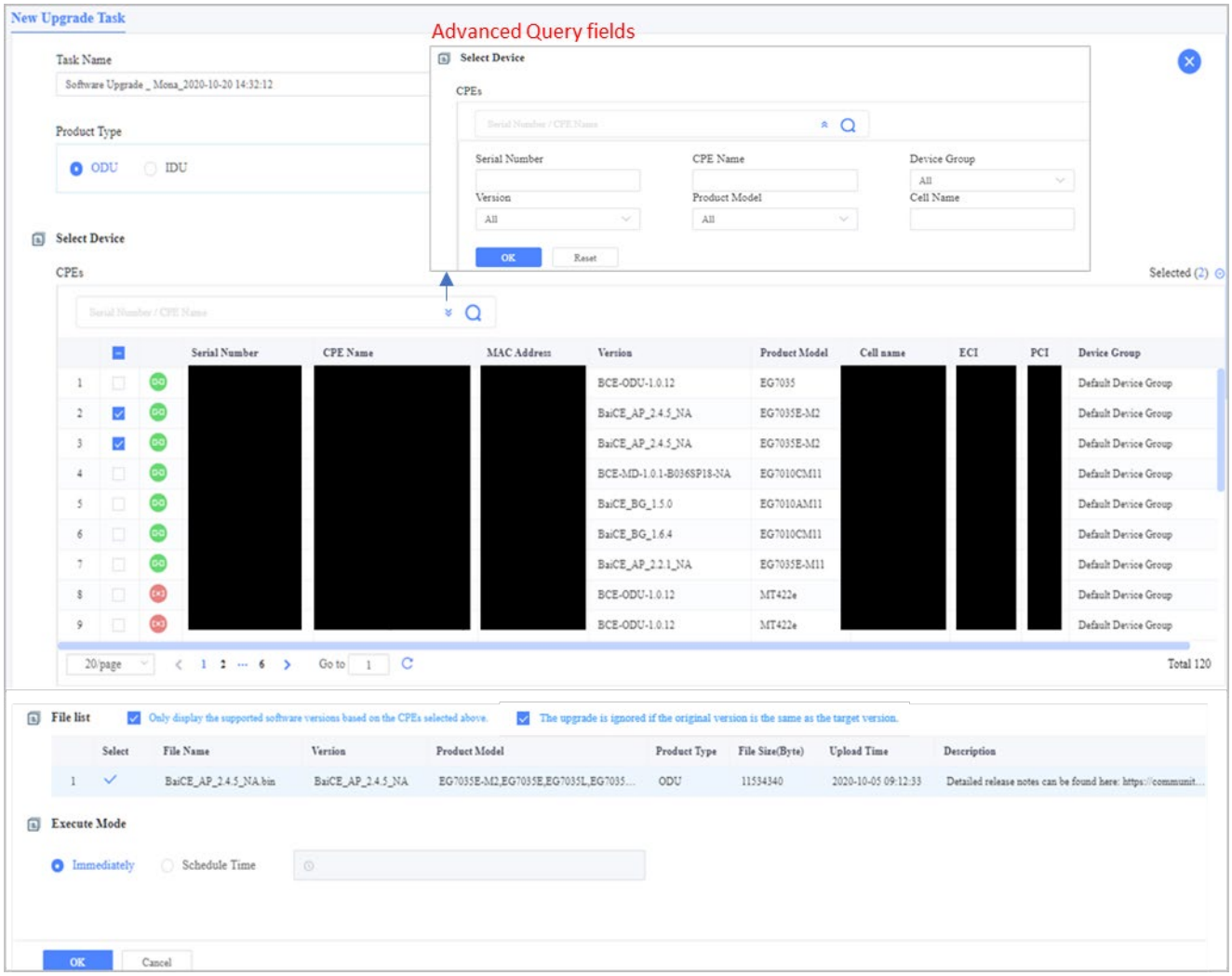
1. Click on the New Task icon in the upper right part of the Image Upgrade File window.
2. Accept the default Task Name or enter a new name.
3. Select the Product Type of ODU or IDU.
4. CPEs of the product type you selected will be listed under Select Device. Select the CPEs to include in the task. There is no limit on the number of CPEs you can include, though only 20 devices will be upgraded

simultaneously. Use the Advanced Query fields to search for a specific device or to limit the list of devices, as shown previously in *section 2.4.3.3.3.4 Advanced Query Fields.*

5. Under File list, the checkbox for "Only display the supported software versions based on the CPEs selected above" is checked by default; uncheck it if you want to see all software versions in the list. Choose the target software version.
6. Under File List, select or deselect the checkbox for "The upgrade is ignored if the original version is the same as the target version." In other words, even if the software version you are upgrading to is the same as the one already on the device, if you leave the box unchecked, the upgrade will still occur (overwriting the existing software).
7. Choose an Execute Mode, per *Table 2-6 Execute Modes*, determining when the task executes.
8. Click on *OK* to save the settings. The new task will appear in the Image Upgrade File window.

After the upgrade task has been executed, verify that the target devices are running the new software version. An error message will be generated if any device fails to get the upgrade.

Figure 2-146: New CPE Upgrade task



2.4.3.5 Device

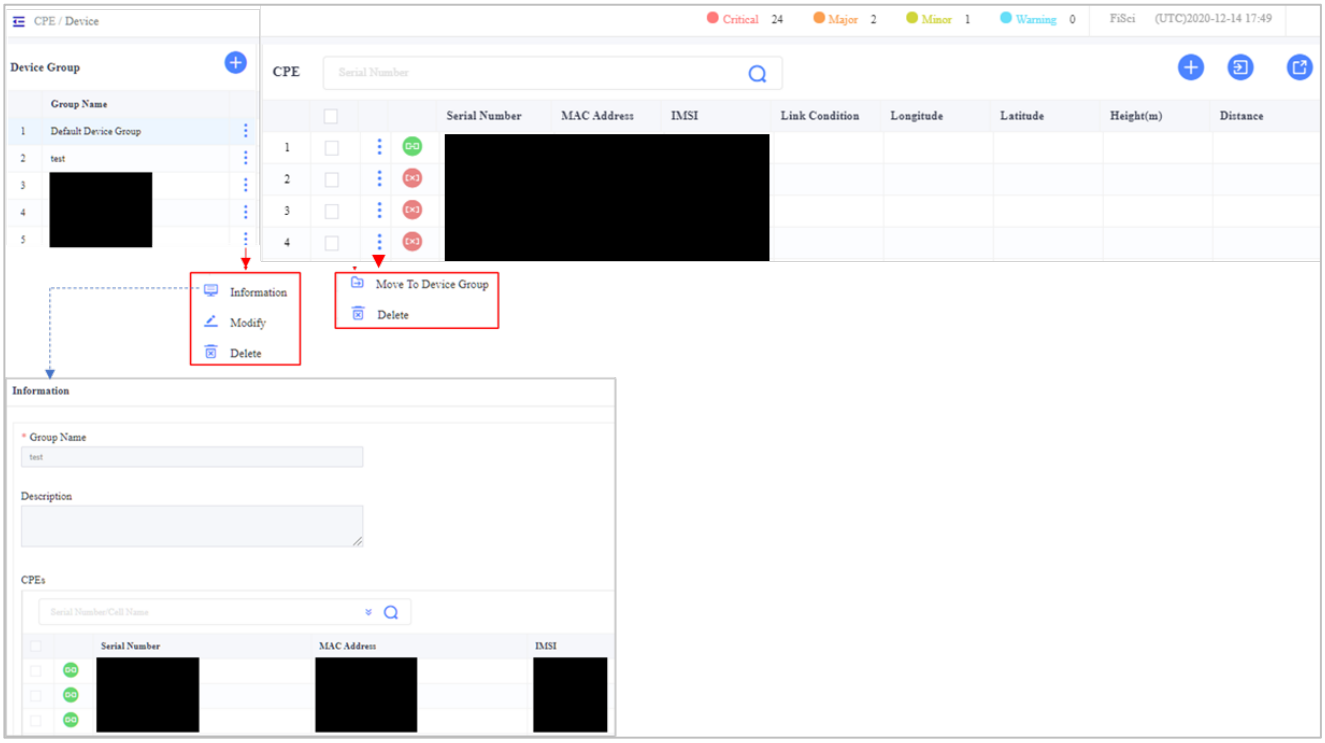
The *CPE > Device* menu is used to create and manage CPE groups and register CPE devices in the operator's OMC account (Figure 2-147). The left pane lists the default device group and any existing customized groups the operator has created. Using device groups makes it easier to manage CPEs and perform specific bulk tasks, such as software upgrades, reboots, PCI Lock, etc. The Device Group operations include (a) Information to view the group details; (b) Modify the device group, and (c) Delete the group.

NOTE: If a CPE is not assigned to a custom group, it will automatically be placed in the default group. You cannot modify or delete the default group.

The right pane lists all of the operator's CPEs, showing each one's status (active or offline), serial number, MAC address, IMSI number, and for outdoor CPEs, the longitude, latitude, height, and distance. The CPE operations are Move to Device Group and Delete the device.

NOTE: If you entered the operator's unique CloudKey in the CPE GUI when the CPE is powered on, it would automatically associate to the operator's account in OMC.

Figure 2-147: Device



To add a device group (Figure 2-148):

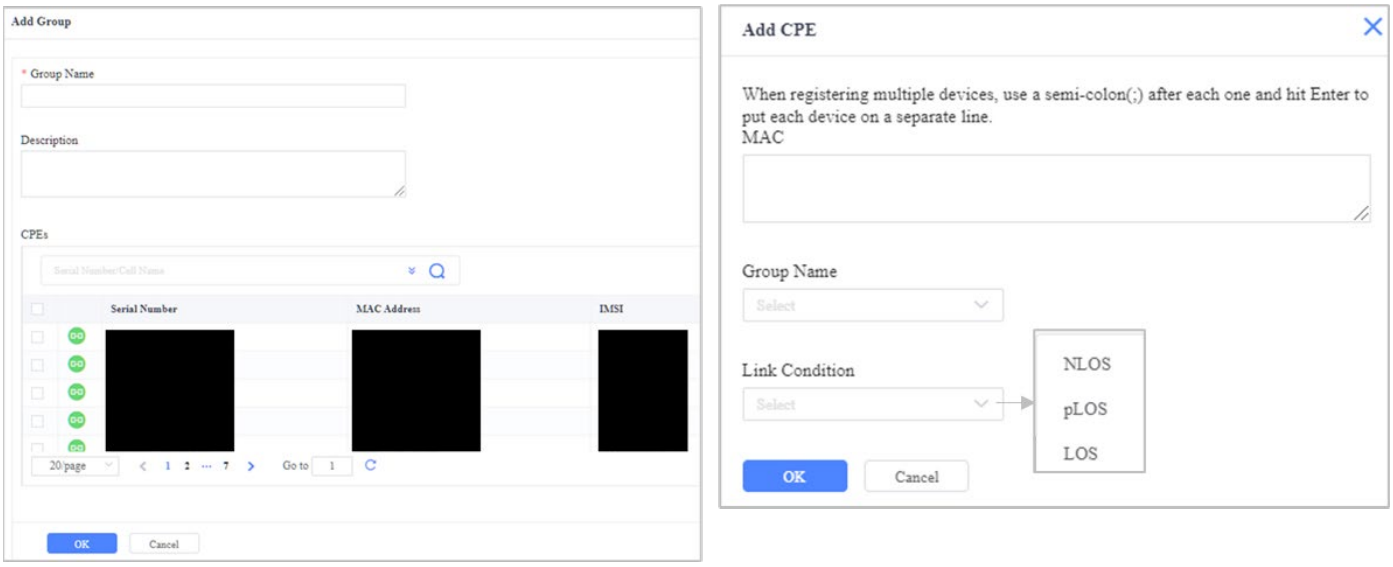
1. Click on the **+** Add icon to open the Add Group window in the left pane.
2. Enter a group name and description.
3. Select the CPEs you want to include in the group.
4. Click on *OK* to save the settings. The new group will appear in the Device Group list.

To add one or more CPE devices (Figure 2-148):

1. Click on the **+** Add icon to open the Add CPE window.
2. Enter the CPE's MAC address. If adding more than one CPE, put each device on a separate line. Use a semi-colon at the end of each line (;) and hit Enter.
3. Select the Group Name in the pull-down list*.
4. Select the Link Condition of NLOS, pLOS, or LOS. This field enables the operator to identify if the path between the CPE and serving eNB is described as Non-Line-of-Sight (NLOS), Partial Line-of-Sight (pLOS), or Line-of-Sight (LOS).
5. Click on *OK* to save. The new CPE(s) will appear in the CPE list.

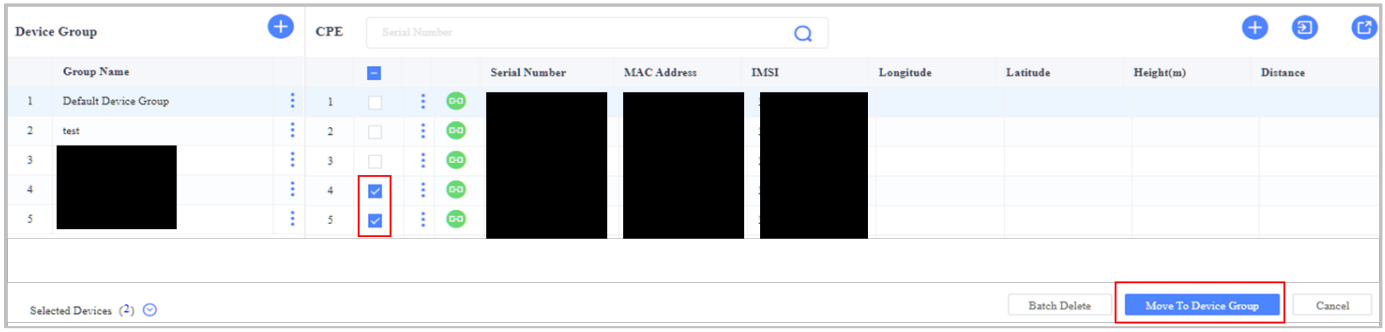
*NOTE: Alternatively, you can put all CPEs in the default group and later use the *Operations > Move to Device Group* function to assign CPEs to groups.

Figure 2-148: Add CPE Device Group, Add CPE(s)



Another quick way to move multiple CPEs to the same device group is by selecting the checkbox next to the CPEs in the main Device window. A dialogue window appears at the bottom (Figure 2-149). Select the *Move to Device Group* button. You can also batch-delete CPEs.

Figure 2-149: Quick Move To Device Group



2.4.4 Alarm Menu

2.4.4.1 Overview

Network alarm conditions are reported in OMC. The types of events that can trigger alarms include issues with communications, Quality of Service (QoS), equipment, environmental conditions, and processing errors.

Alarms are categorized into four severity levels: Critical, Major, Minor, or Warning. Critical alarms are incidents that can cause system outages and should be attended to immediately. Significant alarms are incidents that can cause the poor or degrading quality of service for subscribers and, therefore, should be addressed as soon as possible. Minor alarms indicate a potential issue that needs investigation but will not disrupt service. Warnings are used to indicate errors that probably need to be corrected or at least monitored but do not require any action.

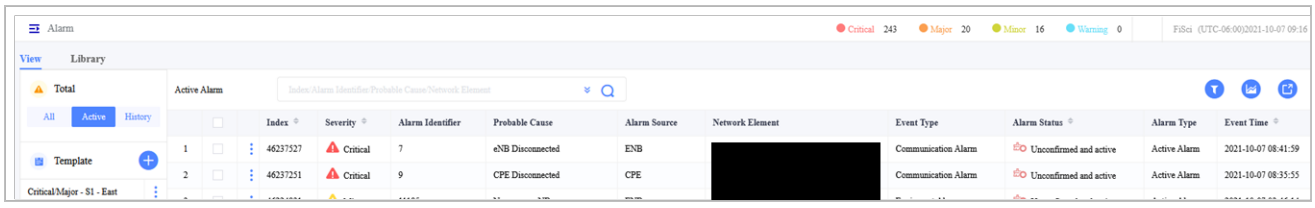
The Alarm menu is where you can create alarm templates to view only the alarm sources or specific alarm IDs you want to see; set up filtering rules to tell the system what actions to take for specific alarm sources and alarms; view all of the operator's currently active and historical alarms, and display a library of all system alarms (Figure 2-150).

Figure 2-150: Alarm Menu

2.4.4.2 Landing Page Description

The Alarm window contains two tabs (View and Library), and the window opens first to the View tab (Figure 2-151). Each tab is described in more detail in the following sections.

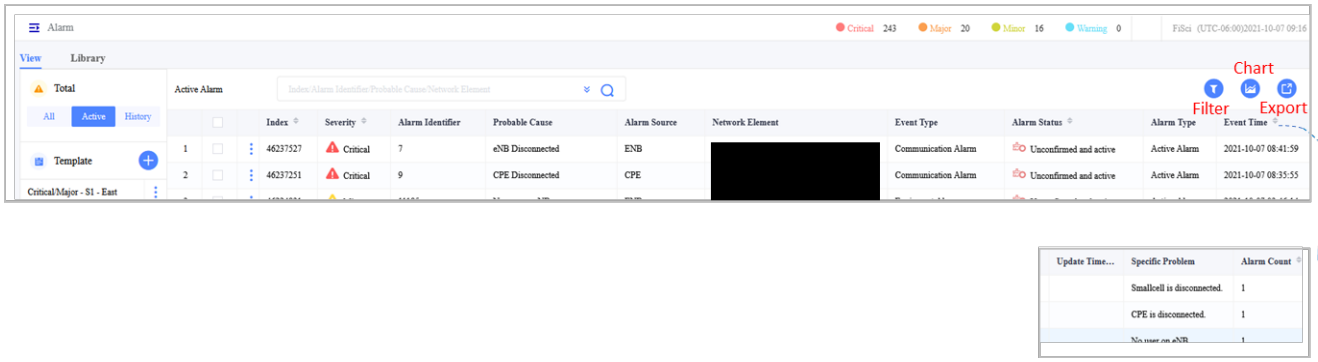
Figure 2-151: Alarm Menu - General Layout



2.4.4.2.1 View Tab Description

The View tab contains two panes of data (Figure 2-152). The left pane provides three tabs for sorting the alarms on the right. The All tab will list all alarms, both active and historical (cleared), for all severity levels. The Active tab is the default view of just the currently active alarms. The History tab will display only historical, inactive alarms. Beneath these three tabs will be any alarm templates that the operator has created. Refer to *section 2.4.4.2.1.1 Add New Alarm Template* on creating an alarm template.

Figure 2-152: View Tab



Use the *Operations* functions to look at alarm detail, invoke an alarm filter, confirm an alarm, unconfirm an alarm, clear an active alarm, or delete a historic alarm (Figure 2-162). An example of an alarm detail is shown in Figure 2-154.

Figure 2-153: Operations

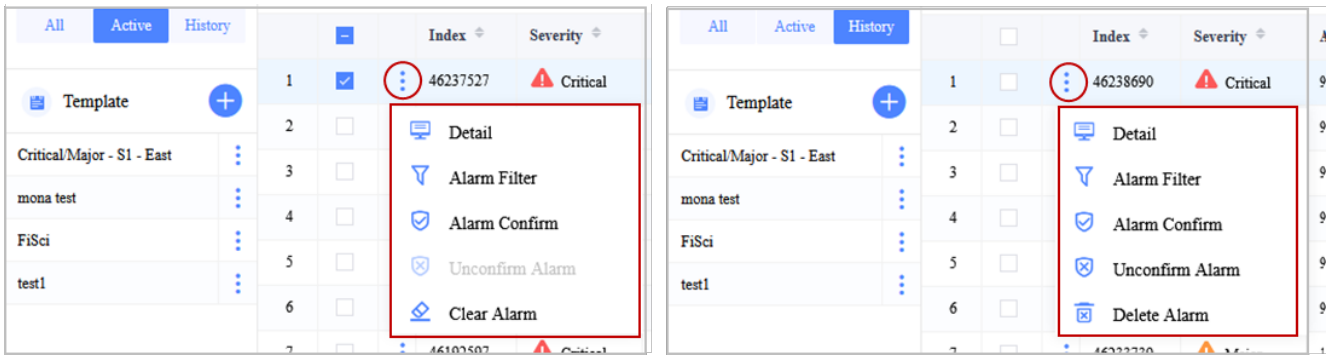
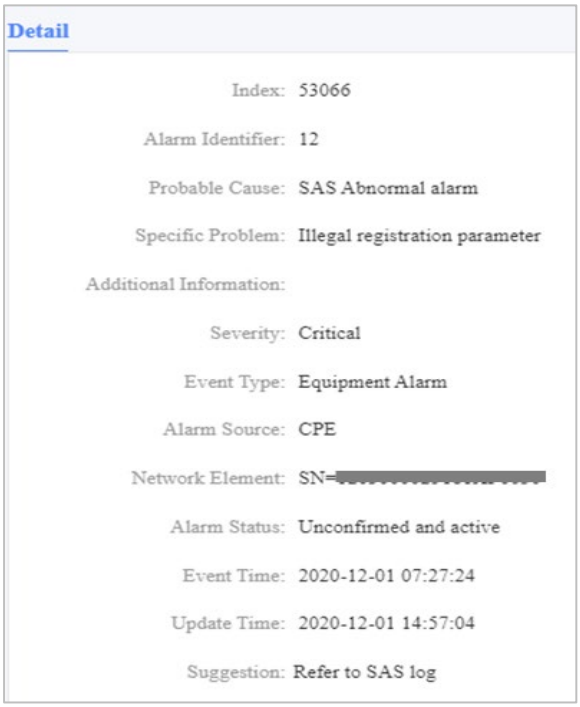


Figure 2-154: Alarm Detail



The three icons in the upper right of the Alarm window are Filter, Chart, and Export, as was shown in Figure 2-152. The Filter function is discussed in *section 2.4.4.2.1.2 Add New Alarm Filter Template*. Clicking on the Chart icon will display the top 10 alarms information in graphical and pie chart formats, by day or by month (Figure 2-155). Hover over any data point on the graph to see the numerical data.

Select Device Group, Device, Device, or Alarm ID, and a date or date range in the pie chart pane. In the figure, the *Device* was selected, and the pie chart displayed the eNB serial numbers for each of the top 10 alarm IDs. Examples of Device Group and Alarm ID are shown in Figure 2-156 and Figure 2-157.

Figure 2-155: Chart View of Top 10 Alarms (by Device)

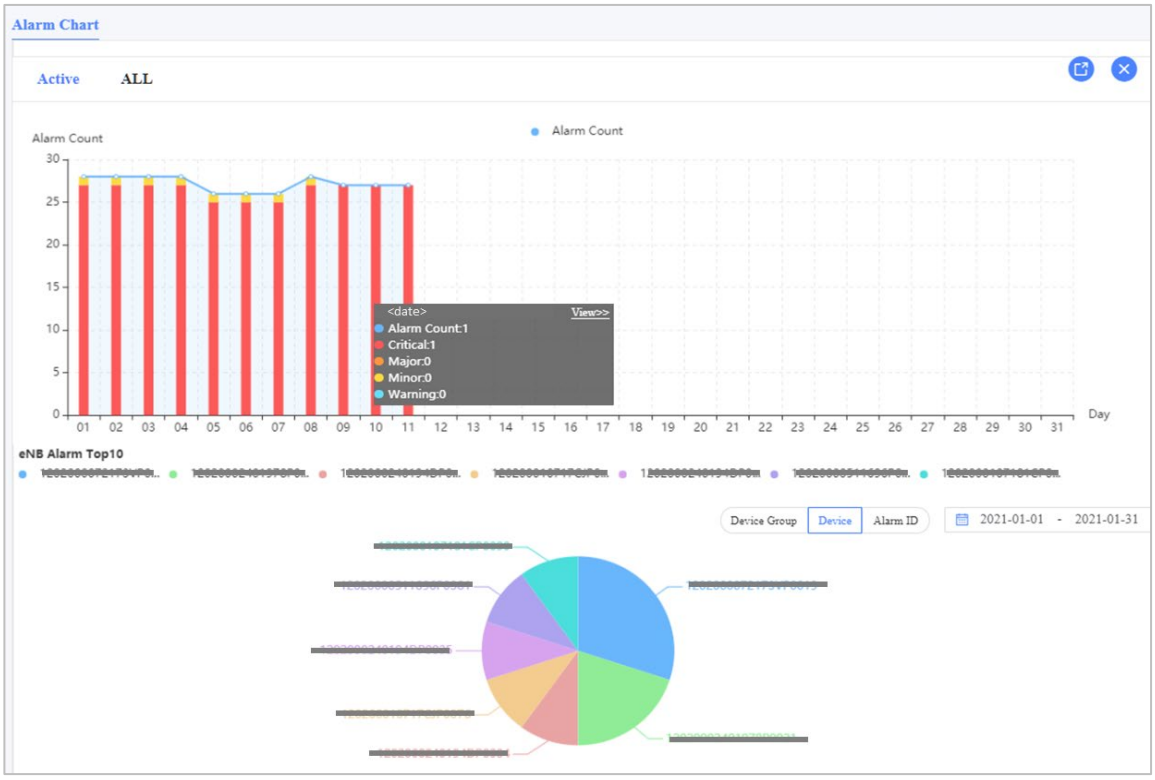


Figure 2-156: Chart View of Top 10 Alarms (by Device Group)

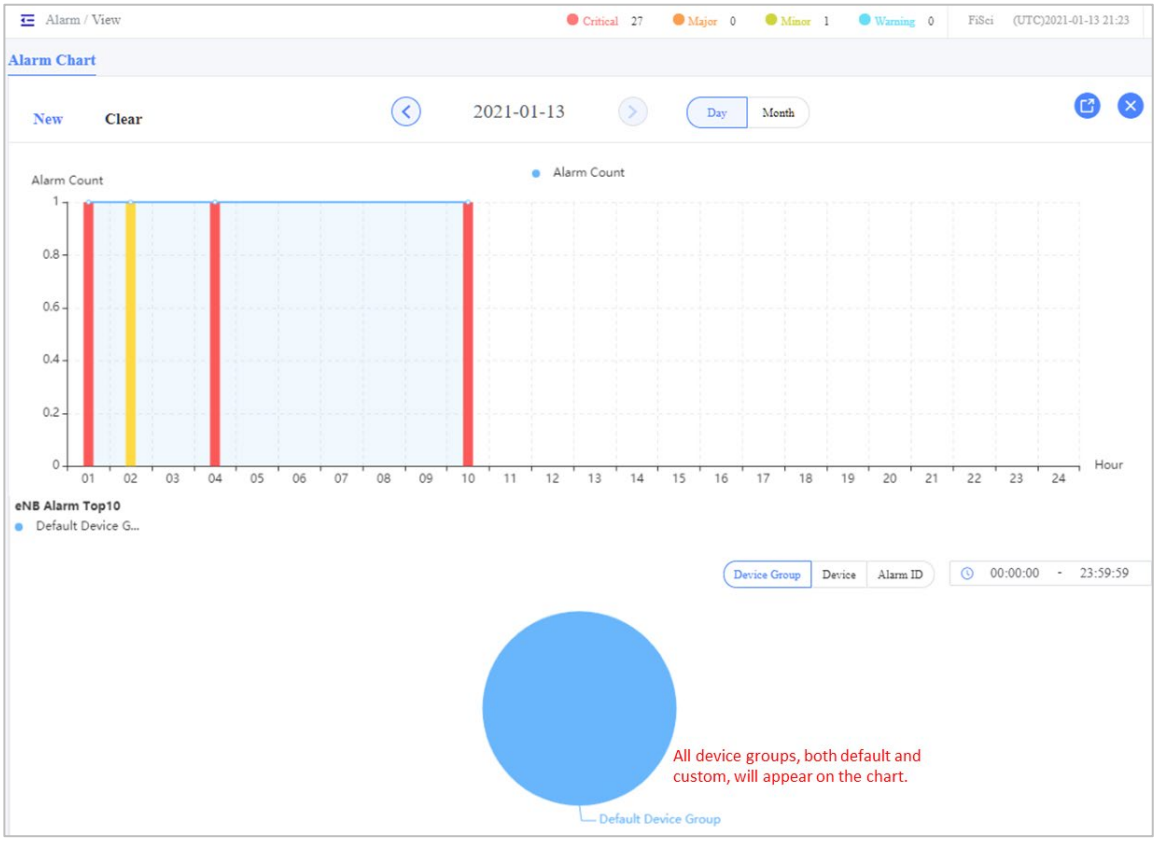
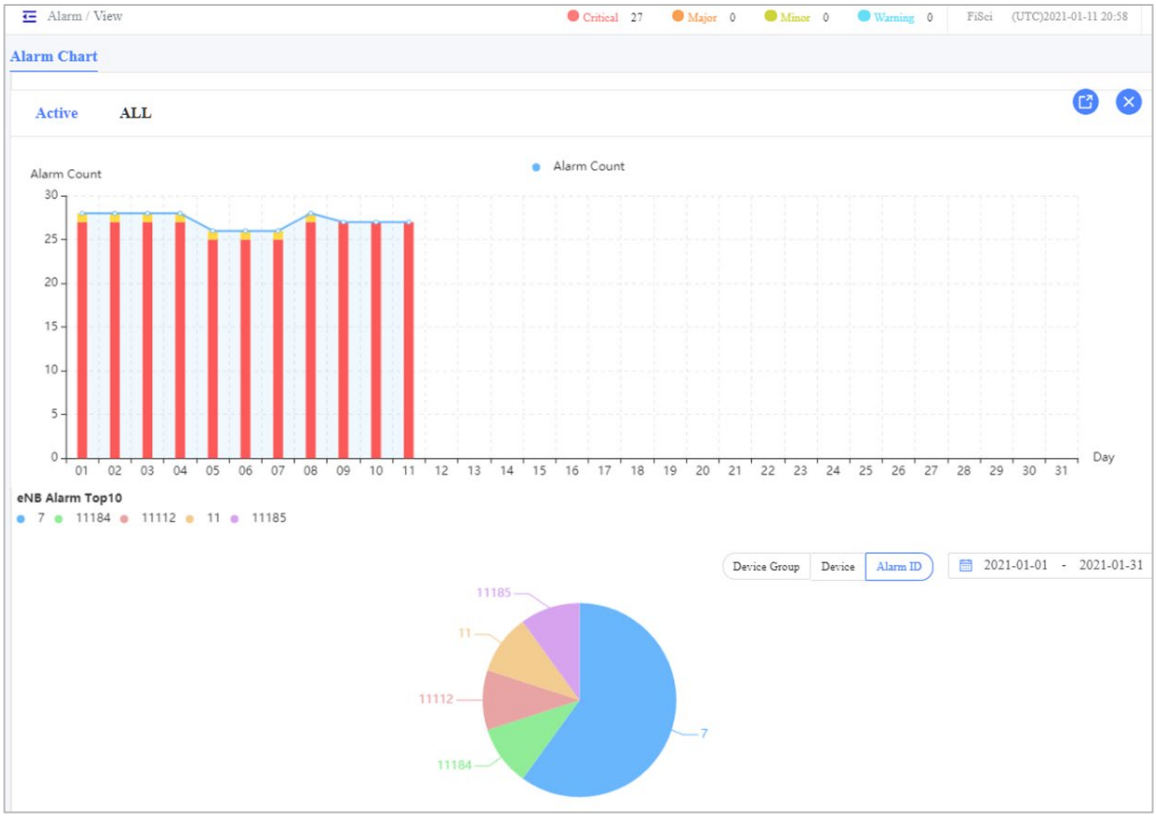


Figure 2-157: Chart View of Top 10 Alarms (by Alarm ID)

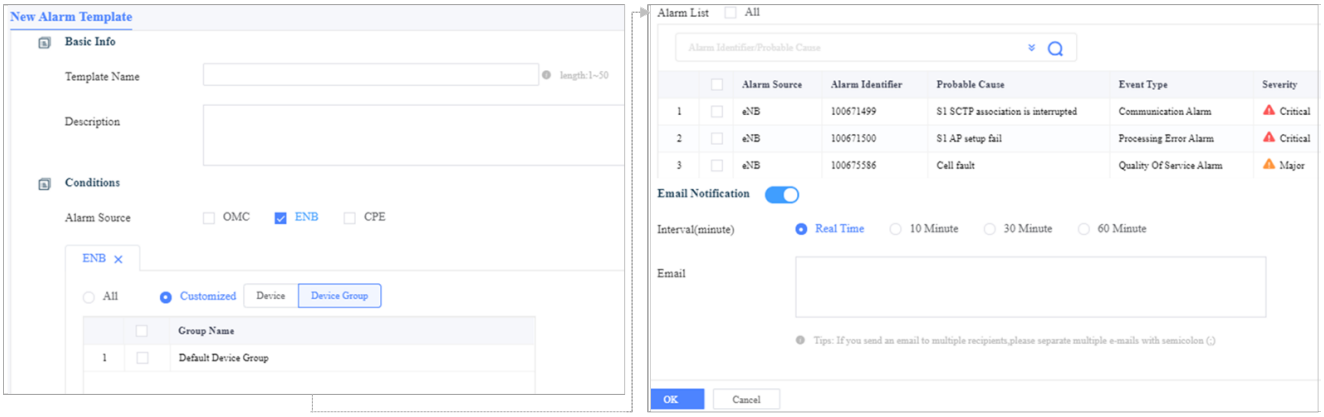


2.4.4.2.1.1 Add New Alarm Template

To add a new alarm template (Figure 2-158):

1. Click on the **+** Add icon under the three tabs in the left pane. This will open the New Alarm Template window.
2. In the Basic Info pane, either accept the auto-generated Template Name or enter a new name. Optionally, add a description.
3. Under Conditions, select one or more alarm sources -- OMC, eNB, CPE. You must select at least one. Your selection will result in a filtered Alarm List beneath it.
4. In the Alarm List, select All to see all alarms for the alarm source(s), choose Device to choose specific devices, or choose Device Group to choose one or more specific device groups.
5. In the Alarm List, select the All checkbox to include all alarms in this template. Or leave the All checkbox unchecked and choose the specific alarms you want to have.
6. For Email Notification, slide the toggle to the right to enable email notifications for the entities and alarms selected above.
7. At the Interval (minute) field, select Real Time, 10 Minute, 30 Minute, or 60 Minute. This will determine how often the system checks for the conditions selected in the template and notifies one or more parties via the email addresses that you enter in the Email box beneath. If you want to enter more than one email address, use a semi-colon (;) after each address.
8. Click on *OK* to save the template. The new template will now be listed in the Alarm window.

Figure 2-158: Add New Alarm Template

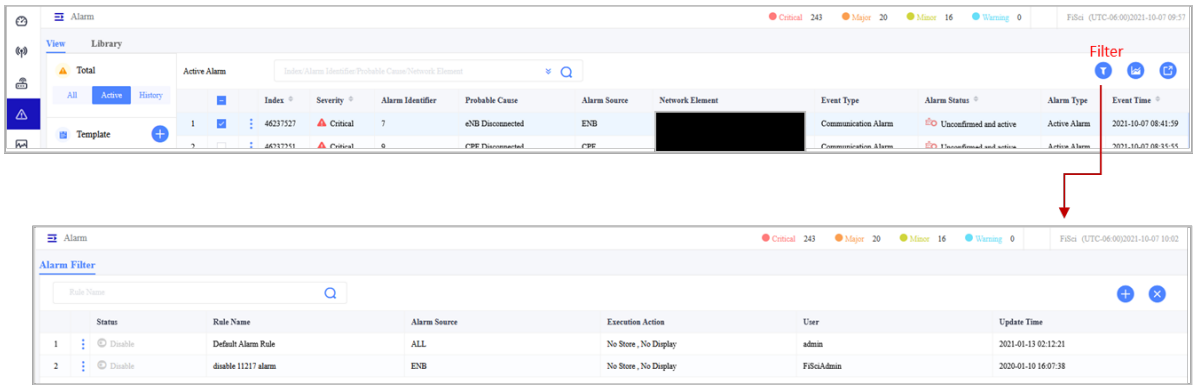


2.4.4.2.1.2 Add New Alarm Filter Template

An alarm filter template provides a way to tell the system what actions to take for specific alarms. The filter icon is on the upper right of the Alarm window (Figure 2-159).

When you click on the icon, the Alarm Filter window opens and shows a default alarm filter template that includes all alarm sources and defaults to an Execution Action of No Store, No Display. The available execution actions will be described below.

Figure 2-159: Alarm Filter



To create a new alarm filter template (Figure 2-160):

1. Click on the **+** Add icon in the upper right of the Alarm window to open the New Alarm Filter Template window.
2. Accept the auto-generated Filter Rule Name or enter a new name.
3. For now, keep the Status of the template as Disable. Once the other parameters have been entered, you can enable the template.
4. Choose an Execution Action to indicate how the system will treat the alarms:
    a. No Store, No Display (default) - The OMC will not store or display the alarms identified in the template.
    b. Only Store, No Display - The OMC will store but not display the alarms identified in the template.
    c. Display, auto-confirm - Each alarm in the template will be auto-confirmed. Confirming an alarm indicates the alarm was acknowledged in the system but not yet resolved.

5. Under Conditions, select one or more alarm sources in the filter template: OMC, eNB, CPE.
6. For the list which follows the Alarm Source field, you can select All OMC alarms, All eNB device groups, and All CPE device groups. Alternatively, use the Customized option to choose between Device and Device Group to view and select specific eNBs or CPEs.
7. The next part of the Conditions pane pertains to the alarms you want to include in this filter template. If you select the All checkbox, all alarm IDs will appear in the list. Only the alarms pertaining to those entities will be listed if you selected only eNB or CPE for the alarm source. Select the checkbox next to the alarms you want to be included in this filter template.
8. Set an Event Time using the Start Time and End Time, which determines the time window when the alarms will be reported.
9. Enable the template:
    a. If you are ready to start using the filter template, go back to the Basic Info section of the window, set the Status to Enable, and click on *OK*. The new alarm filter template will appear in the Alarm Filter list.
    b. If you want to enable the template later, leave the Status as Disable and click *OK*. The new alarm filter template will appear in the Alarm Filter list. Use the *Operations> Enable* action when you are ready to enable the template; use the *Operations > Enable* action (Figure 2-161).

Figure 2-160: Add New Alarm Filter Template

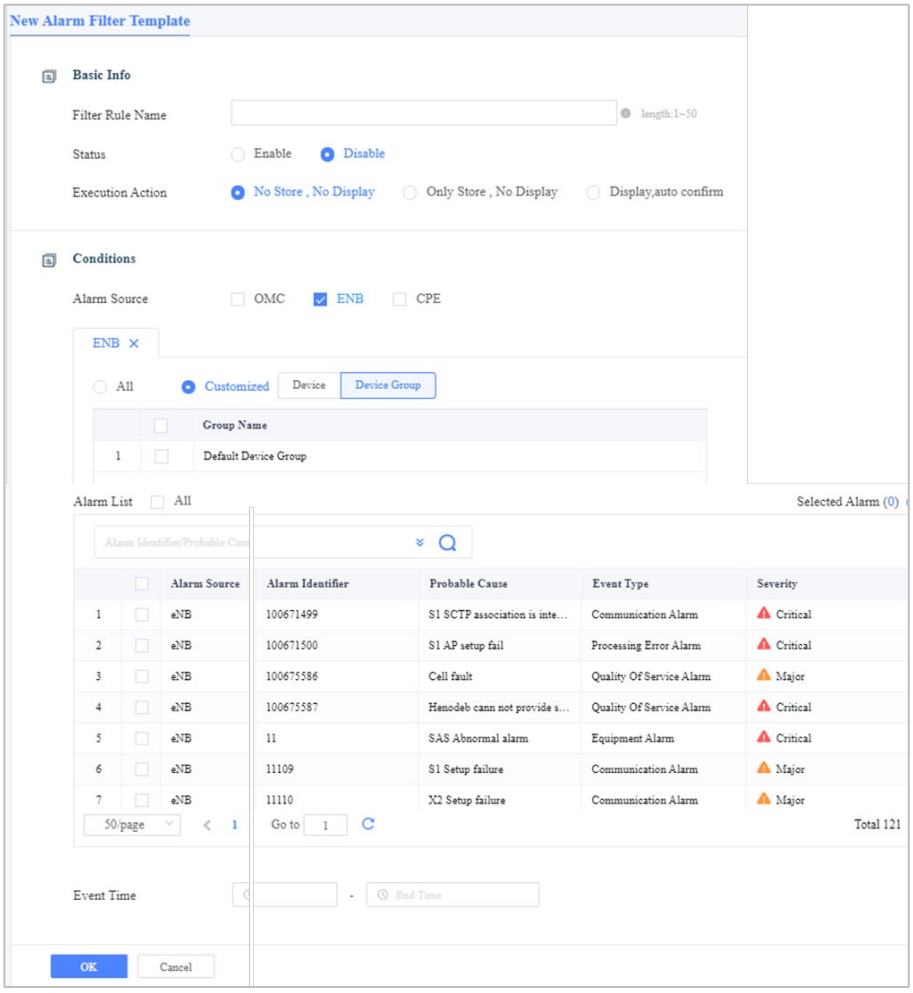
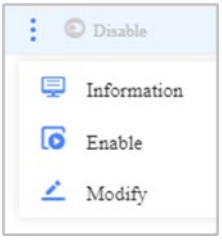


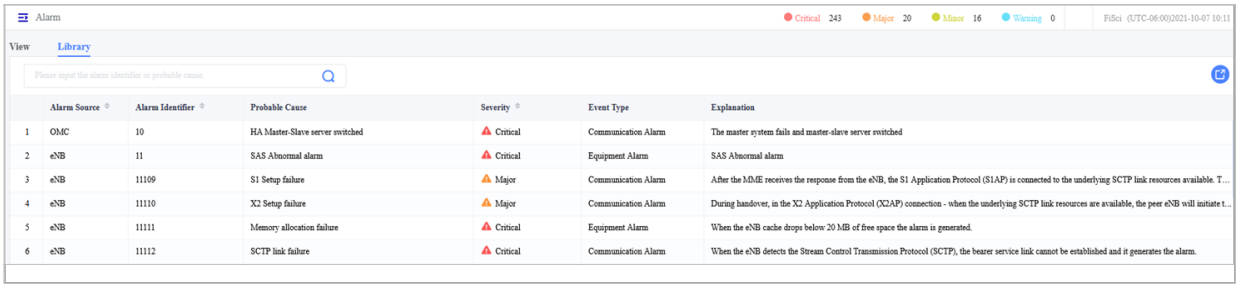
Figure 2-161: Operations



2.4.4.2.2 Library Tab Description

The Library tab displays a list of all possible system alarms, providing a probable cause and the severity level of each alarm (Figure 2-162). You can sort the data in the Device Type, Alarm Identifier, and Severity columns. Use the search bar to look for specific alarm IDs or probable causes. Use the Export icon in the top right of the window to save the list to your computer.

Figure 2-162: Library



2.4.5 Performance Menu

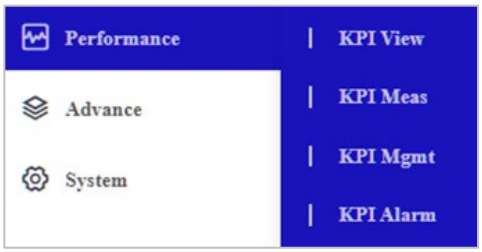
The Performance menu is used to collect LTE Key Performance Indicator (KPI) metrics (Figure 2-163). As the network operators endeavor to provide qualitative service to the subscribers without exhausting the radio resources, monitoring and optimizing radio network performance is critical. Typically, LTE KPI metrics can be characterized into Accessibility KPI, Retainability KPI, Mobility KPI, Integrity KPI, Availability KPI, and Utilization KPI.

- Accessibility KPI: It is the success rate of users able to access the network.
- Retainability KPI: This helps retain the subscribers with the network to provide service.
- Mobility KPI: Handover is crucial to maintaining a moving subscriber connection. This KPI measures the performance in such events.
- Integrity KPI: This KPI measures the exact throughput and latency of the network
- Availability KPI: It measures the availability of the network to serve the users.
- Utilization KPI: To optimize the use of network resources, this KPI helps measure the usage of the resources.

This section helps in creating and configuring the custom and default KPI templates to measure the performance of various radio network resources.

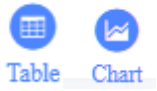
Any eNBs included in a KPI template will collect standard KPI metrics. In addition to standard KPIs, operators can create custom KPI indices. Each function is explained in this section.

Figure 2-163: Performance Menu



2.4.5.1 KPI View

There are two panes in the KPI View window: On the left is a list of KPI templates, where Basic is a default template, and on the right is a list of the operator's eNBs shown in Table format (Figure 2-164). When you click on a KPI Template, you can select the report interval you wish to see: 15Min, 60Min, or 24Hour. Click on a field to display the formula used to calculate the indices.



The Table format and the Chart format (Figure 2-165) can be toggled using the icons in the upper right of the KPI View window. Hover over a data point to view the numerical data.

Figure 2-164: KPI View Table Format

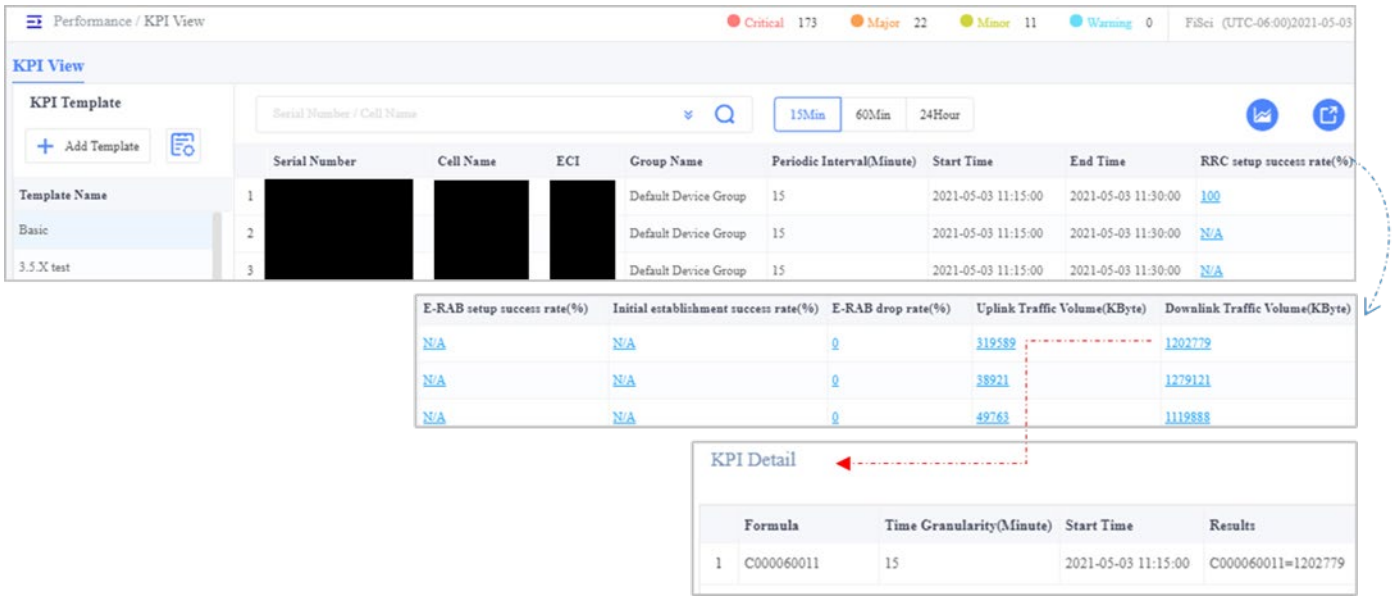
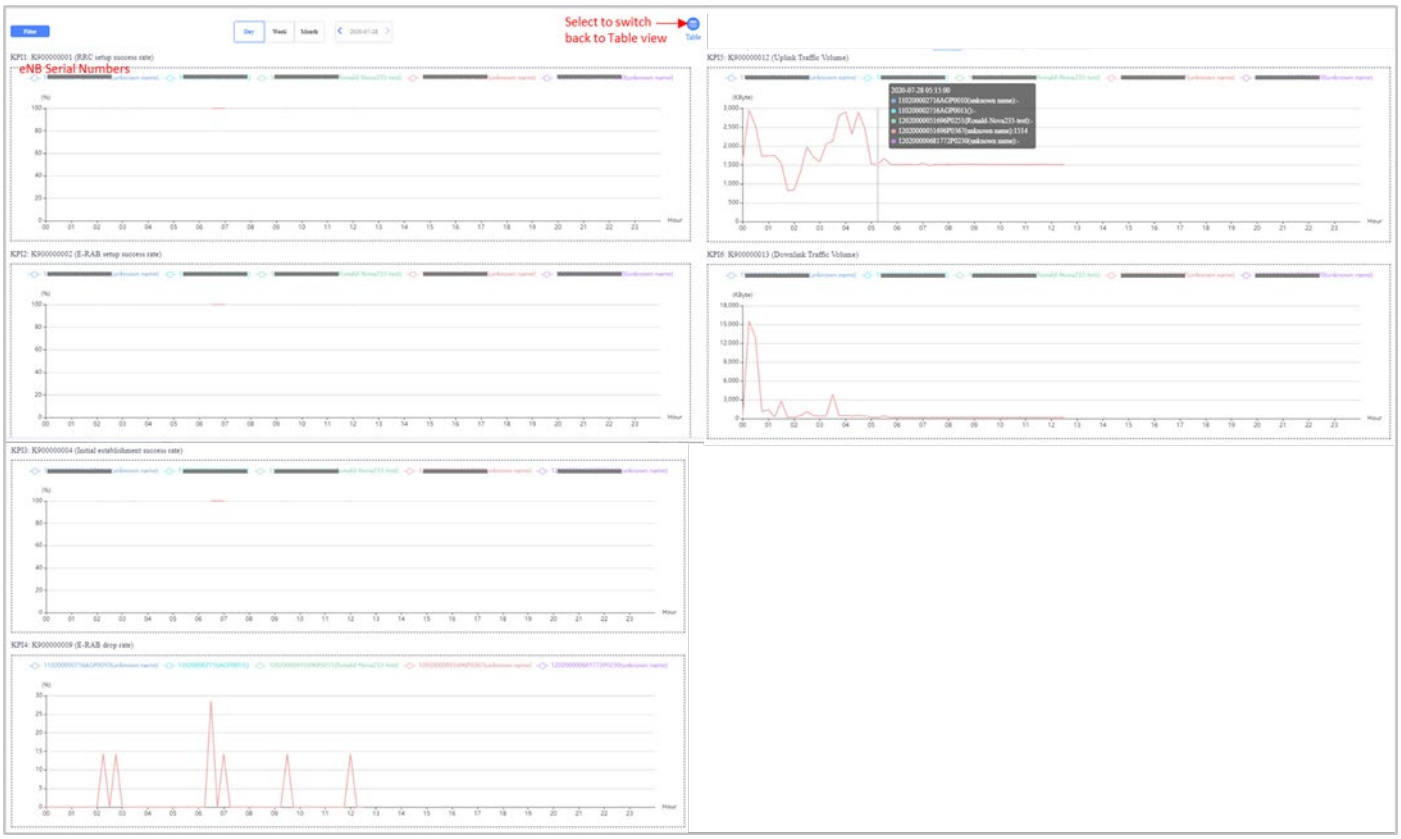
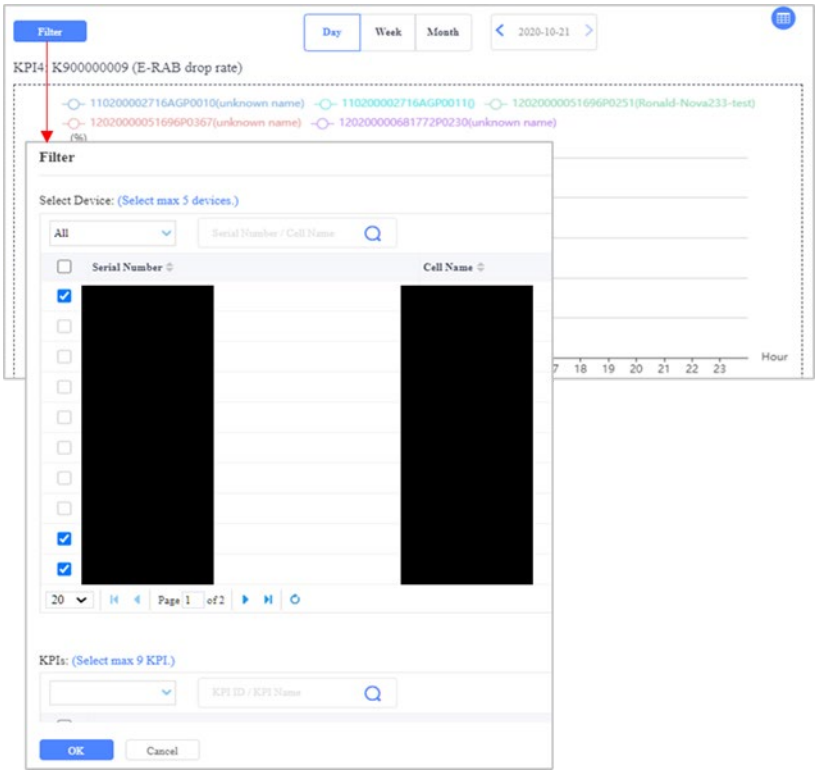


Figure 2-165: KPI View Chart Format



The Filter button provides a way to sort the devices and KPIs you want to see Figure 2-166).

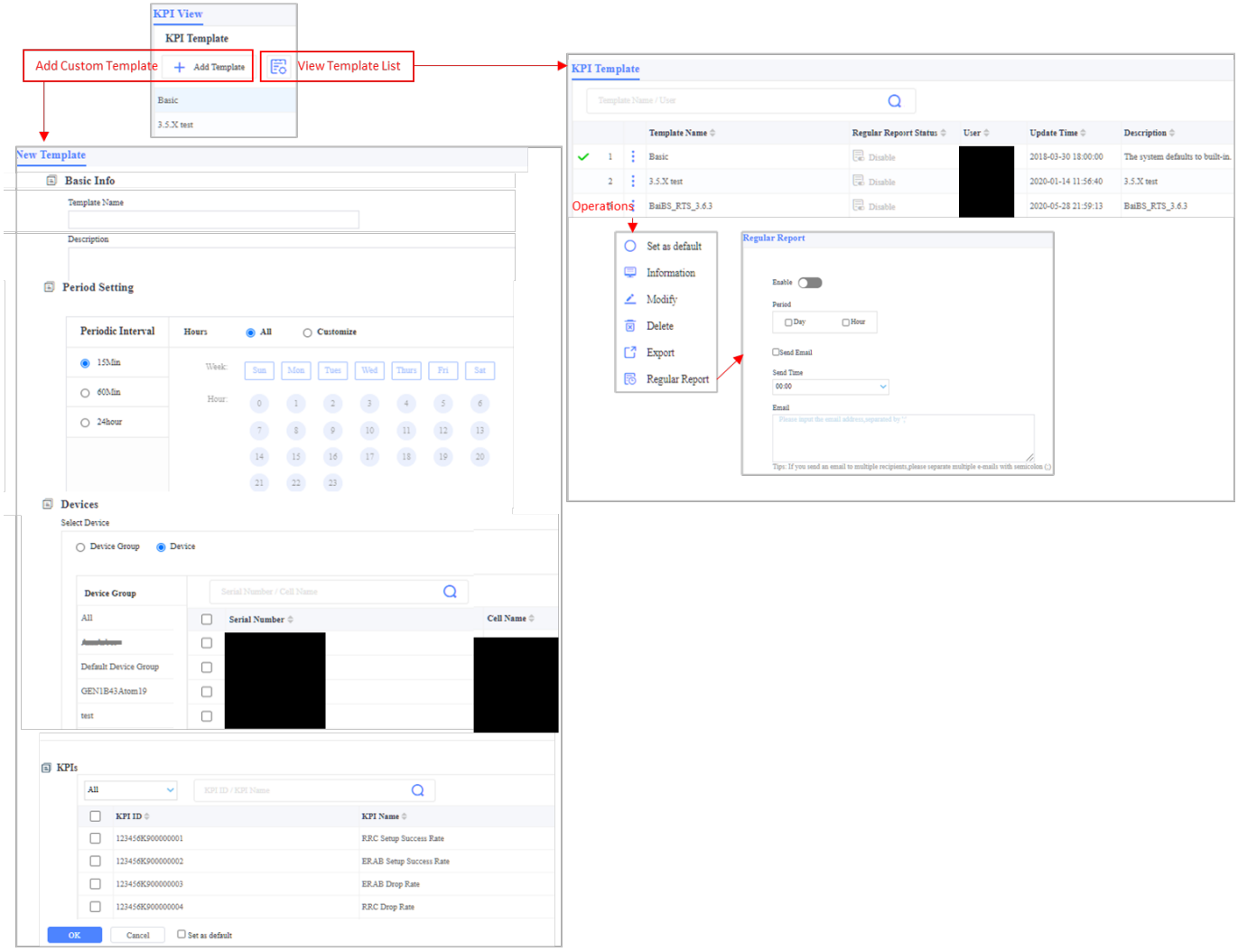
Figure 2-166: Filter KPI View



Customizing KPI indices opens additional ways to look at network performance and facilitates the long-term monitoring of an index group. To create a custom KPI template (Figure 2-167):

1. Click on **+** Add Template to enter the KPI Template window.
2. Enter a Template Name and Description.
3. Under Period Setting, select the Periodic Interval and days of the week plus hours for collecting the data.
4. Select the eNB device group(s) and device(s) you want to monitor.
5. Select the KPIs to report.
6. Click on *OK* to save the settings. The new template will appear in the KPI View list. You have the option to download the results as a .csv file.

Figure 2-167: Add New KPI Template



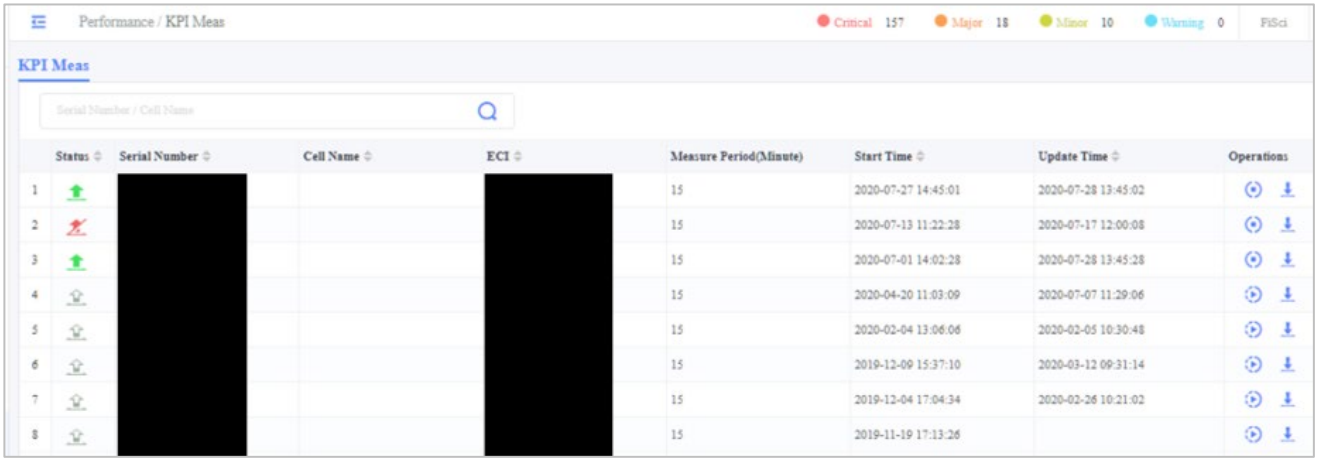
The View Template List icon displays all templates. It provides *Operations* functions: Set as default, view Information about the template configuration, Modify the template configuration, Delete the template, Export the template data, and make this a Regular Report.

If you enable the Regular Report function, you can automate report generation by Day or Hour, create a Send Time, and enter Email addresses where the report will be sent. Use a semi-colon (;) to separate multiple email addresses.

2.4.5.2 KPI Meas

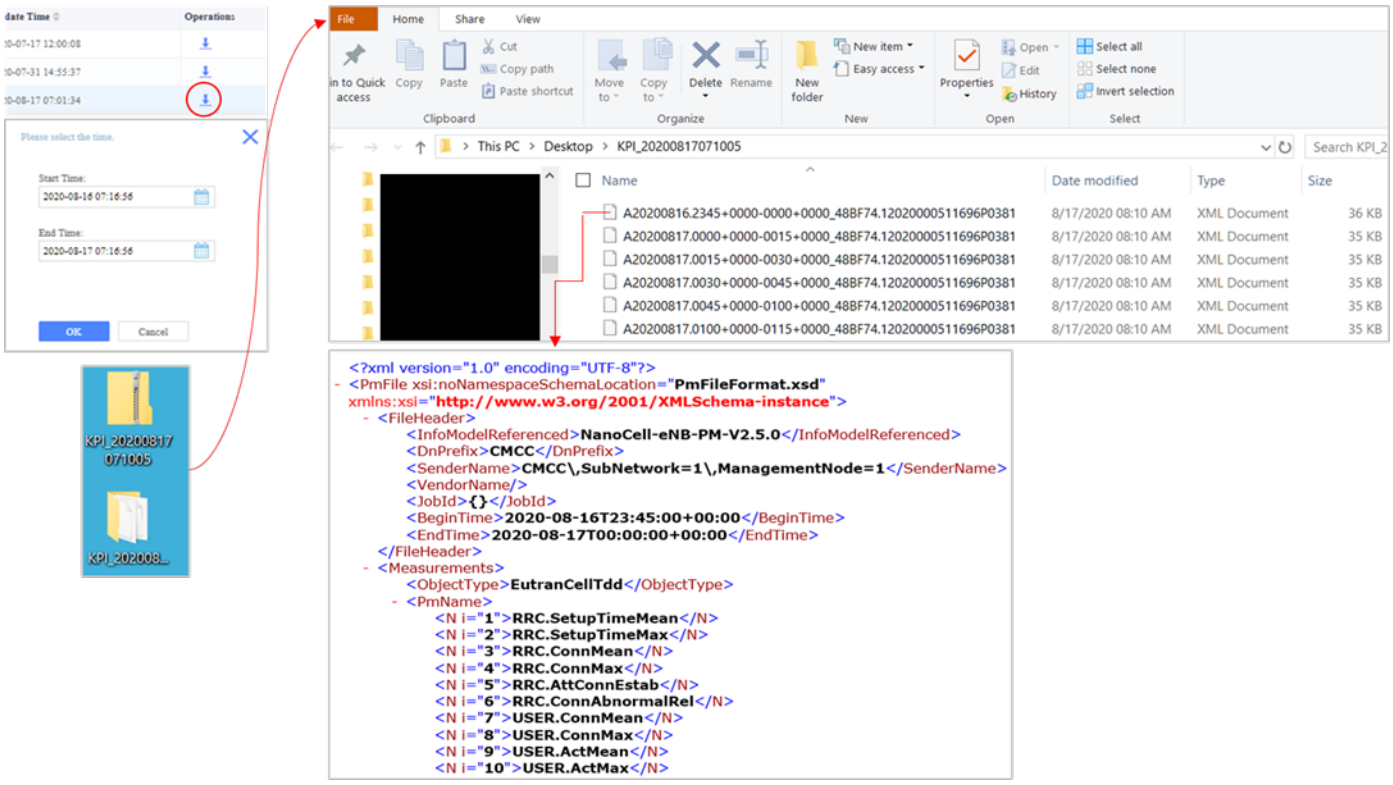
The KPI Meas (measurement) menu is used to check the status of per-eNB KPI measurements via the KPI View template. The column headers include the current measurement period (how long the KPI was tracked), the date and time the measurement started, and the last time the KPI information was updated (Figure 2-168).

Figure 2-168: KPI Meas



Under Operations, select the circle to close the KPI for that eNB. If you select the Download arrow, a pop-up window will ask you to choose the period from the KPI measurements you want to download. The XML files will download as a zip folder. Once extracted, you can open each XML file to examine the raw KPI data (Figure 2-169).

Figure 2-169: Download XML Files



2.4.5.3 KPI Mgmt

The KPI Mgmt (management) menu shows the library of KPI function sets (Figure 2-170). A function set is a grouping of KPIs related to the same operation; for example, the EQPT function set contains all KPI indices related to Layer 1 Physical Layer. Most KPIs are standard LTE indices, like the one shown in Figure 2-171; however, any Baicells-specific KPIs are considered customized and contain a formula that uses multiple standard KPIs.

Use the *Operations > View* function to open the details about a specific KPI. The KPI information includes the KPI name; the function set it belongs to, the unit of measurement used, the KPI ID, the statistic type (e.g., average, mean, sum, etc.), an explanation (description), and if customized, the formula used to calculate the KPI.

Figure 2-170: KPI Mgmt Standard LTE KPI Example

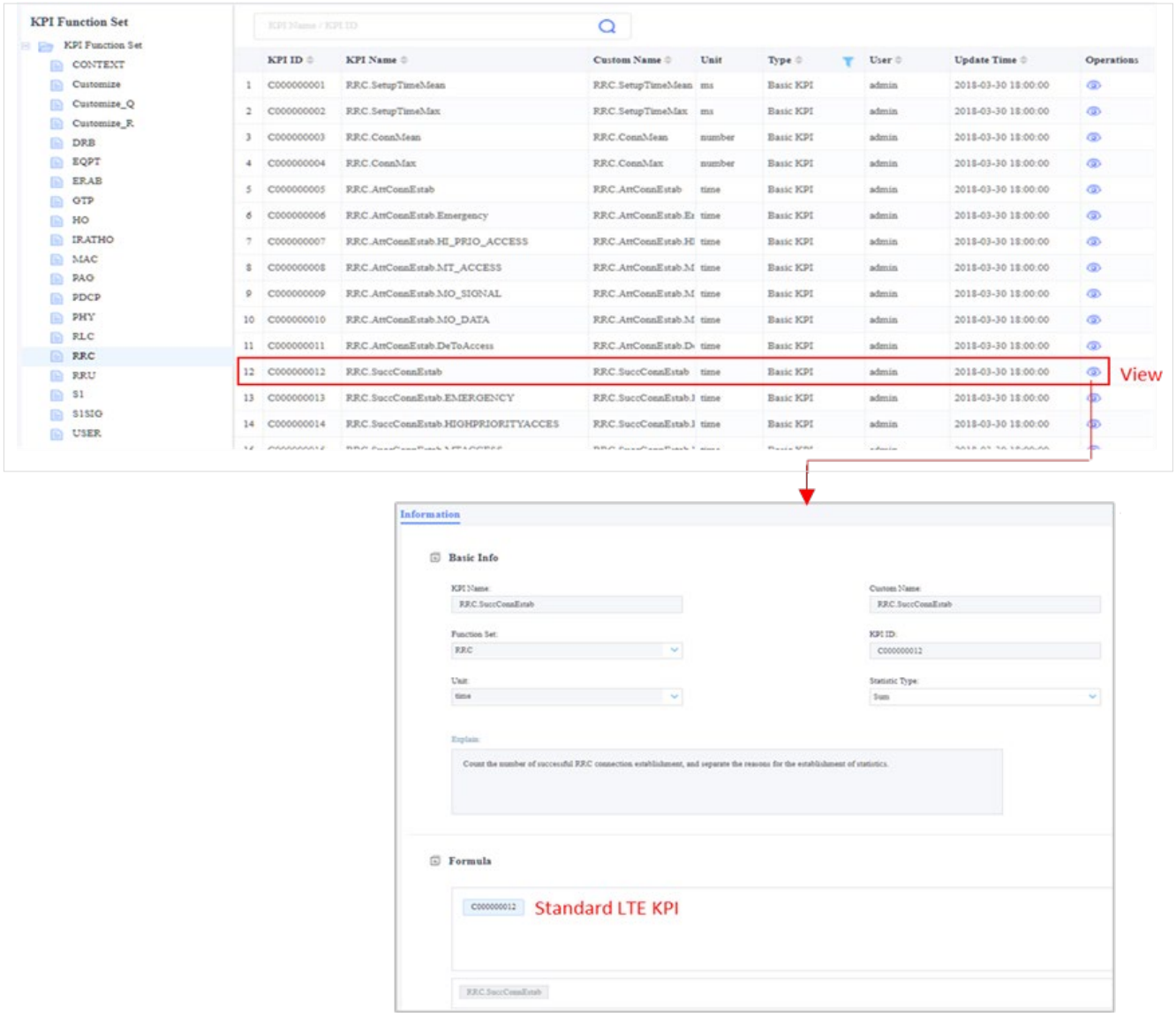
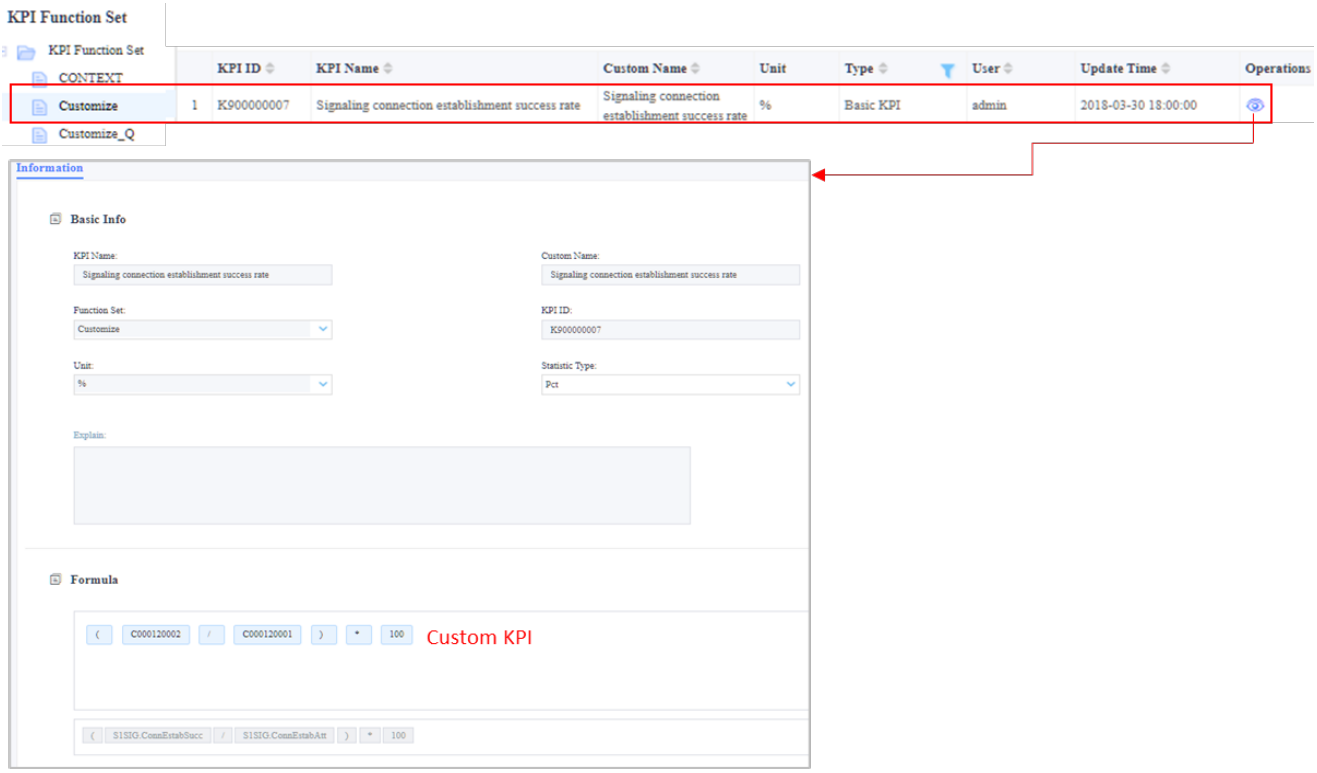


Figure 2-171: KPI Mgmt, Custom KPI Example



2.4.5.4 KPI Alarm

The *Performance > KPI Alarm* function enables operators to create "compare" operations for specific devices (Figure 2-172). A specified threshold is compared to a standard KPI. If the data exceeds the threshold, the system reports the alarm. You can add up to 5 comparisons per template.

The compare operations are:

> Greater than

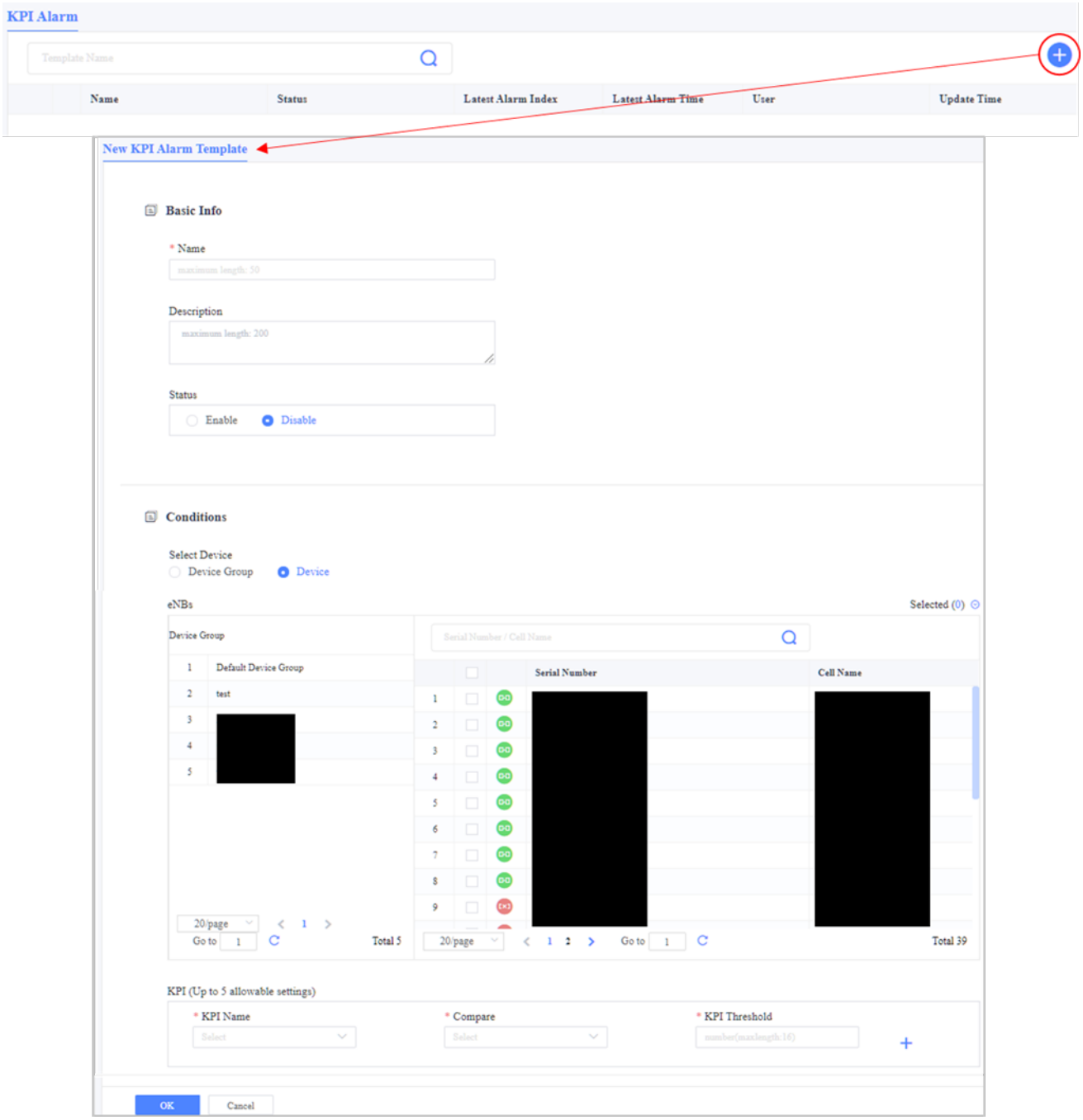
< Less than

= Equal to

≥ Greater than or equal to

≤ Less than or equal to

Figure 2-172: New KPI Alarm Template



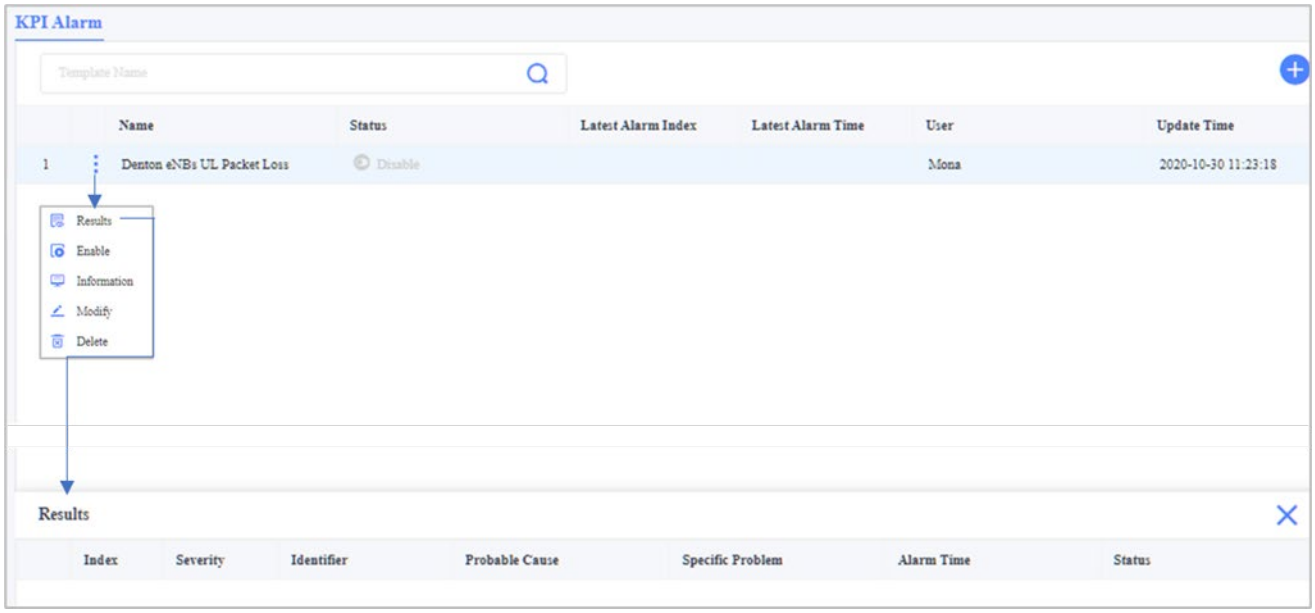
To create a new KPI Alarm template (see Figure 2-172 above):

1. Select the **+** Add icon in the upper right of the window.
2. Enter a template name and, optionally, a description. For now, skip the Status setting; you will enable the template after saving the template information.
3. Under Conditions, select either Device Group or Device to display the eNBs by group or individually.
4. Select the checkbox next to the eNBs you wish to include in the template.

5. Under KPI:
    a. Select the standard KPI Name from the drop-down menu.
    b. Select the Compare operation from the drop-down menu, e.g., less than, greater than, equal to.
    c. Enter the threshold value.
    d. If you wish to add another comparison, select the **+** Add icon and repeat steps 5a-5c.
6. Click on *OK* to save the settings. The template will be added to the KPI Alarm list.

Use the *Operations > Enable* the function to start using the new KPI alarm. To see the results of the data, select *Operations > Results*. The information will display at the bottom of the window (Figure 2-173).

Figure 2-173: Results



2.4.6 Advance Menu

The Advance menu contains the configuration fields for SAS and Plug-and-play (Figure 2-174). These unique functions are explained in this section.

Figure 2-174: Advance Menu

2.4.6.1 SAS

The Citizens Broadband Radio Service (CBRS) Spectrum Access System (SAS) is an operating solution available only in the United States. The solution requires a working knowledge of SAS, preparation of personnel and equipment, and coordinated configuration across device GUIs, the OMC, and the selected SAS vendor's portal. For this reason, Baicells created the *SAS Deployment Guide* to assist operators in planning their deployment of SAS. Refer to that guide for more information about SAS.

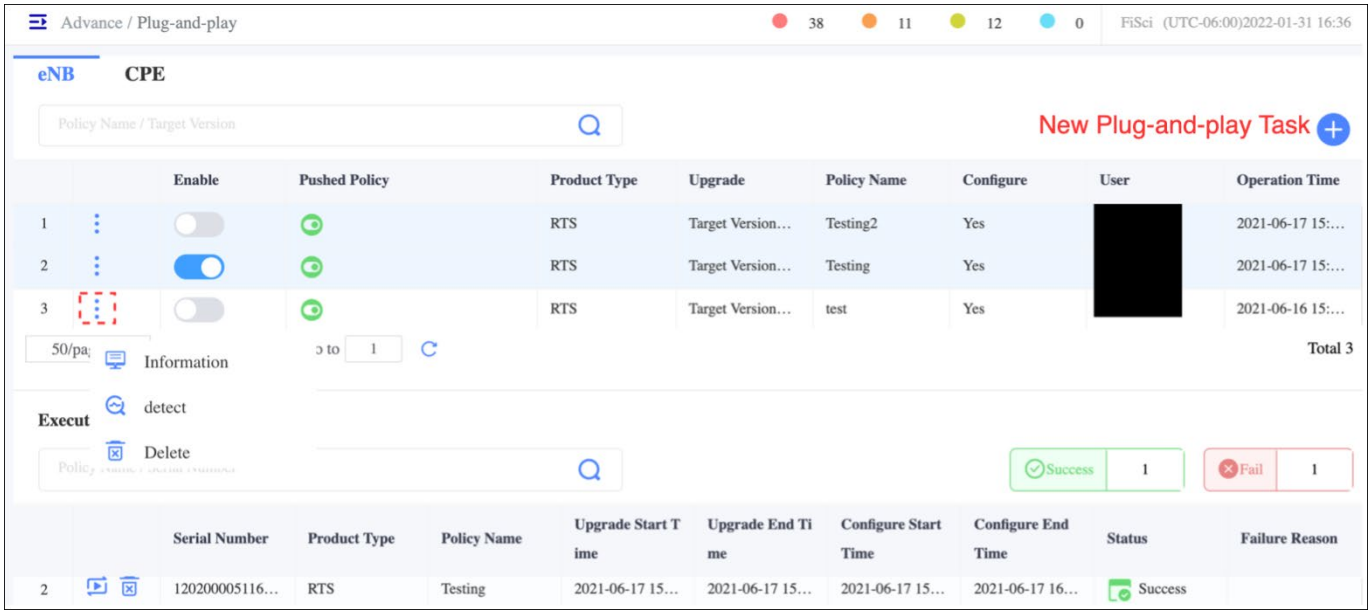
2.4.6.2 Plug-and-play

The OMC supports a plug-and-play mechanism for eNB and CPE. Plug-and-play is configuring software upgrades and adding cell configuration rules on OMC. When a new eNB /CPE is connected to OMC, the device can be configured or upgraded automatically without any intervention from the user. The display of plug-and-play has eNB and CPE.

2.4.6.2.1 eNB and CPE display

To configure new eNBs and CPEs or test upgrade software plug-and-play mechanism can be used. Each new plug-and-play strategy is added to the display. You can view information, detect, or delete each strategy. (Figure 2-175)

Figure 2-175: Plug-and-play eNB Display

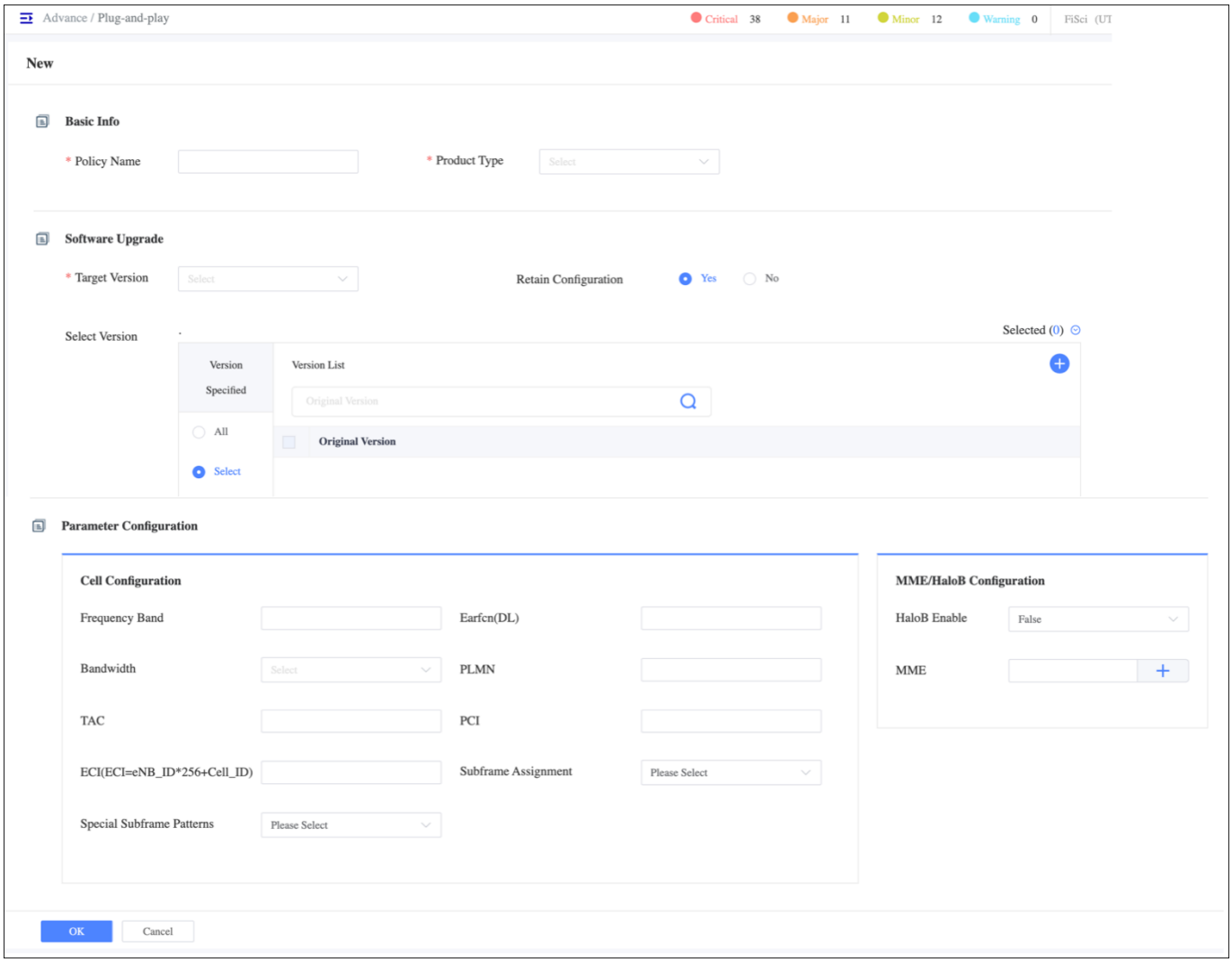


To create a new Plug-and-play task (Figure 2-176)

1. Click on the “+” icon at the top right corner to create a new Plug-and-play strategy.
2. Under Basic Info, enter the policy and product type.
3. In Software Upgrade, select the target version from the drop-down list.
4. Refer to the eNB configuration guide for parameter configuration and enter the parameters.
5. Click *OK* and save the settings.

Note: CPE operation is the same as eNB except for parameter configuration.

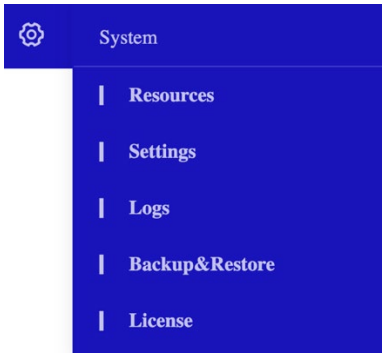
Figure 2-176: New Plug and Play Task



2.4.7 System Menu

The OMC System menu contains settings that the operator can view, create, modify, or delete for specific OMC displays, OMC account logs, and administrative user settings for their account (Figure 2-177). Each function is described in this section.

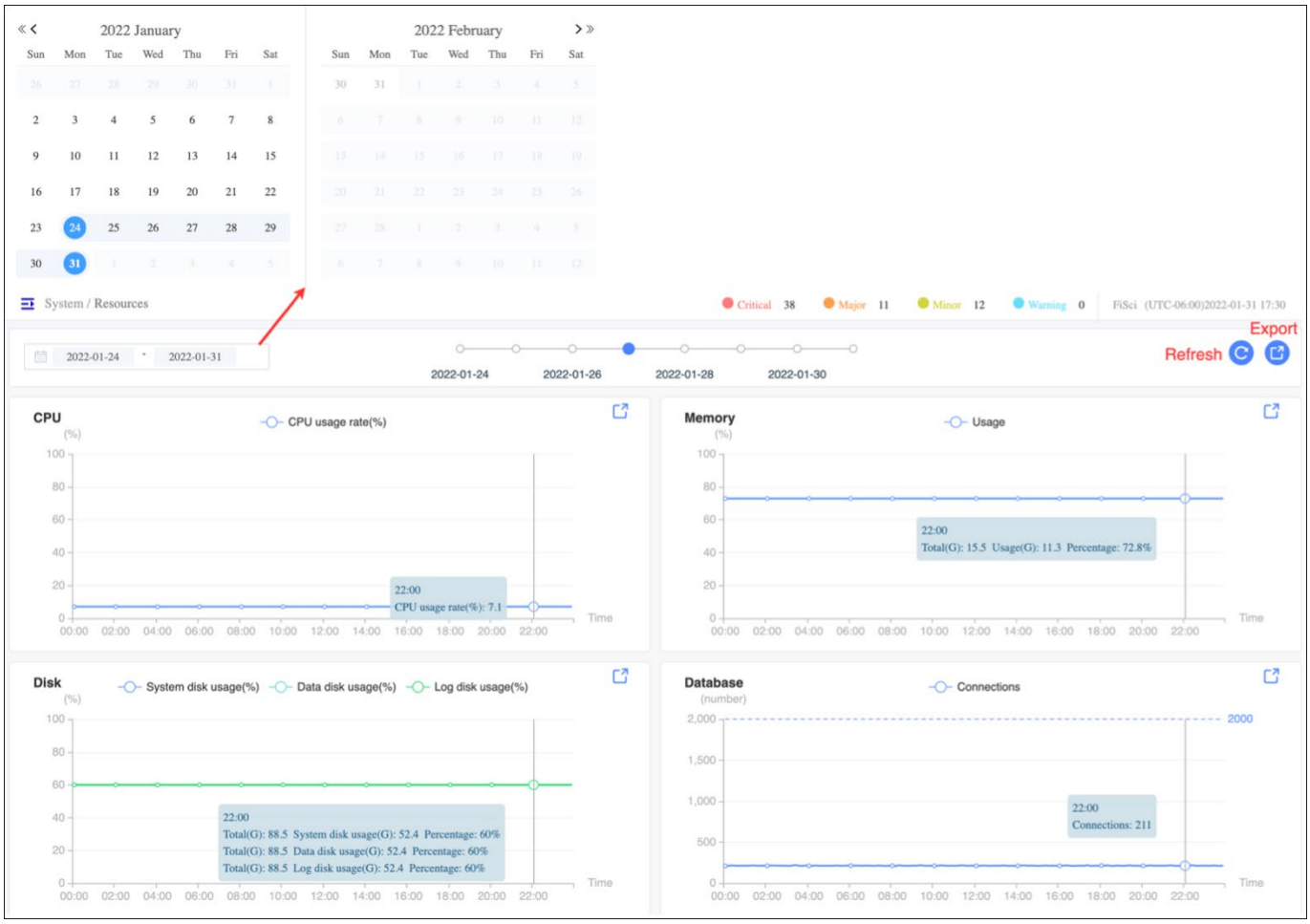
Figure 2-177: OMC System Menu



2.4.7.1 Resources

The *System > Resource* menu shows the utilization of the CPU, disk space, database size, and memory usage. The administrator can refer to the statistics to maintain and optimize the system. To view the Resources landing page, select *System > Resources*, and a graph of resource utilization is seen. To view the usage statistics of resources in a particular period, select the time frame from the calendar. You can also view the usage by hovering over the graph (Figure 2-178). To export the usage as a .csv file, click on the *Export* icon at the top right corner of the page.

Figure 2-178: Resources

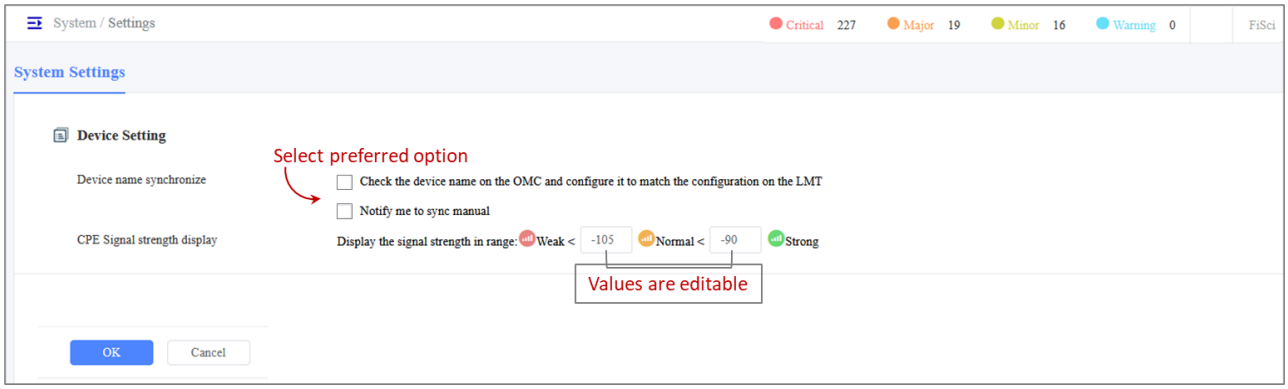


2.4.7.2 Settings

The *System > Settings* menu has two fields: Device name synchronize and CPE Signal strength display (Figure 2-179). For Device name synchronizes, if you click the first checkbox, the OMC will display the same device name in OMC as is used in the device GUI [referred to as Local Maintenance Terminal (LMT) on the screen]. If you click on the second checkbox, OMC will notify you to manually sync the device name in OMC.

For the CPE signal strength (RSSI), you can set the values for what is considered a weak signal threshold and a strong signal threshold for the icons in any of the OMC windows that report signal strength. The closer the dBm value is to zero, the stronger the signal.

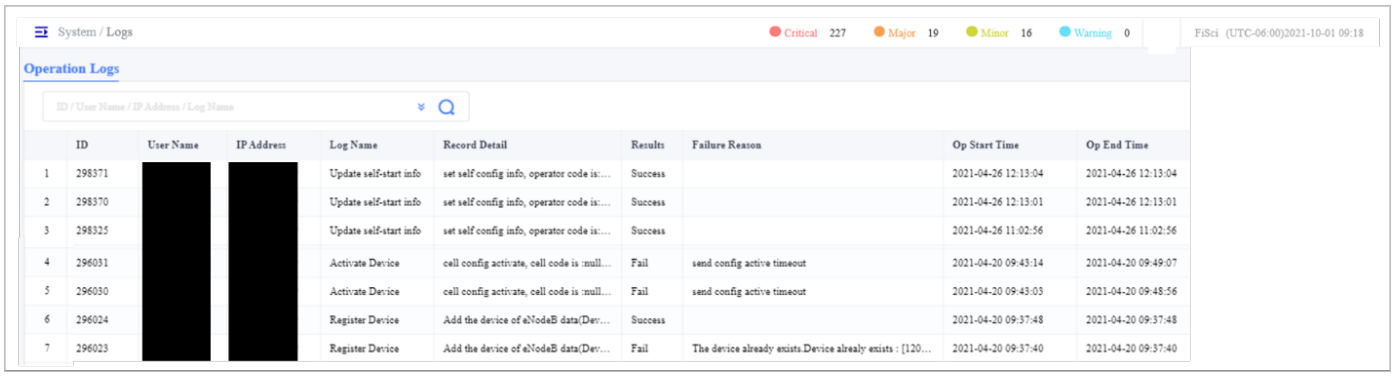
Figure 2-179: Settings



2.4.7.3 Logs

The *System > Logs* menu displays all operational logs concerning OMC usage of the operator's account (Figure 2-180). Each log appears on a separate row and details the event: user's ID, name, IP address; the name of the log, record detail, results, failure reason (if applicable); and the operation's start and stop time. The latest logs will appear at the top of the list. Click on the Export icon to export logs for further analysis.

Figure 2-180: OMC Operation Logs



2.4.7.4 Backup & Restore

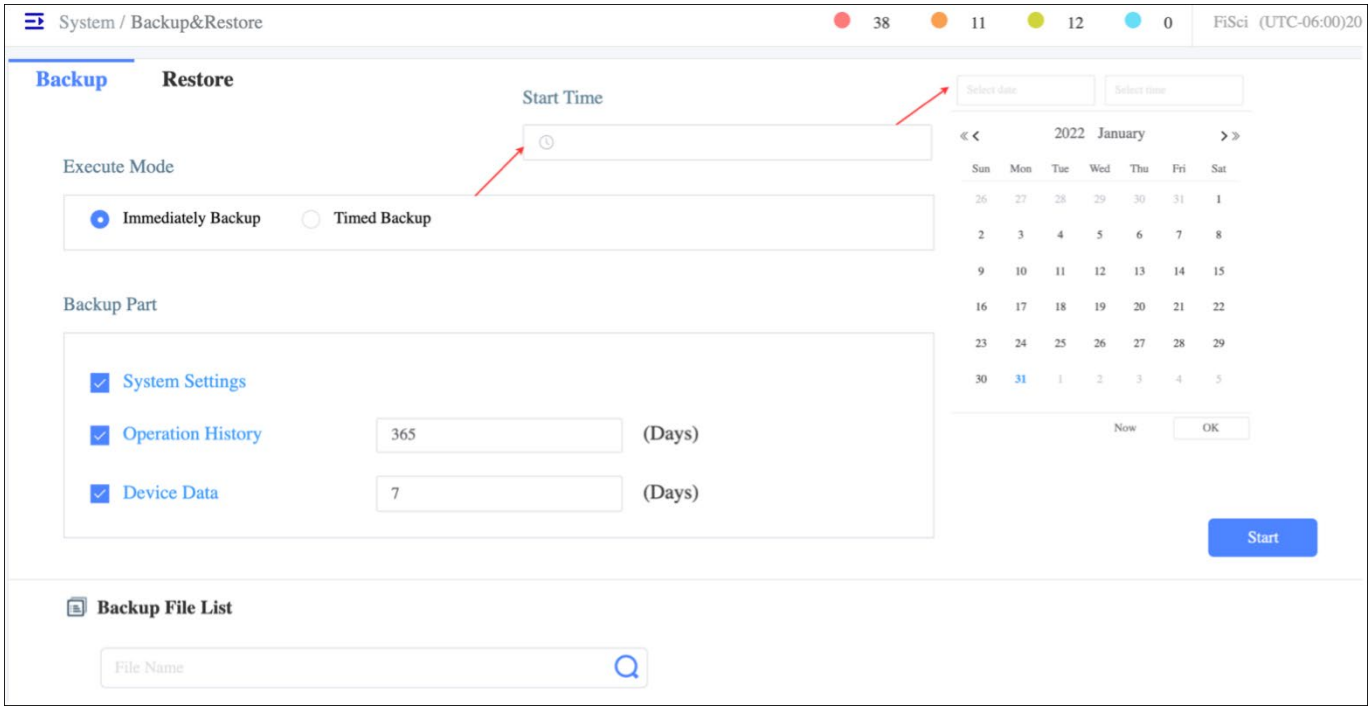
2.4.7.4.1 Backup

Backup is used to store the system settings and device data elsewhere to restore the data in the event of an OMC system crash, natural disaster, or data corruption.

To create a backup (Figure 2-181):

1. Select *System* > *Backup & Restore* to enter the system Backup window.
2. Using the radio button select the Execute Mode, either immediately or timed. For Timed Backup, enter the calendar's start time (Figure 2-181).
3. Select which part of the backup you want to execute, system settings, operation history, or device data.
4. Enter how often you want to perform a backup for each part in days in the text box.
5. To take a Backup on a list of files, enter the files list in the text box and hit search.
6. Click *Start* to start a backup.

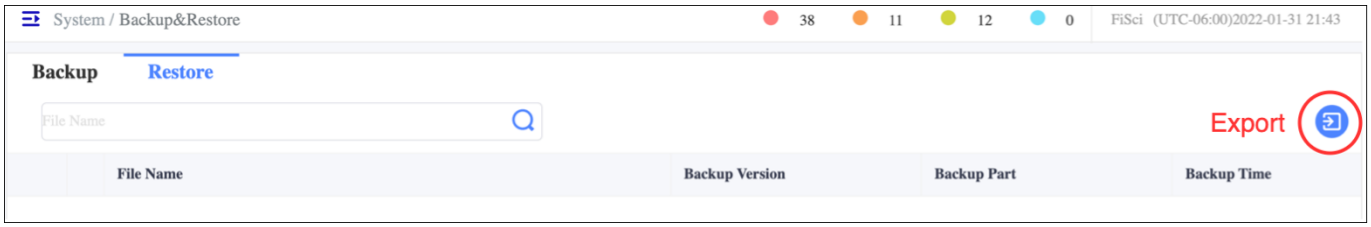
Figure 2-181: Backup



2.4.7.4.2 Restore

To reinstate the files back into the system, select the restore tab in the restore window and enter the file that needs to be restored. Using the search bar search the files. After selecting the files, click on the *Export* icon to restore the files (Figure 2-182).

Figure 2-182: Restore



2.4.7.5 License

The license setting shows the current license of the OMC. The license window shows the basic info like License ID, Expiry Date, and License type. The feature list shows the licenses of various features in the OMC. To update the license lists, click on the *Update* button at the bottom of the page and enter the license file name to import (Figure 2-184). Click *OK* to save the License file.

Figure 2-183: License

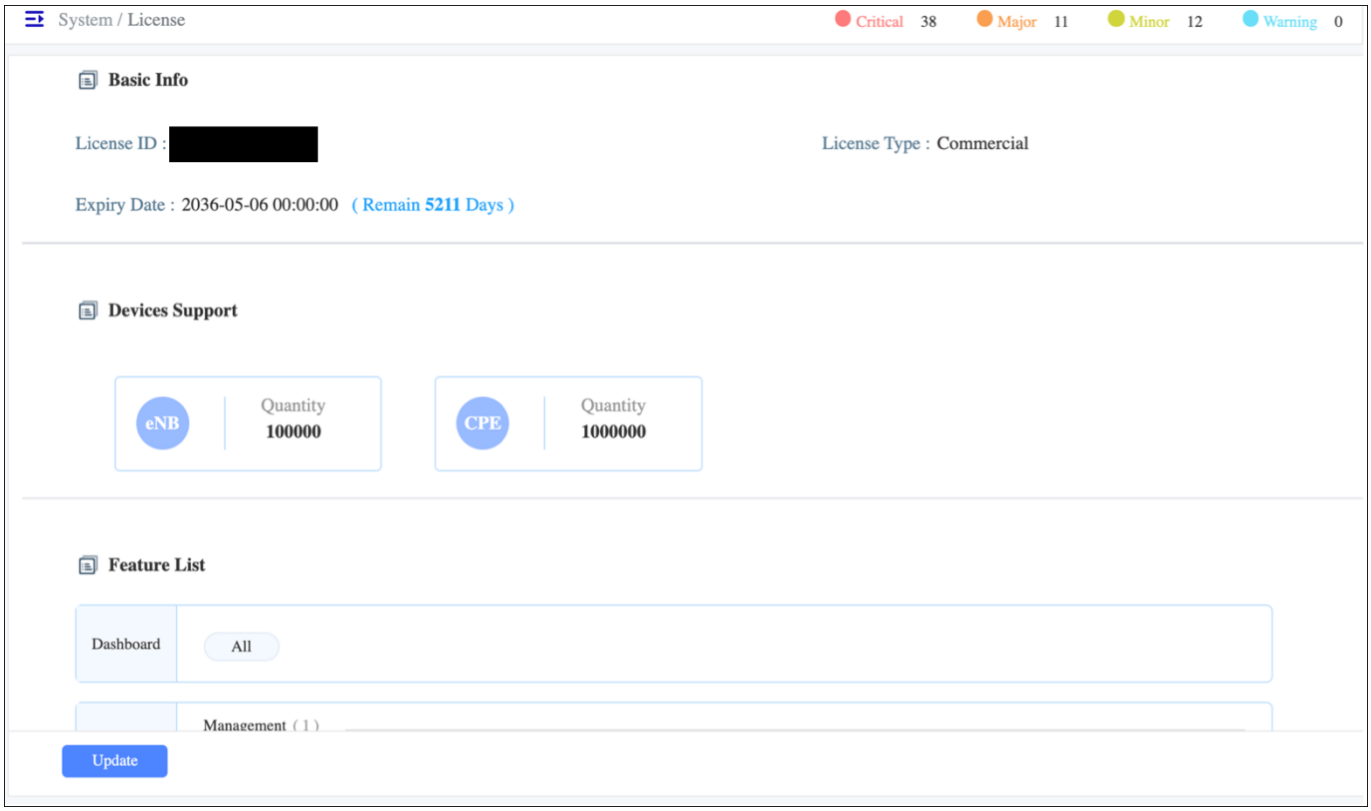
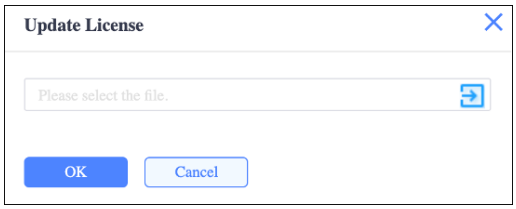


Figure 2-184: Update License

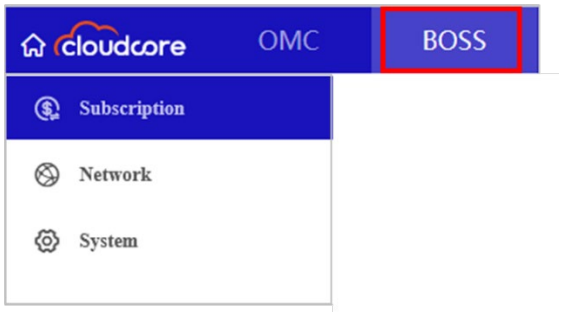


2.5 BOSS

2.5.1 Overview

An operator's CloudCore account includes the Business and Operation Support System (BOSS) module. Operators can use BOSS to add/change/delete subscribers and create/change/delete service plans. Figure 2-185 shows the BOSS menus.

Figure 2-185: BOSS Menu



2.5.2 Subscription Menu

2.5.2.1 Description

The BOSS Subscription menu is where you add, modify, activate/deactivate, or delete existing subscription accounts. Existing subscriptions are shown in the list on the main page. For each existing subscription, you will see the name, SIM card IMSI, the assigned service plan, the status, the name of the CPE being used, the origin (which CloudCore administrator added the subscription), and a description. You can search the IMSI/Name using the text box. Also, by clicking the advanced query filter option, you can filter the required fields and process the search

NOTE: The terms subscription, subscriber, user, and customer are used interchangeably to indicate the entity given access to the network. The general term used is account.

Figure 2-186: Advanced Query Filter

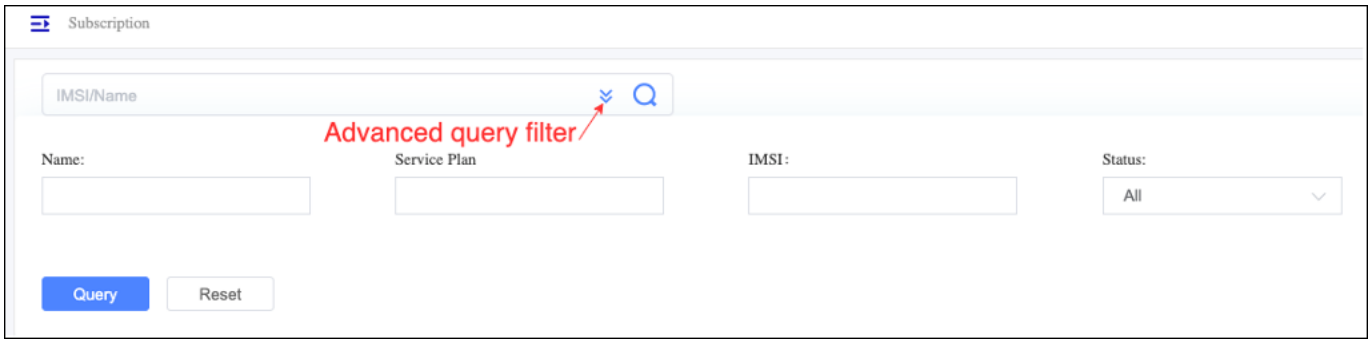
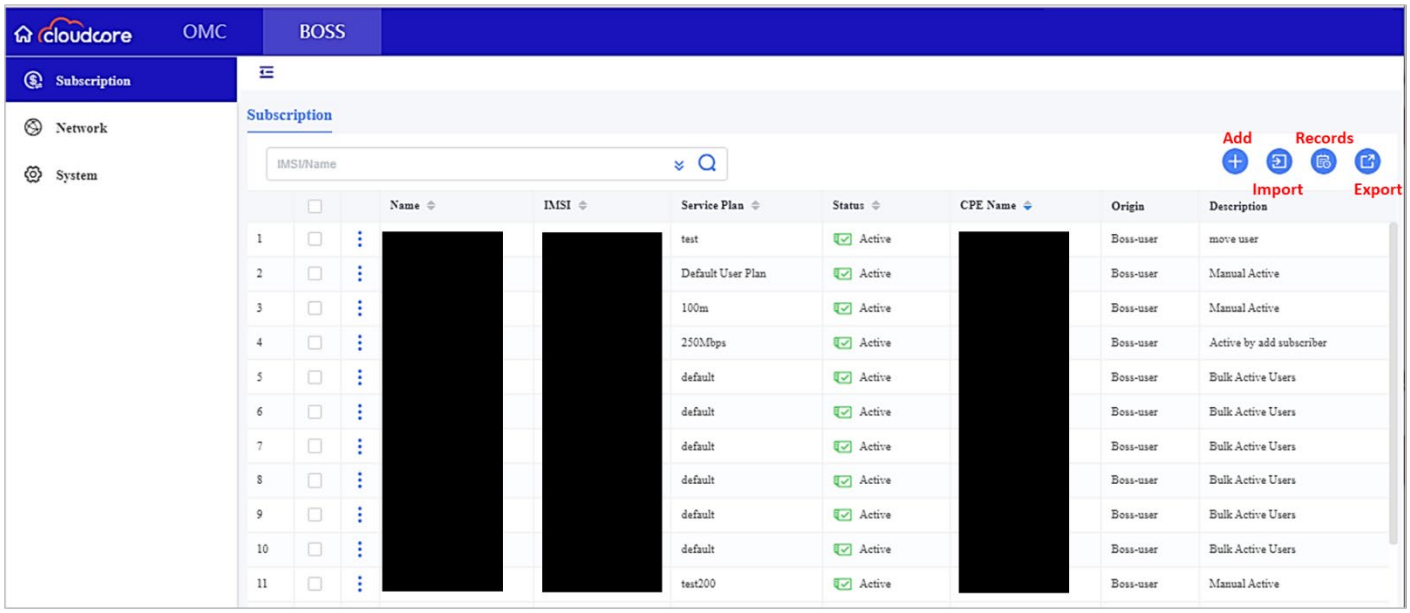


Figure 2-187: Subscription Menu



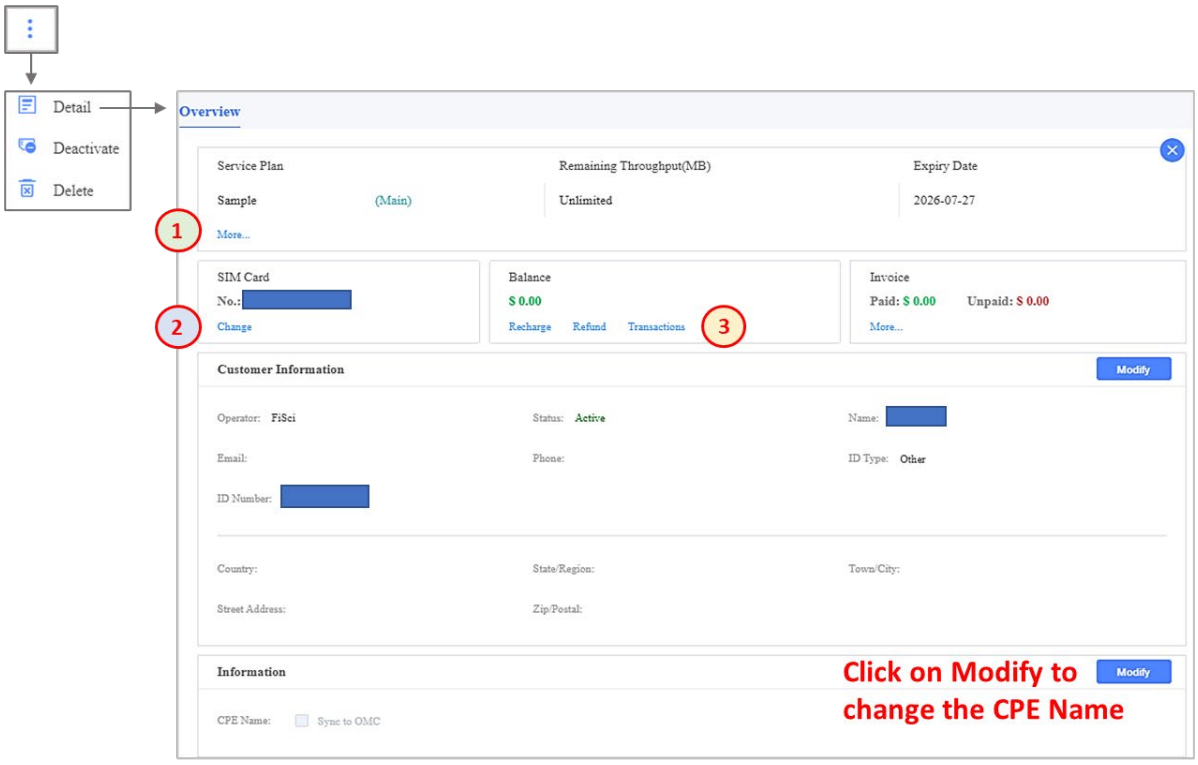
2.5.2.2 Operations

To view more details about an existing subscription, use the *Operations* icon and select Detail. The Overview window opens, displaying the service plan, SIM card, invoice status, and other information (Figure 2-188).

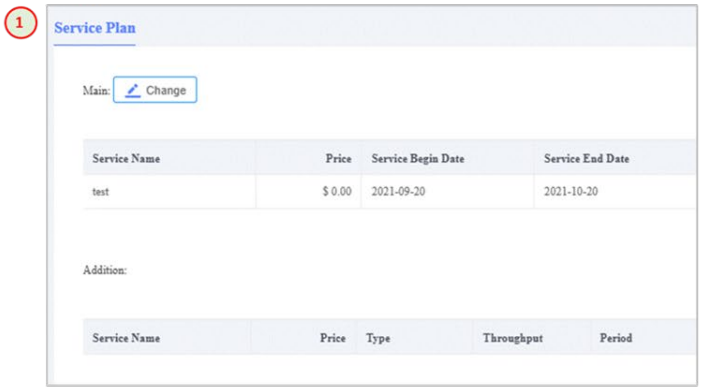
All actions that can be taken from the Overview window - such as More, Change, and Refund - will appear in blue, with hyperlinks or buttons to other dialogue windows, as shown in the figure.

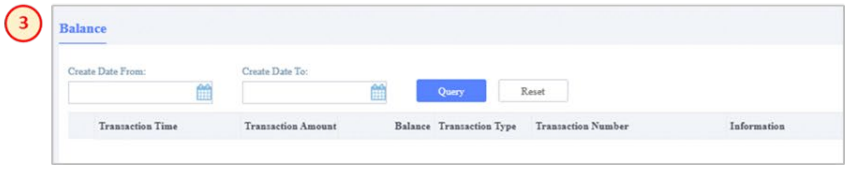
Figure 2-188: Operations Detail

The three hyperlink callouts are shown beneath the main window in the figure.



Hyperlink Call-outs





2.5.2.3 Add Subscription

2.5.2.3.1 Before You Begin

If you have not already done so before you begin adding subscriptions, you should:

- From the BOSS menu, go to *Network > SIM Card* and import the IMSI information for the SIM cards provided by Baicells (*section 2.5.3.1 SIM Card*); and
- Go to *Network > Service Plans* and create custom service plans (*section 2.5.3.2 Service Plans*). Subscriptions left unassigned to a custom plan will be placed in the default plan.

2.5.2.3.2 What Happens After You Add a Subscription

When you add a new subscription - including assigning a SIM card and service plan - and save the information, the subscription and the SIM card will be immediately activated. The user will have access to the network as soon as the subscription status is active:

- Once the CPE is powered on (and if the CloudKey was entered in the CPE's GUI), the CPE is automatically registered in the operator's OMC account.
- The Baicells CloudCore per-active-user billing to the operator begins. For more information, please refer to *section 2.3.1 Billing Menu*.

2.5.2.3.3 Options for Adding Subscriptions

There are multiple ways to add subscriptions. You can (a) add a single subscription "from scratch," that is, by manually entering all of the information into the Add Subscription fields; (b) add a single subscription by copying another subscription's settings and then modifying the information as needed, or (c) bulk upload information for multiple subscriptions using an Excel .csv template.

2.5.2.3.3.1 Adding a Single Subscription

To add a new, single subscription:

1. Click on the **+** Add icon to open the New Subscription window (Figure 2-189).
2. Complete the Customer Information section. For now, disregard the blue hyperlink next to Customer Information called "*Select existing customers.*" This option is explained later in this section.
3. If a CPE Name was configured for the account associated with the CPE, it appears in the CPE Name field. Use the Sync CPE name to the OMC checkbox to sync the CPE's data to the OMC.
4. For SIM Card, select the radio button next to an available IMSI.
5. Under Service Plan (Figure 2-190), select the radio button next to the plan this subscription will use. All service plans previously created are listed under Service Name. The price, periodical (billing recurrence), bill type (time-based is the only option), billing period, throughput, and uplink (UL)/downlink (DL) speeds are displayed. When you select a plan, the plan's name appears at the top of the Service Plan pane, and the Valid Date appears at the bottom. The Valid Date reflects the Service Plan's periodical (billing recurrence) established for the chosen plan. The price of the service plan and other information appears at the bottom.

6. After completing all the fields under New Subscription, click *OK* to save the settings. The subscription is added to the list on the main Subscription window, and the account is activated by default.

NOTE 1: The GUI can take a few minutes to refresh the subscription status from inactive to active.

NOTE 2: Use the *Operations > Deactivate* function to deactivate an account.

Figure 2-189: New Subscription (1 of 2)

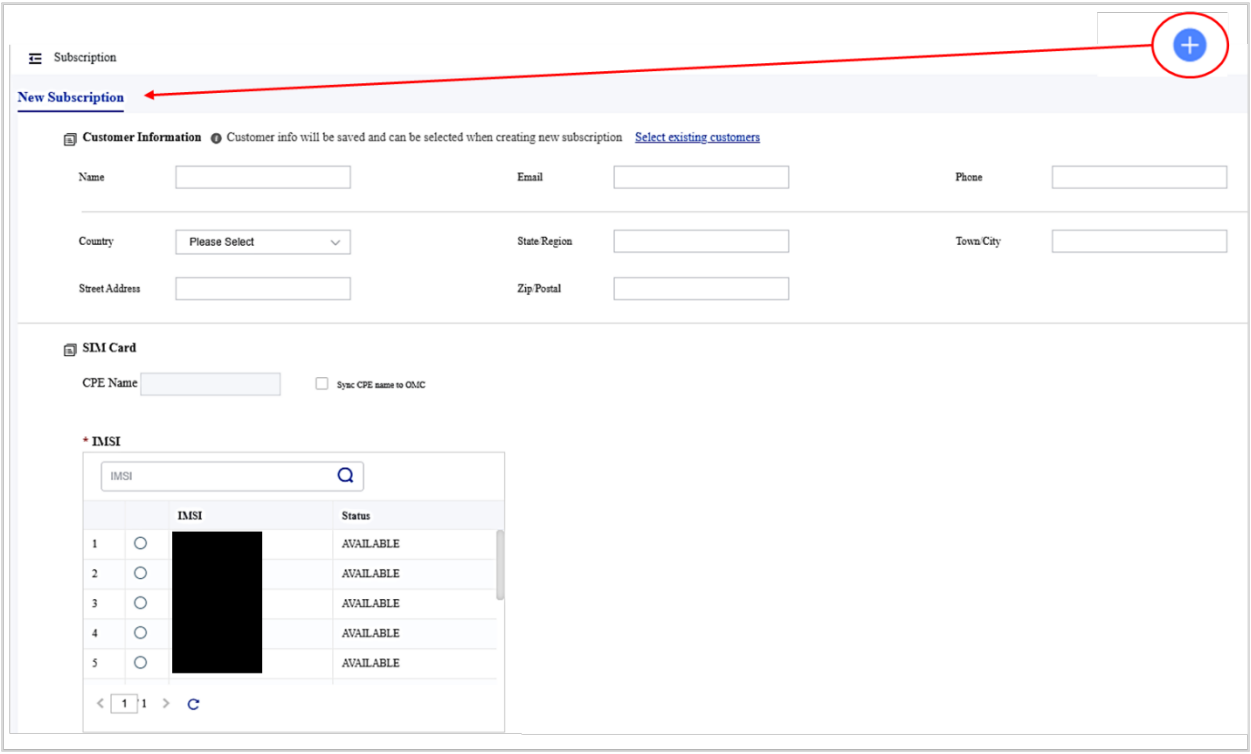
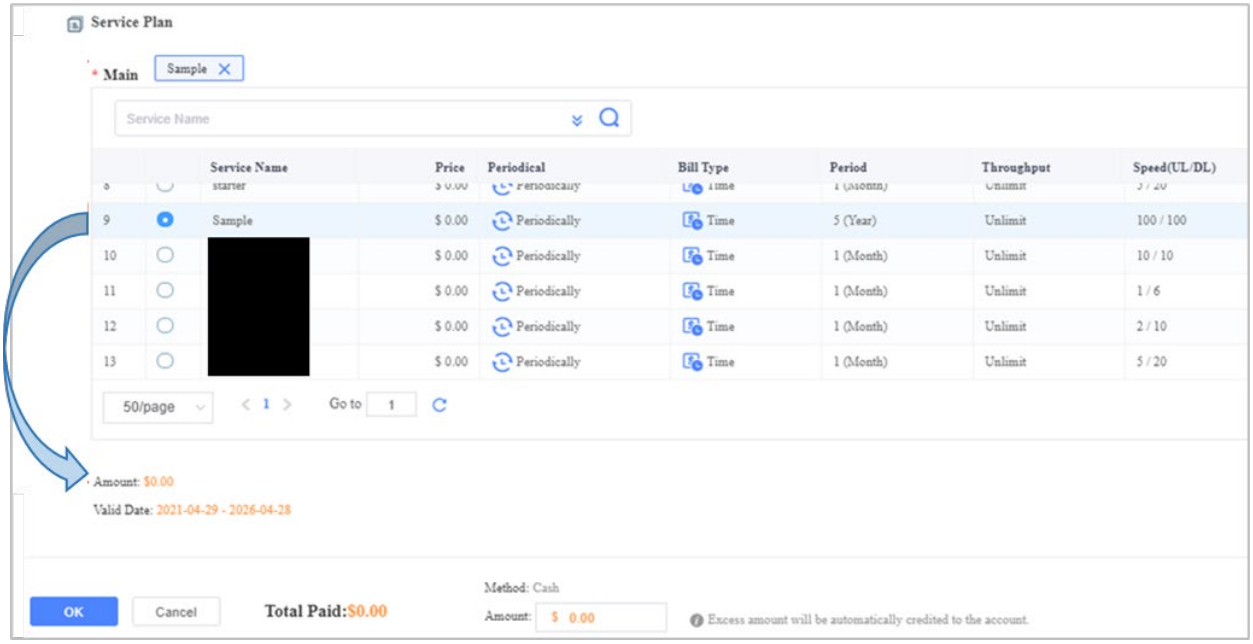


Figure 2-190: New Subscription (2 of 2)

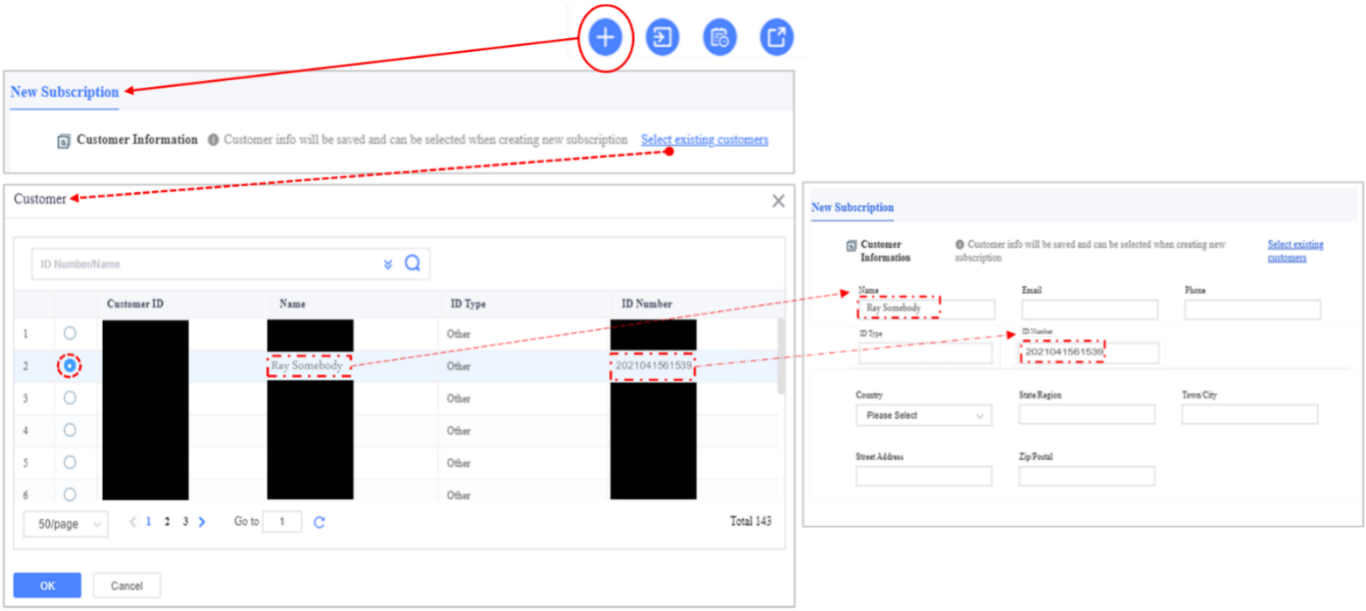


2.5.2.3.3.2 Adding a Single Subscription by Copying an Existing Subscription

To add a single new subscription by copying an existing subscription's account settings:

1. Click on the **+** Add icon to open the New Subscription window (Figure 2-191)
2. Click on the "*Select existing customers*" link to open the Customer window.
3. Find and select the existing customer account you wish to copy.
4. Click on *OK*. The New Subscription window will now display the existing customer's information. Modify any of the fields as needed for the new subscriber. Refer to section 2.5.2.3.3.1 Adding a Single Subscription above to describe the remaining steps.

Figure 2-191 Add Subscription by Copying and Modifying an Existing Subscription



2.5.2.3.3.3 Add Multiple Subscriptions Using Import File

The Import option allows you to simultaneously upload information for multiple subscriptions using an Excel .csv template. Only subscriptions that will use the same service plan should be included in each file you upload.

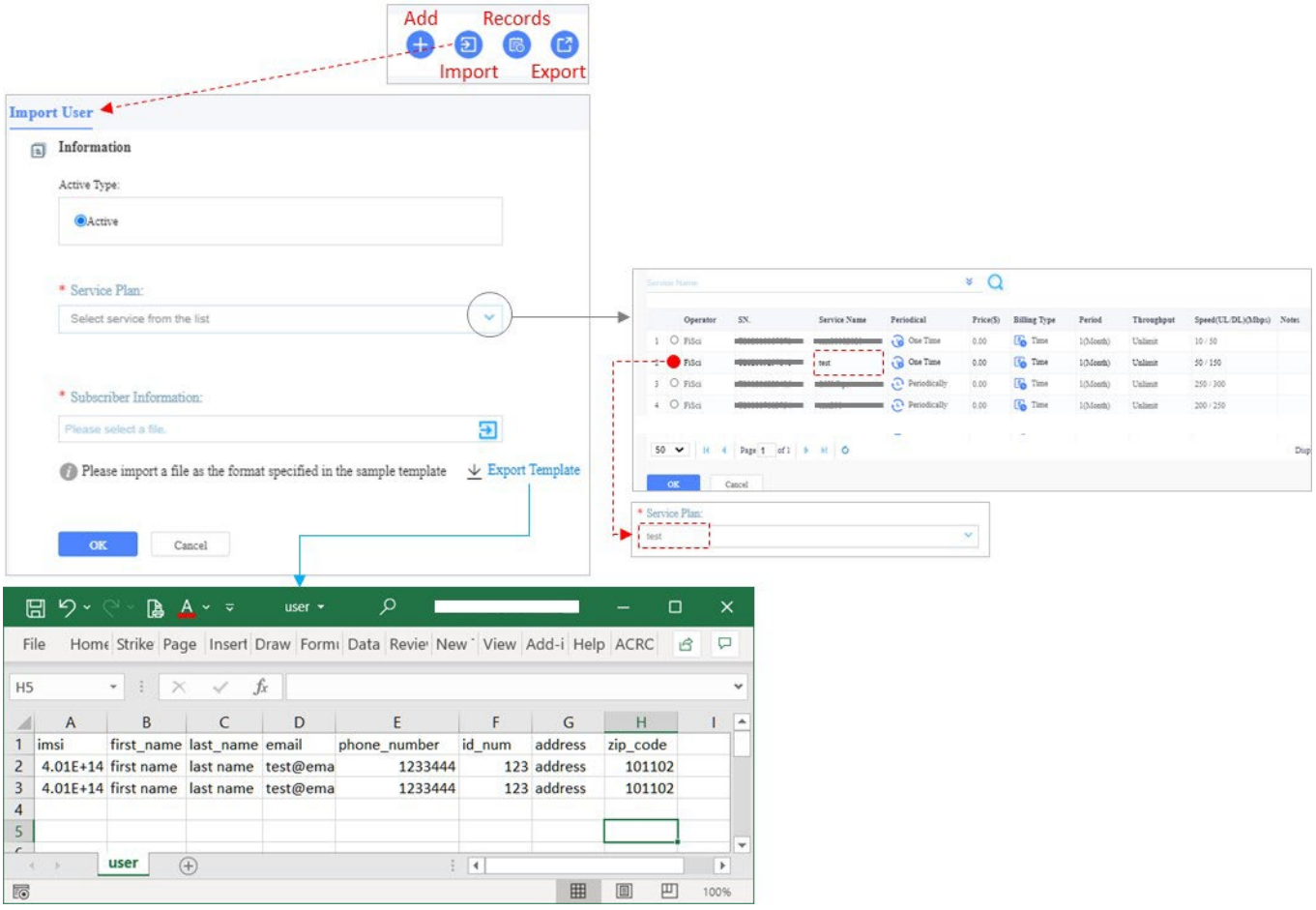
To import subscription information:

1. Click on the *Import* icon shown in the upper right of the Subscription window to open the Import User dialogue box (Figure 2-192). The Active Type field will indicate because subscriptions are automatically activated when added to BOSS.
2. The Service Plan field is mandatory. Select the drop-down menu to open the list of existing service plans.
3. Select the radio button next to the service plan to assign to these subscriptions and click *OK.* The Service Plan field will automatically populate with the name of the selected plan.

4. Click *Export Template* and save the Excel .csv spreadsheet to your computer. The first two rows are filled out as an example; type over the examples and continue until all the subscription information is entered. You must maintain the format as provided in the template. Then select Save (do not change the file name).

5. In the Subscriber Information field, click on the right blue arrow, navigate to the saved Excel .csv file, click Open, then click on *OK* to upload your file. The subscriptions will now be included in the main Subscription list.

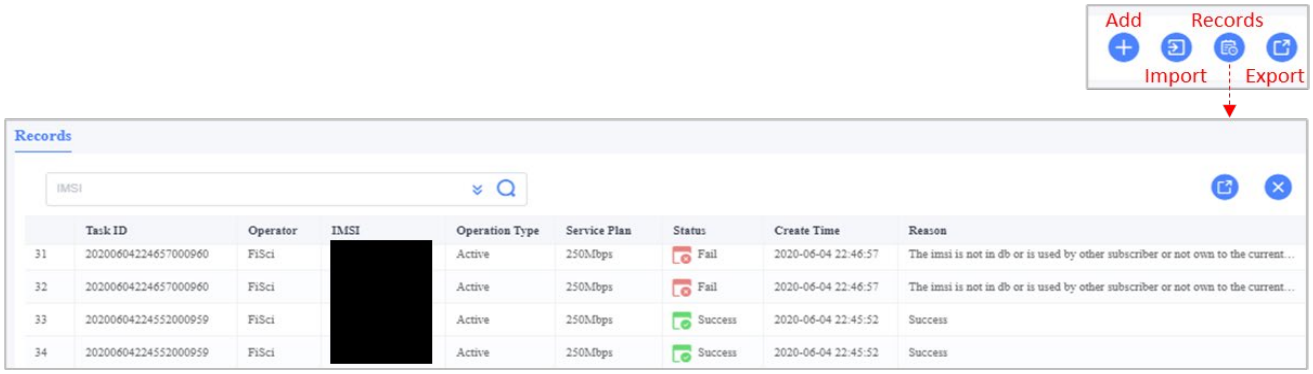
Figure 2-192: Import User



2.5.2.4 Subscription Records

The Records option lists all IMSI-related transactions for that operator's BOSS account. The Status field indicates if the task was successful or failed, as shown in Figure 2-193. If a task fails, the reason is provided in the last column.

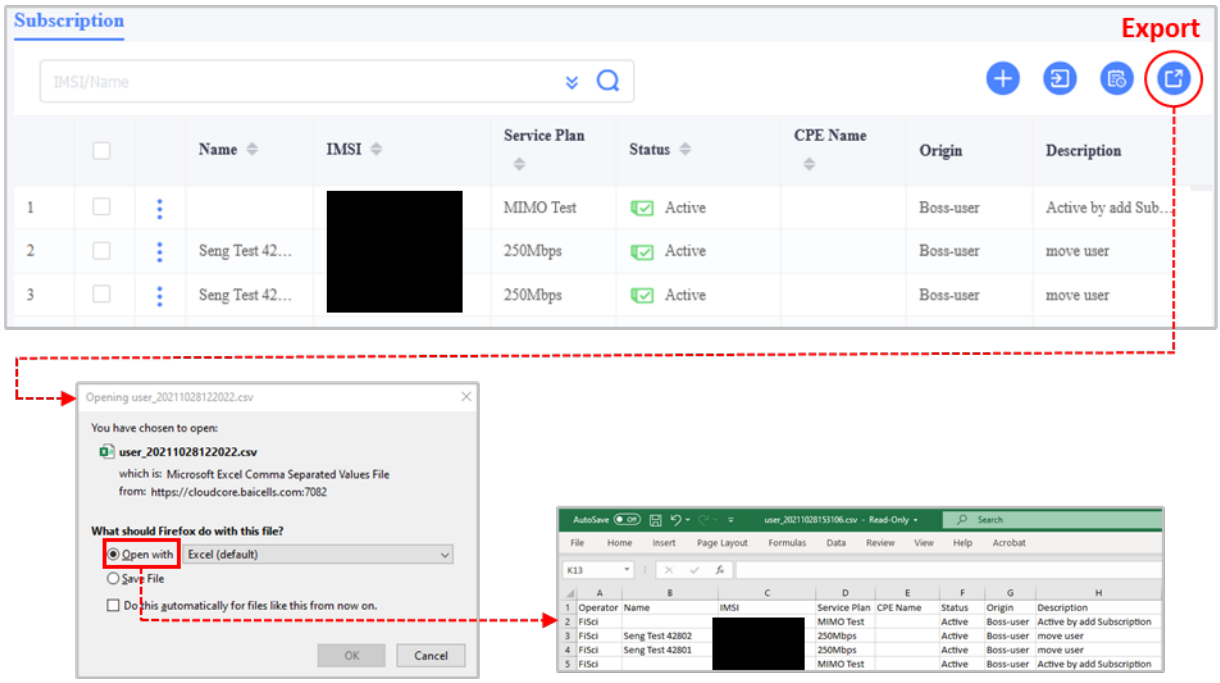
Figure 2-193: Records



2.5.2.5 Export Subscriptions

The Export option enables you to export the list of subscriptions. Click on the *Export* icon and select Open With to open it and save it to your local computer (Figure 2-194).

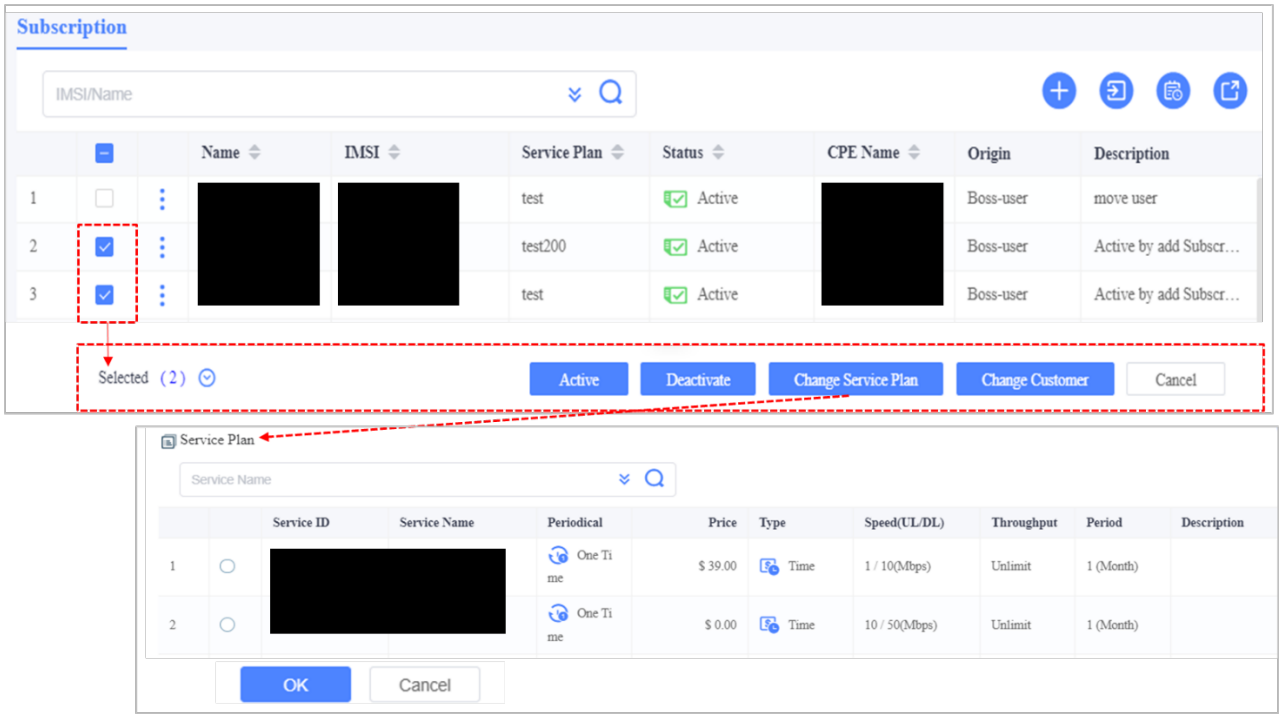
Figure 2-194: Export



2.5.2.6 Bulk Changes

You can activate, deactivate, or change the service plan for multiple existing subscriptions simultaneously (Figure 2-195). Select the checkbox next to each subscription in the main Subscription window and use the action buttons that appear at the bottom of the window to implement the change. If you choose Change Service Plan, a list of existing service plans will open for you to choose from.

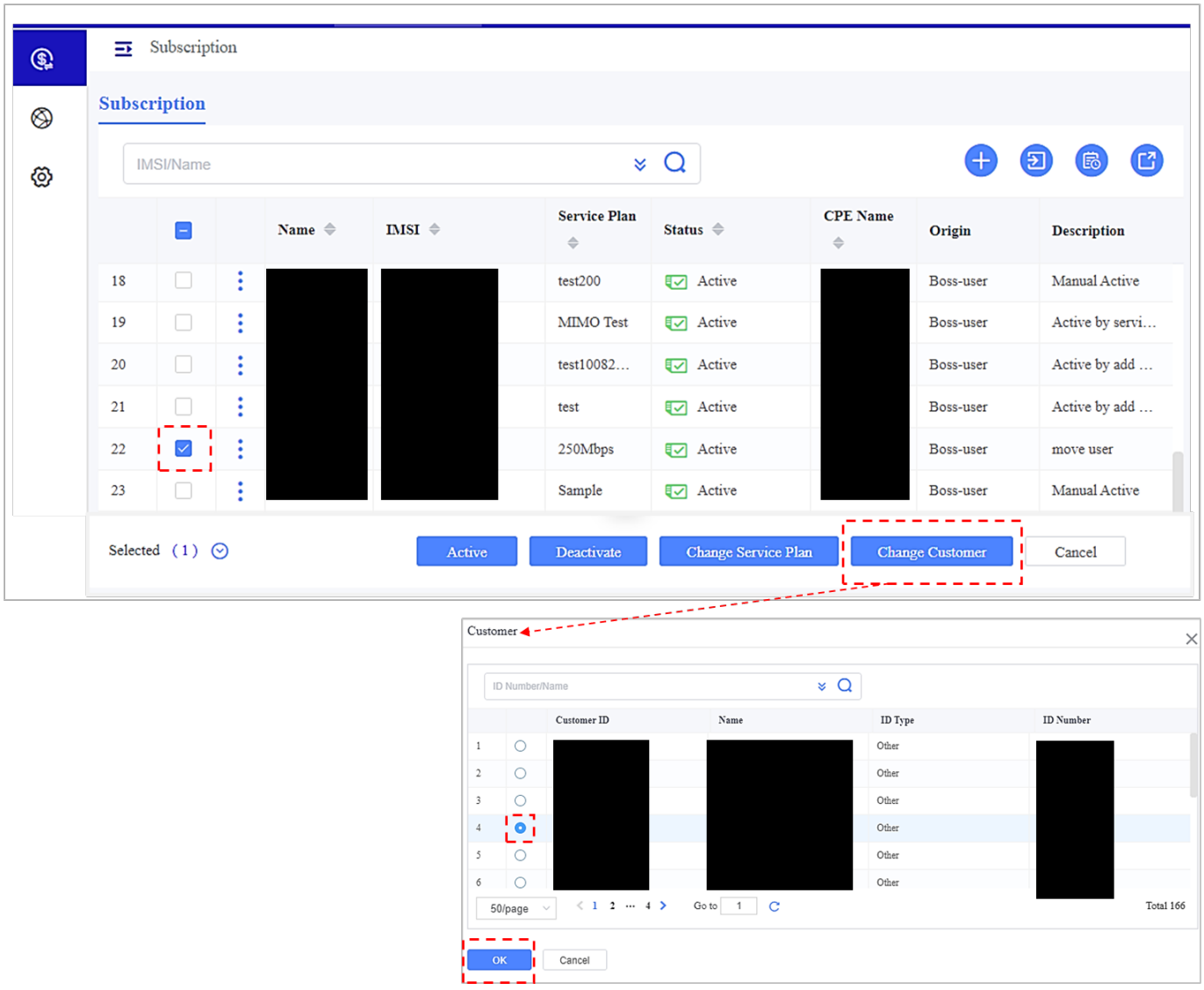
Figure 2-195: Bulk Changes



2.5.2.7 Change Customer

The Change Customer feature allows the operator to move one or more customer/s account information from an existing subscription to another established subscription. On the Subscription page, select the checkbox next to the customer/s whose information you want to move (Figure 2-196), then select the Change Customer button. The Customer window opens with a list of existing customers. Click the checkbox next to the subscription you want to move the customer/s information to and select OK. After completing this action, the accounts will share the same customer information only (i.e., operator, name, ID number, address, etc.); all other account information (i.e., IMSI, CPE name, service plan) will remain the same.

Figure 2-196: Change Customer



2.5.3 Network Menu

The BOSS Network menu lets you activate SIM cards, create service plans, and configure roaming settings (Figure 2-197). Each sub-menu is described below.

Figure 2-197: BOSS Network Menu

2.5.3.1 SIM Card

The SIM card information identifies CPE users:

- IMSI = Subscriber (the person)
- IMEI = Hardware (the CPE unit)

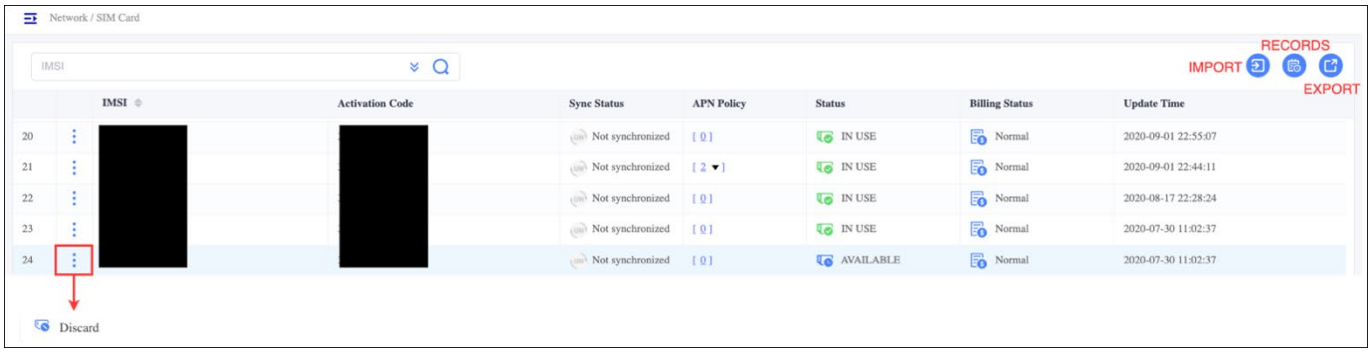
Network operators purchase batches of Baicells SIM cards (Figure 2-198) and activate them by using an activation code on the box label or by batch upload of an IMSI information file. A SIM card is first assigned to a subscriber when adding the subscriber in BOSS. You can later change the designated SIM card if needed. Once a subscriber is added to BOSS, the SIM card and the user become activated. The user will then have access to the operator's network.

NOTE: Proper SIM card insertion and removal is covered in each CPE user manual.

Figure 2-198: SIM Card

You can view the IMSI ID, activation code, sync status, APN policy, card status (in use or available), billing status, and last update time of any previously added SIM card. To view SIM card information, select *Network > SIM Card*. Select the *Operations* icon and choose Discard (Figure 2-199).

Figure 2-199: SIM Card List



2.5.3.1.1 Import SIMs

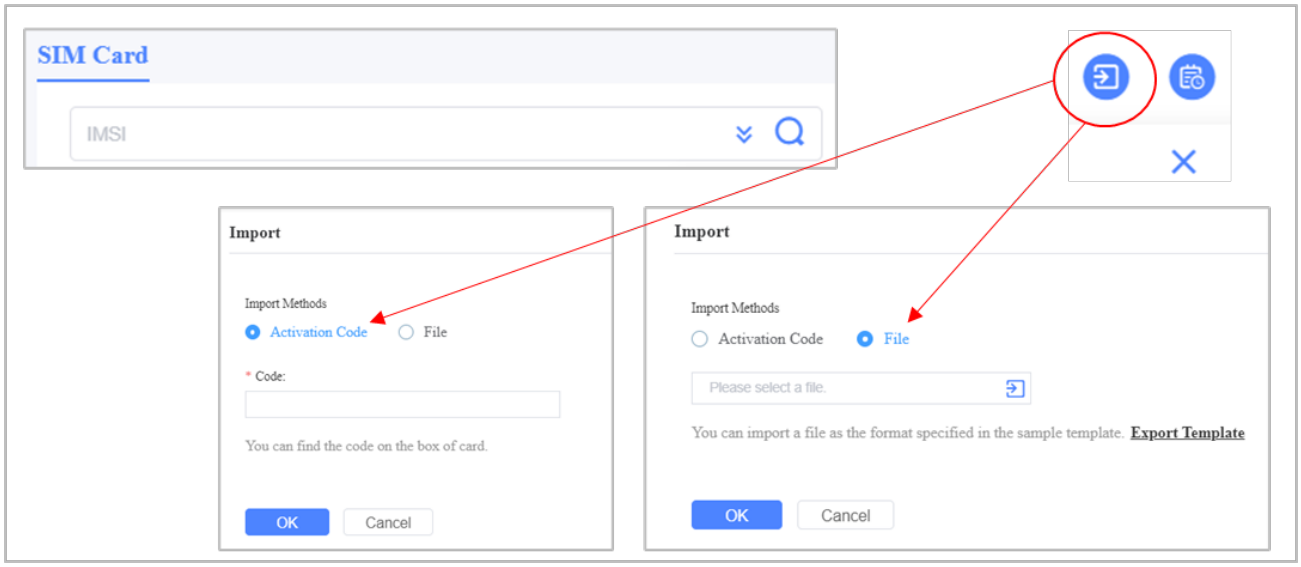
You must first import the SIM card information to activate a SIM card. There are two ways to import SIM card information (Figure 2-200).

1. **Activation (Activate) Code Import** – allows you to import a batch of SIM cards in multiples of 10 (e.g., 10, 20, 30, etc.) all at once using a Baicells activation code (Figure 2-202).

2. **File Import** – allows you to upload a file of unique IMSI numbers if you did not purchase a pack of 10 SIMS and do not have an activation code (Figure 2-203).

Even if you have an activation code, you can still choose the File Import method; however, it would not be as expedient as activating by code number.

Figure 2-200: SIM Card Import



2.5.3.1.1.1 Activation Code Import

Refer to Figure 2-201 to import SIM cards using an activation code:

1. Go to *BOSS > Network > SIM Card* and click on the Import icon.
2. Select the radio button next to *Activation Code* as the Import Method. Enter the code you received from Baicells and click on *OK*. An example of an activation code is shown in Figure 2-202.

Figure 2-201: Import by Activation Code

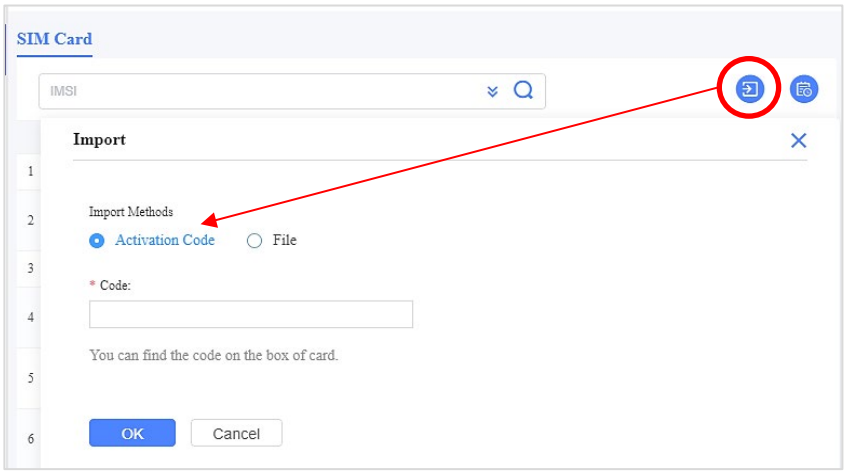


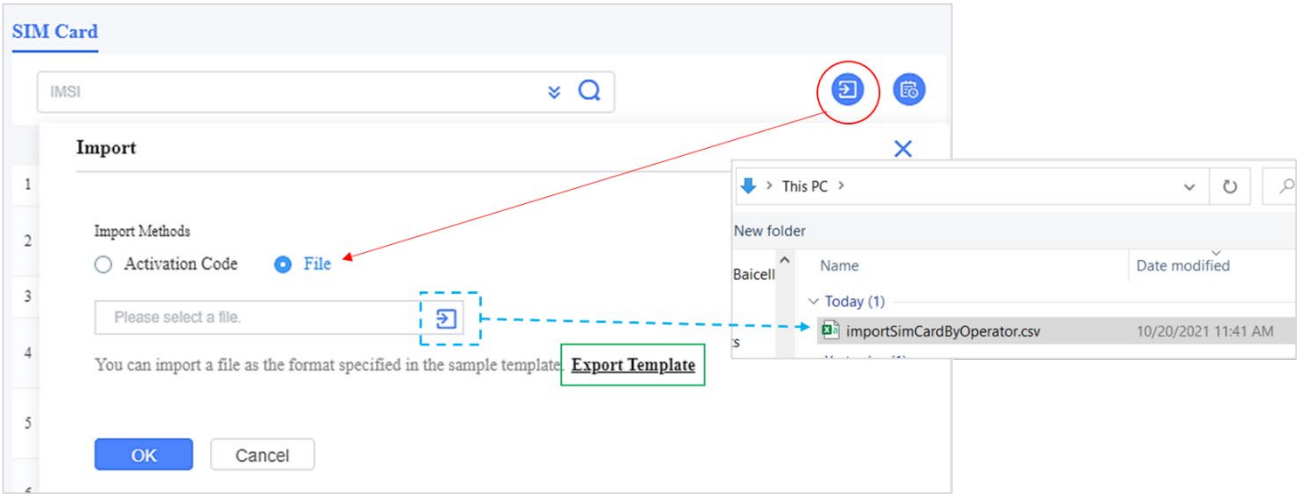
Figure 2-202: Activation Code Example

2.5.3.1.1.2 File Import

Referring to Figure 2-203 to import SIM cards using the File Import method:

1. In BOSS, go to *Network > SIM Card*, click on the Import icon, and for Import Method, select the radio button next to *File*.
2. Choose *Export Template* and save the Excel .csv template to your computer.
3. Enter the IMSIs in the file and save the file. Do not change the file name when you save.
4. Select *Import*, navigate to your saved IMSI file, click *Open*, then click on *OK*.
5. You will see a dialog box showing the number of SIM cards added successfully. Click on *OK*.

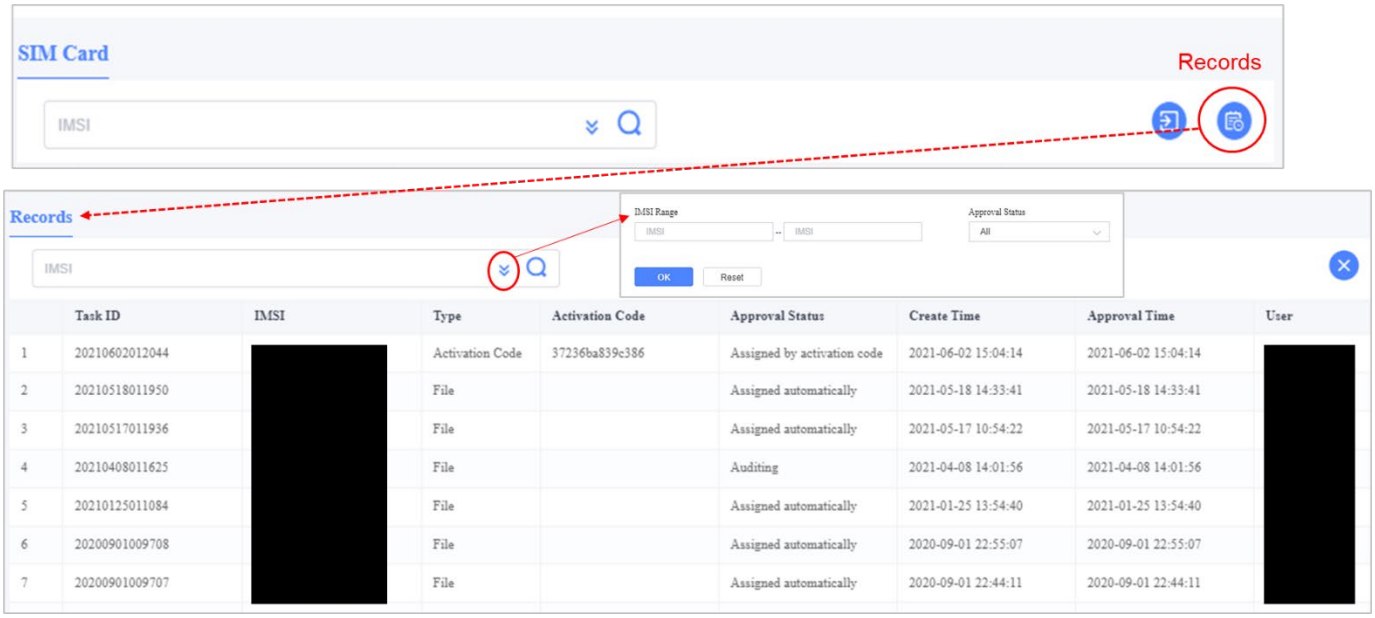
Figure 2-203: Import by File



2.5.3.1.2 SIM Card Records

The Records option lists SIM card-related transactions. The information displayed is shown in Figure 2-204. Use the search bar or advanced query function to find specific SIM card records based on IMSI, IMSI Range, or Approval Status.

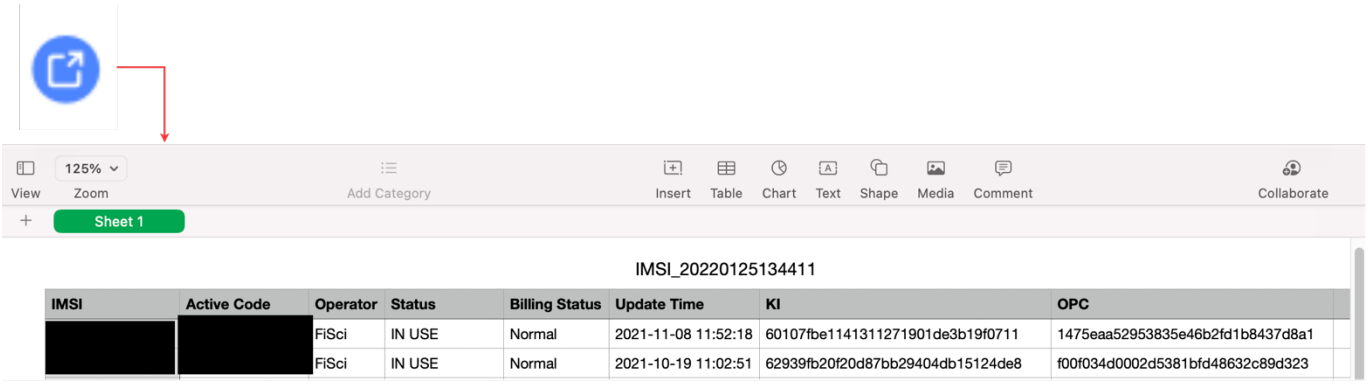
Figure 2-204: SIM Cards



2.5.3.1.3 Export

To enhance the subscriber's privacy, the operators need to access to the cryptographic information in IMSI. Furthermore, IMSI hosts the customer's data, making it critical to specific security vulnerabilities. Therefore, each IMSI has KI (secret key of IMSI) and OPC (secret key of the operator) values. The admin can export the sim card data by clicking the *Export* icon at the top right (Figure 2-205) to view KI and OPC for each IMSI.

Figure 2-205: Export IMSI file



2.5.3.2 Service Plans

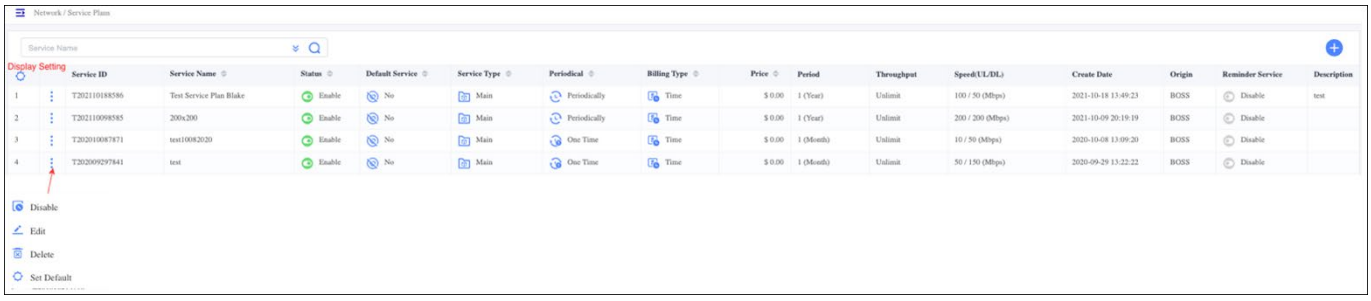
BOSS is preconfigured with a default service plan set to a rate limit of 100 Mbps uplink (UL) and 100 Mbps downlink (DL). You can create custom service plans and billing methods. Billing settings, such as interval and price, can be set for reference.

BOSS does not currently support direct billing for subscriptions. The BOSS API can be used by third-party billing solutions, which then activates/deactivates SIMs and changes service plans.

*NOTE: Refer to the *BOSS API Manual* for integration information.

Existing service plans will be listed on the main Service Plans page, showing the plan status, service type, billing period, billing price, throughput, UL/DL speed, and the date the plan was created (Figure 2-206). The fields are described in the steps below. Use the *Operations* icon to disable, edit, delete, or set a plan as the default.

Figure 2-206: Service Plans



To create a new service plan (Figure 2-207):

1. In BOSS, go to *Network > Service Plans*, click on the **+** Add icon, and click on *Service plan* to open the New Service Plan dialogue window.
2. Click on ⌄ it to view all the service plan sections.
3. Under *Basic Information*, enter the name for this plan under *Service Name*.
4. Enter the Price you will charge subscribers for this plan, as it applies to either a periodic (e.g., monthly) or one-time charge, or select the checkbox for Free.
5. Under *Speed Limit*, you will need to select the desired radio button *Unlimit (*Unlimited) for no speed restrictions or *Limit* for the UL and DL. If you choose the radio button *Limit,* you must enter the maximum Mbps in the UL and DL directions.
6. Enter a description of the plan (optional).
7. Under *Billing Settings*, use the *Time* or *Throughput* radio button to select the Billing Type. An explanation of these options is given below. Figure 2-207 shows screen changes based on your selection.
    - Time-based billing has no throughput limit, and subscribers with this plan will be charged the price entered as a periodic or one-time charge.
    - Throughput-based billing enables you to choose the maximum throughput and length of time this service will be available to subscribers. Select either MB (megabytes) or GB (gigabytes) from the drop-down menu and enter the maximum throughput number.
8. Under *Billing Interval*, select Year, Month, or Day. Then select the radio button to choose either *One Time* or Periodically.
9. If you selected the Throughput billing type, you could offer subscribers with this plan a discount for a window of time by toggling the Discount Time radio button to the right. You can set up two discount times, for example, one with 100% throughput rate from 8:00am - 5:00pm and another with 50% throughput rate from 5:00pm - 8:00am.
10. Under *Reminder Service,* turn on the Service Switch toggle button and enter a value in the text box to set a reminder on the remaining service days, remaining data flow to the customer. Also, select the checkbox to set a reminder on the expiry date.
11. Under *Action When Payment Is Overdue*, select the desired radio button *Deactivate, Limit Speed, Redirect,* or *Continue to use.*
    - Deactivate - Service will stop and not be restored until the payment is made.
    - Limit Speed - Service will continue but at a reduced speed. A pop-up window prompts the UL and DL speed (Mbps) to be entered.
    - Redirect (available only when using private network "Local BOSS"; not available in CloudCore BOSS) – If the operator is using a third-party billing management system, Subscribers will be redirected to a URL where they can make payment.
    - Continue to use - Service will continue per the existing parameters.

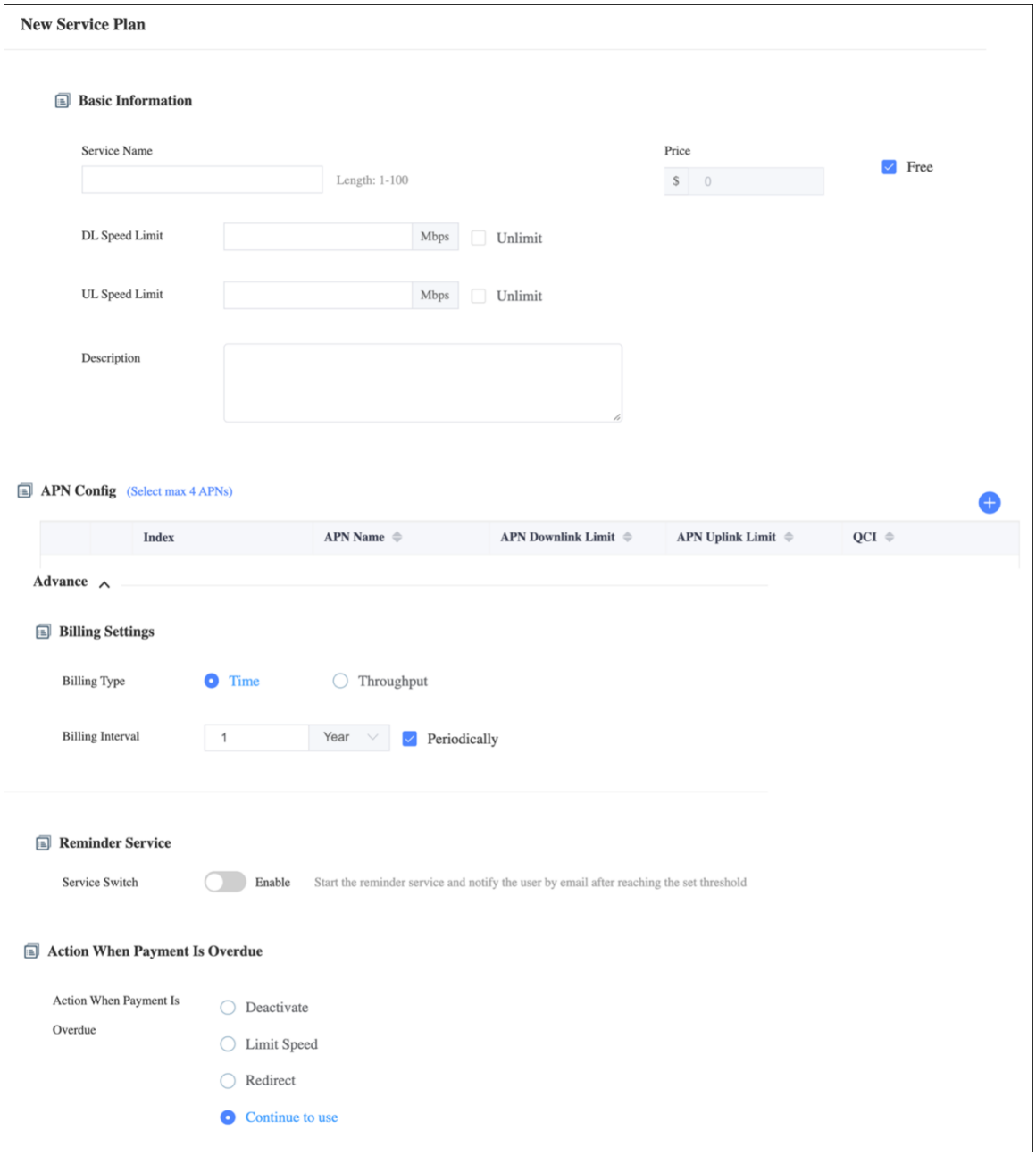
12. If you want this plan to be the default service plan for your network, select the checkbox next to *Set as Default Service*.

    NOTE: If you forgot to select the default checkbox before saving and you want to make this plan your default service plan, use the *Operations > Set Default* action in the main Service Plans list.

13. Click on *OK* to save the settings. The new plan will be added to the main Service Plans list with a Service ID assigned by the BOSS system. However, the plan will not become active and available to assign to subscribers until you complete the next step.

14. When you are ready to activate the new service plan, find the row where the new plan is listed and select *Operations > Enable* in the main Service Plans window.

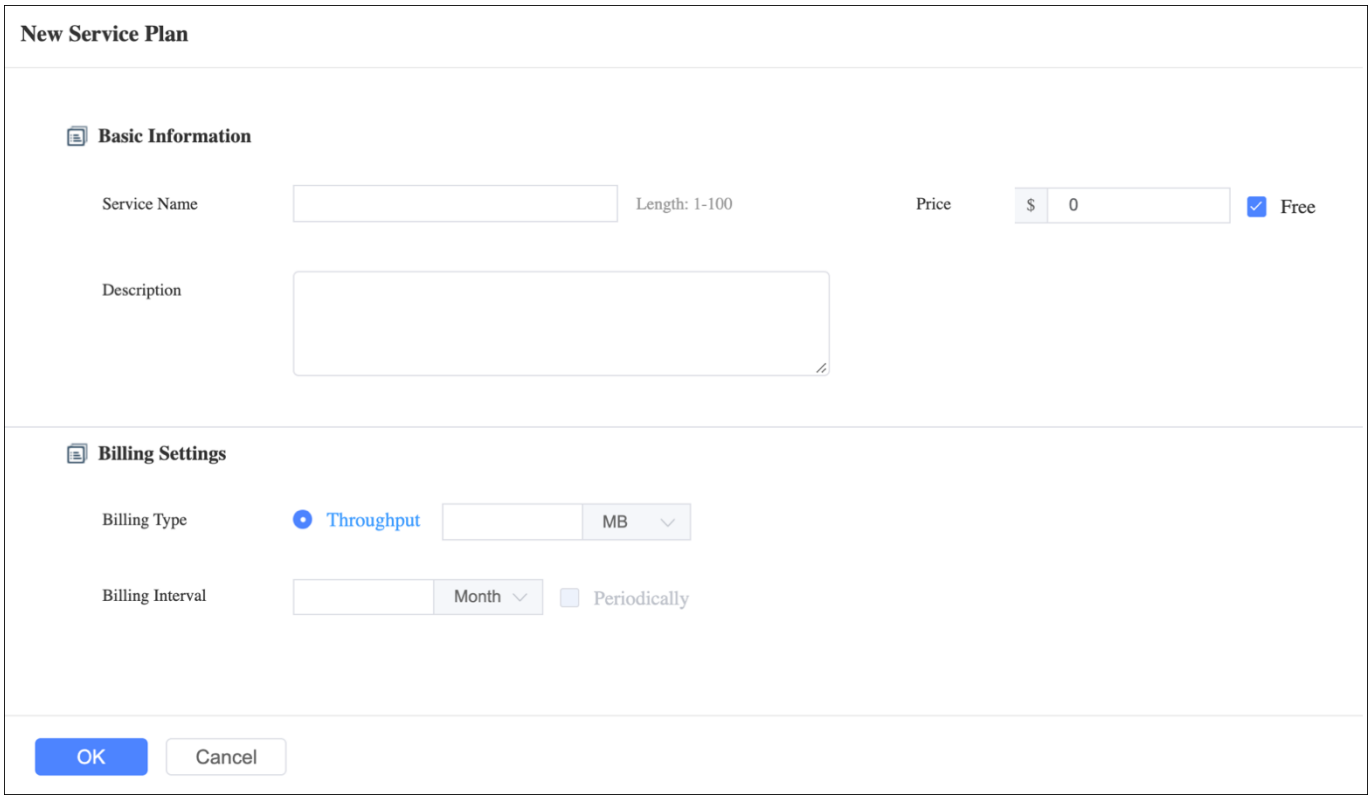
Figure 2-207: New Service Plan



To create a new Flow package (Figure 2-208)

1. Flow Package is used for subscribers who have exhausted all of the allowable throughputs in the main service plan and will pay a one-time charge for additional throughput.
2. In BOSS, go to *Network > Service Plans*, click on the **+** Add icon, and click on Flow Package to open the New Service Plan dialogue window.
3. Under *Basic Information*, enter the name for this plan under Service Name.
4. Enter the *Price* you will charge subscribers for this plan, as it applies to a one-time charge, or select the checkbox for *Free*.
5. Enter a *Description* of the plan (optional).
6. Under *Billing Settings*, choose the billing type as *Throughput*, enter the amount of data usage in the text box, and select MB/GB from the drop-down menu.
7. Enter the *Billing interval* in the text box and choose Year, Month, Day for the break from the drop-down menu.
8. Click on *OK* to save the settings. The new flow package plan will be added to the main Service Plans list with a Service ID assigned by the BOSS system. The plan will not become active and available to assign to subscribers until you complete the next step.
9. When you are ready to activate the new service plan, find the row where the new plan is listed and select *Operations > Enable* in the main Service Plans window.

Figure 2-208: Flow Package

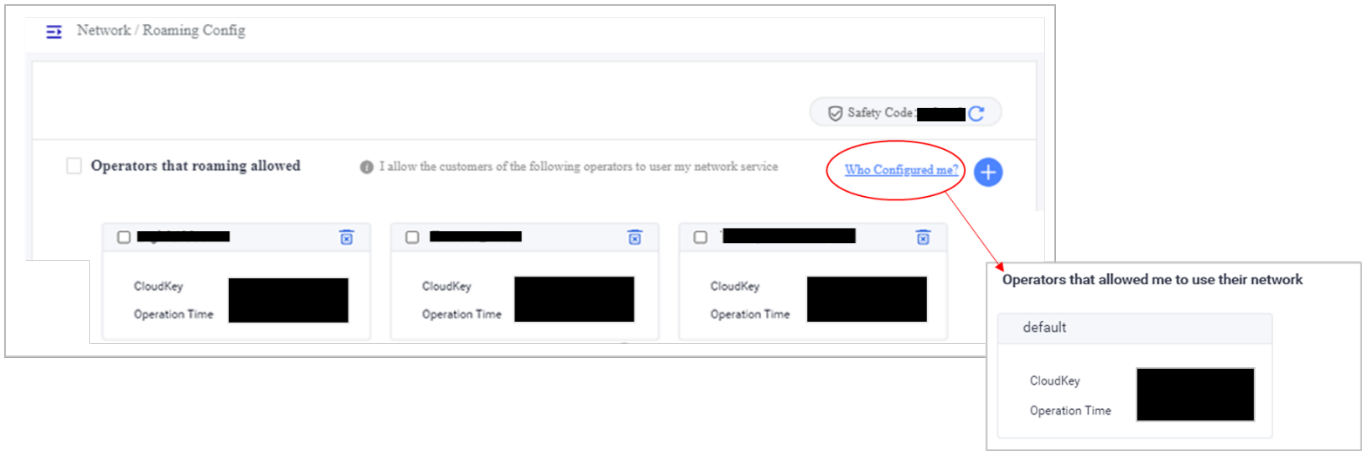


2.5.3.3 Roaming Configuration

A Roaming function is used to configure which operators can roam to your network. It enables roaming to other CloudCore operators to allow other operators' SIMs to attach to their network. The operators can select which operator's subscribers can roam into your network. Roaming Config is where you view, configure, and modify roaming in networks. Select *Network > Roaming Config* to view the roaming configuration page. Click the checkbox next to the operator's name to allow their customers to roam in your network. To remove an operator's permission to roam, click the delete icon next to the operator's name, as shown in Figure 2-209.

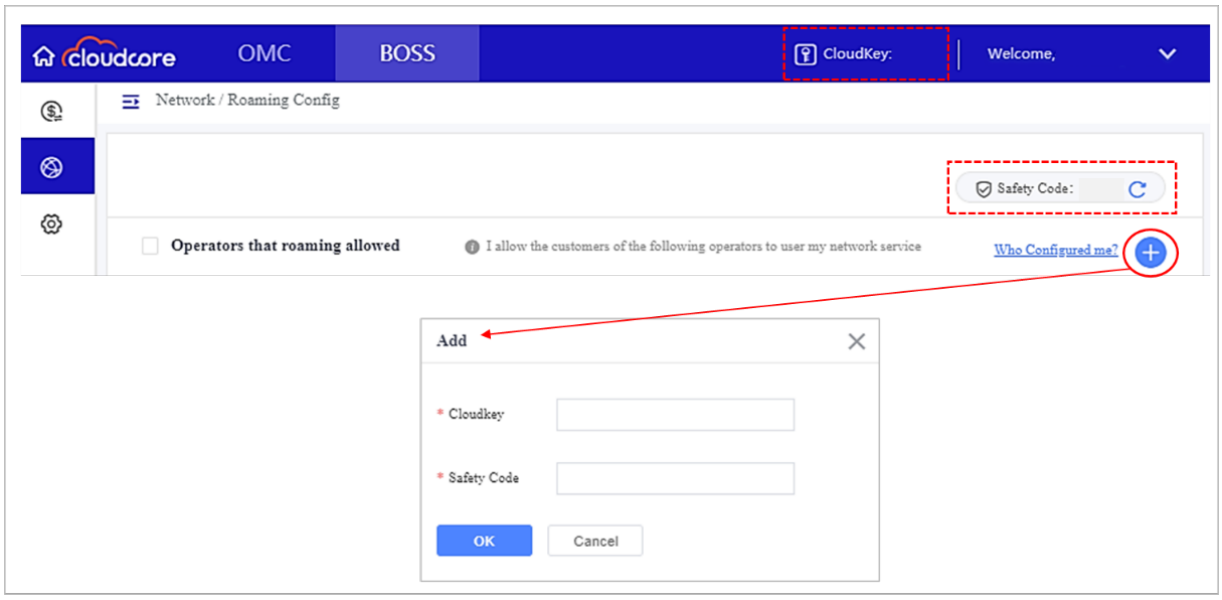
Click *Who Configured Me?* to view a list of operators who have allowed you to roam in their network, as shown in Figure 2-210.

Figure 2-209: Roaming Configuration/View Roaming Operator



To add an operator, click the **+** Add icon. Enter the *Cloudkey* and *Safety Code,* as shown in Figure 2-210 (you must obtain the CloudKey number for the operator). Then enter the *Safety Code* shown at the top of the screen. If the Safety Code does not work, click the refresh icon to obtain a new one. Then click on *OK*.

Figure 2-210: Add Operator to Roam



2.5.4 System Menu

The BOSS System menu (Figure 2-211) enables you to modify or delete admin user groups or role sets and view each subscriber's activity logs (e.g., password resets, service plan changes, etc.). There are two sub-menus: Logs and License.

Figure 2-211: System Menu

2.5.4.1 Logs

The *BOSS System > Logs menu* contains a record of actions that have been taken by BOSS account administrators (Figure 2-212). The list is shown in descending order by date.

The columns display the admin username as User Account; the IMSI affected by the action, as appropriate; the log name (description) of the action; record detail for any activities related to adding a subscriber, user group, or service plan; the results of the action; the failure reason if the action failed; and a timestamp of when the action started and ended. You can export the logs to an Excel .csv file using the *Export* icon in the top right of the window.

Figure 2-212: Logs